Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

ИНТЕРЭКСПО ГЕО-СИБИРЬ

XIX Международный научный конгресс

Сборник материалов в 8 т.

Т. 6

Магистерская научная сессия

«ПЕРВЫЕ ШАГИ В НАУКЕ»

Новосибирск
СГУГиТ
2023

УДК 528
С26

С26 Интерэкспо ГЕО-Сибирь. XIX Международный научный конгресс, 17–19 мая 2023 г., Новосибирск : сборник материалов в 8 т. Т. 6 : Магистерская научная сессия «Первые шаги в науке». – Новосибирск : СГУГиТ, 2023. – 332 с.– ISSN 2618-981X. – Текст : непосредственный.

DOI 10.33764/2618-981X-2023-6

В сборнике опубликованы материалы XIX Международного научного конгресса «Интерэкспо ГЕО-Сибирь», представленные на Магистерской научной сессии «Первые шаги в науке».

Печатается по решению редакционно-издательского совета СГУГиТ

Материалы публикуются в авторской редакции

УДК 528

Сборник включен в систему РИНЦ.

УДК 004.056.53
DOI 10.33764/2618-981X-2023-6-3-10

В. Е. Антипов[1], В. В. Селифанов[1]*

Разработка рекомендаций по улучшению систем управления информационной безопасностью для критической информационной инфраструктуры

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
*e-mail: vvv-antipov@mail.ru

Аннотация. В статье поднимается вопрос о методах внедрения систем управления информационной безопасностью (СУИБ) на значимых объектах критической информационной инфраструктуры (КИИ) с учетом специфики таких объектов. Рассматриваются способы таких реализации в соответствии с актуальной на сегодняшний день нормативной правовой документацией в области КИИ и СУИБ. В процессе анализа, предлагается переработанный подход к оценке рисков и разработка рекомендаций по улучшению действующей СУИБ с применением этого подхода. Также представлены результаты применения и реализации разработанных рекомендаций. Результаты состоят в том, что примененные рекомендации по улучшению СУИБ в организации, являющейся субъектом КИИ, позволили повысить качество и надежность СУИБ, снизить вероятность рисков и сократить время реагирования на инциденты информационной безопасности.

Ключевые слова: критическая информационная инфраструктура, система управления информационной безопасностью, управление рисками

V. E. Antipov[1], V. V. Selifanov[1]*

Development of Recommendations for Improving Information Security Management Systems for Critical Information Infrastructure

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: vvv-antipov@mail.ru

Abstract. The article raises the question of methods of implementing information security management systems (ISMS) on significant objects of critical information infrastructure (CII), taking into account the specifics of such objects. The methods of such implementation are considered in accordance with the current regulatory legal documentation in the field of CII and ISMS. In the process of analysis, a revised approach to risk assessment and the development of recommendations for improving the current ISMS using this approach are proposed. The results of the application and implementation of the developed recommendations are also presented. The results are that the applied recommendations for improving the ISMS in the organization that is the object of the CII allowed to improve the quality and reliability of the ISMS, reduce the likelihood of risks and reduce the response time to information security incidents.

Keywords: critical information infrastructure, information security management system, risk management

Введение

Каждая система, внедряемая в жизненный цикл организации, должна служить интересам организации и не препятствовать существующим бизнес-процессам, а создавать более благоприятную среду для их функционирования. Другими словами, любая система должна внедряться в существующие процессы компании с целью их оптимизации. В случае же, если нарушение процессов несет за собой возможный критический ущерб не только для самой организации, но и для каких-либо сфер государства, то это правило становится абсолютно бескомпромиссным. Значимые объекты критической информационной инфраструктуры Российской Федерации (далее – ЗО КИИ) как раз имеют в своем распоряжении подобные процессы, а значит и внедряемые в них системы должны преследовать конкретные цели. Система безопасности любого объекта состоит из комплекса принятых мер, позволяющих контролировать и противодействовать возможным возникающим рискам физической, экономической и информационной безопасности [1]. Чтобы управлять всем комплексом мероприятий, направленных на обеспечение безопасности в организации, создается специальное подразделение, назначаются ответственные, разрабатывается документация и т.д. Одним из важнейших аспектов обеспечения безопасности любой организации является внедрение системы управления информационной безопасностью (далее – СУИБ). СУИБ имеет в своем составе набор процедур и методов, используемых для обеспечения защиты информации от несанкционированного доступа. Учитывая специфику ЗО КИИ и требуемый к ним уровень обеспечения защиты информации, СУИБ для таких объектов должна базироваться на более специфичных подходах, нежели классических. А для более эффективного функционирования процесс внедрения СУИБ должен предполагать наличие четких и логичных требований. Целью данной статьи является разработка рекомендаций по улучшению СУИБ для ЗО КИИ и реализация разработанных рекомендаций на практике.

Методы и материалы

Для достижения поставленной цели были изучены и проанализированы национальные стандарты семейства СМИБ: ИСО/МЭК 27000 [2], ИСО/МЭК 27001 [3], ИСО/МЭК 27002 [4], ИСО/МЭК 27005 [5] и руководства по их применению, а также Постановление Правительства РФ № 127 [6] (далее – ПП № 127) и Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [7] (далее – Приказ № 239). Основой для разработок являлись не только нормативная правовая документация, но и публикации в разрезе тем, связанных с менеджментом информационной безопасности. Оценка и анализ функционирующей СУИБ проводились в действующей организации, являющейся субъектом КИИ.

Обсуждение

Система безопасности любого объекта состоит из комплекса принятых мер, позволяющих контролировать и противодействовать возможным возникающим рискам физической, экономической и информационной безопасности. Чтобы

управлять всем комплексом мероприятий, направленных на обеспечение безопасности в организации, обязательным решением следует принять внедрение СУИБ. Система управления имеет в своем составе набор процедур и методов, используемых для обеспечения защиты информации от несанкционированного доступа. В задачи СУИБ входит создание специального подразделения, назначение ответственных, разработка различного рода документации и пр. [8]. Говоря в разрезе организаций, являющихся субъектами КИИ, процесс внедрения СУИБ является обязательным шагом для обеспечения целостной безопасности объектов такой организации.

К сожалению, в настоящее время ни один нормативный правовой документ не объясняет в полной мере как реализовывать подобные системы на ЗО КИИ. Рассматривая ПП № 127 [6] в данном контексте, приходим к выводу о необходимость системного подхода к оценке рисков, который включает в себя анализ угроз и уязвимостей, оценку последствий возможных атак, а также определение рисков и мер по их снижению до приемлемого уровня. Иначе говоря, при категорировании ЗО КИИ по ПП № 127 [6] будет проведена работа с неприемлемыми рисками, а как оценивать остальные риски и выстраивать под них защиту не сказано. Данный подход недостаточен для ЗО КИИ, так как в случае таких объектов мало обеспечить безопасность только с технической стороны, необходимо действовать комплексно.

Открывая Приказ № 239 [7], наблюдается отсутствие в нем описания полной реализации СУИБ на объектах КИИ. Однако, данный приказ предписывает реализовать некоторые мероприятия по обеспечению безопасности в ходе эксплуатации значимого объекта субъектом КИИ. В состав этих мероприятий входят:

– планирование мероприятий по обеспечению безопасности ЗО КИИ;

– анализ угроз безопасности информации на ЗО КИИ и последствий от их реализации;

– управление (администрирование) подсистемой безопасности ЗО КИИ;

– управление конфигурацией ЗО КИИ и его подсистемой безопасности;

– реагирование на компьютерные инциденты в ходе эксплуатации ЗО КИИ;

– обеспечение действий в нештатных ситуациях в ходе эксплуатации ЗО КИИ;

– информирование и обучение персонала, работающего на ЗО КИИ;

– контроль за обеспечением безопасности ЗО КИИ.

На данном этапе, логичным будет обратиться к ГОСТ 27001 [3] и ГОСТ 27002 [4], так как первый определяет требования к разработке и внедрению мер для системы менеджмента информационной безопасности, а второй представляет перечень общепринятых мер обеспечения информационной безопасности и рекомендации по их внедрению. В совокупности эти два стандарта должны помочь реализовать требуемые мероприятия из Приказа №239 [7] и реализовать все необходимые меры для покрытия неприемлемых рисков, которые в свою очередь выявляются при категорировании ЗО КИИ [9] в соответствии с ПП № 127 [6]. Однако, говоря о КИИ мы приходим к выводу о том, что не можем

использовать в отношении оценки рисков стандарты ИСО/МЭК 27001 [2] и ИСО/МЭК 27002 [3] из-за разного подхода к рискам. Критические объекты информационной инфраструктуры с точки зрения безопасности имеют определенную специфику. Из определения значимого критического объекта вытекает отсутствие конструктивного механизма исчисления ущерба от инцидентов информационной безопасности, хотя категория ущерба в этом случае существенно шире множества субъектов управления безопасностью. Когда речь идет о значимом критическом объекте, нет оснований для определения уровня допустимого остаточного риска, так что это понятие становится несущественным. Ранее владельцы информационных активов принимали остаточный риск, но теперь его роль утрачивается. Традиционный метод управления, который использует уровень остаточного риска в качестве критерия для управления безопасностью, теперь уже неприменим.

Стоит упомянуть также и о не менее важном аспекте управления информационной безопасностью – моделировании угроз. Процесс моделирования угроз безопасности позволяет определить угрозы, их свойства и особенности, исходя из определенного набора агрессивных факторов. При моделировании учитываются облик, намерения и потенциал злоумышленника, векторы и сценарии возможных атак, а также информационные активы, которые могут быть наиболее уязвимыми. Моделирование угроз несомненно является неотъемлемой частью СУИБ и представляет собой процессно-циклическую деятельность. В различии подходов к моделированию угроз, нельзя однозначно сказать, что один подход «лучший» или «единственно правильный». Каждый из существующих подходов имеет слабые и сильные стороны, и для достижения максимальной эффективности необходимо комбинировать различные альтернативы. Методология совместной функциональной оценки угроз и концепция использования такой оценки базируется на известной модели Клементса-Хоффмана [10], которая строится, исходя из правила, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути воздействия злоумышленника на информационную систему. Для описания такой защиты информации рассматриваются три множества: множества угроз, множества объектов защиты и множество механизмов защиты. Элементы множеств угроз и защиты находятся в отношениях «угроза – объект». Угроза в данном случае соотносится с сущностью «объект». Каждая угроза может распространяться на любое число объектов, а объект в свою очередь может быть уязвим со стороны более чем одной угрозы. Цель такой методики состоит в том, чтобы множество механизмов защиты перекрывала множество объектов защиты от множества возможных угроз. Такая модель определяет основные векторы развития моделирования угроз несмотря на то, что добиться полного перекрытия всех смоделированных угроз практически невозможно.

Обратимся к стандартам 27000 [2] и 27005 [5], и на их основе выведем переработанные и адаптированные под КИИ требования, и методы взаимодействия с рисками информационной безопасности в рамках СУИБ. ГОСТ 27000 [2] предлагает нам следующую схему работы с рисками: оценка рисков – выбор подхода

к обработке рисков – выбор и реализация мер по снижению рисков до приемлемого уровня. Предлагаемая схема будет изменена в части реализации мер, а именно планируется исключить понятие приемлемого уровня как такового. И как итог, особенностями предлагаемого переработанного метода будут являться:

– многоуровневый подход. В рамках данного подхода выделяются несколько уровней управления рисками: стратегический, тактический и оперативный. Каждый из этих уровней имеет свои задачи, функции и методы работы с рисками;

– интеграция с процессами управления. Работа с рисками должна быть тесно интегрирована с процессами управления информационной безопасностью в целом. Это позволяет более эффективно управлять рисками, так как предполагается рассматривать их не отдельно от других процессов, а в контексте общей стратегии управления безопасностью;

– анализ контекста. Особое внимание стоит уделить анализу контекста, в котором функционирует ЗО КИИ. Это позволит определить специфические риски и угрозы, свойственные данному контексту, и разработать наиболее эффективные меры по их управлению;

– ориентированность на результат. Основное внимание уделяется не процессам, а результатам работы с рисками. Это позволяет более эффективно выявлять и управлять рисками на ЗО КИИ.

Этапы по внедрению данного подхода в организацию будут следующими:

1) идентификация уязвимостей объекта критической информационной инфраструктуры;
2) оценка уровня риска, связанного с этими уязвимостями;
3) выбор мер по управлению рисками на основе анализа результатов оценки рисков;
4) реализация выбранных мер управления рисками;
5) оценка эффективности реализованных мер по управлению рисками и необходимости их корректировки.

Как уже было сказано ранее, такой подход базируется не на методе остаточного риска, используемого в качестве критерия для управления процессами безопасности, а на осознании бесконечной вероятности возникновения инцидента, что влечет за собой возможность постоянного снижения этой вероятности путем расширения перечня защитных мер.

В ходе собственного проведенного в рамках работы анализа функционирующей СУИБ в одной из организаций, являющейся субъектом КИИ, было выявлено, что анализируемая система не соответствуют требованиям ГОСТ 27001 [3] и ГОСТ 27002 [4]. Анализ показал разногласия между работой СУИБ в организации и требованиями указанных стандартов, а также отсутствие реализации некоторых позиций из этих требований. Несоответствия были связаны с отсутствием политик безопасности, недостаточной оценки рисков, отсутствием контроля над изменениями, недостаточным мониторингом и анализом событий. Результаты анализы достаточно предсказуемы, потому что, как уже говорилось,

настоящие нормативные правовые документы не позволяют проводить полноценную оценку рисков, а сложность структуры КИИ и малое количество методических материалов не позволяют внедрить и развернуть полноценную СУИБ. И как следствие допускаемое организациями пренебрежение полноценным обеспечением защиты ЗО КИИ, на наш взгляд, недопустимо.

На основе анализа и выявленных несоответствий были разработаны следующие рекомендации по улучшению СУИБ на ЗО КИИ с использованием, разработанного в рамках работы подхода к управлению рисками:

– разработать политику безопасности, которая будет описывать требования и правила по обеспечению безопасности информации в организации;

– проводить периодичную оценку рисков, по итогам которой разработать соответствующие меры по управлению рисками;

– усовершенствовать или внедрить процедуры управления доступом сотрудников к информационным ресурсам организации;

– разработать систему контроля над изменениями в информационных ресурсах;

– усовершенствовать мониторинг событий, а также анализ инцидентов информационной безопасности.

По итогам внедрения и реализации в вышеупомянутой организации, являющейся субъектом КИИ, разработанных рекомендаций, сотрудниками этой организации была проведена проверка эффективности СУИБ, спустя шесть месяцев после внедрения. Проверка, по итогам которой был составлен отчет показала, что следование разработанным рекомендациям действительно повысило качество и надежность СУИБ в организации. Итоговый отчет содержал в себе следующие результаты:

– разработка политики безопасности привела к увеличению осведомленности сотрудников об информационной безопасности и улучшению процедур по ее обеспечению;

– снижение рисков, связанных с обработкой и хранением конфиденциальной информации, благодаря внедрению соответствующих мер по управлению рисками и использования нового подхода;

– уменьшение вероятности несанкционированного доступа к информационным ресурсам организации после улучшения процедур управления доступом;

– уменьшение времени реакции на инциденты информационной безопасности на 10%, а также повышение качества их решения.

Заключение

В качестве заключения можно отметить, что СУИБ для критической информационной инфраструктуры является крайне важным элементом обеспечения безопасности и стабильности функционирования таких объектов. При этом реализация данной системы требует учета специфики работы критической информационной инфраструктуры. Правильная реализация СУИБ позволяет минимизировать возможность инцидентов, а в случае их возникновения – оперативно

реагировать и устранять их последствия. При внедрении СУИБ на ЗО КИИ, необходимо использовать подходы учитывающие особенности таких объектов, и отказаться от стандартных методов по управлению и оценке рисков, чтобы достичь максимально эффективного результата в обеспечении безопасности инфраструктуры. Также не следует забывать, что КИИ нуждается не только в информационной безопасности, но и в безопасности со всех других сторон многогранной структуры, которые могут быть подвержены атаке злоумышленников и нарушению своей целостности и доступности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Анализ теоретических основ и программных средств аудита системы управления информационной безопасностью / А. Г. Серова. – Текст : электронный // Социально-экономические и естественно-научные парадигмы современности : [материалы XIII Всероссийской научно-практической конференции]. – 2018. – С. 829–837 (дата обращения: 20.03.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

2. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология = Information technology. Security techniques. Information security management systems. Overview and vocabulary : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 813-ст : введен впервые : дата введения 2013-12-01 / подготовлен Федеральным бюджетным учреждением "Консультационно-внедренческая фирма в области международной стандартизации и сертификации. – Москва : Стандартинформ, 2019. – Текст : непосредственный.

3. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования = Information technology. Security techniques. Information security management systems. Requirements : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. N 1653-ст: взамен ГОСТ Р ИСО/МЭК 27001-2006 : дата введения 2022-01-01 / подготовлен Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Открытым акционерным обществом "Информационные технологии и коммуникационные системы" (ОАО "ИнфоТеКС") и Федеральным автономным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФАУ "ГНИИИ ПТЗИ ФСТЭК России"). – Москва : Стандартинформ, 2022. – Текст : непосредственный.

4. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норма и правил менеджмента информационной безопасности = Information technology. Security techniques. Code of practice for information security management : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. N 423-ст: взамен ГОСТ Р ИСО/МЭК 17799-2005 : дата введения 2014-01-01 / подготовлен Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл") и Обществом с ограниченной ответственностью "Информационный аналитический вычислительный центр" (ООО "ИАВЦ"). – Москва : Стандартинформ, 2019. – Текст : непосредственный.

5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности = Information technol-

ogy. Security techniques. Information security risk management : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст: взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007 : дата введения 2011-12-01 / подготовлен Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл"), Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России"). – Москва : Стандартинформ, 2019. – Текст : непосредственный.

6. Российская Федерация: Постановления Правительства. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : Постановление Правительства № 127 : [утвержден Правительством Российской Федерации 8 февраля 2018 г.] – Москва : Стандартинформ, 2022. – Текст : непосредственный.

7. ФСТЭК России : Приказ ФСТЭК России от 25 декабря 2017 г. N 239. – Текст : электронный. – 2021. – URL: https://fstec.ru/ (дата обращения: 15.04.21) – Режим доступа: официальный сайт ФСТЭК России.

8. Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799) / Н. В. Андреева. – Текст : электронный // Научно-технический вестник Санкт–Петербургского государственного университета информационных технологий, механики и оптики. – 2007. – С. 40–44 (дата обращения: 06.04.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

9. Внедрение международного стандарта ИСО/МЭК 27001 – основа управления информационной безопасностью предприятия / А. А. Кайсарова, А. К. Тулекбаева, А. А. Токтабек. – Текст : электронный // Вестник науки Южного Казахстана. – 2018. – № 4(4). – С. 103–106 (дата обращения: 10.04.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

10. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк. – Текст : электронный // Экономика и качество систем связи. – 2017. – С. 42–48 (дата обращения: 19.04.2023). – Режим доступа: Научная электронная библиотека eLIBRARY.RU.

УДК 004.045:004.046:004.047
DOI 10.33764/2618-981X-2023-6-11-14

А. И. Балабанов[1]*, *Е. Ю. Воронкин*[1]

Исследование возможности использования мультиагентных систем для распределения кода и данных

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: aleks_2000_2332@mail.ru

Аннотация. В статье приводится исследование возможности использования мультиагентных систем для распределения кода и данных. Целью исследования является рассмотрение возможностей взаимодействия системы с пользователями. Разработан прототип мультиагентной системы. Рассмотрено практическое применение мультиагентных систем для распределения кода и данных. Исследование показало, что мультиагентные системы могут быть эффективным инструментом для распределения кода и данных, а также для управления различными процессами. Кроме того, такие системы могут эффективно взаимодействовать с пользователями, что повышает их удобство и функциональность.

Ключевые слова: мультиагентная система, распределение данных и кода, взаимодействие системы

A. I. Balabanov [1]*, *E. Yu. Voronkin* [1]

Research of the Possibility of Using Multi-Agent Systems for the Distribution of Code and Data

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: aleks_2000_2332@mail.ru

Annotation. The article provides research of the possibility of using multi-agent systems for the distribution of code and data. The purpose of the study is to consider the possibilities of interaction between the system and users. A prototype of a multi-agent system was developed. The practical application of multi-agent systems for the distribution of code and data was considered.

Keywords: multi-agent system, data and code distribution, system interaction

Введение

В современном мире разработка программного обеспечения становится все более сложной и требует от команд разработчиков высокой организованности и эффективности. Одним из ключевых аспектов этого процесса является распределение кода и данных между участниками команды. В этой связи возникает необходимость использования инновационных технологий, которые позволят улучшить процесс разработки и повысить его эффективность.

В данной статье рассмотрена возможность применения мультиагентных систем для распределения кода и данных в процессе разработки программного обеспечения. Рассмотрены основные принципы работы мультиагентных систем, их преимущества и недостатки, а также возможности их применения в различных сферах разработки программного обеспечения.

Методы и технологии

Рассмотрены основные методы и технологии, используемые в мультиагентных системах для распределения кода и данных.

Одним из ключевых методов является метод распределенного хранения данных. Он позволяет распределить данные между участниками команды, что уменьшает нагрузку на центральный сервер и повышает скорость доступа к данным. Для реализации этого метода используются различные технологии, такие как распределенные базы данных, блокчейн и технологии P2P-сетей.

Еще одним методом является метод распределенной отладки программы. Он позволяет распределить процесс отладки программы между участниками команды, что уменьшает время отладки и повышает производительность. Для реализации этого метода используются различные технологии, такие как distcc, icecream и Incredibuild [1–3].

Также в мультиагентных системах используются методы распределенного тестирования и сборки. Они позволяют распределить эти процессы между участниками команды, что уменьшает время отладки и повышает качество программного обеспечения. Для реализации этих методов используются различные технологии, такие как Jenkins, Travis CI и CircleCI.

Кроме того, в мультиагентных системах используются методы распределенного контроля версий. Они позволяют распределить процесс контроля версий между участниками команды, что уменьшает время на слияние изменений и повышает качество программного обеспечения. Для реализации этих методов используются различные технологии, такие как Git, Mercurial и SVN [4–7].

Таким образом, использование мультиагентных систем для распределения кода и данных требует применения различных методов и технологий, которые позволяют повысить эффективность и качество процесса разработки программного обеспечения.

Результаты

Представленые результаты исследования возможности использования мультиагентных систем для распределения кода и данных. Были произведены анализ существующих подходов к распределению кода и данных, а также разработан и реализован прототип мультиагентной системы для демонстрации возможностей данного подхода. В ходе экспериментов были оценены производительность, масштабируемость и надежность предложенной системы.

Для демонстрации возможностей мультиагентных систем в распределении кода и данных был разработан прототип системы (рис. 1), состоящий из следующих компонентов:

– агенты-исполнители: отвечают за выполнение задач, получение и обработку данных, а также взаимодействие с другими агентами;

– агенты-координаторы: отвечают за распределение задач между агентами-исполнителями, а также за мониторинг их состояния;

– центральный сервер: отвечает за хранение кода и данных, а также за координацию работы агентов.

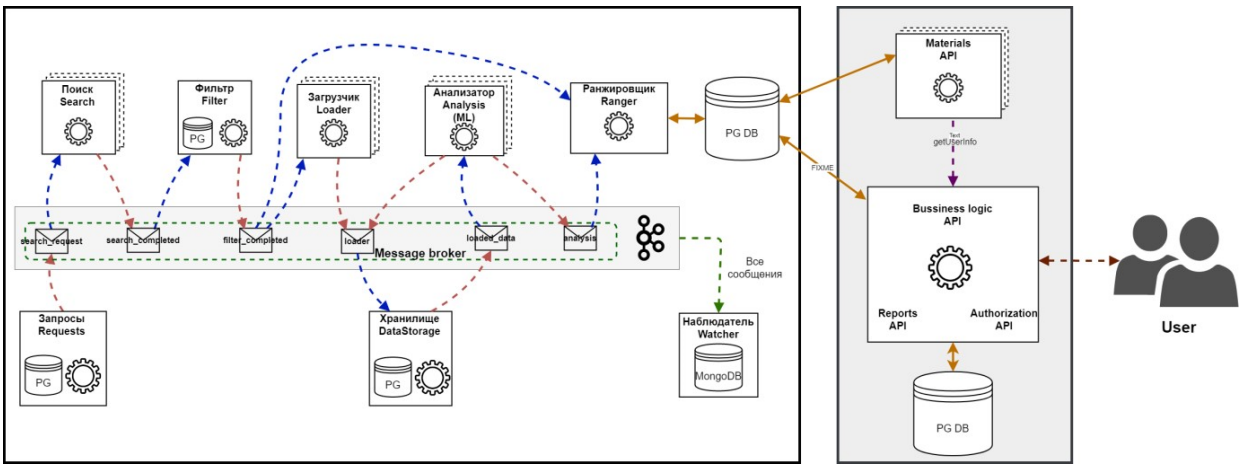


Рис. 1. Прототип системы

В ходе экспериментов были оценены следующие параметры системы:

Производительность: Сравнение времени выполнения задач с использованием мультиагентной системы и традиционных подходов к распределению кода и данных.

Масштабируемость: Оценка способности системы адекватно функционировать при увеличении количества агентов и объема данных.

Надежность: Оценка способности системы продолжать функционировать при возникновении сбоев в работе отдельных агентов или сетевых проблем.

Результаты показали, что мультиагентная система обеспечивает значительное улучшение производительности по сравнению с традиционными подходами к распределению кода и данных. Кроме того, система продемонстрировала хорошую возможность работать под большой нагрузкой и надежность, что делает ее привлекательной для использования в реальных приложениях.

Выводы

Исследование возможности использования мультиагентных систем для распределения кода и данных показало, что данный подход обладает рядом преимуществ перед традиционными методами. Мультиагентные системы позволяют улучшить производительность, масштабируемость и надежность распределенных приложений, что делает их перспективным направлением для дальнейшего развития.

В дальнейшем исследовании планируется углубиться в оптимизацию работы мультиагентных систем, а также разработать методы для автоматического адаптирования системы к изменяющимся условиям работы и нагрузке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аксенов К. А. Теория и практика средств поддержки принятия решений: монография / К. А. Аксенов. Saarbrucken (Germany): LAP LAMBERT Academic Publishing GmbH & Co. KG, 2011. – 341 с.

2. Инструментальные средства для разработки мультиагентных систем промышленного масштаба [Электронный ресурс] / Скобелев П. О. [и др.] // СамНЦ РАН : [сайт]. URL: http://www.ssc.smr.ru/media/ipuss_conf/06/5_01.pdf (дата обращения: 01.05.2023).

3. Граничин О.Н. Как действительно устроены сложные информационно-управляющие системы? // Стохастическая оптимизация в информатике. – 2016. – Vol.12. – P.3 – 19 с.

4. Ломазова И.А. Вложенные сети Петри и моделирование распределенных систем // Программные системы: теория и приложения. – М.: Наука. Физматлит, 2004. – С. 337–352.

5. Мультиагентные системы [Электронный ресурс] / [сайт]. URL: https://habr.com/ru/articles/70446/ (дата обращения: 01.05.2023).

6. Теория и методы решения многовариантных неформализованных задач выбора : монография / Лазарсон Э. В. – Старый Оскол : ООО «Тонкие наукоемкие технологии», 2018. – 240 с. – ISBN 978-5-94178-042-6

7. Интеллектуальные системы: нечеткие системы и сети : учебное пособие / Горбаченко В. И., Ахметов Б. С., Кузнецова О. Ю – Москва : Издательство Юрайт, 2018. – 103 с. – ISBN 978-5-534-03678-7

УДК 528.71
DOI 10.33764/2618-981X-2023-6-15-19

Д. Г. Вавилов[1], С. Н. Новиков[1]*

Алгоритм альтернативной оценки требований к защищенности персональных данных

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: vavilov.d@mail.ru

Аннотация. Оценка требований к защищенности персональных данных является важным этапом в процессе разработки системы обработки данных. Однако, метод оценки на основе уровня защищенности имеет недочеты, которые могут привести к недостаточной защищенности данных. Основной недостаток метода оценки на основе уровня защищенности заключается в том, что он недостаточно учитывает важность количества субъектов персональных данных, обрабатываемых в системе. В связи с этим, предлагается альтернативное решение – определение требований к защищенности персональных данных, опираясь не только на уровень защищенности, но и на иные, целочисленные факторы. Такой подход позволяет учитывать контекст обработки данных и определять требования к защищенности персональных данных более точно. Кроме того, он может помочь разработчикам систем обработки данных выбрать наиболее подходящие меры по защите данных.

Ключевые слова: уровень защищенности, субъекты информации, персональные данные

D. G. Vavilov[1], S. N. Novikov[1]

Alternate Valuation Algorithm Information Processed in Personal Data Information Systems

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: vavilov.d@mail.ru

Abstract. Assessment of requirements for the security of personal data is an important step in the development of a data processing system. However, the method of evaluation based on the level of security has flaws that can lead to insufficient data security. The main disadvantage of the method of assessment based on the level of security is that it does not sufficiently take into account the importance of the number of personal data subjects processed in the system. In this regard, an alternative solution is proposed - the definition of requirements for the security of personal data, based not only on the level of security, but also on other integer factors. This approach makes it possible to take into account the context of data processing and determine the requirements for the security of personal data more accurately. In addition, it can help developers of data processing systems choose the most appropriate data protection measures.

Keywords: level of security, subjects of information, personal data

Введение

Математическая оценка значимости информации в настоящее время определяется исходя из уровня защищенности в соответствии с требованиями следующих нормативно-правовых актов:

– Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [1];

– Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [2];

– Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [3].

– Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [4].

Постановление Правительства РФ N 1119 [3] регламентирует 4 уровня защищенности информационной системы персональных данных (далее ИСПДн), которые устанавливают на основании категории обрабатываемых персональных данных (далее ПДн) и количества субъектов ПДн в рассматриваемой информационной системе. Такой подход означает, что двум одинаковым системам с незначительной разницей в количестве обрабатываемой информации могут быть присвоены разные уровни защищенности. Таким образом, незначительное количество уровней и использованный подход в установлении числа субъектов ПДн [3] обусловливает недостаточную точность в оценке защищенности ПДн. Поэтому подход к оценке защищенности ПДн, применяемый в настоящее время, является в некоторой степени субъективным и недостаточно точным.

В литературе описаны иные предложения оценки угроз информации [5].

На основании вышеизложенного, цель настоящей работы заключается в разработке альтернативного алгоритма оценки требований к защищенности ПДн.

Методы и материалы

Альтернативный метод оценки защищенности информации предлагается представить в виде математической формулы, результатом которой будет являться коэффициент защищенности ПДн (далее – КЗПДн)

Для разработки методики необходимо иметь следующие исходные данные:

– вид субъекта;
– количество субъектов;
– категории ПДн;
– ценность (финансовые потери);
– тип угроз.

За основу математического представления берется уровень защищенности. Идея заключается в том, чтобы исключить недостатки подхода путем наслаивания новых переменных. В первую очередь устанавливается уровень защищенности ИСПДн, опираясь на условные, заранее известные, исходные данные. Определения типа угрозы осуществляется организацией самостоятельно, основываясь на Модели угроз для системы.

Весь процесс будет рассмотрен на примере условной системы с данными, представленными в табл. 1.

Таблица 1

Исходные данные

Субъект	Количество субъектов	Категории ПДн	Тип угроз	Ценность (Финансовые потери в рублях)
Клиент	150 000	Общие	1	750 млн
Сотрудник	75 000	Общие Специальные Биометрические	3	750 млн

Оценка финансовых потерь осуществляли на основе реальной информации, полученной при утечке данных Яндекса [6]. В первую очередь определяли уровень защищенности для каждого субъекта ПДн.

Результаты

ПДн клиентов системы являются общедоступными, количество превышает 100 тысяч, при этом клиенты не являются работниками предприятия. Актуальные для клиентов угрозы относятся к первому типу. На основании Постановления Правительства РФ N 1119 [3] можно сделать вывод, что информацию необходимо отнести ко второму уровню защищенности.

Информация о сотрудниках относится к трем категориям: общедоступная, биометрическая и специальная. Количество субъектов не превышает 100 тысяч, а актуальными являются угрозы 3 типа. Поэтому на основании Постановления Правительства РФ N 1119 [3] делаем вывод, что информация относится к четвертому уровню защищенности.

Следует заметить, что при присваивании уровней защищенности не рассматривался фактор финансовых потерь при утечке. Для коммерческих организаций данный критерий является основополагающим, поэтому для более точной оценки его необходимо учитывать. Взаимосвязь перечисленных факторов может быть представлена в виде математической зависимости (1):

$$k = \frac{S}{m*y} \ , \qquad (1)$$

где S – ценность информации; m – количество субъектов; y – уровень защищенности информации.

Отношение ценности информации к количеству субъектов представляет собой ценность одного субъекта информации. Значение уровня защищенности в данной формуле призвано увеличить значение количества субъектов. При первом уровне защищенности КЗПДн будет равен финансовым потерям утечки информации об одном субъекте ПДн.

Произведем оценку КЗПДн по предлагаемой методике для условной системы, исходные данные которой представлены в таблице 1. Результат вычислений 2500 у. е.

КЗПДн для сотрудников так же 2500 у. е.

Данный показатель более широко и точно определяет характеристику защищенности информации, чем уровень защищенности. Его преимущество заключается в том, что показатель не имеет числовых границ и является универсальным, для предприятий любого масштаба.

Исходные данные изначально задумывались так, чтобы наглядно показать, зависимость КЗПДн от качества и количества информации.

На основании вышеописанной формулы, можно сделать вывод, что значение КЗПДн прямо пропорционально значимости информации.

Обсуждение

Разработанный алгоритм оценки требований к защищенности позволяет шире рассматривать защищенность ПДн, чем уровень защищенности. Однако, для его успешной реализации необходимо провести дополнительные исследования и применить метод оценки к различным предприятиям с уникальными исходными данными. Только тогда можно будет определить средний показатель и дать сравнительную оценку защищенности ПДн для схожих по масштабам систем.

Заключение

Данный метод оценки требований к защищенности является альтернативным подходом к оценке защищенности информации, но его ценность проявится только с течением времени. Если постепенно, в качестве эксперимента вводить КЗПДн в различных организациях и проводить сравнительный анализ, то такая статистика положительно скажется на обеспечении безопасности ПДн.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ: официальный сайт. – Россия. - URL:https://www.consultant.ru/document/cons_doc_law_61801 (дата обращения: 20.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ: официальный сайт. – Россия. - URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 20.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: официальный сайт. – Россия. - URL: https://www.consultant.ru/document/cons_doc_LAW_137356 (дата обращения: 20.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

4. Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Пра-

вительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»: официальный сайт. – Россия. - URL: http://www.consultant.ru/document/cons_doc_LAW_167862/ (дата обращения: 29.03.2023) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

5. Статья «Метод определения опасности угрозы персональным данным при их обработке в информационной системе» официальный сайт. – Россия. - URL: https://izv.etu.ru/assets/files/sh-tbtvtp-2017_10_p19-26.pdf (дата обращения: 09.04.2023) – Текст: электронный. - Режим доступа: общедоступный.

6. Новостная статья «Суд постановил выплатить 13 пользователям сервиса доставки «Яндекс Еда» по 5 тыс. рублей за утечку персональных данных» официальный сайт. – Россия. - URL: https://habr.com/ru/news/t/698402/ (дата обращения: 29.03.2023) – Текст: электронный. - Режим доступа: общедоступный.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-20-26

Ю. Е. Востриков[1], А. В. Шабурова[1]*

Исследование производительности компьютерных систем с применением SSD накопителей в организации ФППК Роскадастр

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: vostrikov.iury@gmail.com

Аннотация. Данная научная публикация посвящена изучению целесообразности замены жестких дисков HDD на твердотельные накопители SSD в организации ФППК «Роскадастр». В работе подробно рассматриваются основные причины, по которым организация может задуматься о замене жестких дисков, а также проводится анализ теоретических и практических аспектов использования SSD накопителей. Для осуществления эксперимента была создана выборка, включающая компьютеры с HDD и SSD накопителями. При анализе производительности были учтены важные параметры, включая время загрузки операционной системы и запуска программ. Путем сбора и обработки данных, включая время загрузки операционной системы и запуска программ, было проведено сравнительное исследование производительности компьютеров с различными типами накопителей. Результаты данного исследования помогут принять решения относительно замены HDD на SSD и так же, могут послужить основой для разработки плана модернизации компьютерных систем в организации, способствуя повышению их эффективности и производительности.

Ключевые слова: HDD, SSD, компьютер, тестирование, метод t–тест Стьюдента

Y. E. Vostrikov[1], A. V. Shaburova[1]*

Research of Performance of Computer Systems Using SSD Drives in the Organization of FPPK Roskadastr

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: vostrikov.iury@gmail.com

Abstract This scientific publication is devoted to the study of the feasibility of replacing HDD hard drives with SSD solid-state drives in the organization of the FPPK "Roskadastr". The paper discusses in detail the main reasons why an organization may think about replacing hard drives, and also analyzes the theoretical and practical aspects of using SSD drives. To carry out the experiment, a sample was created, including computers with HDD and SSD drives. During the performance analysis, important parameters were taken into account, including the time of loading the operating system and running programs. By collecting and processing data, including the boot time of the operating system and the launch of programs, a comparative study of the performance of computers with different types of drives was conducted. The results of this study will help to make decisions regarding the replacement of HDD with SSD and can also serve as a basis for the development of a plan for the modernization of computer systems in the organization, contributing to their efficiency and productivity.

Keywords: HDD, SSD, computer, testing, Student's t–test method

Введение

В последние годы было проведено множество исследований, посвященных сравнению производительности HDD и SSD накопителей. Некоторые из этих исследований показывают, что SSD накопители имеют значительно более высокую производительность по сравнению с HDD, особенно в отношении скорости чтения и записи данных. Однако, есть также исследования, которые показывают, что разница между производительностью HDD и SSD накопителей не так велика, как могло бы показаться [8].

Целью работы является определение преимуществ и недостатков перехода на SSD накопители, а также оценка его практической значимости. Для достижения этой цели были поставлены следующие задачи:

– провести обзор литературы по теме;

– сравнить производительность HDD и SSD;

– провести экспериментальное исследование.

Теоретическая значимость исследования заключается в обобщении существующих знаний о твердотельных накопителях и их применении на предприятиях. Практическая значимость заключается в возможности принятия обоснованных решений о модернизации компьютеров в организации с учетом экономических и технических факторов. Результаты исследования показывают, что переход на SSD может значительно повысить производительность компьютеров.

Методы и материалы

Для проведения исследования была выбрана организация ФППК «Роскадастр» с целью изучения влияния использования SSD накопителей на скорость работы компьютеров. В аудитории, которая использовалась для обучения сотрудников, находилось 10 компьютеров. Из них 5 компьютеров оборудовали SSD накопителями на 1 ТБ, в то время как у оставшихся 5 компьютеров были установлены HDD накопители. Все компьютеры имели одинаковую конфигурацию, за исключением типа накопителя.

Характеристики компьютеров с HDD:

– материнская плата Gigabyte H310M S2H 2.0;

– процессор Intel Pentium G5400 3.7 GHz;

– видеоадаптер Intel UHD Graphics 610;

– оперативная память 2x Netac Basics 4 ГБ;

– блок питания 430W;

– накопитель HDD WD Caviar Blue WD10EZEX, 1ТБ.

Характеристики компьютеров с SSD:

– материнская плата Gigabyte H310M S2H 2.0;

– процессор Intel Pentium G5400 3.7 GHz;

– видеоадаптер Intel UHD Graphics 610;

– оперативная память 2x Netac Basics 4 ГБ;

– блок питания 430W;

– накопитель SSD KINGSPEC P3–1TB 1ТБ.

На основе предварительного исследования и анализа характеристик различных моделей твердотельных накопителей. Проведенное исследование показало, что KINGSPEC SSD демонстрируют высокую производительность в сравнении с аналогами других производителей, а также обладают устойчивостью к повреждениям и долгим сроком службы. В связи с этим, было принято решение о закупке и установке именно этой модели накопителей на 5 компьютеров для дальнейшего исследования производительности в сравнении с HDD.

Были выбраны различные задачи, включающие в себя запуск программ, работу с документами, использование интернет–ресурсов и запуск ОС. Каждая задача была запущена на всех компьютерах в случайном порядке. Для каждой задачи было измерено время, которое затратил компьютер на ее выполнение.

Для проверки статистически значимых различий между двумя выборками, полученными в результате эксперимента по сравнению производительности HDD и SSD, можно применить метод t–теста Стьюдента [1]. Этот метод является одним из самых распространенных инструментов для анализа статистических различий между двумя выборками. Данный метод основывается на проверке гипотезы о равенстве средних значений двух выборок и позволяет оценить значимость различий между ними. Также, необходимо учитывать, что для применения t–теста необходимо проверить нормальность распределения выборок и равенство дисперсий, что мы и сделаем дальше.

Расчет будет производится с помощью формулы [4]:

$$t = \frac{\overline{x}_1 - \overline{x}_2}{\sqrt{m_1^2 + m_2^2}}, \tag{1}$$

где $\overline{x}_1$ – средняя арифметическая первой сравниваемой группы; $\overline{x}_2$ – средняя арифметическая второй сравниваемой группы; m_1^2 – средняя ошибка первой средней арифметической; m_2^2 – средняя ошибка второй средней арифметической.

Для расчета t–статистики по методу Стьюдента, нам понадобятся следующие формулы.

Для расчета среднего значения выборки [4, 6]:

$$\overline{x} = \frac{(\sum x_i)}{n}, \tag{2}$$

где $\overline{x}$ – среднее значение выборки; $\sum x_i$ – сумма всех значений выборки; n – количество значений в выборке.

Для расчета среднего отклонения используем формулу [4, 6]:

$$\sigma^2 = \frac{\sqrt{\sum (x_i - \overline{x})^2}}{(n-1)}, \tag{3}$$

где σ – среднее отклонение выборки; $\sum$ – сумма значений выборки; x_i – значение выборки; $\bar{x}$ – среднее значение выборки; n – количество значений в выборке.

Для расчета стандартной ошибки используем формулу [4, 6]:

$$m = \frac{\sigma}{\sqrt{n}}, \tag{4}$$

где m – стандартную ошибку среднего значения; σ – среднее отклонение выборки; n – количество значений в выборке.

Для оценки производительности было измерено время загрузки операционной системы и запуск ряда программ на каждом компьютере. Полученные результаты представлены в табл. 1 и приведены значения выборочного среднего, стандартного отклонения [2]. В дальнейшем, на основе этих данных будет проведен анализ различий между выборками при помощи t–теста Стьюдента, что позволит понять целесообразность модернизации на SSD накопитель.

Результаты

Для проведения анализа различий между выборками, полученными в результате эксперимента, использовался критерий t–Стьюдента. В табл. 1 представлены результаты проведенных измерений времени загрузки операционной системы и запуска ряда программ. Эти данные могут помочь определить, какой тип накопителя HDD или SSD имеет более высокую производительность.

Таблица 1

Результаты после измерений

HDD				SSD			
№ ПК	запуск ОС	запуск ME	запуск GC	№ ПК	запуск ОС	запуск ME	запуск GC
	x_1, с	x_3, с	x_5, с		x_2, с	x_4, с	x_6, с
1	36	11	9	1	16	4	4
2	39	16	8	2	19	5	4
3	44	15	9	3	15	3	3
4	42	11	7	4	21	7	6
5	38	13	10	5	12	4	5

Изучив табл. 1, мы можем сделать вывод, что время, необходимое для загрузки операционной системы и запуска программ на компьютерах с установленным SSD накопителем, значительно меньше по сравнению с компьютерами, использующими HDD накопители [7].

Приведенная ниже табл. 2 содержит результаты проведенного эксперимента, данные позволяют оценить время загрузки операционной системы и за-

пуска программ для компьютеров, использующих SSD и HDD накопители. Анализ этих результатов позволяет сделать выводы о преимуществах и недостатках каждого типа накопителя в контексте производительности.

Таблица 2

Результаты после расчетов на ПК с HDD

HDD диски	Расчетные показатели				
	$\bar{x}$	$\sum x_i$	σ^2	σ	m
x_1	39,8	40,8	10,2	3,19	1,43
x_3	13,2	20,8	5,20	2,28	1,02
x_5	8,20	2,80	0,70	0,84	0,37

Таблица 3

Результаты после расчетов на ПК с SSD

SSD диски	Расчетные показатели				
	$\bar{x}$	$\sum x_i$	σ^2	σ	m
x_2	16,6	49,20	12,30	3,51	1,57
x_4	4,60	9,20	2,30	1,52	0,68
x_6	4,40	5,20	1,30	1,14	0,51

На основе полученных данных, рассчитаем *t*–критерий Стьюдента для каждой из выборок:

$$t_1 = \frac{39,8 - 16,6}{\sqrt{1,43^2 + 1,57^2}} = 10,94$$

$$t_2 = 6.82$$

$$t_3 = 5.91$$

Значения t_1, t_2 и t_3 свидетельствуют о том, что разница между двумя выборками является статистически значимой [9]. Это говорит в пользу того, что использование твердотельных накопителей может значительно повысить производительность компьютеров при загрузке операционной системы и запуске программ.

Обсуждение

Сравнение полученных результатов с результатами других авторов также показало, что наша выборка подтверждает общую тенденцию к уменьшению времени запуска программ [8], что может быть полезным при выборе оптимального типа накопителя для повышения производительности компьютерных си-

стем. Однако, разница во времени может различаться в зависимости от характеристик компьютера и особенностей программного обеспечения, что необходимо учитывать при интерпретации результатов.

Заключение

Анализ результатов исследования показал, что среднее время запуска программы на компьютерах с SSD было меньше, чем на компьютерах с HDD. Разница между средними значениями составила 4,23 секунды, что свидетельствует о статистически значимой разнице между этими двумя типами компьютеров.

Также было обнаружено, что разброс значений времени запуска программы на компьютерах с HDD был больше, чем на компьютерах с SSD, что подтверждается большим значением стандартного отклонения в выборке компьютеров с HDD [4, 9]. Это может объясняться более низкой скоростью чтения и записи на жестких дисках в сравнении с твердотельными накопителями.

На компьютерах с SSD наблюдалась более плавная работа программ, без существенных прерываний или задержек, в то время как на компьютерах с HDD были выявлены периодические простои и задержки в работе программы [1].

Таким образом, результаты нашего исследования подтверждают рекомендации по использованию SSD–накопителей в качестве оптимального решения для повышения производительности компьютеров при работе с тяжелыми приложениями и большими объемами данных.

Благодарность

Автор выражает благодарность ФППК «Роскадастр» за предоставленные данные и информацию, необходимые для проведения исследования и написания данной статьи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Клячкин, В. Н. Статистические методы анализа данных : учебное пособие / В. Н. Клячкин, Ю. Е. Кувайскова, В. А. Алексеева. – Москва : Финансы и Статистика, 2021. – 240 с.

2. Кулаичев, А. П. Методы и средства комплексного статистического анализа данных : учебное пособие / А.П. Кулаичев. – 5–е изд., перераб. и доп. – Москва : ИНФРА–М, 2022. – 484 с.

3. Назаров, С. В. Измерительные средства и оптимизация вычислительных систем [Электронный ресурс] / С. В. Назаров. – Москва : Радио и связь, 1990. – 248 с.

4. Назаров, С. В. Производительность вычислительных систем / С. В. Назаров, А. В. Мурин, А. Г. Барсуков. – Москва : Энергоатомиздат, 1993. – 248 с.

5. Пушкарёва, Т. П. Основы компьютерной обработки информации: учебное пособие / Пушкарёва Т.П. - Краснояр.:СФУ, 2016. - 180 с.

6. Соколов, Г. А. Основы математической статистики : учебник / Г.А. Соколов. – 2–е изд. – Москва : ИНФРА–М, 2022. – 368 с.

7. Тюнина, Н. А. DVD/VCR/HDD–рекодеры и проигрыватели. Устройство и ремонт : практическое пособие / под ред. Н. А. Тюнина и А. В. Родина. – Москва : СОЛОН–ПРЕСС, 2020. – 136 с.

8. Хорошевский, В. Г. Архитектура вычислительных систем : учебное пособие / В. Г. Хорошевский. – 2–е изд., перераб. и доп. – Москва : МГТУ им. Баумана, 2008. – 519 с.

9. Царев, Р. Ю. Основы распределенной обработки информации: учебное пособие / Царёв Р.Ю., Прокопенко А.В., Никифоров А.Ю. - Краснояр.:СФУ, 2015. - 180 с.

10. Чернов, В. Ю. Введение в технику эксперимента и основы обработки результатов измерений : учебное пособие / В. Ю. Чернов, Э. А. Анисимов. – Йошкар–Ола : ПГТУ, 2020. – 68 с.

УДК 004.9
DOI 10.33764/2618-981X-2023-6-27-34

Н. С. Головачев[1], П. Ю. Бугаков[1]*

Разработка методики создания ГИС для учета и контроля малых архитектурных форм

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: tel1386@mail.ru

Аннотация. В статье описываются основные элементы методики создания геоинформационной системы (ГИС) для учета и контроля малых архитектурных форм (МАФ). Проектируемая геоинформационная система строится на основе базы данных (БД), содержащей сведения о малых архитектурных формах, полученных в процессе их каталогизации. Каталогизация подразумевает размещение на МАФ специальных меток, позволяющих однозначно идентифицировать объект и получить необходимые сведения из семантической базы данных ГИС. По данным меткам пользователи ГИС смогут оставлять обращения в случае выявления дефектов объекта. На основе описанной концепции создается прототип системы реализующий основные функции ГИС для тестирования и сбора дополнительной информации о пригодности в использования подобных систем. Благодаря результатам тестирования будет доработана методика создания ГИС для учета и контроля малых архитектурных форм.

Ключевые слова: геоинформационная система, управляющие организации, система контроля, малые архитектурные формы, детские площадки

N. S. Golovachev[1], P. Yu. Bugakov [1]*

Development of a GIS Creation Methodology for Accounting and Control of Small Architectural Forms

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: tel1386@mail.ru

Abstract. The article describes the main elements of the methodology for creating a geoinformation system (GIS) for accounting and control of small architectural forms (SAF). The geoinformation system is built on the basis of a database containing information about small architectural forms obtained during their cataloging. Cataloging involves placing special tags on the SAF that allow you to uniquely identify the object and get the necessary information from the semantic GIS database. According to these tags, GIS users will be able to send requests in case of detection of defects in the object. Based on the described concept, a prototype of the system is being created that implements the main functions of GIS for testing and collecting additional information about the suitability of using such systems. Due to the test results, the methodology for creating GIS for accounting and control of small architectural forms will be finalized.

Keywords: geoinformation system, management organizations, control system, small architectural forms, playgrounds

Введение

В целях надлежащего обслуживания детских площадок, управляющая организация обязана осуществлять их регулярный визуальный осмотр, проверку функционирования (примерно раз в 1–3 месяца), а также ежегодный основной осмотр [1–3].

Для автоматизации данных процессов предлагается использовать геоинформационную систему (ГИС), которая позволит хранить всю информацию о состоящих на балансе управляющей организации (УО) объектах малых архитектурных форм (МАФ), а также предоставит возможность гражданам принять участие в контроле за надлежащим состоянием данных объектов [4].

Для разработки и апробации методики создания ГИС учета и контроля малых архитектурных форм необходимо выполнить следующие действия:

– разработать и описать концептуальную схему функционирования ГИС;

– выделить группы пользователей ГИС;

– описать процесс каталогизации объектов;

– разработать структуру данных ГИС, представить ее в виде концептуальной модели;

– выполнить реализацию функциональных модулей ГИС и провести их тестирование.

Концептуальная схема функционирования ГИС

Каждый объект МАФ, который вносится в геоинформационную систему, будет иметь уникальную метку, позволяющую однозначно идентифицировать объект в системе. Любой гражданин, сотрудник УО или контролирующих органов может получить информацию из базы данных (БД) ГИС, используя метку, которая представляет собой QR-код с уникальным 36-символьным номером МАФ (UUID), сгенерированным при внесении в БД [5–8]. Эта система поможет быстрее выявлять дефекты за счет участия граждан и автоматизации приема обращений.

Фотофиксация неисправного объекта происходит при помощи смартфона или планшета, оснащенного фотокамерой. Пользователь фотографирует QR-код и делает несколько снимков, которые отражают характер и масштаб выявленных дефектов. Затем фотографии загружаются на сервер ГИС, после чего автоматически формируется обращение в управляющую организацию на устранение зафиксированной неисправности. В случае отсутствия действий по устранению неисправностей и внесения соответствующих данных в ГИС, система автоматически уведомит государственную жилищную инспекцию (ГЖИ) [9]. Все МАФ будут отмечаться в виде условных знаков на картографической основе из открытых источников (например, OpenStreetMap) [10]. ГИС должна предоставлять сотрудникам ГЖИ возможность осуществлять сбор и анализ статистической информации по выбранной территории.

На рис.1 изображены серверы УО и ГЖИ, куда будут отправляться копии уведомлений о выявленных проблемных объектах, отправленных пользователями ГИС через внешние web-интерфейсы или приложения на смартфонах. Данная схема показывает принцип функционирования ГИС.

На рис. 1 связи 1, 2, 3 обозначают процесс сканирования с помощью смартфона QR-метки объекта МАФ. Пользователь может инициировать этот процесс, чтобы получить информацию об объекте или внести информацию об объекте в систему.

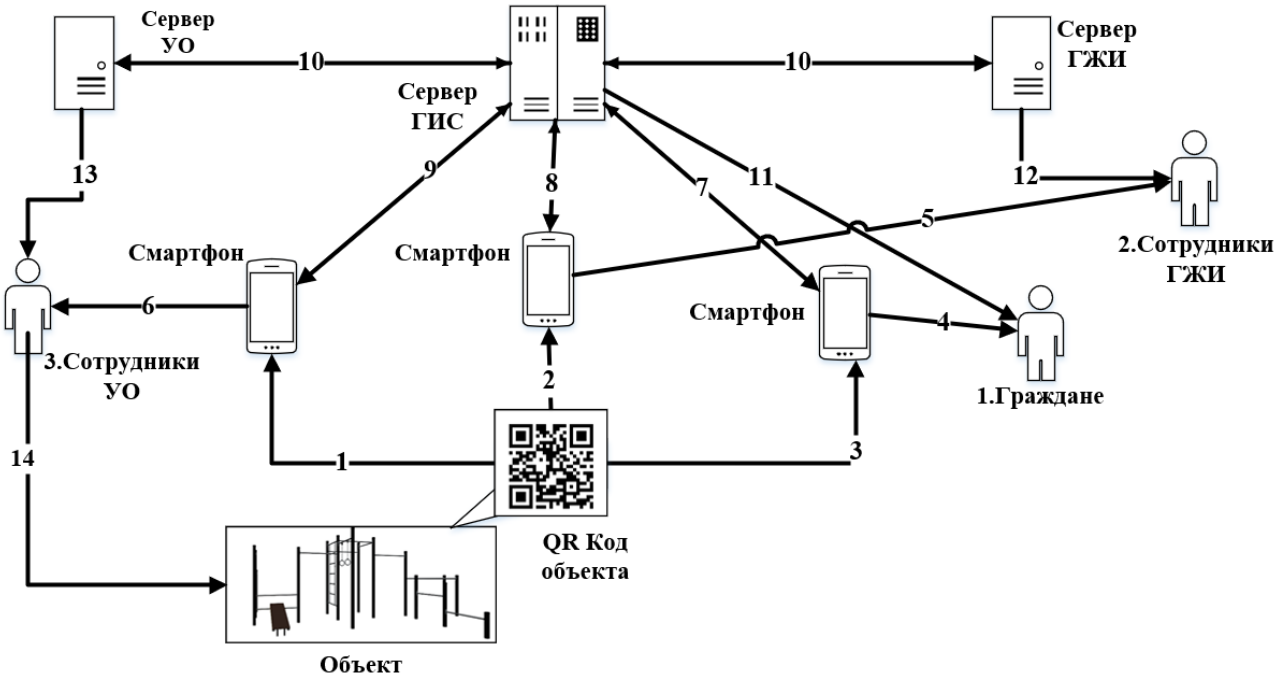


Рис. 1. Концептуальная схема функционирования ГИС

Связи 4, 5 и 6 обозначают доступ пользователей различных уровней к информации об объектах. Каждому пользователю будет доступен набор информации, который зависит от роли пользователя в системе. Все пользователи смогут получить информацию о количестве жалоб на объект.

Связь 7 показывает передачу сервером ГИС информации об объекте на смартфон пользователя, а также предоставление возможности подачи обращения о наличии дефектов на объекте МАФ.

Связь 8 показывает передачу информации об объекте на смартфон сотрудника ГЖИ, а также предоставление возможности оставить заявку на устранение дефекта объекта. Сотрудники ГЖИ имеют расширенные возможности для ознакомления с информацией и составления заявок на устранение дефектов МАФ.

Связь 9 показывает получение сотрудником УО доступа к возможности вносить информацию об объектах и обновлять статус обращений граждан. Эта информация будет сохраняться на сервере и станет доступна всем остальным пользователям.

Связь 10 показывает обмен информацией между сервером ГИС и серверами ГЖИ или УО. Сервер ГИС будет предоставлять информацию о количестве, времени подачи и другой статистики по обращениям граждан.

Связь 11 показывает получение гражданином уведомления о выполнении работ по его обращению. В случае игнорирования обращения гражданина сотрудниками УО, сведения по нему будет автоматически перенаправлено сотрудникам ГЖИ, о чем система также уведомит гражданина.

Связь 12 показывает процесс получения сотрудниками ГЖИ информации о необходимости проверки любого УО.

Связь 13 показывает поступление уведомлений сотрудникам УО о всех обращениях граждан и сроках устранения нарушений, по истечении которых система автоматически уведомит ГЖИ о нарушении.

Связь 14 показывает процесс установки QR-меток на объекты сотрудниками УО.

Процесс каталогизации объектов для ГИС

Управляющие организации, которые планируют использовать ГИС, должны внести в нее информацию о находящихся у них на балансе МАФ. Каталогизация объектов осуществляется путем проведения натурного обследования территории и идентификации объектов МАФ, которые должны быть внесены в базу данных. Данные о МАФ включают в себя вид, назначение, производителя, артикул, координаты объекта, адрес дома, информацию об управляющей организации и фотографии объекта. Один из вариантов каталогизации МАФ показан на рисунке 2.

Сотрудники управляющей организации создают новую запись о МАФ в базе данных ГИС и вносят всю соответствующую информацию, при этом система автоматически генерирует идентификатор объекта (стрелка 1.1 на рисунке 2). Вся информация о МАФ на территории управляющей организации заносится в базу данных, а затем генерируются QR-коды, соответствующие количеству объектов в базе данных ГИС (стрелка 1.2 на рисунке 2). Сотрудники управляющей организации подготавливают физические QR-метки, которые передаются сотрудникам УО (стрелка 1.3 на рисунке 2). После размещения QR-метки на соответствующем МАФ, сотрудник УО может сканировать QR-код и просмотреть информацию о МАФ и его местоположении. Этот метод каталогизации МАФ является простым и оперативным.

Рис. 2. Процесс каталогизации МАФ

Структура данных ГИС

Основные данные, необходимые для работы ГИС, могут быть разбиты на 6 сущностей, каждая из которых будет представлена в базе данных отдельной таблицей (рис. 3).

Таблица «Артикулы производителей» содержит каталог типовых МАФ, используемых на детских и спортивных площадках в городе или регионе, упрощает последующую каталогизацию объектов в полевых условиях.

Таблица «Объекты» содержит уникальный идентификационный номер МАФ, пространственные координаты объекта, фотографии объекта МАФ для его определения на дворовой территории.

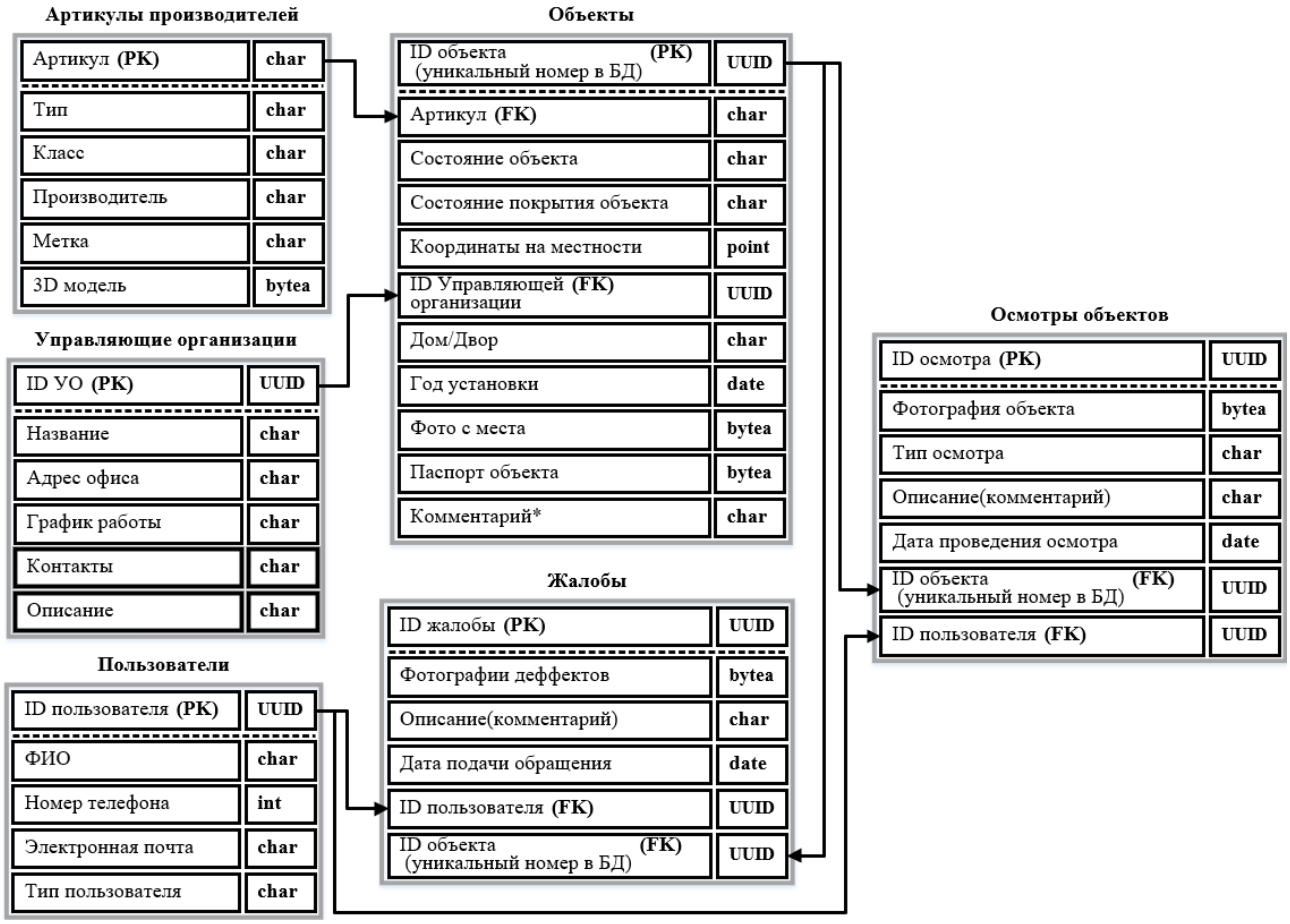


Рис. 3. Концептуальная модель структуры данных ГИС

Таблица «Управляющие организации» содержит данные об управляющей организации, включая контактную информацию.

Таблица «Пользователи» содержит информацию о пользователях и их правах доступа к системе, которая используется для автоматического уведомления сотрудников управляющей организации, подключенных к ГИС, и оповещения граждан, подавших обращение.

Таблица «Жалобы» содержит информацию о функциональных дефектах или других проблемах, возникших с объектами МАФ, а также дату подачи обращения для определения сроков реагирования управляющей организации. Для обращения в таблице используется идентификатор объекта, полученный из QR-кода, фотографии дефекта и текстовое описание проблемы.

Таблица «Осмотры объектов» хранит фотографию, описание и время проведенного осмотра объекта. Поскольку законодательством подразумевается проведение как минимум 3-х видов осмотров МАФ, для некоторых из них может потребоваться составление отчетной ведомости. Данные в этой таблице должны храниться до следующего однотипного осмотра того же объекта, после чего новая информация заменяет устаревшую.

Реализация функциональных модулей ГИС

Основным интерфейсом коммуникации между пользователями и базой данных объектов ГИС должно стать мобильное приложение, которое позволит реаизовать весь необходимый функционал. Для тестирования и анализа результатов работы системы, необходимо разработать прототип мобильного приложения.

Тестовое мобильное приложение разработано для операционной системы (ОС) Android [12–14]. Выбор основан на открытости данной ОС, возможности установки программы через установочный APK-файл и распространенности на территории России. Согласно данным сервиса «Яндекс радар» 77,53 % смартфонов, используемых в России, работают под управлением ОС Android [15]. В будущем это позволит провести активное тестирование прототипа на большем числе устройств для выявления возможных недоработок в системе.

Согласно разработанной концептуальной структуре данных (рис. 3) была реализована БД при помощи СУБД PostgreSQL. Работа с PostgreSQL может осуществляться с помощью приложения с открытым исходным кодом PgAdmin [16–18]. Благодаря встроенному графическому интерфейсу, PgAdmin упрощает администрирование баз данных и обеспечивает доступ ко всей функциональности PostgreSQL. Помимо простого хранения данных PostgreSQL позволяет расширять функциональность БД с помощью созданных пользователем функций и хранимых процедур. Это понадобится при настройке удаленного сервера БД, с которым будут связываться мобильные приложения [19–20]. В процессе работы с PgAdmin были созданы 6 таблиц по заранее составленной схеме данных.

Используя разработанное приложение, был осуществлен сбор информации об объектах МАФ на территории жлого комплекса «Чистая слобода». Собранные данные позволили идентифицировать все МАФ на указанной территории путем сканирования QR-кода (рис. 4).

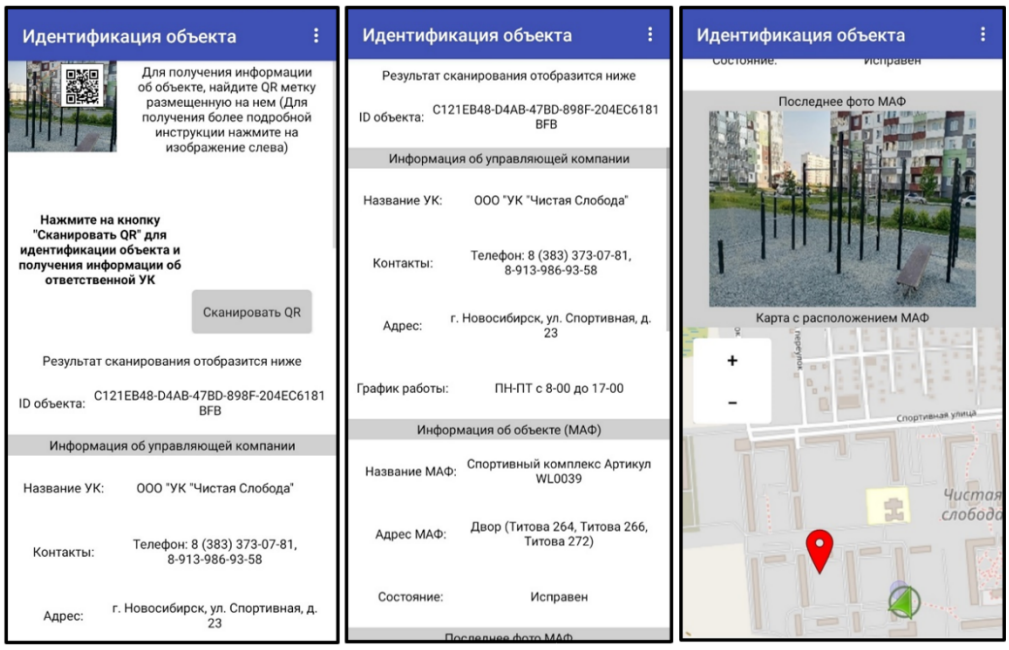


Рис. 4. Пример результата идентификации объекта по QR метке

Заключение

В результате работы для теоретического анализа эффективности системы и ее частей разработана концептуальная схема функционирования ГИС. В данной схеме отражены основные возможные элементы системы и основные связи обмена данными между ними. Разграничение функциональных возможностей ГИС осуществляется за счет выделения нескольких групп пользователей. Для собираемой и хранимой в ГИС информации о объектах МАФ разработана структура данных, соответствующая всем аспектам концептуальной модели. Принцип функционирования ГИС описан в форме последовательности действий каталогизации МАФ. Выполнена разработка научно-методических основ создания ГИС для учета и контроля малых архитектурных форм.

На основе полученных теоретических материалов были реализованы функциональные модули ГИС, ключевыми из которых являются мобильное приложение пользователя и единая база данных. По результатам проведенного тестирования на реальных данных будет произведена доработка теоретических аспектов методики, а также выполнено совершенствование прототипа системы с расширением его функционала.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Ответственность за содержание детских площадок во дворах [Электронный ресурс]. – Режим доступа: http://gji.nso.ru/news/1686 (дата обращения: 20.04.2023).

2 УК отвечает за детские площадки [Электронный ресурс]. – Режим доступа: https://www.garant.ru/news/1414865/ (дата обращения: 21.04.2023).

3 Содержание детских площадок [Электронный ресурс]. – Режим доступа: https://www.burmistr.ru/blog/obshchee-imushchestvo-mkd/soderzhanie-detskikh-ploshchadok/ (дата обращения: 21.04.2023).

4 Бугаков, П. Ю., Головачев Н.С. Концептуальное проектирование геоинформационной системы для учета технического состояния малых архитектурных форм // Вестник СГУГиТ. – 2022. – Т. 27, № 6. – С. 98-107.

5 Тип данных UUID [Электронный ресурс]. – Режим доступа: https://postgrespro.ru/docs/postgrespro/9.5/datatype-uuid (дата обращения: 30.03.2023).

6 D. ADC. QR Code essentials, 2011. Retrieved 12 March 2013

7 Кузнецов С. А., Сотникова А. Ю., Колесников А. А. Применение QR-кодов в картографии // 27-я Региональная научная студенческая конференция. 2019. – С. 315-319.

8 Михальчук Н. Е. Библиотечные QR-проекты в цифровом пространстве // Научные и технические библиотеки. – 2021. – № 9. – С. 91-102.

9 Чем занимается жилищная инспекция [Электронный ресурс]. – Режим доступа: https://pravovik.guru/chem-zanimaetsya-zhilishhnaya-inspektsiya/ (дата обращения: 21.03.2023).

10 Янкелевич С. С., Лебзак А. О., Лебзак Е. В. Технологические аспекты создания веб-ГИС объектов культурного наследия для пространственного развития территории на примере Новосибирской области // ИнтерКарто. ИнтерГИС. – 2020. – Т. 26. – № 4. – С. 311-319.

11 Головачев, Н. С., Бугаков П.Ю. Разработка концептуальной модели ГИС для учета и контроля эксплуатационных параметров малых архитектурных // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 21-30.

12 Android Studio - the official Integrated Development Environment (IDE) for Android app development. [Электронный ресурс]. – Режим доступа: https://developer.android.com/studio (дата обращения: 13.03.2023).

13 ECLIPSE IDE The Leading Open Platform for Professional Developers [Электронный ресурс]. – Режим доступа: https://eclipseide.org (дата обращения: 02.03.2023).

14 IntelliJ IDEA – the Leading Java and Kotlin IDE [Электронный ресурс]. – Режим доступа: https://www.jetbrains.com/idea (дата обращения: 02.02.2022).

15 Мобильные ОС в России | Яндекс.Радар [Электронный ресурс]. – https://radar.yandex.ru/mobile?selected_rows=F1A6ay%252CUk4F3H (дата обращения: 18.03.2023).

16 Спицин К.В. Сидоренко Д.А. Барсукова А.А. Использование PostGIS в сфере картографии // XXX Международная научно-практическая конференция. Пенза, 2021. – С. 13-15.

17 Hans-Jürgen Schönig. Build, administer, and maintain database applica-tions efficiently with PostgreSQL / Mastering PostgreSQL 15 // Published by Packt Publishing Ltd. – 2023

18 PostgreSQL – Introduction to Stored Procedures [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/postgresql-introduction-to-stored-procedures (дата обращения: 18.01.2022).

19 Дорошенко Р.А., Запорожец И.И. Исследование производительности клиент-серверных СУБД MYSQL, FIREBIRD И POSTGRESQL при выполнении запросов на выборку // Инновационные технологии в машиностроении, образовании и экономике. Т. 25. № 4.2019. – С. 29-32.

20 Курако, Е. А., Орлов В. Л. К вопросу миграции баз данных из среды Oracle в среду PostgreSQL // Программная инженерия. – 2022. – Т. 13, № 1. – С. 32-40.

УДК 52-17
DOI 10.33764/2618-981X-2023-6-35-41

*Е. Ф. Голубь[1], Т. Ю. Бугакова[1]**

Моделирование пространственно-временных состояний техногенных систем по геодезическим данным для обеспечения безопасного функционирования

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: kaf.pi@ssga.ru

Аннотация. Современные технические средства наблюдений позволяют получить цифровое описание пространственного объекта. Применение математических методов, дает возможность аппроксимировать координатные данные объекта и представить его в виде математической модели, изучение которой позволяет получить любую информацию об изменении состояния объекта в пространстве и времени для предупреждения аварийных ситуаций и безопасного функционирования. В статье рассмотрены практические примеры построения математических моделей для определения пространственной ориентации объекта, крена фундамента жилого здания и оценки его интегральной деформации методом математической аппроксимации. Построение и анализ математической модели по пространственной цифровой информации об объекте позволяет определить пространственное положение всего инженерно-технического сооружения в виде математического объекта, анализ которого дает возможность выполнять комплексную оценку пространственно-временного состояния объекта в целом и его геометрических параметров.

Ключевые слова: пространственно-временное состояние, инженерно-технические сооружения, математические модели, методы аппроксимации

*E. F. Golub[1], T. Yu. Bugakova[1]**

Modeling of Spatio-Temporal States of Technogenic Systems Based on Geodetic Data to Ensure Safe Operation

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: kaf.pi@ssga.ru

Abstract. Current technical means of observation make it possible to obtain a digital description of a spatial object. The use of mathematical methods makes it possible to approximate the coordinate data of an object and present it in the form of a mathematical model, the study of which allows obtaining any information about changes in the state of the object in space and time to prevent emergencies. The article considers practical examples of building mathematical models for determining the spatial orientation of an object, the roll of the foundation of a residential building and assessing its integral deformation by mathematical approximation. The building and analysis of a mathematical model based on spatial digital information about an object determine the spatial position of the entire engineering and technical structure in the form of a mathematical object, the analysis of which makes it possible to perform a comprehensive assessment of the spatial and temporal state of the object as a whole and its geometric parameters.

Keywords: spatial-temporal state, engineering structures, mathematical models, approximation methods

Введение

Контроль пространственно-временного состояния (ПВС) инженерно-технических сооружений является одной из важнейших задач обеспечения безопасности их эксплуатации [16–18]. Любые инженерно-технические сооружения (ИТС) подвержены воздействию внешних и внутренних факторов, что способствует изменению их состояний. Сегодня существует множество примеров аварийных ситуаций, техногенных катастроф и чрезвычайных ситуаций, связанных с эксплуатацией зданий и инженерных сооружений (объектов) [13, 20]. Совершенствуются технологии строительства, инструменты и средства наблюдений за пространственно-временным состоянием объектов, однако все это не гарантирует полную безопасность таких объектов. Современные технические средства наблюдений позволяют получить цифровое описание пространственного объекта [14–16]. Применение математических методов, дает возможность аппроксимировать координатные данные объекта и представить его в виде математической модели, изучение которой позволяет получить любую информацию об изменении состояния объекта в пространстве и времени для предупреждения аварийных ситуаций и безопасного функционирования [24].

Методы и материалы

В основу современных программных продуктов (ПО) заложены математические алгоритмы, позволяющие определить параметры вертикальных и горизонтальных смещений, деформаций, а также визуализировать изменения пространственно-временного состояния ИТС и их конструктивных элементов [1, 4–6]. Однако, на сегодняшний день, данные программы имеют некоторые недостатки [10–12].

1. Пользователь не может изменить математические алгоритмы, которые заложены в таких программах, что усложняет оценку ПВС ИТС, т.к. в некоторых случаях необходимо учитывать их индивидуальные конструктивные особенности и особенности влияния внешних факторов.

2. Использование большинства программ для детализированной оценки ИТС, подразумевает подключение нескольких модулей, что в свою очередь значительно повышает затраты для использования ПО в исследованиях ПВС ИТС.

3. Программные продукты имеют ограниченное количество математических алгоритмов, что затрудняет проведение комплексного и полного анализа состояния ИТС.

4. В условиях импортозамещения возникают сложности использования зарубежного ПО.

Для комплексного контроля пространственно-временного состояния ИТС систем необходимы данные о геометрических свойствах объекта, как функциях времени. К ним относятся форма, размеры, положение в пространстве и другие свойства, характеризующие взаимное расположение множества точек объекта относительно внешней среды и относительно друг друга [6–9]. Выполнить непосредственное измерение таких параметров даже современными техническими

средствами чаще всего не удается и поэтому для их определения применяют методы математического моделирования [2, 3, 26–29].

Объектом исследований определения ПВС является жилой дом в городе Новосибирск по адресу: ул. Октябрьская, дом № 40 (рис. 1).

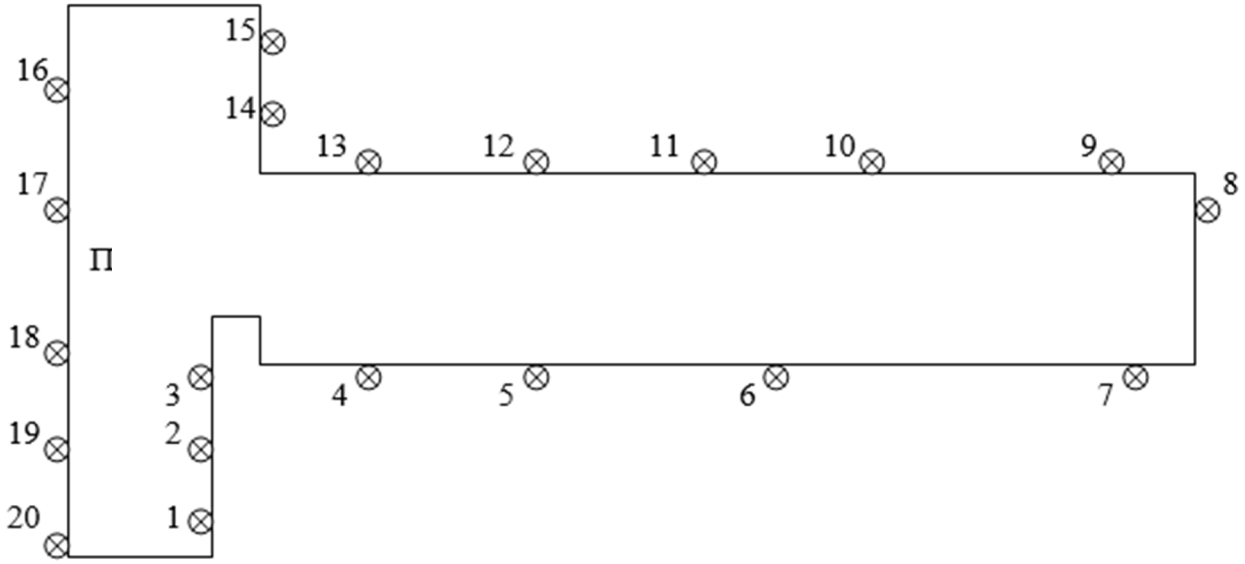


Рис. 1. План размещения геодезических марок в стене жилого здания по ул. Октябрьская, 40

Для геодезического контроля в фундамент здания заложено 20 геодезических марок (контрольных точек). В результате 12 циклов геодезических наблюдений получены высотные координаты марок $H_i(t)$, где $i=1,2..20$, $t=1,2..12$. Координаты X_i и Y_i, определены относительно условной системы координат.

Целью исследований является определение пространственной ориентации фундамента жилого здания (крена) [1–5] и определение интегральной деформации объекта в целом [10–13].

Результаты исследований

Для определения пространственной ориентации фундамента здания была выполнена аппроксимация множества контрольных точек математической моделью плоскости S для каждого цикла наблюдений [24–26]. Пример результата аппроксимации, выполненной в программе MathCad, изображен на рис. 2 (а – для цикла №1, б – цикла №12.

Изменение пространственной ориентации фундамента объекта определяется углом α^o между нормалью $N_{t=1}$, проведенной к плоскости на момент t_1 и нормалями $N_{t=2,3..12}$, определенными на другие моменты времени. Результаты вычислений углов между нормалями представлены в табл. 1.

Полученные данные свидетельствуют об изменении ориентации объекта (общий крен фундамента) [11–13, 22, 25].

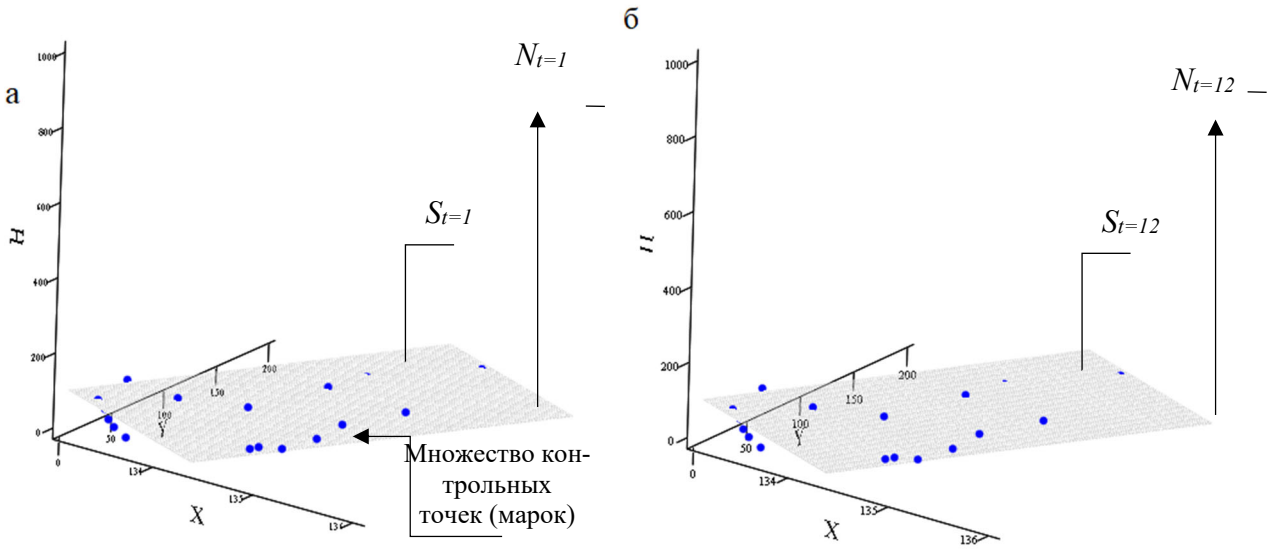


Рис. 2. Аппроксимация множества контрольных точек плоскостью
(а – 1 цикл наблюдений; б – 12 цикл наблюдений)

Таблица 1

Углы между нормалями

α t_1–t_2	α t_1–t_4	α t_1–t_5	α t_1–t_9	α t_1–t_{11}	α t_1–t_{12}
03°07'55,2"	03°08'24,0"	03°08'27,6"	03°08'27,6"	3°08'27,6"	03°08'27,6"

Для определения интегральной деформации был выбран метод аппроксимации множества контрольных точек объекта сферой [29, 30]. Интегральная деформация характеризуется изменением радиуса *R* сферы. На рис. 3 представлены результаты аппроксимации объекта сферой, выполненной в программе MathCad.

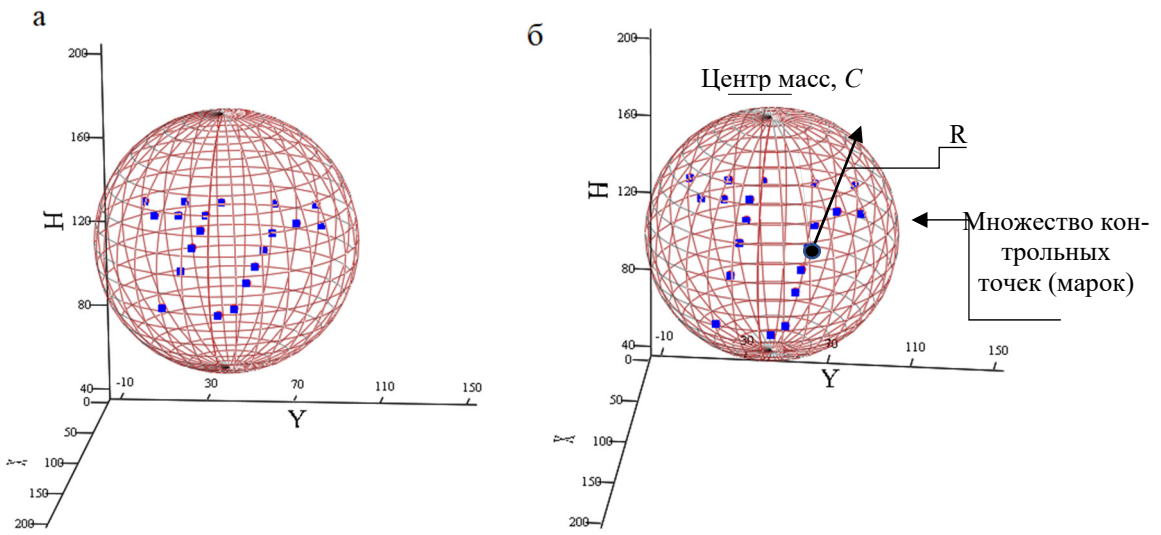


Рис. 3. Аппроксимация облака точек сферой
(а – 1 цикл наблюдений; б – 12 цикл наблюдений)

В табл. 2 представлены разности длин радиусов, вычисленного на момент t_1 и на другие моменты времени.

Таблица 2

Разность длин радиусов ΔR, *м*

ΔR 1–2	ΔR 1–4	ΔR 1–5	ΔR 1–9	ΔR 1–10	ΔR 1–11	ΔR 1–12
0,0001	0,0002	0,0010	0,0009	0,0010	0,0010	0,0000

В ходе выполнения аппроксимации множества контрольных точек объекта сферой: было обнаружено изменение радиуса, а также смещение центра масс сферы C=0,001. При допустимом отклонении высотных координат контрольных точек H=±0,005 м., можно сделать вывод, что интегральная деформация отсутствует (является незначительной) [14–21].

Заключение

Любая дополнительная информация, полученная на основании исходных данных об объекте крайне важна для контроля инженерно-технических сооружений и позволит существенно снизить риск возникновения чрезвычайных и аварийных ситуаций, тем самым обеспечить безопасность эксплуатации сооружений.

Построение и анализ математической модели по пространственной цифровой информации об объекте позволяет определить пространственное положение всего ИТС в виде математического объекта, анализ которого дает возможность выполнять комплексную оценку пространственно-временного состояния ИТС в целом и его геометрических параметров. В зависимости от формы объекта и задач определения изменения состояния ИТС необходимо подбирать наиболее подходящую модель для дальнейшего анализа.

Для более точной аппроксимации объекта математической моделью рекомендуется использовать в качестве исходных данных результаты лазерного сканирования всего объекта в целом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Белов, П. Г. Системный анализ и моделирование опасных процессов в техносфере [Текст]: учебное пособие для вузов / П.Г. Белов. – М.: Академия, 2003. – 512 с.

2. Бугакова Т. Ю. Моделирование изменения пространственно-временного состояния инженерных сооружений и природных объектов по геодезическим данным // Вестник СГУГиТ. – 2015. – Вып. 1 (29). – С. 34–42.

3. Бугакова Т. Ю. Оценка устойчивости состояний объектов по геодезическим данным методом фазового пространства: автореф. дис. на соискание ученой степени кандидата технических наук. – Новосибирск: СГГА, 2005.

4. Бугакова Т. Ю., Борисов Д. А., Яковлев Д. А. Программная реализация метода делоне для определения формы и размеров техногенных объектов по геопространственным данным // Изв. вузов. Геодезия и аэрофотосъемка. – 2014. – № 4С. – С. 15–19.

5. Бугакова Т. Ю., Вовк И. Г. Определение вращательного движения объекта по результатам многократных геодезических измерений [Текст] // Интерэкспо Гео-Сибирь – 2013: IX Междунар. науч. конгр., 15-26 апр. 2013, – Новосибирск: СГГА, 2013. - С.88-92.

6. Бугакова Т. Ю., Шарапов А. А. Применение мультиагентного подхода для определения пространственно-временного состояния техногенных систем, XII Международный Форум «Интерэкспо ГЕО-Сибирь 2016» 18 апреля 2016, Новосибирск: СГУГиТ, С. 189–194.

7. Бугакова Т. Ю., Шляхова М. М., Кноль И. А. Структурная декомпозиция объекта методами математического моделирования с последующей визуализацией на основе WebGL. Интерэкспо ГЕО-Сибирь-2016. XII Междунар. науч. конгр., 18–22 апреля 2016 г., Новосибирск: Междунар. науч. конф. «Геодезия, геоинформатика, картография, маркшейдерия»: сб. материалов в 2 т. Т. 1. – Новосибирск: СГУГиТ, 2016. – 244 с. – С. 142 –147

8. Вовк И. Г. Математическое моделирование пространственно-временного состояния систем по геометрическим свойствам и оценка техногенного риска методом экспоненциального сглаживания [Текст]: Вестник СГГА / И. Г. Вовк, Т. Ю. Бугакова. – Новосибирск: СГГА, 2012. – Выпуск 4 (20). – С. 47–58.

9. Вовк И. Г. Определение геометрических инвариантов поверхности в прикладной геоинформатике // Вестник СГГА. – 2012. – Вып. 4 (20). – С. 59–69.

10. Вовк И. Г. Системно-целевой подход в прикладной геоинформатике // Вестник СГГА. – 2012. – Вып. 2 (18). – С. 115–124.

11. Жуков, Б. Н. Руководство по геодезическому контролю сооружений и оборудования промышленных предприятий при их эксплуатации [Текст]: учебное пособие для вузов / Б. Н. Жуков. – Новосибирск: СГГА, 2004. – 376 с

12. Использование GNSS оборудования [Электронный ресурс] – Режим доступа: http://www.eft-gnss.ru/ – Загл. с экрана.

13. Карпик А.П. Анализ состояния и проблемы геоинформационного обеспечения территорий. Известия высших учебных заведений. Геодезия и аэрофотосъемка. 2014. № 4. С. 3-7.

14. Мазуров Б.Т. Геодинамические системы (кинематические и деформационные модели блоковых движений) // Вестник СГУГиТ. – 2016. – Вып. 3 (35). – С. 5–15.

15. Национальный стандарт российской федерации ГОСТ Р 22.1.12-2005, Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования. Москва, ИПК, Издательство стандартов, 2005

16. Роберт Лафоре. Структуры данных и алгоритмы JAVA. Питер, 2013.

17. Хиллер Б., Ямбаев Х.К. Разработка и натурные испытания автоматизированной системы деформационного мониторинга // Вестник СГУГиТ. – 2016. – Вып. 1 (33). – С. 48–61.

18. Яковлев Д. А. Текстурирование модели техногенного объекта и его привязка к системе координат в среде 3d studio max 2009 // Интерэкспо ГЕО-Сибирь-2012. VIII Междунар. науч. конгр. : Междунар. науч. конф. «Геодезия, геоинформатика, картография, маркшейдерия» : сб. материалов в 3 т. (Новосибирск, 10 20 апреля 2012 г.). Новосибирск: СГГА, 2012. Т. 3. С. 149–152.

19. Carcanague S., Julien O., Vigneau W., Macabiau C., Hein G. Finding the right algorithm - Low-Cost, Single-Frequency GPS/GLONASS RTK for Road Users//Inside GNSS. 2013. Vol. 8, No. 6. P. 7-80.

20. F. Zarzoura, R. Ehigiator -Irughe, B. Mazurov. Utilizing of Mathematical Frame Work in Bridge Deformation Monitoring Asian Journal of Engineering and Technology (ISSN: 2321 -2462) Volume 02 -Issue 04, August 2014. -Pp. 293-300.

21. François Mazuyer and Marc Vanderschueren. TS01E -Surveying Practice across the world -6676. FIG Working Week 2013 Environment for Sustainability Abuja, Nigeria, 6-10 May 2013

22. Geologic-engineering and geomechanical models of the rock mass in the bed of the dam at the Sayano-Shushenskaya HPP/A. I. Savich, M. M. Il'in, V. P. Elkin, V. I. Rechitskii, A. B. Basova//Power Technology and Engineering. 2013. Vol. 47. № 2. Pp. 89-101

23. Ghiasian M., Ahmadi M.T. Effective model for dynamic vertical joint opening of concrete arch dam//Proc. of the int. symp. on dams for a changing word-80th annual meet. and 24th cong. of ICOLD. Kyoto, Japan. 2012. Pp. (4) 41-46.

24. GPS for geodesy. Teunissen P.J.G., Kleusberg A. (Eds.). – Berlin: Springer, 1998 – 650 p. – Англ.

25. Hofmann-Wellenhof B., Lichtenegger H., Wasle E. GNSS -Global Navigation Satellite Systems GPS, GLONASS, Galileo and more. -Wien, New-York: Springer. -2008. -516 p.

26. Mazuyer F., Vanderschueren M. TS01E -Surveying Practice across the world -6676 // FIG Working Week 2013 Environment for Sustainability (6–10 May). – Abuja, Nigeria, 2013.

27. Neuner H., Schmitt C., Neumann I. Modelling of terrestrial laser-scanning profile measurements with // Proceedings of the 2nd Joint international Symposium on Deformation Monitoring. – Nottingham, England, 2013.

28. Studies on the static and dynamic behavior of the Sayano-Shushenskaya arch gravity dam/A. I. Savich, V. I. Bronshtein, M. E. Groshev, E. G. Gaziev, M. M. Il'in, V. I. Rechitskii//International Journal on Hydropower and Dams. 2013. Vol. 20. № 6. Pp. 453-58.

29. Tatiana Bugakova, Artem Sharapov . Modeling of a prototype multi-agent system monitoring man-made objects// Engineering Studies, Issue 3 (2), Volume 8. "Taylor & Francis", 2016. - Pages C.430–440.

30. Vorobev A.V., Shakirova G.R. Web-Based Geoinformation System for Exploring Geomagnetic Field, Its Variations and Anomalies. Geographical Information Systems Theory, Applications and Management. Volume 582 of the series Communications in Computer and Information Science, 2016, pp. 22-35.

УДК 004.052
DOI 10.33764/2618-981X-2023-6-42-49

А. С. Грехов[1]*, *А. Н. Поликанин*[1], *Д. Н. Титов*[1]

Разработка программного обеспечения для расчета дальности действия тепловизора

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: grehov084@gmail.com

Аннотация. В статье приведен краткий обзор методик расчета дальности действия тепловизионных систем, одна из которых легла в основу разрабатываемой программы. *Целью работы* является автоматизация процесса расчета дальности действия тепловизоров, включая дальность распознавания и идентификации. *Актуальность работы* обусловлена широким распространением тепловизионного оборудования в разведывательных целях, в качестве средств наблюдения в ночное время и условиях ограниченной видимости, а также как средство обнаружения каналов утечки информации. В статье приведены результаты разработки программного интерфейса, позволяющего рассчитать дальность действия тепловизионных систем на основе параметров температурной чувствительности и разрешения. На сегодняшний день в российском сегменте рынка практически нет программного обеспечения, позволяющего автоматизировано производить расчет дальности действия тепловизионных систем по характеристикам используемого прибора. *Результатом* работы является разработанное программное обеспечение, позволяющее проводить автоматизированный расчет дальности действия тепловизионных систем на основе объединенных параметров температурной чувствительности и разрешения.

Ключевые слова: тепловизоры, дальность действия, обнаружение, идентификация, разработка, программный интерфейс

A. S. Grehov[1]*, *A. N. Polikanin*[1], *D. N. Titov*[1]

Development of Software for Calculating the Range of a Thermal Imager

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: grehov084@gmail.com

Abstract. The article provides a brief overview of methods for calculating the range of thermal imaging systems, one of which formed the basis of the developed program. *The aim* of the work is to develop software based on the method for calculating the range of thermal imagers, including the range of recognition and identification based on one of the existing methods for calculating the range of thermal imaging devices. *The relevance* of the work is due to the widespread use of thermal imaging equipment for reconnaissance purposes, as a means of observation at night and conditions of limited visibility, as well as a means of detecting information leakage channels. The article presents the results of the development of a software interface that allows calculating the range of thermal imaging systems based on the parameters of temperature sensitivity and resolution. Today in the Russian segment of the market there is practically no software that allows you to automatically calculate the range of thermal imaging systems according to the characteristics of the device used. *The result* of the work is the developed software that allows for automated calculation of the range of thermal imaging systems based on the combined parameters of temperature sensitivity and resolution.

Keywords: thermal imagers, range, detection, identification, development, software interface

Введение

В современном мире тепловизионное оборудование получает все более широкое распространение в системах безопасности как средства наблюдения в темное время суток и сложных погодных условиях. Наблюдение с помощью тепловизора имеет ряд преимуществ относительно иных средств, предназначенных для съемки в ночное время, таких как ИК камеры с подсветкой поля зрения или приборов ночного видения [1], [6].

Одним из главных параметров тепловизора является его дальность действия, которая также включает в себя понятия дальности обнаружения, распознавания и идентификации [10].

Цель работы заключается в автоматизации процесса расчета дальности действия тепловизоров, включая дальность распознавания и идентификации.

Для достижения поставленной цели были решены следующие задачи:

1) сравнительный анализ методики расчета дальности действия тепловизионных приборов;

2) создание пользовательского интерфейса и программного обработчика событий, инициируемых пользователем;

3) апробация программного продукта.

Методы и материалы

Для разработки программного интерфейса была выбрана методика расчета, на основе которой разрабатывалась программа. Для этого был проведен сравнительный анализ трех методик: методики расчета с использованием геометрических характеристик каналов, методики расчета с использованием энергетических характеристик каналов и методики расчета с использованием энергетических характеристик каналов на основе перехода объединенных параметров температурной чувствительности и разрешения [2].

Основные формулы каждой методики, по которым производится расчет дальности действия, представлены ниже.

$$l = \nu \frac{f' h_{кр}}{N}, \tag{1}$$

$$l = \frac{h_{кр} \gamma 0 x}{C\sigma} \sqrt{-\frac{0.7}{\ln(1-p)}}, \tag{2}$$

$$l = \frac{hr_{\Sigma}(\nu)\Delta T_{\text{раз}} \left(T_e \cdot f_k\right)^{1/2} C_2 D^* \left(d/f'\right)^2 f' \cdot \int_{\lambda_1}^{\lambda_2} \left[\begin{matrix} S(\lambda)\tau_{\text{o}}(\lambda)\tau_{\text{a}}(\lambda)\times \\ \times\varepsilon(\lambda)W(\lambda,T)\lambda^{-1} \end{matrix} \right] d\lambda}{6\sqrt{2}k_{\text{э}}T^2 \sqrt{\Delta f_{\text{R}}} N \cdot m}. \tag{3}$$

Методики расчета с использованием геометрических характеристик каналов, методики расчета с использованием энергетических характеристик каналов имеет ряд несовершенств, одним из которых является наличие ряда пространственных фильтров между точкой, для которой измеряется $\Delta T_{\text{пор}}$ и получаемым изображением. Это такие фильтры, как источники шумов, например, инерционность приемника, экран с получаемым изображением и глаз оператора, рассматриваемый с позиции пространственно-частотного оптического фильтра. Также в методике не уделяется внимание влиянию простарнственно-частотных характеристик самого объекта [3].

На основании анализа литературы [2] по энергетическим методам расчета параметров тепловизионных камер можно сделать вывод, что основное внимание инженеров, разрабатывающих тепловизионные системы, направлено на минимизацию зависимости параметров ΔТпор и ΔТраз, что оптимизирует все параметры тепловизионной камеры, входящие в первоначальные расчеты, вследствие чего повышается их эффективность. С другой стороны, вследствие этого оценке дальности действия не уделяется должного внимания.

В результате проведенного анализа методик, для разработки программного обеспечения была выбрана методика расчета на основе объединенных параметров температурной чувствительности и разрешения. Основные формулы, по которым производится расчет требуемой величины, представлены на ниже:

$$\Delta T_{\text{пор}} = \frac{\pi k_э T^2 m \sqrt{ab\Delta f_R}}{D^* \alpha\beta C_2 A_0 \int_{\lambda_1}^{\lambda_2} S(\lambda)\tau_o(\lambda)\tau_a(\lambda)W(\lambda,T)\lambda^{-1}d\lambda}, \quad (4)$$

$$\Delta T_{\text{раз}} = \frac{3\Delta T_{пор}\nu\sqrt{\alpha\beta}}{r_\Sigma(\nu)\sqrt{\tau\Delta f_R T_e f_k}}, \quad (5)$$

$$l = \frac{hr_\Sigma(\nu)\Delta T_{\text{раз}}\left(T_e \cdot f_k\right)^{1/2} C_2 D^* \left(d/f'\right)^2 f' \cdot \int_{\lambda_1}^{\lambda_2} \left[\begin{matrix} S(\lambda)\tau_{\text{o}}(\lambda)\tau_{\text{a}}(\lambda)\times \\ \times\varepsilon(\lambda)W(\lambda,T)\lambda^{-1} \end{matrix}\right] d\lambda}{6\sqrt{2}k_э T^2 \sqrt{\Delta f_{\text{R}}}\, N \cdot m}. \quad (6)$$

где D* и S(λ) – удельная обнаружительная способность и относительная спектральная чувствительность приемника оптического изображения (ПОИ); (a, b) и Δf_R –линейные размеры и шумовая полоса частот электрической схемы включения ПОИ; (λ1, λ2) – границы спектральной чувствительности ПОИ; kэ – коэффициент использования ПОИ излучения эталонного источника; m – отношение «сигнал/шум»; A0 и (α,β) – площадь входного зрачка и линейные углы мгновенного поля зрения объектива тепловизора по строке и по кадру; W(λ,T) – спек-

тральная светимость АЧТ с температурой T; T(x,y) и Tф(x,y) – функции распределения температуры по поверхности объекта и фона в случае наблюдения прибором неоднородных тепловых полей объектно-фоновой обстановки; и – среднее значение температуры поверхности объекта и фона; ε(λ) и εф(λ) – спектральный коэффициент излучения поверхности объекта и фона; τо(λ) и τа(λ) – спектральный коэффициент пропускания оптической системы тепловизора и слоя атмосферы между объектом и прибором; C2 – постоянная в формуле Планка; ΔW(λ,T(x,y),) и ΔWф(λ,Tф(x,y),) – абсолютный контраст спектральной светимости АЧТ, имеющих температуры аналогичные температурам поверхности объекта и фона соответственно; Te и fk – постоянная времени глаза и частота кадров тепловизора; ν – пространственная частота в пространстве предметов, рад-1; K(Фф) – коэффициент, учитывающий увеличение порогового сигнала ПОИ за счет засветки постоянной составляющей фона; r_{Σ} (ν) – результирующий модуль передаточной функции (МПФ) всех звеньев тепловизора; αф=α-α0; βф= β-β0; (x0,y0), (xф,yф) – декартовые координаты поверхности объекта и фона в пространстве предметов [4].

Результаты

Алгоритм работы разрабатываемой программы был построен на основе описанной методики расчета с использованием формул (4)-(6) при учете передаточных функций и представлен на рис. 1 в виде блок схемы. На первом этапе создавали пользовательский интерфейс с использованием инструментов среды разработки VisualStudio 2021. При создании интерфейса применялись следующие компоненты: label, textbox, button. Компонент label применялся для создания поясняющих подписей, компонент textbox – для ввода необходимых значений соответствующих параметров, компонент button – для запуска обработчиков расчетов. Разместив все необходимые элементы на форме и произведя их настройки, получили интерфейс будущей программы, представленный на рис. 2 [5].

На втором этапе было необходимо создать обработчик события Click кнопки «Рассчитать». При нажатии на данную кнопку все введённые в поля параметры записываются в соответствующие переменные, создаются необходимые для расчетов константы. Далее обработка события происходит согласно разработанной блок – схеме. Для снижения общей сложности программы было произведено разбиение на отдельные методы, в которых происходит расчет конкретных величин [7].

При вызове метода spectral_luminosity в него передаются необходимые параметры и происходит расчет спектральной.

При вызове метода temperature_resolution происходит передача необходимых параметров и расчет величин $\Delta T_{пор}$ и $\Delta T_{раз}$.

В программе также был реализован фильтр вводимых в соответвующие поля символов путем считывания кода нажимаемых клавиш. Данная функция необходима для исключения ввода некорректных символов, например, буквенных или специальных символов, в поля ввода значений величин.

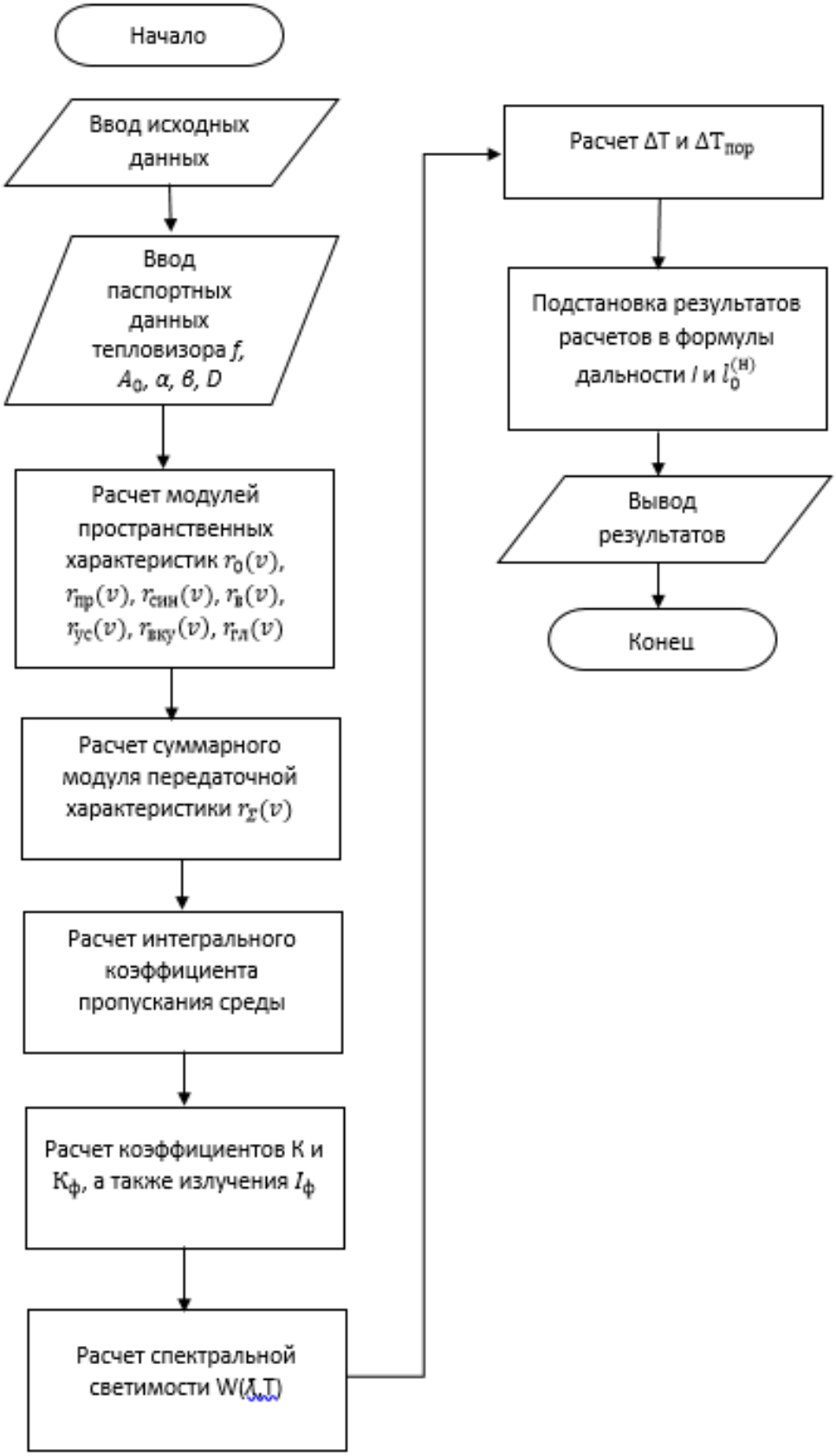


Рис. 1. Блок-схема алгоритма расчетов

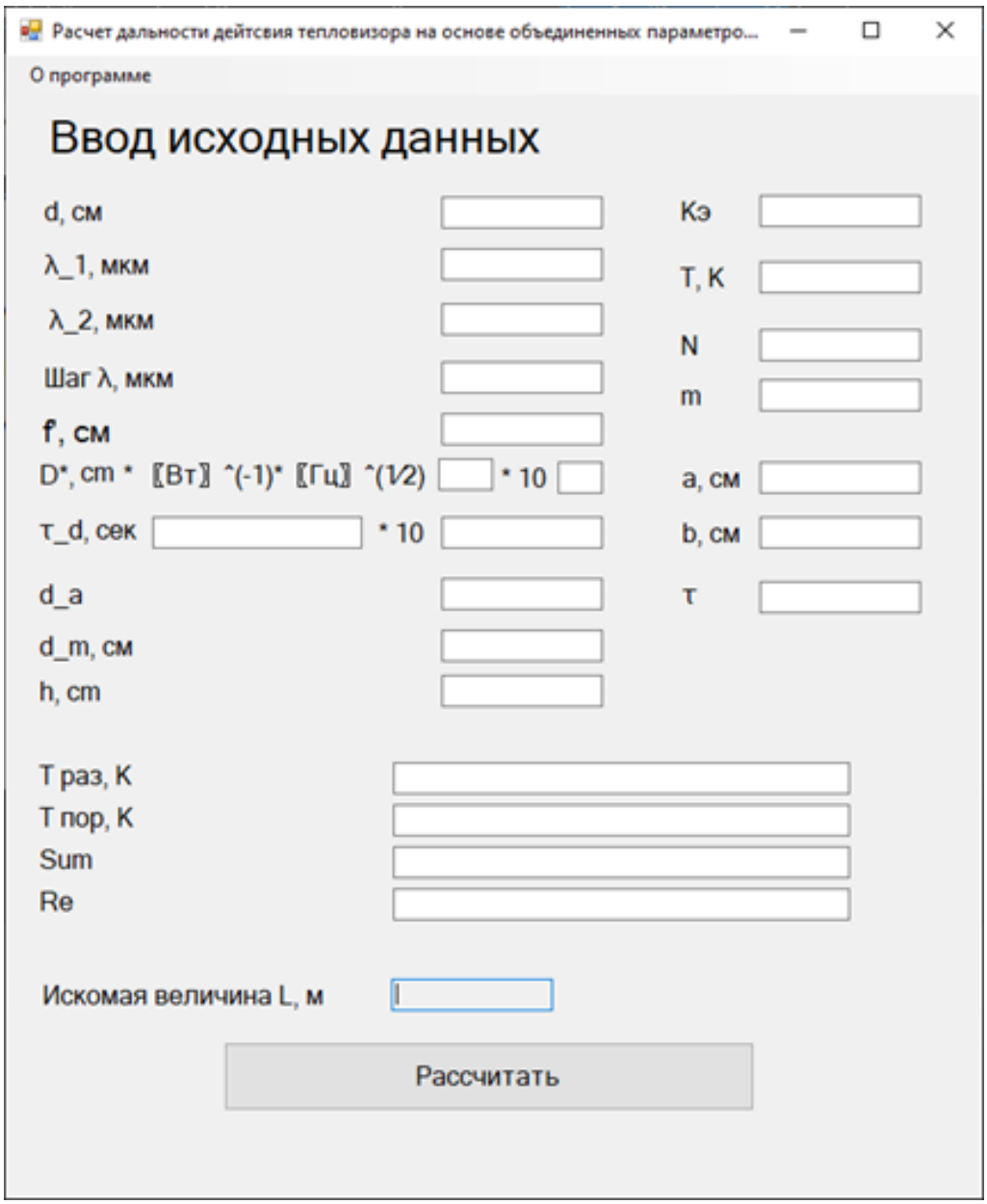


Рис. 2. Интерфейс разрабатываемой программы

Для тестирования данного проекта был выбран метод модульного тестирования, так как он является наиболее удобным и информативным в данных условиях [8], [9].

После окончания разработки и отдельного тестирования каждого модуля проекта, было проведено общее тестирования приложения с целью поиска, ошибок работы программы в целом, конфликтов скриптов. Тестирование не выявило каких-либо проблем в работе приложения. Результат тестирования представлен ниже (рис. 3).

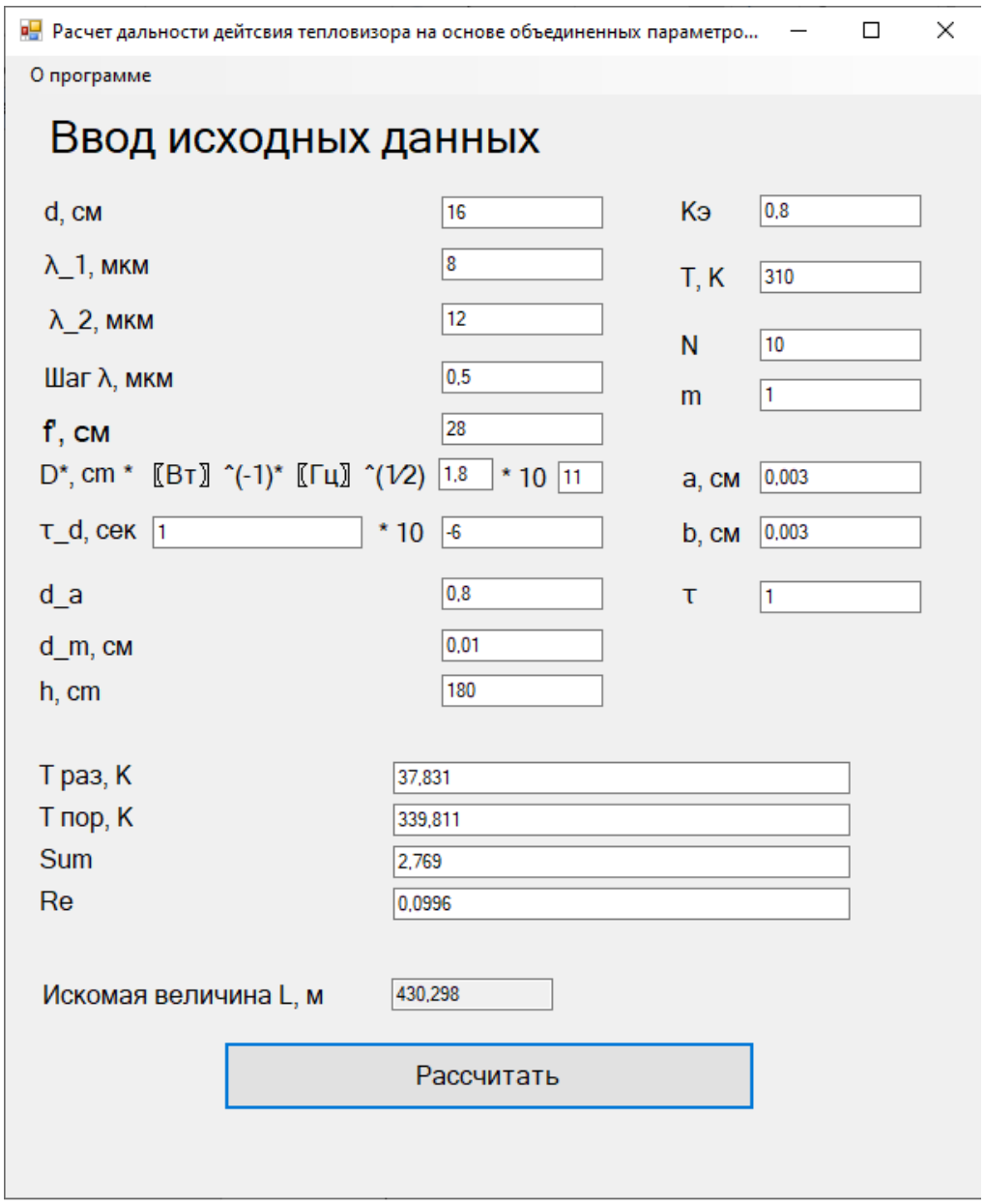


Рис. 3. Результат тестирования приложения

Заключение

В результате выполненных работ был проведен анализ существующих методик, позволяющих рассчитать дальность действия тепловизионного устройства. На основании данного анализа в основу разрабатываемого программного обеспечения легла методика, позволяющая наиболее точно рассчитать необходимую характеристику.

Тепловизор может использоваться совместно с квадрокоптером для ведения свободной воздушной разведки, что ставит под угрозу коммерческую и государственную тайну.

Беспилотный летательный аппарат или обычный квадрокоптер является основным устройством, используемым для воздушной разведки. Совместив тепло-

визионную камеру наблюдения с ним, можно получить необходимые сведения о наблюдаемом объекте.

В результате выполненных работ было разработано программное обеспечение, позволяющее рассчитать дальность действия тепловизионного устройства.

Перспективами развития разработанного программного обеспечения является выпуск новой версии, основными нововведениями будут: работа с базами данных, в том числе просмотр результатов предыдущих расчетов, расчет дальности действия в неоднородном поле температур.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Военное обозрение: официальный сайт. – Москва. – Обновляется в течение суток. – URL: https://vpk.name (дата обращения: 10.04.2023). – Текст: электронный.

2 Информационно-аналитический журнал Рубеж: официальный сайт. – URL : https://rubezh.ru/andrej-lunev/36461-gradus-bezopasnosti-vosem-zadach-kotoryie-reshayut-teplovizoryi (дата обращения : 15.04.2021). – Текст : электронный.

3 Кулакова Н.Н., Мишин С.В. Анализ результатов расчета дальностей обнаружения, распознавания и идентификации тепловизионной системы по двум методикам / Н. Н, Кулакова, С. В Мишин // Котненант. - 2015. - Т. 14. - № 1. - С. 49–53.

4 Новиков С.Н., Поликанин А.Н. Методика расчета дальности действия тепловизора на основе объединенных параметров температурной чувствительности и разрешения / С. Н. Новиков, А. Н. Поликанин – Текст: непосредственный // Труды учебных заведений связи. - 2019– № 5 (4). – С. 6–14.

5 Образовательная платформа GeekBrains: официальный сайт. – URL: https://gb.ru/posts/c_sharp_ides (дата обращения : 20.05.2021). – Текст: электронный.

6 Пеграм: официальный сайт. – URL : https://www.pergam.ru/articles/teplovizor.htm (дата обращения : 15.04.2021). – Текст : электронный.

7 Филин Е. Д., Киричек Р. В. Методы обнаружения малоразмерных беспилотных летательных аппаратов на основе анализа электромагнитного спектра / Е. Д. Филин, Р. В. Киричек. – Текст: непосредственный // Информационные технологии и телекоммуникации. – 2018. – Т. 6. – № 2. – С. 87–93.

8 Developer.com : официальный сайт. – URL : https://www.developer.com/guides/what-is-c/ (дата обращения : 27.05.2021) – Текст : электронный.

9 Edureka.co: официальный сайт. – URL: https://www.edureka.co/blog/visual-studio-tutorial/ (дата обращения : 20.05.2021). – Текст : электронный.

10 EVIDENCE : Использование тепловизоров в системах безопасности : сайт. – URL: https://e-vidence.ru/ (дата обращения : 20.04.2023). – Текст : электронный.

УДК 004.056.53
DOI 10.33764/2618-981X-2023-6-50-57

А. А. Емелина[1], Н. Е. Карпова[1], А. А. Саранский[1]*

Исследование действий пользователей в информационной среде

[1] Самарский государственный технический университет, г. Самара,
Российская Федерация
*e-mail: esib@samgtu.ru

Аннотация. Актуальной задачей является разработка и совершенствование методов обнаружения недопустимых событий в функционировании информационной системы, которые, как правило, является следствием действия пользователей в компьютерной системе. Сложности, с которыми сталкиваются разработчики моделей, связаны с тем, что все методы касаются описания поведения человека, которое плохо поддается формализации. В данной работе предложена математическая модель байесовской сети, а также разработан алгоритм выявлния неспецифичных действий пользователя в информационной системе. В результате анализа был сделан вывод, что сети Байеса являются наиболее гибким и адекватным математическим аппаратом, позволяющим даже в условиях некоторой неопределённости классифицировать поведение пользователя в информационной среде и определять необходимые меры по противодействию возможной реализации угрозы.

Ключевые слова: информационная безопасность, система мониторинга за действиями пользователя, сети Байеса, вредоносные действия пользователя, несанкционированный доступ, программно – аппаратные средства защиты информации

A. A. Emelina[1], N. E. Karpova[1], A. A. Saranskii[1]*

Research of User Actions in the Information Enviroment of the Enerprise

[1] Samara State Technical University, Samara, Russian Federation
*e-mail: esib@samgtu.ru

Abstract. An urgent task is the development and improvement of methods for detecting unacceptable events in the functioning of an information system, which, most commonly, are the result of user's actions in the computer system. The main difficulty faced by the developers of such systems is that it is necessary to choose a method that could describe the whole variety of human behavioral characteristics. The article presents a classification of threats emanating from a person, as well as analyzes existing methods for detecting and preventing these threats. This paper proposes a mathematical model of a Bayesian network and an algorithm of a system for determining the anomalous behavior of employees in the information environment of an enterprise. As a result of the analysis, it was concluded that Bayesian networks are the most flexible and adequate mathematical apparatus that allows, even under conditions of some uncertainty, to classify user's behavior in the informational environment and to determine the necessary measures to counter the possible implementation of the threat.

Keywords: information security, user activity monitoring system, Bayesian networks, malicious user actions, risk, unauthorized access, classification of information threats

Введение

С растущим объемом информации, которая обрабатывается в электронном виде и передается между различными информационными системами (ИС) в сети Интернет, организации и отдельные пользователи все чаще сталкиваются с необходимостью обеспечения её безопасности.

В настоящее время важной задачей является разработка и совершенствование методов обнаружения недопустимых событий в работе информационной системы. Обычно такие события происходят из-за неправомерных или ошибочных действий пользователей в компьютерной среде. Исследования показывают, что самой большой угрозой для любого предприятия являются его сотрудники. Поэтому необходимо выявлять как новые типы нарушений работы сети, так и вредоносные действия, продолжительные во времени. В настоящее время все большее значение приобретают программные и аппаратные средства защиты информации [1].

Мониторинг за действиями пользователя позволяет отслеживать не только текущее состояние, но и изменения как в динамической системе.

Мониторинг безопасности информационной среды требует анализировать все виды угроз, однако если естественные факторы достаточно просто формализируются в плане рисков и защита от них достаточно понятна, то к угрозам, имеющим причиной человеческий фактор необходимо особое внимание, так как невозможно предсказать действия человека даже при условии того, что он не намерен причинить вреда. Разработчики моделей сталкиваются с трудностями, поскольку все методы, связанные с описанием поведения человека, трудно поддаются формализации. Однако стоит отметить, что поведенческие системы более гибкие по сравнению с биометрическими и могут использоваться для анализа действий пользователя в информационной среде, включая выявление ранее неизвестных аномалий поведения. В общем, мониторинг действий пользователя может рассматриваться как непрерывное наблюдение за факторами, влияющими на функционирование информационной среды, а также как анализ результатов этого наблюдения.

Существует несколько видов классификации информационных угроз, например, угрозы делят по факторам возникновения.

Информационные угрозы по фактору возникновения:

а) природные угрозы;

б) человеческий фактор:

1) умышленные угрозы:

1.1 активные угрозы;

1.2 пассивные угрозы;

1.3 внутренние угрозы;

1.4 внешние угрозы;

2) непреднамеренные угрозы.

Заметим, что большая часть угроз информационной безопасности связана с отсутствием у сотрудников необходимых компетенций, а также неисполнение служебных инструкций.

Также важным компонентом для разработки эффективной системы обнаружения вторжений в критическую инфраструктуру являются наборы данных, характеризующие различные виды атак (в т.ч. эксплуатация критических уязвимостей), а также анализ исходящего сетевого трафика.

Методы мониторинга:

– анализ эксплуатаций уязвимостей;
– анализ ресурсов, к которым обращается пользователь;
– анализ входящих соединений, с потенциально – опасных ресурсов.

В [4] приведен обзор некоторых наиболее важных аспектов безопасности Active Directory. Автор подчеркивает, что Active Directory является ключевым компонентом большинства сетей Windows и важно обеспечивать ее безопасность. Первая область, на которую обращает внимание автор, – это авторизация. Авторизация в Active Directory определяет, кто может получить доступ к данным и ресурсам в сети. Для обеспечения безопасности в этой области автор рекомендует использовать принцип наименьших прав, который позволяет ограничить доступ пользователей только к необходимой им информации.

Вторая область – это аудит безопасности. Логи событий в Active Directory могут использоваться для идентификации попыток несанкционированного доступа к данным и для определения уязвимостей в системе. Автор советует настроить систему аудита таким образом, чтобы она получала логи событий с наивысшим приоритетом.

Нейросетевой детектор атак, предложенный в работе [5], идентифицирует пользователя на основе количества запусков различных команд в течение дня. Авторы используют подход, основанный на машинном обучении с использованием многослойной нейронной сети. Для обучения был использован набор данных, содержащий информацию о пользователе и его поведении при работе с компьютером. В данной модели учитывается только количество команд и не учитывается их последовательность. Кроме того, количество подаваемых на вход нейронной сети команд ограничено (100 команд), хотя в реальных условиях оно может быть значительно выше.

Для описанных выше систем были разработаны математические модели, которые описывают действия пользователя. Примеры таких моделей включают модели принятия решения на основе теории вероятности с помощью экспертов, модели оперативного контроля с использованием математической статистики, модели, которые описывают схемы и потоки информационной системы на основе теории графов, модели, которые используют нечеткие множества, системы, которые используют нейронные сети, и методы раннего обнаружения внутренних нарушителей информационной безопасности, основанные на сетях Байеса [6 - 9].

Угрозами информационной безопасности (ИБ) могут являться кража информации, изменение конфигурации, шифрование данных и пр. Поэтому крайне важно максимально своевременно обнаруживать и предотвращать данные угрозы. Для решения данной задачи предлагаем использовать систему, построенную на основе сети Байеса.

Для составления математической модели обнаружения нарушителя ИБ требуются более глубокие исследования его поведения, поэтому выявление внутренних нарушителей ИБ с использованием байесовских сетей позволяет избавиться от недостатков, присущих описанным выше методам и средствам, а также создать инструмент для осуществления полноценного анализа поведенческих особенностей человека.

Методы и материалы

С помощью теоремы Байеса можно вычислить вероятность события при условии, что произошло другое событие, которое связано с ним статистически. Формула Байеса позволяет точнее учесть известную информацию и учесть новую информацию, полученную в результате наблюдений.

Байесовская сеть позволяет получать ответы на следующие типы вероятностных запросов [9]:

– поиск вероятности доказательства;

– определение априорных предельных вероятностей;

– определение апостериорных маргинальных вероятностей, в том числе:

а) предсказание или прямой вывод, - определение вероятности события по наблюдаемым причинам;

б) диагностика, или обратный вывод (похищение), - определение вероятности возникновения причины с наблюдаемыми последствиями.

Байесовские сети относятся к категории вероятностных графических моделей

Байесовская сеть представляет собой граф, которой ориентирован и ацикличен, где каждая вершина соответствует случайной величине, а связи между вершинами отображают условную независимость между этими переменными. В графе могут быть представлены различные типы переменных с помощью взвешенных параметров, скрытых переменных или гипотез. Модели неопределенных ориентированных графов основаны на изменении вероятностного происхождения событий, где для каждого случайного значения применяется таблица условной вероятности. Это позволяет моделировать вероятностную последовательность событий. Формула Байеса в общем виде (1):

$$P(A|B)=\frac{P(B|A)P(A)}{P(B)}, \quad (1)$$

где P(A) – априорная вероятность гипотезы; P(A|B) – вероятность гипотезы A при наступлении события B (апостериорная вероятность); P(B|A) – веро-

ятность наступления события B при истинности гипотезы A; P(B) – полная вероятность наступления события B.

Преимущества байесовских сетей [11]:

– в модели устанавливаются связи между всеми переменными. Это позволяет легко обрабатывать те случаи, когда значения некоторых параметров отсутствуют;

– Байесовские сети позволяют проводить анализ возможных вариантов при прогнозном моделировании.

Все вышеизложенные преимущества делают применение сетей Байеса оправданным для моделирования поведения пользователя, так как данный математический аппарат позволяет учитывать инвариативность поведения пользователя, прогнозировать вероятность наступления события даже в условии некоторой неопределенности, а также находить связи между разными рассматриваемыми параметрами и находить зависимость между ними, что позволяет с более высокой точностью отнести поведение пользователя к категории «аномальное», «подозрительное» или «нормальное» поведение.

Для выявления нарушителей ИБ необходимо накопить информацию о поведенческих особенностях человека, после чего определить эталон поведения пользователя. При отклонении поведения пользователя от эталона пользователь переходит в группу потенциальных злоумышленников. В проектировании сложных систем, как правило, используется метод экспертных оценок. Сущность методов экспертных оценок заключается в том, что в основу принятого решения, прогноза, вывода закладывается мнение специалиста или коллектива специалистов, основанное на их знаниях и практическом профессиональном опыте. Человек с профильным образованием и опытом в области исследования считается экспертом.

Результаты

С математической точки зрения сеть Байеса – это модель для представления вероятностных зависимостей, а также отсутствия этих зависимостей.

Выходом каждой сети является мера принадлежности события к конкретному классу нарушений ИБ.

В нашем случае, выходом сети является рекомендация сотруднику службы безопасности или системе реагирования на инциденты о необходимой мере, которую следует применить к учетной записи или конечному узлу информационной системы, а именно:

1) заблокировать;

2) подозрение на инцидент – требуется проведение дополнительной экспертизы;

3) легитимные действия пользователя.

Сначала необходимо выявить определенные триггеры.

К компьютерным триггерам можно отнести аномальную почтовую активность, аномальную активность в мессенджерах, анализ журналов событий сред-

ствами Microsoft Windows, а именно события с индикатором 5136 – 5145. Данные события позволяют проанализировать доступ к объектам сетевого ресурса, выявить тип доступа, с которым пользователь обращался к объекту, а также определить, были ли модифицированы объекты. События с индикатором 4624 регистрируют все успешные входы в систему с указанием времени, учетной записи, типом входа, а также хоста-инициатора и целевого хоста и пр. Подробное описание данных событий описано в [14].

Также анализ событий средствами антивирусного программного обеспечения (АВПО), например, Kaspersky, а именно анализ действий со съемными устройствами.

Далее необходимо создать сеть Байеса. В данном случае можно предположить, что все триггеры являются условно независимыми друг от друга. Это позволяет считать, что кража информации может произойти при срабатывании любого триггера, а также при срабатывании нескольких триггеров одновременно. Список факторов, влияющих на наступление инцидент ИБ, может быть уменьшен или увеличен для каждой конкретной компании. Каждому триггеру также будет присвоено свое значение вероятности.

Данные вероятности можно получить различными методами:

– методами экспертных оценок (опрос n-го количества экспертов);

– на основе субъективной оценки определенного человека (например, руководителя отдела информационной безопасности) и пр.

После чего составляется сеть Байеса, а также заполняется таблица априорных вероятностей для каждого триггера.

Пример моделирования сети Байеса в программе GeNie представлен на рис. 1.

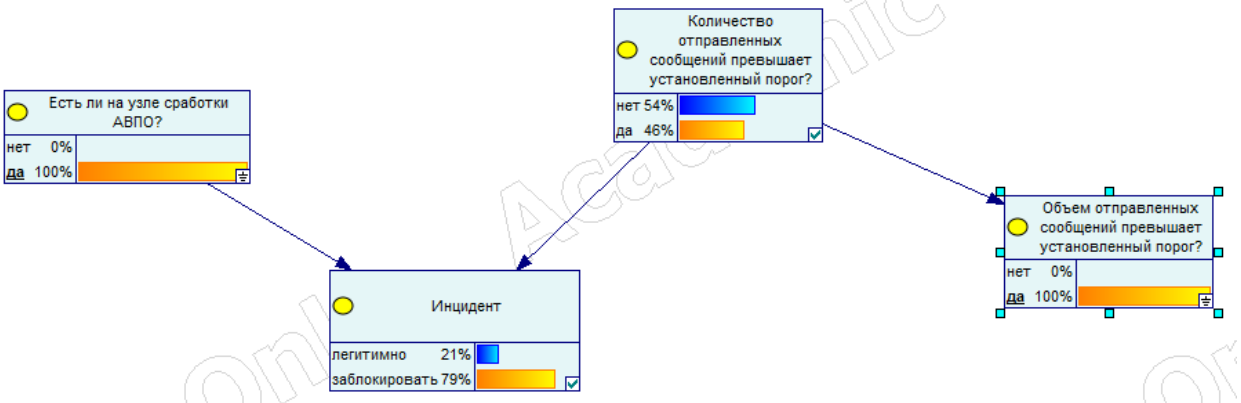


Рис. 1. Модель Сети Байеса для выявления нарушения информационной безопасности

На основании проведенного исследования был предложен алгоритм (рис.2) выявления неспецифичных действий пользователя в информационной системе,

основанный на сетях Байеса, затем на основе данного алгоритма разработан программный модуль для выявления подозрительной активности пользователя.

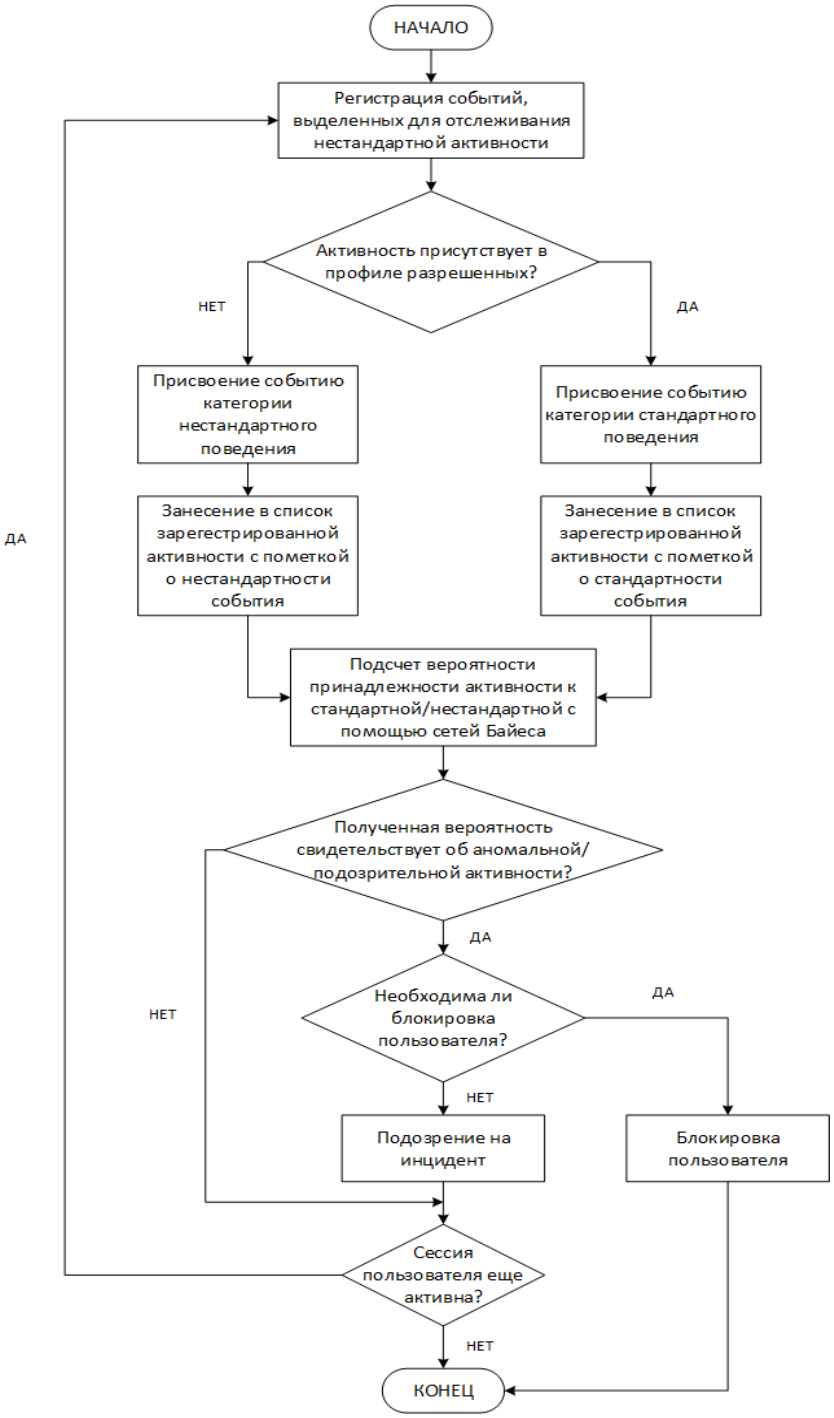


Рис. 2 Алгоритм анализа действий пользователя в информационной системе

Заключение

Сети Байеса являются наиболее гибким и адекватным математическим аппаратом, позволяющим даже в условиях некоторой неопределённости классифицировать поведение пользователя в информационной среде и определять необходимые меры по противодействию возможной реализации угрозы.

Таким образом в статье был произведен анализ угроз, исходящих от действий пользователя, проанализированы существующие системы мониторинга, а также рассмотрены математические аппараты, применяющиеся для задачи мониторинга действий пользователя. Авторами был выбран наиболее гибкий математический аппарат для определения риска кражи информации на предприятии, составлена байесовская сеть и предложена структурная схема системы, построенной на основе сети Байеса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Tara Seals Fear of Insider Threats Hits an All-Time High, URL: https://www.infosecurity-magazine.com/news/fear-of-insider-threats-hits-an/ (дата обращения 14.03.2023).
2. Karpova N., Panfilova I. Ensuring the Safety of Information Processes in Sociotechnical Systems Based on an Analysis of the Behavioral Characteristics of a Person as a Subject of Such a System // XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP), Samara, 2019. P. 751–753.
3. Sriram Raghavan S. V. Raghavan SDN Security: Developing an organic escalation framework for operational automation on security incidents //SpringerLink. URL: https://link.springer.com/article/10.1007/s40012-020-00266-8. (дата обращения 18.04.2023).
4. Doug White. Three Key Areas in Active Directory Security/ Security Weekly. URL: https://securityweekly.com/2018/09/06/three-key-areas-in-active-directory-security/ (дата обращения 02.03.2023).
5. Obaidat M.S., Macchairolo D.T. A multilayer neural network system for computer access security. EEE Trans. On Syst., Man. And Cybern. Vol. 24, No 5. Pp. 806-813, (1994).
6. Domanetska I., Khaddad A., Krasovska H., Yeremenko B. Corporate System Users Identification by the Keyboard Handwriting based on Neural Networks. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, vol. 9, iss. 1, pp. 4156–4161.
7. Elike H., Xavier B., Andrew H., Pierre-Louis D., Ephraim I., Christos T., Robert A. Threat analysis of IoT networks using artificial neural network intrusion detection system. Proceedings of the 3th International Symposium on Networks, Computers and Communications (Hammamet, Tunisia, 11-13 May 2016). New York, IEEE, 2016. DOI: 10.1109/ISNCC.2016.7746067.
8. Zvyagin L.S. Iterative and non-iterative methods of Monte Carlo as actual computing methods Bayesian analysis. Proceedings of 20th IEEE International Conference on Soft Computing and Measurements (St. Petersburg, Russia, 24-26 May 2017). New York, IEEE, 2016. DOI: 10.1109/SCM.2017.7970482.
9. Zhou Z.-H. Rule Extraction: Using neural networks or for neural networks? Journal of Computer Science and Technology, 2004, vol. 19, iss. 2, pp. 249–253.
10. Adnan Darwiche. Modeling and Reasoning with Bayesian Networks. – Cambridge University Press, 2009. – 526 p.
11. Judea Pearl. Causality: Models, Reasoning, and Inference. – 2-nd Edition. – Cambridge University Press, 2009. – 464 p.
12. D. MacKay. Information Theory, Inference, and Learning Algorithms. - Cambridge University Press, 2003 – 640 p.
13. Звягин Л.С. Метод байесовских сетей и ключевые аспекты байесовского моделирования / Л.С. Звягин // XXII Международная конференция по мягким вычислениям и измерениям (SCM-2019). Сборник докладов. Санкт-Петербург. 23-25 мая 2019 г. - СПб.: СПбГЭТУ «ЛЭТИ». - С. 30-34.
14. Security auditing. URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/security-auditing-overview (дата обращения 04.04.2023).

УДК 658.8
DOI 10.33764/2618-981X-2023-6-58-63

Н. С. Казанцева[1], М. И. Ананич[1]*

Особенности продвижения в медицине: инновационные инструменты и технологии

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: kazantseva4071@mail.ru

Аннотация. В данной научной работе представлены основные актуальные маркетинговые инструменты продвижения в медицине. На сегодняшний день существует большое многообразие инструментов продвижения продукта на рынок, однако не каждый подходит для продвижения медицинских продуктов в силу особенностей данного рынка и специфики самих продуктов. Актуальность исследования была определена снижением эффективности классических методов продвижения и появлением новых тенденций в развитии российского рынка медицины. Цель исследования заключалась в выявлении особенностей продвижения в медицине с учетом основных барьеров российского законодательства и определении инновационных инструментов для продвижения. С целью исследования были определены наиболее актуальные и эффективные инструменты, благодаря которым медицинский продукт способен охватить целевую аудиторию, повысить узнаваемость продукта и заработать компании хорошую репутацию.

Ключевые слова: маркетинг, продвижение, реклама, стимулирование продаж, медицинские продукты, инновационные инструменты

N. S. Kazantseva[1], M. I. Ananich[1]*

Features of Advancement in Medicine: Innovative Technologies and Innovative Tools

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: kazantseva4071@mail.ru

Abstract: This scientific paper presents the main current marketing tools for promotion in medicine. To date, there is a wide variety of tools for promoting a product to the market, but not everyone is suitable for promoting medical products due to the peculiarities of this market and the specifics of the products themselves. The relevance of the study was determined by the decrease in the effectiveness of classical methods of promotion and the emergence of new trends in the development of the Russian market of medicine. The purpose of the study was to identify the features of promotion in medicine, taking into account the main barriers of Russian legislation and identifying innovative tools for promotion. For the purpose of the study, the most relevant and effective tools were identified, thanks to which a medical product is able to reach the target audience, increase product awareness and earn the company a good reputation.

Keywords: marketing, promotion, advertising, sales promotion, medical products, innovative tools

Введение

На сегодняшний день медицина – это одна из стремительно развивающихся областей науки, с большим объемом знаний, связанными с научно-техническими разработками и их внедрением. К 2023 году медицина шагнула очень далеко,

развитие новых технологий и их наличие расширило все границы, однако в век цифровизации в данной сфере появились новые проблемы, риски и потребности в отношении продвижения продуктов на рынок медицины.

Комплекс методов продвижения всегда играл и будет играть важную роль в успешности развития любой организации, так как он выполняет ряд важнейших функций: налаживание и поддержание коммуникации с отдельными потенциальными клиентами или их группами, а также привлечение новых, увеличение объемов реализации продуктов, содействие прочному укреплению организации на рынке. Комплексно используя все многообразие технологий и инструментов продвижения, организация может завоевать положительную репутацию, а также укрепить свои позиции и повысить конкурентоспособность [9].

Сам термин «продвижение» (от англ. «promotion») в настоящий момент принято трактовать как комплекс маркетинговых мероприятий, целями которых являются увеличение доли продуктов, поставляемых на рынок, а также увеличение их узнаваемости, привлечение новых клиентов, повышение эффективности продаж [1].

Особую актуальность в современных условиях приобретают вопросы разработки комплекса мероприятий по продвижению в сфере медицины, так как эта сфера является довольно специфичной и имеет ряд особенностей [2].

Актуальность исследования состоит в том, что при сложившихся условиях на фармацевтическом рынке компаниям-производителям необходим новый механизм продвижения продукта на рынок, учитывающий специфику данного рынка, факторы, влияющие на потребителя, существующие риски и т.д. для нивелирования возможных негативных последствий при выводе новинки на рынок и увеличения шансов на ее успех, так как товары медицинского назначения всегда являлись и будут являться предметами высокого спроса.

Цель проведения исследования: выявление особенностей комплекса маркетинговых мероприятий по продвижению в медицине, направленных на увеличение спроса и стимулирование продаж.

В данной статье рассмотрены особенности продвижения продуктов в сфере медицины, основные инновационные технологии и инструменты.

Методы исследования

Для получения результатов исследования были использованы такие методы исследования как анализ, описание, обобщение.

Поскольку анализ – это процесс разложения объекта на составные части для детального, более глубокого изучения, данный метод был применен при изучении отдельных маркетинговых инструментов как составных частей продвижения.

Описательный метод был применен касаемо инновационных инструментов продвижения в медицине – он позволил дать точное и систематическое описание инструментам.

Обобщение, как метод исследования, было применено для определения результатов исследования и составления выводов.

Результаты

Продвижение продуктов сферы медицины – специфичная ниша для рекламы. Сегодня маркетологам приходится балансировать между уникальным конкурентоспособным предложением и ограничениями в законодательстве.

Заранее следует отметить, что к особенностям продвижения продуктов на рынок медицины можно отнести:

– спецификацию товаров медицинского назначения;

– узкую направленность использования;

– нетипичность распространения для массового рынка;

– востребованность по случаю возникновения форс-мажорных обстоятельств;

– узкую аудиторию потенциальных клиентов [3].

На сегодняшний день существует несколько соответствующих законов, регулирующих продвижение медицинских продуктов и фармацевтическую рекламу. Основным и главным из них является Федеральный закон Российской Федерации от 13.03.2006 г. №38-ФЗ «О рекламе», Статья 24. Реклама лекарственных средств, медицинских изделий и медицинских услуг, методов профилактики, диагностики, лечения и медицинской реабилитации, методов народной медицины [8]. Реклама лекарственных средств не должна:

– обращаться к несовершеннолетним (при этом обращение к родителям несовершеннолетних детей не запрещается законом);

– содержать ссылки на конкретные случаи излечения от заболеваний, улучшения состояния здоровья человека в результате применения объекта рекламирования;

– содержать ссылок на слова публичных людей, персон – лидеров мнений;

– содержать выражение благодарности физическими лицами в связи с использованием объекта рекламирования;

– создавать представление о преимуществах объекта рекламирования путем ссылки на факт проведения исследований, обязательных для государственной регистрации объекта рекламирования;

– содержать утверждения или предположения о наличии у потребителей рекламы тех или иных заболеваний либо расстройств здоровья;

– способствовать созданию у здорового человека впечатления о необходимости применения объекта рекламирования;

– создавать впечатление ненужности обращения к врачу;

– содержать утверждений, подталкивающих на самостоятельную постановку диагноза;

– гарантировать положительное действие объекта рекламирования, его безопасность, эффективность и отсутствие побочных действий;

– представлять объект рекламирования в качестве биологически активной добавки и пищевой добавки или иного не являющегося лекарственным средством товара;

– содержать утверждения о том, что безопасность и (или) эффективность объекта рекламирования гарантированы его естественным происхождением;

– содержать изображений с измененным под воздействием травмы (заболевания) телом (или его частей) [5].

При всем этом любая реклама медицинских продуктов обязательно должна сопровождаться предупреждением: «Имеются противопоказания. Необходима консультация врача (специалиста)».

Медицинский маркетинг к 2023 году претерпел изменения благодаря технологическим достижениям и инновационной политике. Сегодня медицинский маркетинг направлен не только на привлечение новых клиентов, но и на инвестирование в онлайн-репутацию, расширение искусственного интеллекта и аналитики, и т.д.

По этой причине в наши дни для продвижения чаще всего используется digital-маркетинг (цифровой маркетинг) – комплекс цифровых инновационных технологий и инструментов для привлечения потенциальных клиентов и удержания их в качестве потребителей. От интернет-маркетинга он отличается тем, что использует не только Всемирную паутину Интернет, но и офлайн-инструменты, такие как smart-гаджеты, печатные СМИ и наружные баннеры, POS-терминалы (от англ. «Point Of Sale» – точка продажи), промо-акции, мероприятия и прочие [10]. Офлайн-реклама как традиционный метод продвижения все еще остается актуальным, но для достижения лучших результатов его стоит комбинировать с digital-маркетингом, инструменты которого позволят клиентам ощутить удобство, комфорт и с легкостью довериться продукту или организации, особенно, когда дело касается здоровья. Ниже рассмотрены основные актуальные инновационные инструменты для продвижения продуктов на рынок медицины.

SEO (от англ. «Search engine optimization») – поисковая оптимизация. Считается самым эффективным инструментом сегодня для продвижения продуктов в сфере медицины, благодаря которому можно легко получить органический трафик (потенциальных клиентов, которые ищут конкретный товар или услугу, или конкретную организацию) [4]. SEO улучшает и оптимизирует поисковые возможности в Интернете благодаря прописки ключевых слов, заголовка и географической привязке: к примеру, если потенциальный клиент будет искать клинику, которая предоставляет нужный ему продукт (будь то товар или услуга), поисковик ему предоставит список ближайших от клиента клиник, а не клиники на другом конце города, и уж тем более страны. Также эффективным будет включение поисковой оптимизации на основе местоположения в свою контент-стратегию, используя такие ключевые слова, как «лучшая клиника Новосибирска» или «самые доступные цены на МРТ в Новосибирске» и так далее. Также следует заявить права на свою страницу Google My Business (полезно, если вы хотите появляться на Картах Google) и геотегировать объявления в социальных сетях, чтобы люди в вашем районе могли легко вас найти.

Таргетированная реклама аккаунтов и групп в социальных сетях. Данный инструмент доставляет рекламные сообщения покупателю в соответствии с его

конкретными чертами, интересами и предпочтениями. Эту информацию можно получить путем отслеживания профилей потребителей и их активность в Интернете. Этот инструмент также считается очень эффективным, поскольку попадет точно в нужную целевую аудиторию.

Веб-сайт продукта или организации, продвигающей продукт. Следует отметить, что веб-сайт должен быть профессионально разработан, а именно: иметь большой функционал, иметь адекватный дизайн без перебора изображений и большой текстовой нагрузки, высокую скорость загрузки и должен быть совместим с мобильными устройствами и оптимизирован с поисковыми системами. Также стоит рассмотреть вариант наличия чат-бота на сайте для решения базовых задач – не всякое обслуживание клиентов требует присутствия живого человека. Иногда разговаривать с человеком даже неудобно, например, когда клиент хочет задать быстрый вопрос, но должен ждать несколько минут по телефону, чтобы связаться с кем-то.

Телемедицина – возможность проконсультироваться с врачом или специалистом насчет продукта через видео- или аудиочат. Данный инструмент поможет привлечь больше клиентов, в том числе немобильных (без транспорта, без свободного времени или физически ограниченных людей), а также продемонстрирует клиентоориентированность. В некоторых случаях этот вариант поможет даже снизить распространение какого-либо заболевания при отсутствии физического контакта [7].

Контент-маркетинг – еще один инструмент медицинского маркетинга, выполняющий одновременно несколько задач. В первую очередь он привлекает органический трафик на сайт и позволяет таким образом коммуницировать с теми, кто не готов записаться на прием прямо сейчас, но ищет информацию о процедуре или болезни [6]. С помощью понятных полезных статей, блогов и видеоматериалов продукт заявляет о себе потребителям, а те могут подсознательно запомнить компанию и в следующий раз выбрать ее, а не конкурентов. Контент-маркетинг формирует репутацию продукта и организации не менее эффективно, чем отзывы и рекомендации. Люди начинают больше доверять бренду, если видят, что он помогает им хотя бы на уровне контента, а значит – повышается их лояльность. Контент – это не продажа, а построение доверия.

Заключение

Делая выводы, следует отметить, что на сегодняшний день существует большое многообразие инструментов продвижения продукта на рынок, однако не каждый подходит для продвижения медицинских продуктов в силу особенностей данного рынка и специфики самих продуктов. Маркетинг меняется и растет каждый день, и больше нет предела тому потенциалу, который можно реализовать. Вышеуказанные инновационные инструменты способны помочь достичь успеха маркетинговой кампании, особенно, если сочетать их с оффлайн-маркетингом.

Несмотря на существующие законодательные барьеры, в наше время рынок медицинских продуктов, как и вся сфера здравоохранения, считается одним из

самых перспективных. В данную отрасль сегодня инвестируют большой объем финансовых ресурсов, поэтому подбор инновационных инструментов и каналов продвижения напрямую связан с достижением высокой экономической эффективности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аллен К. Р. Продвижение новых технологий на рынок : учеб. пособие. М. : БИНОМ Лаборатория знаний, 2014. 26 с.
2. Волин А. Ю., Беркович М. И., Брагина З. В. Особенности продукта фармацевтической отрасли как инновационного товара : учеб. пособие. Новосибирск : Теоретическая экономика, 2021. 4 с.
3. Городнова И. В., Городнова А. В., Особенности продвижения на рынке с помощью инновационных инструментов : учеб. пособие.– М : Бизнес Информ, 2019. 3 с.
4. Кадырова Э. Ф. Особенности рыночного продвижения медицинских услуг [Электронный ресурс] : продвижение медицинских продуктов // Евразийский международный научно-аналитический журнал. 2022. URL: http://www.m-economy.ru/art.php?nArtId=2461 (дата обращения : 12.03.2023).
5. Петровичева А. В. Особенности рекламы медицинских услуг [Электронный ресурс] : особенности продвижения в медицине // Новосибирск : Directline. 2022. URL: https://www.directline.pro/blog/reklama-meditsinskikh-uslug/ (дата обращения : 12.03.2023).
6. Степченко Т.С. Комплекс маркетинга в здравоохранении : учеб. пособие. М : Новая наука: Проблемы и перспективы. 2016. 236 с.
7. Суворова А. А. Маркетинговые инструменты продвижения продукции на рынке медицинских услуг : учеб. поосбие для студентов. Саратов : Астрель, 2021. 3 с.
8. Федеральный закон "О рекламе" от 13.03.2006 N 38-ФЗ (последняя редакция) [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_58968/ Доступ из справ.-правовой системы «КонсультантПлюс». (дата обращения: 14.03.2023).
9. Тарасов Ю. В. Становление и дальнейшее развитие современного фармацевтического продвижения [Электронный ресурс] : современные исследования социальных проблем // Вестн. РФФИ. 2015. № 12 (32). URL: www.sisp.nkras.ru (дата обращения : 15.03.2023).
10. Чупандина Е. Е., Дагир С. Обзор основных подходов и особенностей в продвижении лекарственных препаратов на российском рынке : учеб. пособие. Воронеж : Экономика и бизнес, 2018. 6 с.

УДК 535.8
DOI 10.33764/2618-981X-2023-6-64-69

П. А. Кайсин[1]*

Поиск оптимальных комбинаций спектральных диапазонов для панорамных объективов, работающих в нескольких диапазонах спектра

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Kaysin-PA2021@sgugit.ru

Аннотация. В статье рассматривается актуальность разработки современных оптических систем панорамного обзора, работающих в нескольких диапазонах спектра для беспилотных аппаратов. Сформирована проблематика, связанная с потребностью производства более сложных в техническом плане систем панорамного обзора. Рассмотрены основные задачи, решаемые устройствами подобного типа. Рассмотрены достоинства и недостатки различных спектральных диапазонов. Проведено сравнение оптических диапазонов при комбинировании для решения поставленных задач. Приведены примеры использования различных диапазонов спектра при съемке. Представлены сопоставления коэффициентов отражения для некоторых объектов в выбранных диапазонах спектра. Выбран оптимальный диапазон спектра для использования в комбинации с видимым диапазоном, решающий поставленные задачи. Сформирован вывод касательно использования рассмотренной комбинации спектральных диапазонов в системах панорамного обзора для мониторинговых и навигационных целей БПА.

Ключевые слова: системы панорамного обзора, двухканальная система, видимый и инфракрасный диапазоны спектра, навигационная видеокамера, ближний инфракрасный диапазон

P. A. Kaisin[1]*

Search for Optimal Combinations of Spectral Ranges for Panoramic Lenses Operating in Several Ranges at the Same Time

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: Kaysin-PA2021@sgugit.ru

Annotation. The article discusses the relevance of the development of modern optical panoramic viewing systems operating in several spectrum ranges for unmanned vehicles. The problems related to the need for the production of more technically complex panoramic viewing systems have been formed. The main tasks solved by devices of this type are considered. The advantages and disadvantages of various spectral ranges are considered. The comparison of optical ranges when combined to solve the tasks is carried out. Examples of using different ranges of the spectrum when shooting are given. Comparisons of reflection coefficients for some objects in selected spectral ranges are presented. The optimal range of the spectrum has been selected for use in combination with the visible range, which solves the tasks set. A conclusion has been formed regarding the use of the considered combination of spectral ranges in panoramic viewing systems for monitoring and navigation purposes of the BPA.

Keywords: panoramic viewing systems, dual-channel system, visible and infrared spectrum ranges, navigation video camera, near infrared range

Введение

Современные панорамные объективы, работающие в нескольких диапазонах спектра, предоставляют возможность получения высококачественных изображений в различных условиях эксплуатации. Однако для достижения наилучшего результата необходимо правильно подобрать комбинацию спектральных диапазонов. Актуальность разработки оптических систем панорамного обзора, работающих в нескольких спектральных диапазонах, для беспилотных аппаратов (БПА) определяется:

- необходимостью использовать БПА в различное время суток;
- повышенным спросом на навигационные и мониторинговые системы БПА для тактических и наблюдательных целей;
- усовершенствованием технологий, позволяющих проектировать более компактные системы панорамного обзора;

В данной статье рассматриваются актуальные задачи и способы их решения при разработке оптических систем панорамного обзора для беспилотных аппаратов.

Главная задача данной работы – определение оптимальной комбинации спектральных диапазонов оптического излучения, которая может быть использована при проектировании систем с панорамной оптикой, решающей задачи формирования и анализа панорамного изображения пространства в области, близкой к полусфере.

Методы и материалы

Для получения результатов использовались системный подход, поиск, обзор и анализ тематической информации, доступной в сети Интернет и профильной технической литературе.

Результаты и обсуждение

Активное применение БПА, в том числе и летательных (БПЛА), в последние годы, показало принципиальную необходимость в усовершенствовании навигационных и мониторинговых систем, которыми оснащаются дроны. Большое разнообразие БПЛА, применяемых как для гражданских нужд, так и для военных, позволило статистически выявить плюсы и минусы каждой модификации, а также указать направления для развития всей области конструирования БПЛА в целом. Главными задачами оптических систем, используемых в БПЛА, по-прежнему остаются: обнаружение объектов, целеуказание, сопровождение, мониторинг и обеспечение навигационных потребностей дрона. Однако, конечный потребитель всегда хочет получать больше возможностей в одном устройстве, а в случае с БПЛА появляется необходимость в использовании устройства в сложных условиях, таких как недостаточная видимость и плохие погодные условия. Для решения данной задачи подходят мультидиапазоные камеры, позволяющие

сохранять функционал БПЛА в любое время суток и практически при любых погодных условиях [1].

Неотъемлемой частью такого рода камер остается необходимость контроля со стороны оператора, осуществляющего управление дроном и корректирующего его движение в реальном времени, а значит необходим объектив, работающий в видимом диапазоне спектра (VIS). Передача видео в видимом диапазоне минимизирует время на его постобработку и снижает нагрузку на вычислительные мощности, позволяя незамедлительно реагировать на меняющуюся обстановку в пространстве. Для наблюдения в условиях недостаточной освещенности необходим объектив, работающий в инфракрасном диапазоне спектра (ИК) [7]. Инфракрасное излучение является важным сектором электромагнитного спектра, расположенным между волнами видимого диапазона и радиоволнами. В зависимости от длины волны, инфракрасное излучение может быть разделено на пять групп [14]:

– ближний инфракрасный диапазон (NIR) с длиной волны от 0,75 до 1,4 мкм;

– коротковолновый инфракрасный диапазон (SWIR) с длиной волны от 1,4 до 3 мкм;

– средневолновый инфракрасный диапазон (MWIR) с длиной волны от 3 до 8 мкм;

– длинноволновый инфракрасный диапазон (LWIR) с длиной волны от 8 до 15 мкм;

– дальний инфракрасный диапазон (FIR) с длиной волны от 15 до 1000 мкм.

В ближнем инфракрасном диапазоне работают инфракрасные светодиоды, лазеры для систем оптической связи, телевизионные камеры и приборы ночного видения на основе электронно-оптического преобразователя (ЭОП) [1, 3, 6].

В коротковолновом инфракрасном диапазоне достигаются более высокие уровни природных контрастов. Типичными сенсорами, используемыми при обычной съемке в SWIR диапазоне, являются сенсоры на основе арсенида-индия-галлия (InGaAs), способные захватывать область от 0,550 нм до 2,5 нм [3-5].

MWIR позволяет измерять температуру объектов и обнаруживать тепловые аномалии. В MWIR диапазоне тела, нагретые до 600 °C, начинают испускать электромагнитное излучение, фиксируемое электронно-оптическим преобразователем. В этом диапазоне чувствительны тепловые головки самонаведения систем ПВО и тепловизоры [9].

В LWIR диапазоне излучают тела с температурами около 0 °C. В этом диапазоне чувствительны тепловизоры и приборы ночного видения.

В FIR диапазоне источниками излучения являются лазеры дальнего ИК диапазона. В оптике для работы в FIR диапазоне используются специальные приборы и оптические материалы, способные пропускать излучение FIR диапазона.

Для улучшения конечного изображения при работе в условиях недостаточной видимости достаточным будет применение NIR или SWIR диапазонов. NIR диапазон является пограничным к видимому спектральному диапазону, что су-

щественно упростит задачу в подборе материалов при конструировании компонентов объектива и положительно скажется на массогабаритных характеристиках устройства.

Преимущества использования NIR диапазона, а не ультрафиолетового (УФ) канала [7]:

– квантовая чувствительность многих кремниевых фотоприемников при длине волны электромагнитного излучения в диапазоне от 800 до 1000 нм, значительно выше, чем в области 300 нм;

– мощность естественного излучения в NIR диапазоне несколько выше, чем в УФ;

– NIR диапазон имеет более короткую длину волны, что означает, что более высокие частоты могут быть переданы на большом расстоянии без искажений;

– ближний ИК диапазон требует меньшей мощности для связи, что приводит к меньшему потреблению энергии и большей эффективности.

Комбинирование VIS и NIR диапазонов позволяет получить некоторое техническое преимущество при использовании на БПЛА. Комбинация двух диапазонов ведет к созданию полного спектра данных, которые БПЛА может использовать для определения местоположения объектов, анализа территории, поиска и спасения людей, мониторинга и контроля транспортных потоков, а также для других задач. Таким образом, комбинирование VIS и NIR диапазонов позволяет беспилотным летательным аппаратам работать более эффективно в различных условиях и выполнять задачи с большей точностью и эффективностью.

На рис. 1 приведены примеры изображений, снятые в различных спектральных диапазонах. Изображение объектов в видимом диапазоне спектра показано на рис. 1, *а*, в NIR диапазоне – на рис. 1, *б*, в LWIR диапазоне – на рис. 1, *в* [7-9].

Коэффициент отражения зависит от молекулярного состава материала и от спектра его излучения. В табл. 1 представлены коэффициенты отражения для некоторых объектов, для которых они существенно различаются в видимом и ИК диапазонах длин волн. Из наиболее существенных отличий следует отметить слабое отражение в NIR-диапазоне для воды и неба, что позволяет искать на их фоне малоконтрастные объекты. Другая особенность связана с тем, что глубина проникновения падающего излучения в материалы прямо пропорциональна длине волны. Так излучение в коротковолновом диапазоне спектра поглощается только на поверхности материала (проникновение на глубину не более 90 нм), в то время как излучение с длиной волны около 1000 нм проникает в слои материала до 10 мм [6].

а) б) в)

Рис. 1. Примеры изображений в различных спектральных диапазонах:
а) видимый спектр RGB-изображения; *б)* NIR-изображение;
в) LWIR-изображение

Таблица 1

Коэффициенты отражения в видимом и ближнем ИК диапазонах

Объект	Диапазон длин волн	
	VIS	NIR
	Коэффициент отражения	
Небо	от 0,20 до 0,80	0,10
Вода	от 0,20 до 0,70	0,10
Песок	от 0,50 до 0,60	0,45
Бетон	от 0,40 до 0,50	0,35
Листья деревьев, трава	от 0,20 до 0,60	0,65
Кора деревьев	от 0,15 до 0,25	0,35

Заключение

Современная технологическая и элементная база позволяет панорамным системам работать для навигационных и мониторинговых целей в нескольких диапазонах спектра, определяя объекты с высоты более 30 м над уровнем земли, в условиях плохой освещенности и при плохих погодных условиях [15]. Комбинация VIS и NIR диапазонов спектра решает поставленные задачи, проста в реализации и расширяет горизонты возможностей современных БПЛА.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Wu D., Da-Wen Sun. Advanced applications of hyperspectral imaging technology for food quality and safety analysis and assessment: A review. Pt. II: Applications // Innovative Food Science & Emerging Technologies. – 2013. – V. 19. – P. 15-28.

2. Egorenko M.P., Efremov V.S. «Mirror-lens camera system for underwater drones», Proc. SPIE 11560, 26th International Symposium on Atmospheric and Ocean Optics, Atmospheric Physics, 115602O //. – 2022. – URL: https://doi.org/10.1117/12.2573572.

3. Firmenich D., Brown M. SGsstrunk S. Multispectral interest points for RGB-NIR image registration // Proc. IEEE int. conf. on image processing (ICIP). – Brussels. – 11-14 Sept. 2011. – URL: http://infoscience.epfl.ch/record-/167479/files/FBS11.pdf (дата обращения 09.05.2023).

4. Canzek L. Neue Richtung in der Entwicklung der katadioptrischen Objektive // Optica acta. 1979. №2. P. 279–287. DOI: 10.1080/713819973.

5. Егоренко М.П., Ефремов В.С. Хроматические свойства зеркала Манжена в нескольких диапазонах спектра // Изв. вузов. Приборостроение. – 2009. – Т. 52. № 6. – С. 53–57.

6. Near infrared (NIR) cameras. – URL: http://www.jai.-com/en/products/nearinfrared (дата обращения: 09.05.2023).

7. Real time megapixel multispectral bioimaging / J. Eichenholz, N. Barnett, Y. Juang et al. // Proc. SPIE: Imaging, manipulation, and analysis of biomolecules, cells, and tissues VIII. – 2010. – Vol. 7568. -URL: http://www.pixelteq.com/wp-content/uploads/2013/01/PIXELTEQ_Real-time-Megapixel-Multispectral-Bioimaging.pdf (дата обращения: 09.05.2023).

8. Соломатин В. Панорамная видеокамера // Фотоника. – 2009. – № 4. – С. 26-29.

9. Панорамная зеркально-линзовая система с видеокамерой: Пат. 2335003. Россия, G02B 17/08 (2006.01), G03B 37/06 (2006.01). Колючкин В.Я., Тимашова Л.Н., Колобов К.В., Князев А.А.; ООО «Лаборатория трехмерного зрения». № 2006133677/28; Заявл. 27.03.2008; Опубл. 27.09.2008. Бюл. № 27.

10. Панорамная двухспектральная зеркально-линзовая система: Пат. 2728321. Россия, МПК, G 02B 17/08, G 03B 37/06, G 02B 13/06. Егоренко М.П., Ефремов В.С.; Сиб. гос. ун-т геосистем и техн. № 2020100496; Заявл. 12.02.2020; Опубл. 29.07.2020. Бюл. № 22.

11. Ленгауэр Г.Г., Михельсон Н.Н., Никанорова И.Н. Теория сверхширокоугольной камеры Г.Г. Ленгауэра // Изв. ГАО АН СССР. – 1989. – № 206. – С. 75-79.

12. НПП «Фотоника» [Электронный ресурс]. – URL: https://www.npk-photonica.ru/ (дата обращения 01.05.2023).

13. Новоситной портал Hongkiat [Электронный ресурс]. - URL: https://www.hongkiat.com/blog/360cam-first-hd-360-camera/ (дата обращения 09.05.2023).

14. Русинов М.М., Грамматин А.П., Иванов П.Д., Андреев Л.Н., Агальцова Н.А., Ишанин Г.Г., Василевский О.Н., Родионов С.А. / под общ. ред. Русинова М.М. Вычислительная оптика: справочник. Изд. 2-е, М.: URSS. – 2008. – С. 424 с.

15. Кайсин, П. А. Принципы разработки оптических систем панорамного обзора для беспилотных аппаратов / П. А. Кайсин, В. С. Ефремов // Интерэкспо ГЕО-Сибирь. XVIII Междунар. науч. конгр., 18–20 мая 2022 г., Новосибирск : сборник материалов в 8 т. Т. 6 : Магистерская научная сессия «Первые шаги в науке». – Новосибирск : СГУГиТ. – 2022. – Т. 6. – С. 76-81. – DOI 10.33764/2618-981X-2022-6-76-81.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-70-76

Р. Е. Калиакпаров[1]*

Создание модели распространения загрязнений в атмосферу от Цементного завода и ТЭЦ в г. Семей

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: kaliakparov1@vk.com

Аннотация. Для прогнозирования загрязнения воздуха от стационарных источников, а также при повышенных технологических или аварийных выбросах, используются модели распространения примесей в атмосфере. В данной работе целью было определить концентрацию загрязняющих веществ от одного источника с помощью модели Паскуилла-Гиффорда на территории города Семей в Республике Казахстан. Построение итоговой модели загрязнения происходило в программном продукте ArcGIS и включало три этапа: подготовку картографической основы, сбор информации о стационарном источнике загрязнения и моделирование загрязнения от одного источника. За картографическую основу была принята базовая карта Open Street Map, а информация о стационарном источнике загрязнения была получена из открытых источников, включая высоту дымовой трубы ТЭЦ-1 и количество выбросов в атмосферу за год. В результате работы была получена модель концентрации примеси, которая была представлена в виде струи с гауссовым распределением по вертикали и в поперечном направлении ветра от непрерывного точечного источника (ТЭЦ-1).

Ключевые слова: Модель загрязнения, точечный источник загрязнения, расчет концентрации выбросов в атмосферу, представление на карте концентрации веществ

R. E. Kaliakparov[1]*

Building a Model for the Spread of Pollutants from Cement Plant and Thermal Power Plant Into the Atmosphere in the City of Semey

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: kaliakparov1@vk.com

Abstract. Models of pollutant dispersion in the atmosphere are built to forecast pollution from stationary sources and for cases of increased technological or accidental emissions. The aim of this study is to calculate the concentration of pollutants from a single source using the Pasquill-Gifford model in the city of Semey, Kazakhstan. This model is widely recognized as the most advanced of the practically applicable models. The process of building the final pollution model took place in the ArcGIS software and consisted of three stages: preparing the cartographic base, collecting information about the stationary pollution source, and modeling pollution from a single source. The base map used was Open Street Map (OSM), and data on the stationary pollution source were obtained from open sources (the height of the smokestack of the TPP-1 and the amount of emissions into the atmosphere per year). The result of the study was the presentation of the concentration of pollutants emitted by a continuous point source (TPP-1) as plumes with Gaussian distributions in the vertical and crosswind directions.

Keywords: Pollution model, point source of pollution, calculation of emission concentration into the atmosphere, representation of substance concentration

Введение

Загрязнение атмосферы – это одна из основных проблем экологии современного мира. Все большее количество различных веществ попадает в атмосферу и влияет на здоровье человека и окружающую среду. Для того, чтобы эффективно бороться с этой проблемой, необходимо использовать математические модели, которые позволяют оценить и прогнозировать уровень загрязнения в различных условиях и на разных территориях [1].

Одной из основных экологических проблем города Семей в течение многих лет являются повышенные выбросы вредных веществ от промышленных предприятий и объектов теплоснабжения города. После многочисленных жалоб горожан эксперты проверили предприятие (ТЭЦ) и подтвердили факты нарушения экологических норм. Выбросы на ТЭЦ превышали допустимые нормы в 21 раз, а котельные устарели и имели дыры на некоторых трубах [2]. Все это связано с тем, что на большинстве теплоэлектроцентралей в Казахстане используются котельные установки и прочее оборудование, которые были спроектированы и построены несколько десятилетий назад. В то время основным приоритетом для инженеров и персонала, занимающегося эксплуатацией, было обеспечение эффективного сжигания топлива: высокий КПД, минимальные потери и долгосрочная безотказная работа. Но так как глобально и оперативно изменить ситуацию очень трудно (сроки постройки и введения в эксплуатацию новой ТЭЦ-3 пока неизвестны), то в данный момент остается актуальной задача построения математических моделей, которые позволяют оценить и прогнозировать уровень загрязнения [6].

В 2010 году житель города подал официальную жалобу в областную природоохранную прокуратуру, указывая на нарушение экологического законодательства заводом. В ответ на жалобу власти провели проверку и обнаружили, что выбросы пыли в воздух превышают предельно допустимые концентрации (ПДК) [3].

Используемая в данной работе модель Паскуилла-Гиффорда основывается на представлении концентрации примеси, выделяемой непрерывным точечным источником в атмосфере, в виде струй с гауссовыми распределениями в вертикальном и поперечном направлениях относительно направления ветра.

Модель применима для описания распределения примеси от высоких точечных источников, которые действуют непрерывно. Это означает, что примесь распространяется на значительное расстояние, превышающее размеры самого источника, и время его работы достаточно для установления стационарного поля концентрации. На практике это означает, что время работы источника должно быть не менее нескольких десятков минут или даже нескольких часов. Примерами таких источников могут быть дымовые трубы и вентиляционные системы промышленных предприятий.

Цель работы заключается в определении выбросов загрязняющих веществ от двух предприятий с помощью модели Паскуилла-Гиффорда для выявления частей города, которые наиболее подвержены вредному воздействию.

Для достижения цели были выполнены такие *задачи*, как:

изучение принципа и технологии модели Паскуилла-Гиффорда;

выбор соответствующего программного обеспечения для построения выбранной модели;

выбор двух объектов, выбрасывающих в атмосферу примеси;

построение модели.

Характеристика объектов исследования

Исследуемые объекты находятся на территории г. Семей в Абайской области. Люди, проживающие вблизи двух промышленных объектов, не имеют сведений о содержании выбросов цементного завода и о том, как они могут негативно сказаться на их здоровье, поскольку эта информация недоступна. При построении модели используются условные данные, которые могут являться приближенными к фактическим. Пусть ТЭЦ-1 и Цементный завод выбрасывают в атмосферу чуть более 13-ти и 15-ти тысяч тонн газовых отходов соответственно. Отмечается, что в составе примесей, выбрасываемых ТЭЦ-1, могут содержаться радионуклиды. Это связано с тем, что в течение более 30-ти лет в качестве сырья для топки котлов используется уголь из месторождения

«Каражыра», расположенного на территории бывшего Семипалатинского испытательного ядерного полигона [4].

Создание картографической основы

Как было указано выше, в качестве картографической основы была принята базовая карта Open Street Map (OSM) в программе ArcGIS [11]. Данную карту необходимо задать в проекции Гаусса-Крюгера (Pulkovo 1942 GK Zone 14N, т.к. этот параметр дает минимальные искажения форм и масштабов).

Внесение данных об источнике загрязнения

Для внесения данных об источнике загрязнения в программу необходимо создать shape-файл в приложении ArcCatalog. Shape-файл представляет собой формат хранения геометрического местоположения и атрибутивной информации географических объектов. Для данного файла также необходимо задать проекцию Гаусса-Крюгера. Отмечу, что вся дальнейшая модель будет создаваться для ТЭЦ-1, а затем, построенную модель для ТЭЦ-1 можно применить и для Цементного завода, изменив исходные данные.

С помощью инструмента создания объектов отмечается на карте необходимый объект (ТЭЦ-1) и вносится в таблицу атрибутов информация о названии объекта, высоте трубы, количества выбросов в атмосферу в год. Далее рассчитывается количество выбросов в секунду (рис. 1).

	ShortName	H	Q_t_t_y	Q_g_sec
▶	ТЭЦ-1	80	13,354	423,452606

Рис. 1. Внесенные и рассчитанные данные ТЭЦ-1 в таблице атрибутов

Построение модели Паскуилла-Гиффорда от источника загрязнения

Модель Паскуилла и Гиффорда – эмпирическая, предназначена для прогноза загрязнения стационарными источниками и для случаев повышенных технологических или аварийных выбросов. В основе модели – представление концентрации примеси, выбрасываемой непрерывным точечным источником в атмосфере, как струи с гауссовыми распределениями по вертикали и в поперечном к ветру направлении:

$$q(x,y,z)=\frac{Q}{2\pi\sigma_y(x)\sigma_z(x)u}\times f_F f_W\times\exp(-\frac{y^2}{2\sigma_y^{\,2}(x)})\times(\exp(-\frac{(z-h)^2}{2\sigma_z^{\,2}(x)})+\exp(-\frac{(z-h)^{\,2}}{2\sigma_z^{\,2}(x)})), \qquad (1)$$

где *x, y, z* – декартовы координаты, ось *z* – вверх, ось *x* – по ветру; *h* – эффективная высота источника (то есть высота с учетом первоначального подъема перегретой струи); *Q* – мощность источника выброса; *q* - концентрация примеси в данной точке пространства; *u* - скорость ветра, усредненная по слою перемешивания; σ_Y (x) и σ_Z (x) – вертикальное и поперечное среднеквадратические отклонения концентрации примеси в атмосфере; f_F и f_W – поправки на обеднение облака за счет сухого осаждения примеси и ее вымывания осадками.

Сумма экспонент в формуле (1) соответствует поверхности земли, не поглощающей примесь, при абсолютном поглощении будет разность.

Основное содержание модели – обобщающие многочисленные экспериментальные данные, конкретные функции $\sigma_y(x)$ *и* $\sigma_Z(x)$ и выражения для *h,* f_F *и* f_W [5].

Для проведения моделирования использовался инструмент Model Builder. Сначала необходимо получить растр ограничивающий область моделирования. Для этого применялся инструмент «Объекты в растр». В результате получается растр с размером пикселя 10 м, который будет соответствовать размеру области моделирования.

Требуется установить систему координат, которая начинается в месте источника загрязнения, используя «Евклидово направление» в качестве инструмента.

Для перехода к прямоугольной системе координат используется «Растровый калькулятор».

Может быть использовано скалярное произведение векторов, чтобы заново вычислить координаты точек в системе координат, которая связана с направлением ветра. Для этого применен «Растровый калькулятор», создающий два новых растровых слоя U и V.

Для учета турбулентности и скорости перемещения загрязняющих веществ в горизонтальном и вертикальном направлениях, можно ввести новые переменные. Для этого снова применен «Растровый калькулятор», создающий два дополнительных растровых слоя для σY и σZ.

Для расчета концентрации загрязнений используется информация о количестве выбросов из поля Q_q_s и о высоте трубы из набора данных. Затем, исполь-

зуя модель Паскуила-Гиффорда, формула разделяется на три части и с помощью растрового калькулятора вычисляется каждая из них.

Далее производится фильтрация полученных результатов. Это нужно, чтобы убрать некоторые визуальные дефекты, округлить значения и изменить цветовую схему. В конечном итоге, получаются результаты, изображенные на рис. 2 и 3.

Согласно модели, созданной для ТЭЦ-1, наиболее высокий уровень концентрации веществ в облаке с условием скорости ветра 2 м/с наблюдается на протяжении 350 м от источника. Умеренный уровень концентрации сохраняется на протяжении 3 км.

Для применения данной модели для расчета концентрации выбросов от Цементного завода необходимо добавить новый shape-файл с информацией об объеме выбросов предприятия. Затем созданный файл вводится в модель. Результат показан на рис. 3.

Согласно вычисленной модели для цементного завода, при скорости ветра 2 м/с наибольшая концентрация веществ в облаке наблюдается в пределах 500 м от источника, после чего уровень концентрации умеренный и сохраняется на расстоянии 4 км.

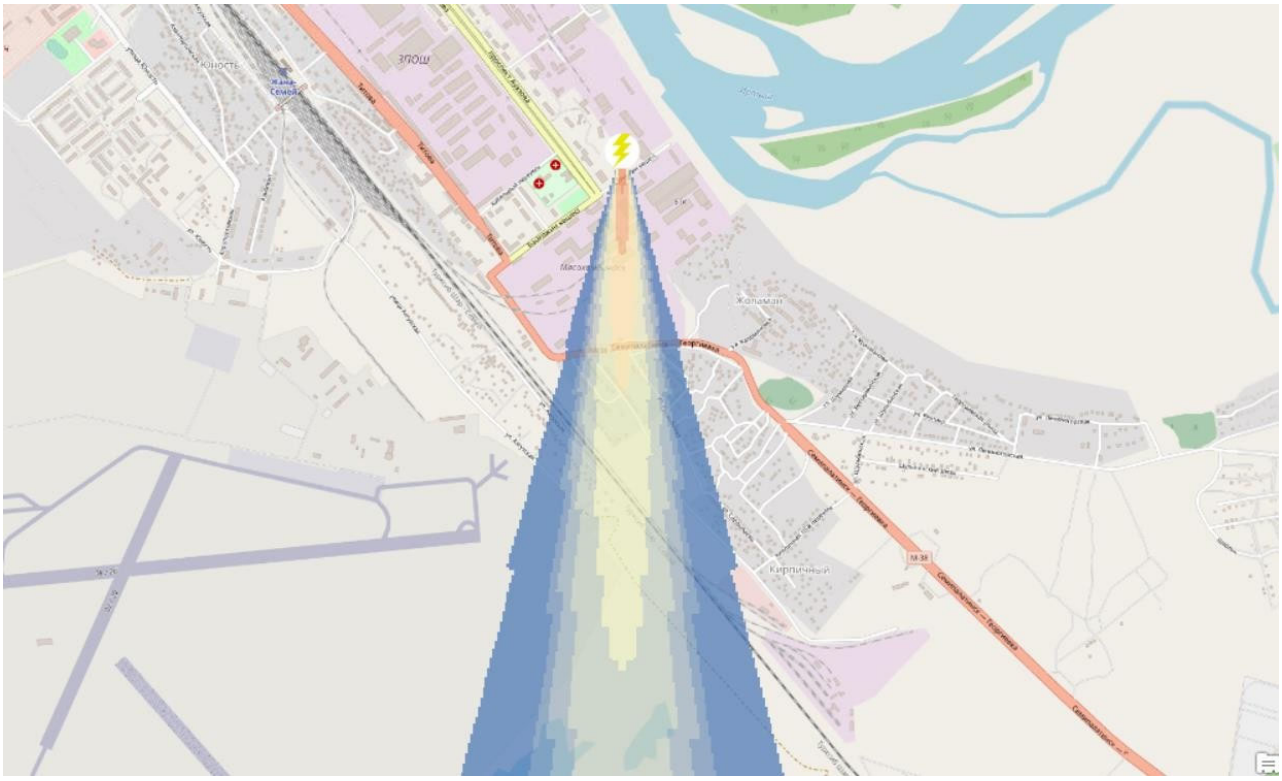


Рис. 2. Итоговый результат. Модель загрязнения ТЭЦ-1. Масштаб 1:20 000

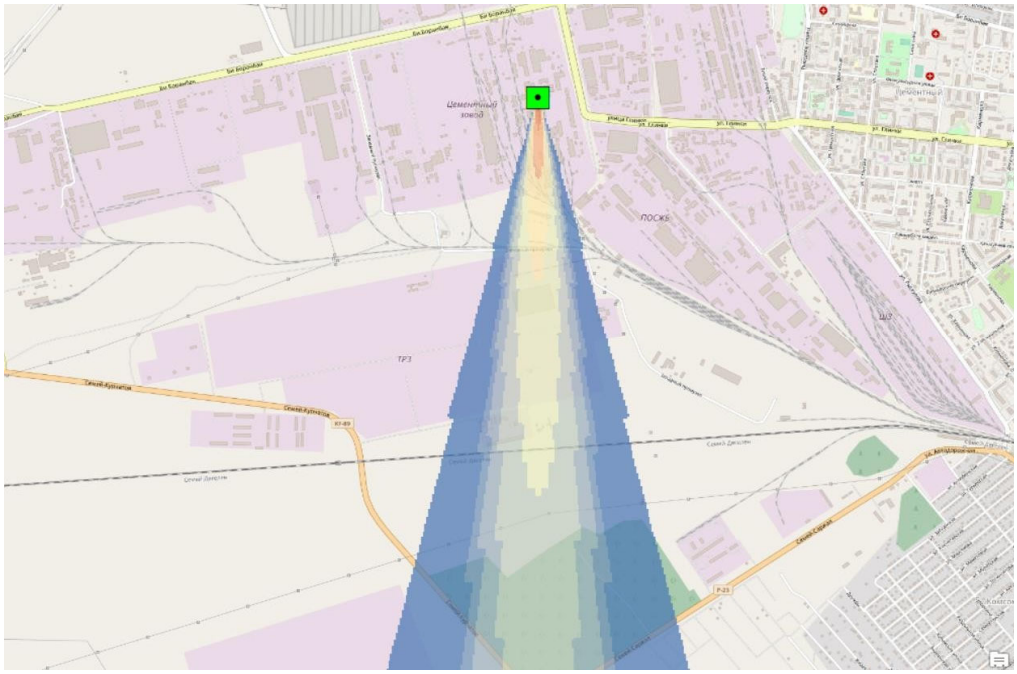


Рис. 3. Итоговый результат. Модель загрязнения Цементного завода. Масштаб 1:20 000

Применение результатов модели при оценке стоимости участков, подверженных влиянию выбросов

Одним из способов применения модели возможна оценка кадастровой стоимости участков с учетом экологического фактора. На государственном сайте «Управления земельных отношений Восточно-Казахстанской области» размещен модуль, который рассчитывает кадастровую стоимость участков, а также стоимость земельного налога и арендной платы [10]. Фрагмент геопортала изображен на рис. 4. Используя построенную модель с внесенными актуальными значениями выбросов за единицу времени, можно определить ареалы загрязнения от предприятий и ввести коэффициент за экологический фактор.

Рис. 4. Фрагмент геопортала с изображением участка в м. Бобровка с указанием кадастровой стоимости и налога

Заключение

В данной работе построена модель концентрации загрязняющих веществ от двух объектов согласно модели Паскуилла-Гиффорда на территории города Семей. Как отмечалось выше, модель может послужить для прогнозирования и определения повышенных выбросов в атмосферу, а также может применяться для целей градостроительства при постройки жилых домов с целью минимизации влияния загрязняющих веществ. При появлении новых сведений для конкретной местности модель несложно изменять.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Загрязнение воздуха – одна из главных угроз для человека и планеты. Режим доступа: https://news.un.org/ru/story/2021/09/1409462, свободный (Дата обращения: 11.04.2023).
2. Kazakhstan Today. В Семее выбросы ТЭЦ превысили норму в 21 раз. Режим доступа: https://www.kt.kz/rus/ecology/v_semee_vybrosy_tets_prevysili_normu_v_21_raz_1377910885.htm l, свободный (дата обращения 16.04.2023).
3. Борьба семейчан за чистый воздух. Режим доступа: https://rus.azattyq.org/a/cement-dust-all-over-the-house-semey-residents-fight-for-clean-air/31017136.html, свободный (дата обращения 16.04.2023).
4. Краткие сведения о ТЭЦ-1. Режим доступа: https://energybase.ru/power-plant/semey-tpp-1, свободный (дата обращения 16.04.2023).
5. Модель Паскуилла-Гиффорда. Режим доступа: http://www.ecologyman.ru/97/38.htm, свободный (дата обращения 17.04.2023).
6. Рябышенков А.С., Волкова Е.А. «Построение автоматизированной системы мониторинга окружающей среды» // В сборнике: Синтез науки и образования в решении экологических проблем современности. материалы Международной научно- практической конференции, посвященной Всемирному дню охраны окружающей среды. Воронеж, 2022. С. 243-249.
7. Васильев А.В, Комлик Е.А., Терещенко Ю.П. «Динамические карты загрязнений окружающей среды» // Научный журнал Российского НИИ проблем мелиорации. 2017. № 4 (28). С. 106-120.
8. Сидорова Г.П., Авдеев П.Б., Якимов А.А., Овчаренко Н.В., Маниковский П.М. «Мониторинг состояния окружающей среды на территориях, вовлеченных в обращение углей с повышенным содержанием естественных радионуклидов» // Горный информационно-аналитический бюллетень (научно-технический журнал). 2019. № 12. С. 102-113.
9. «Краткие сведения о Цементном заводе г. Семей» – [Электронный ресурс] // https://energybase.ru : [сайт]. – URL: https://energybase.ru (дата обращения 16.04.2022). – Режим доступа : общий доступ.
10. «Управление земельными отношениями Восточно-Казахстанской области» – [Электронный ресурс] // https://vkomap.kz : [сайт]. – URL: https://vkomap.kz/web/ (дата обращения 05.12.2022). – Режим доступа : общий доступ.
11. Open Street Map – картографическая основа» – [Электронный ресурс] // https://www.openstreetmap.org/ : [сайт]. – URL: https://www.openstreetmap.org/ (дата обращения 05.12.2022). – Режим доступа : общий доступ.

УДК 339.1
DOI 10.33764/2618-981X-2023-6-77-84

А. А. Каминский[1], М. И. Ананич[1]*

Анализ трендов рынков аддитивных технологий

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
*e-mail: sashoven000@mail.ru

Аннотация. Данная статья посвящена анализу трендов рынка аддитивных технологий. В статье приведены последние тенденции на рынке аддитивных технологий. Аддитивные технологии, также известные как 3D печать, являются одним из наиболее перспективных направлений в современной промышленности. Они позволяют создавать сложные детали и конструкции, которые трудно или невозможно произвести с помощью традиционных методов производства. Это открывает новые возможности для индивидуального проектирования и изготовления изделий, а также ускоряет процесс разработки и сокращает расходы на создание прототипов. Аддитивные технологии – это изготовление детали с послойным наложением материала друг на друга. Целью научной статьи является выявление современных трендов в сфере аддитивных технологий, а также рассмотрение рынка аддитивных технологий стран, потенциальных конкурентов российским компаниям на отечественном рынке, на наличие следования трендам. Проблемой научной статьи является отсутствие знаний и непонимание современных трендов. В научной статье был проведен анализ трендов на основе исследований тренд-хантеров 2022-2023 годов. Были выявлены следующие тренды: новые материалы; экологичность; новые технологии; доступность аддитивных технологий; комбинаторность; новые области применения; новый взгляд производства на 3D принтеры.

Ключевые слова: аддитивные технологии, 3D печать, тренды

A. A. Kaminskiy[1], M. I. Ananich[1]*

Analysis of Trends in the Markets of Additive Technologies

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: sashoven000@mail.ru

Abstract. This article is devoted to the analysis of additive technologies market trends. The article presents the latest trends in the market of additive technologies. Additive technologies, also known as 3D printing, are one of the most promising areas in modern industry. They allow you to create complex parts and designs that are difficult or impossible to produce using traditional manufacturing methods. This opens up new opportunities for custom design and manufacturing, as well as speeding up the development process and reducing prototyping costs. Additive technologies are the production of a part with a layer-by-layer imposition of material on top of each other. The purpose of the scientific article is to identify modern trends in the field of additive technologies, as well as to consider the market of additive technologies in countries that are potential competitors to Russian companies in the domestic market, for the presence of trend following. The problem of a scientific article is the lack of knowledge and misunderstanding of modern trends. In a scientific article, a trend analysis was carried out based on the research of trend hunters in 2022-2023. The following trends were identified: new materials; environmental friendliness; new technologies; availability of additive technologies; combinatoriality; new areas of application; a new look at 3D printer manufacturing.

Keywords: additive technologies, 3D printing, trends

Введение

Развитие прорывных технологий представляется промышленными революциями, в которых катализатором изменений жизненных укладов становится новый вид энергии (паровая, электрическая, атомная) или новые производственные технологии (цифровые двойники, аддитивные технологии, робототехника). Такие инновации не только сильно влияют на экономику и промышленность, но и изменяют нашу жизнь и повседневные привычки. Например, промышленная революция, связанная с электрической энергией, позволила людям работать в ночное время, улучшить условия жизни и сократить время производства товаров. Сегодня же, благодаря цифровым технологиям и Интернету, мы можем получать доступ к информации и связи практически из любой точки мира, а робототехника помогает автоматизировать многие производственные процессы, что позволяет повысить эффективность и снизить издержки. Аддитивные технологии, также известные как 3D печать, являются одним из наиболее перспективных направлений в современной промышленности. Они позволяют создавать сложные детали и конструкции, которые трудно или невозможно произвести с помощью традиционных методов производства. Это открывает новые возможности для индивидуального проектирования и изготовления изделий, а также ускоряет процесс разработки и сокращает расходы на создание прототипов. Аддитивные технологии – это изготовление детали с послойным наложением материала друг на друга. Также аддитивные технологии представляют из себя 3D моделирование, 3D проектирование и программирование в этой области. На западе, слова «additive technologies» и «3D printing» часто используются как синонимы, поскольку 3D печать и есть аддитивная технология. 3D печать осуществляют 3D принтеры, которые с помощью подвижных экструдеров способны изготавливать детали из различных материалов, в частности, из различных видов пластмассы. Но ничего не стоит на месте, времена меняются. Так, раньше тяжело было представить, что 3D принтер будет способен изготавливать деталь сразу из нескольких материалов одновременно, как например 5D принтеры компании ООО «Stereotech», которые к тому же российского производства. Поэтому, при создании 3D принтеров, да и в принципе любой продукции, очень важно следить за современными трендами отрасли.

Целью научной статьи является выявление современных трендов в сфере аддитивных технологий, а также рассмотрение рынка аддитивных технологий стран, потенциальных конкурентов российским компаниям на отечественном рынке, на наличие следования трендам. Проблемой научной статьи является отсутствие знаний и непонимание современных трендов компаниями в секторе 3D печати.

Материалы

Для проведения анализа трендов на рынке аддитивных технологий были использованы исследования тренд-хантеров, в частности платформа Trend-Hunter: Create The Future, которая проводит исследования по запросам пользователей са-

мых популярных поисковых систем, а также с помощью собственного искусственного интеллекта, которые был разработан еще в 2005 году [1].

Выявление трендов рынков аддитивных технологий

Для выявления трендов аддитивных технологий необходимо обратиться к исследователям данной сферы. Тренды исследуют и формируют тренд-хантеры, или же тренд-вочер. Они проводят исследования рынка, компаний, мировой экономики, данные поисковых запросов и множества других факторов. В научной статье был проведен анализ трендов на основе исследований тренд-хантеров 2022-2023 годов [1]. Проведя анализ, можно обозначить следующие тренды в сфере аддитивных технологий:

– изменения используемых материалов и их количество на одну деталь. Появляются новые материалы, из которых возможно изготовить новые виды деталей (например, полимерная печать). Стало возможным использовать сразу несколько материалов при изготовлении деталей [2];

– экологичность. В 2020 году стал набирать популярность тренд на экологию, который включает в себя экологически чистые продукты, производство, «безотходные» материалы и многое другое. Тренд задел почти все отрасли мира, в том числе и аддитивные технологии. Компании, которые занимаются производством оборудования с использованием аддитивных технологий, начали сокращать транспортные издержки, использовать более безопасные, и с меньшим количеством отходов, материалы. Также, при изготовлении деталей стали применяться биоразлагаемые материалы [2];

– совершенствование технологий. Развитие технологий тоже не стоит на месте. Современное программное обеспечение для управления 3D принтером, в большинстве своих случаях, имеет понятный и простой в использовании интерфейс, некоторые даже обладают мультиплатформой. Технологический прогресс позволил 3D принтерам принимать различные формы и дизайн [3];

– доступность аддитивных технологий. Широкое распространение 3D принтеры во всем мире получили после окончания патента на технологию FDM в 2010 году. Технология стала более доступной для обычного пользователя в виде частного лица, а не компании. Сейчас средняя цена бюджетного 3D принтера составляется около 20 тысяч рублей на российском рынке. Сократилось общее время на постобработку (определение, какие характеристики определить для детали) [3];

– кобминаторность. К современным 3D создаются дополнительные элементы, которые идут отдельно и выполняют ту или иную функцию. Комбинаторность проявляется не только в сочетании 3D принтера и дополнительного элемента, но и в сочетании с такими же 3D принтерами. Таким образом появились линейки из 3D принтеров, которые способны одновременно изготавливать одинаковые или же напротив, разные детали. Посредством использования таких линеек стали образовывать 3D-фабрики [4];

– расширение области применения. 3D принтер используется в медицинской сфере, сфере науки и образования, производстве и прототипировании, в ар-

хитектуре и строительстве, в производстве пищевых продуктов и в других отраслях. В будущем планируется внедрить 3D принтеры на производство микроэлектроники [4];

– тренды развития аддитивных технологий в России. Отдельный тренд аддитивных технологий можно выделить для России. Поскольку множество компаний, которые занимались поставками 3D принтеров в Россию, и занимали рыночные ниши, ушли, в связи с санкциями, сработала причинно-следственная связь, это в свою очередь вызвало потребность в создании собственных компаний по производству 3D принтеров. Также 3D принтеры в какой-то степени смогут обеспечить импортозамещение подсанкционных товаров [5];

– рост производства с использованием аддитивных технологий. Множество компаний, от крупных до малых, разглядели выгоду в 3D принтерах. Так, один принтер на предприятии способен частично решить задачу замены деталей, станков или другого оборудования [5];

– помимо всего вышеперечисленного, рынку необходимы инновации в сфере аддитивных технологий. В данный момент этот тренд сильно прослеживается в России, по большей части из-за «повестки дня». Правительство выделяет субсидии из государственного бюджета на развитие технологии [6]. За последние годы в России появилось много компаний, занимающихся созданием 3D принтеров. Каждая компания желает занять свою долю на отечественном рынке. В современных реалиях это вполне возможно, так как западные «мастодонты рынка» аддитивных технологий его покинули. По данным исследовательской компании Grand View Research, к 2025 году рынок 3D-печати в России должен достичь 25,2 миллиарда рублей, с ростом в годовом исчислении на 27,6% [7]. В России аддитивные технологии навиваются очень активно, есть прорывные решения, например, 5D принтеры (компании Stereotech), преимуществами которого является большее качество за меньшую цену. При этом качество деталей улучшается не только за счет многоосевой печати, но и за счет использования углеродной нити в процессе печати. Снижение цены обеспечивается отсутствием подложки и направляющих для печати. Особенностью продвижения в компании Stereotech является наличие собственного программного обеспечения, позволяющего создавать цифровые двойники деталей и формировать их в библиотеки. Также важно вовлечение в процессы аддитивных технологий школьников и студентов. За российский рынок аддитивных технологий также могут потягаться производители 3D принтеров из СНГ и Азии [8]. Чтобы понять, способны ли российские производители конкурировать с производителями СНГ или Азии, необходимо провести анализ рынка этих стран. Из стран СНГ будут проанализированы рынки Казахстана и Беларуси, а из Азии – Китай.

Анализ некоторых трендов развития аддитивных технологий на рынках Казахстана, Беларуси и Китая

Рассмотрим рынок аддитивных технологий Казахстана. В первую очередь хочется обратить внимание на нежелание государства финансировать данную отрасль, несмотря на то, что вопрос стоит также остро, как и в России [9]. Множества

западных экспортеров 3D принтеров поставляли свои принтеры через Россию, но в связи с положением в мире, они это делать перестали. Из-за невозможности поставлять 3D принтеры многие покинули казахстанский рынок. Другие изменили логистику поставок, тем самым увеличили стоимость своей продукции. Это хороший шанс, чтобы начать развивать собственное производство 3D принтеров и занять рынок, несмотря на такого крупного конкурента как Китай. Китай является монополистом на рынке среди бюджетных 3D принтеров [10]. Такие принтеры рассчитаны под простые задачи. Например, они не подойдут под печать запчастей для станков или оборудования, или же для медицинской сферы [11].

Последняя попытка Казахстана в развитии аддитивных технологий была в 2017 году, когда АО «НАТР» (ныне «QazTech Ventures») проинвестировали компанию ТОО (ТОО – Товарищество с ограниченной ответственностью) «3DInnovations» на 4,3 млн. тенге, что по нынешнему курсу рубля (1 рубль = 5,50 тенге, на 15 апреля 2023 г.) эквивалентно 781820 рублям [12]. Данный бюджет очень мал для тех лет. Компания разрабатывала свой принтер на основе российского стартапа «Кипарис» и посещала выставку в «Сколково» 2017 года, касательно 3D принтеров. Многие схемы и комплектующие были выкуплены у российской компании по производству 3D принтеров ООО «PICASO 3D», которые являются одними из лидеров по производству 3D принтеров в России. Несмотря на все это, компания потерпела крах в создании собственных 3D принтеров, так и не выпустив свою разработку на рынок. Одной из главных причин краха продукта компании стала нехватка квалифицированных кадров [12].

В Беларуси же ситуация иная. О развитии аддитивных технологий начали активно говорить уже в 2014 году. Главным центром в области аддитивных технологий в Беларуси является Национальная академия наук Беларуси, которая возглавляет исследования и разработки в этой области [14]. Академия создала несколько исследовательских центров и лабораторий, занимающихся развитием аддитивного производства, уделяя особое внимание исследованию материалов, оптимизации процессов и разработке приложений [13].

Правительство по сей день уделяет много внимания развитию аддитивных технологий в стране, предоставляет гранты и субсидии. В Беларуси были созданы принтеры следующими компаниями: компания TTF Group – принтер M3 Duo, компания Z-Bolt и 3D принтеры с таким же названием. Несмотря на то, что эти 3D принтеры достаточно посредственные для современного времени, они могут послужить конкурентами китайским бюджетным 3D принтерам. Также созданная в России 3D-Fab фабрика с 3D принтерами, была частично перенесена в Беларусь. Она занимается печатью литейных форм и 3D моделированием [14]. В январе 2023 г. проходила выставка «Беларусь интеллектуальная», на которой был представлен 3D принтер, который способен печатать пищевую продукцию, в качестве примера было напечатано мясо. Новостей о том, что авторы 3D принтера собираются вывести его на рынок пока нет. Россия в области аддитивных технологий находится на ступень выше, чем Беларусь. Причиной тому является более ранний заход России на рынок аддитивных технологий и большее количе-

ство инвестиций. Сильным толчком к развитию также послужили санкции, которые затрагивают каждую отрасль страны [14].

Последние десять лет в Китае стремительно развивались аддитивные технологии. Китай стал мировым лидером в области аддитивного производства со значительными достижениями в различных отраслях, включая аэрокосмическую и автомобильную сферу, здравоохранение, потребительские товары и многое другое. Правительство Китая также активно поддерживает развитие аддитивных технологий посредством политических стимулов, финансирования и исследовательских инициатив [15]. Китайское правительство уделяет первостепенное внимание технологическим достижениям, включая аддитивное производство в рамках своей стратегии «Сделано в Китае 2025», целью которой является превращение страны в глобальный центр высокотехнологичного производства. Правительство Китая активно поддерживает развитие аддитивных технологий с помощью различных политических мер [15]. Например, оно создало инновационные центры аддитивного производства, научно-исследовательские институты и промышленные парки для развития сотрудничества и инноваций. Китай в данный момент является одним из главных конкурентов на российском рынке. В основном это бюджетные версии, но также есть и принтеры «премиум» класса, например, принтеры фирмы Raise3D. В дальнейшем Китай может перестать поставлять те или иные 3D принтеры из-за давления со стороны западных стран с помощью санкций [15].

Также компаниям, занимающимся аддитивными технологиями, стоит помнить про кадры. Недостаток кадров сильно сказывается на развитие данной сферы. В качестве примера можно рассмотреть Казахстан, где недостаток кадров погубил всю сферу. В наборе кадров помогают специальные программы по их формированию, которые в нынешнее время практикуются в школах и вузах. Плюсом таких программ является ранее ознакомление будущих кадров с аддитивными технологиями. Поскольку огромной проблемой является отсутствие знаний у нынешних специалистов. Такие программы обучают школьников и студентов:

- созданию прототипов и впоследствии их печать на 3D принтерах;
- работе с специализированным ПО и обучению базовым принципам;
- работе с материалами для печати.

Также проводятся олимпиады по программированию, связанные с аддитивными технологиями. Участники могут создавать программы для управления 3D принтером, а также для моделирования и обработки данных для печати. Такая олимпиада поможет развить навыки программирования и подготовить кадры, способные работать в области аддитивных технологий. Проведение олимпиад может стимулировать интерес школьников к аддитивным технологиям, помочь им понять принципы работы и применение 3D-печати, а также мотивировать на дальнейшее изучение этой области.

Следует отметить, что для успешного проведения таких олимпиад необходима квалифицированная команда организаторов, включающая специалистов в

области 3D-печати, программирования и образования. Также нужны спонсоры, которые могут обеспечить финансовую поддержку проведения олимпиад и предоставить оборудование для участников.

Одним из форматов обучения является наставничество, когда опытные специалисты компании Stereotech работают с учащимися, помогая им освоить основы работы с 3D принтерами и создавать свои проекты. Формат наставничества предполагает индивидуальный подход к каждому ученику и его потребностям. Наставники помогают школьникам понять основные принципы работы с оборудованием для 3D печати, научиться использовать специальное программное обеспечение для создания моделей и подбирают задания, соответствующие возрасту и уровню подготовки каждого ученика.

Stereotech не только организует олимпиады и мастер-классы, но также проводит исследования и разработки в области аддитивных технологий, разрабатывает и производит свое собственное оборудование для 3D печати.

Компания Stereotech также активно сотрудничает с университетами и другими образовательными учреждениями, чтобы создать программы обучения для студентов, которые заинтересованы в изучении аддитивных технологий. Эти программы позволяют студентам получить глубокие знания в этой области и получить необходимый опыт работы с современным оборудованием, что является важным фактором для будущей карьеры в этой отрасли. Олимпиады и другие мероприятия, организуемые компанией Stereotech, помогают привлечь внимание учащихся к этой области и подготовить их к будущей карьере. Такие усилия содействуют развитию отрасли аддитивных технологий в России и создают новые возможности для развития экономики страны.

Заключение

Исходя из трендов рынка и проведенного анализа рынка аддитивных технологий Казахстана, Беларуси и Китая, можно сделать вывод, что российские производители способны конкурировать с ними и занять отечественный рынок практически полностью. К таким компаниям, которые соответствуют трендам рынка аддитивных технологий, можно отнести «Stereotech», «Total Z», «Импримта», «PICASO 3D» и другие.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Платформа Trend-Hunter. Текст : электронный. – URL: https://www.trendhunter.com/results?search=3D+printing (дата обращения 15.04.2023).

2. Статья Startus Insights. Тренды аддитивных технологий в 2023 году. Текст : электронный. – URL: https://www.startus-insights.com/innovators-guide/additive-manufacturing-trends/ (дата обращения 15.04.2023).

3. Статья Autonomous Manufacturing. 4 важные тенденции в сфере аддитивных технологий – 2022 год. Текст : электронный. – URL: https://amfg.ai/2022/10/25/the-top-4-trends-in-additive-manufacturing-2022/ (дата обращения 15.04.2023).

4. Статья TctMagazine. Тенденции аддитивного производства и 3D-печати в 2022 году. Текст : электронный. – URL: https://www.tctmagazine.com/additive-manufacturing-3d-printing-industry-insights/latest-additive-manufacturing-3d-printing-industry-insights/trends-additive-manufacturing-3d-printing-2022-beyond/ (дата обращения 15.04.2023).

5. Статья EOS. 5 важных тенденций промышленной 3D-печати в 2023 году. Текст : электронный. – URL: https://www.eos.info/en/blog/additive-manufacturing-trends-2023~b~11532 (дата обращения 15.04.2023).

6. Гэри С., Давид Р. Технологии аддитивного производства. – 3-е изд. / С. Гэри, Р. Давид, 2021. – 150-153 с - Текст: непосредственный.

7. Статья Grand View Research. Текст : электронный. – URL: https://www.grandviewresearch.com/industry-analysis/healthcare-additive-manufacturing-market (дата обращения 15.04.2023).

8. Гэри С., Джон С. 3D–сканирование для передового производства, проектирования и строительства / Гэри С., Джон С., 2023. - 112-115 с - Текст: непосредственный.

9. Ханг З. Аддитивное фрикционное соединение материалов / З. Ханг., 2022. - 52-55 с - Текст: непосредственный.

10. Гибсон Я. Технологии аддитивного производства. Трехмерная печать, быстрое прототипирование и прямое цифровое производство / Я. Гибсон, Д. Розен, 2020. - 39-42 с - Текст: непосредственный.

11. Голубев И. Перспективное применение аддитивных технологий // И. Голубев, 2022. - 102-110 с - Текст: непосредственный.

12. Мухамадеева Р. М. Аддитивные технологии в Казахстане / Р. М. Мухамадеева, 2016. – 1-8 с - Текст: непосредственный.

13. Малевич Д. М. Перспективы развития аддитивных технологий в Республике Беларусь / Д. М. Малевич, 2018. - 10-19 с - Текст: непосредственный.

14. Толочко Н. К. Аддитивные технологии в Беларуси: как все начиналось / Н. К. Толочко, 2014. - 6-7 с - Текст: непосредственный.

15. Чен Л. Цифровая эра: Революция аддитивных технологий / Л. Чен, 2022. - 198-202 с - Текст: непосредственный.

УДК 528.9
DOI 10.33764/2618-981X-2023-6-85-92

*Э. В. Кандаурова[1] *, С. Ю. Кацко[1], И. П. Кокорина[2]*

Геоинформационное картографирование угольных месторождений Кемеровской области

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Институт систематики и экологии животных СО РАН, г. Новосибирск, Российская Федерация
* e-mail: s.katsko@ssga.ru

Аннотация. Статья посвящена разработке геоинформационной системы для анализа запасов и прогнозных ресурсов угля в Кемеровской области. Одной из главных проблем, рассмотренных в исследовании, является отсутствие тематических карт и ГИС угольных разрезов на территории регионаВ статье подробно описываются этапы работы с данными и обработки картографической информации, такие как выбор космических снимков, тематическое дешифрирование угольных разрезов и шахт, определение масштабного ряда проекта, создание общегеографической основы ГИС, создание атрибутивной таблицы тематических слоев. Результатом работы является ГИС запасов и прогнозных ресурсов угля Кемеровской области, которая может быть использована для проведения исследований и решения производственных задач в сфере добычи угля.

Ключевые слова: геоинформационное картографирование, автоматизированное дешифрирование, полезные ископаемые

*E. V. Kandaurova[1] *, S. Yu. Katsko[1]*, I. P. Kokorina[2]*

Geoinformation Support for the Coal Industry of the Kemerovo Region

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Institute of Systematics and Ecology of Animals, Novosibirsk, Russian Federation
*e-mail: s.katsko@ssga.ru

Abstract. The article is devoted to the development of a geographic information system for analyzing coal reserves and forecasted resources in the Kemerovo region. One of the main issues addressed in the study is the lack of thematic maps and GIS of coal deposits in the region. The article provides a detailed description of the stages of data processing and cartographic information, such as selection of satellite images, thematic deciphering of coal seams and mines, determination of the project's scale range, creation of the general geographic basis of GIS, and creation of the attribute table of thematic layers. The result of the work is a GIS of coal reserves and forecasted resources in the Kemerovo region, which can be used for research and solving production tasks in the coal mining industry.

Keywords: geoinformation mapping, automated interpretation, minerals

Введение

Разработка и создание геоинформационных систем, как основы для исследований и решения производственных задач, является актуальным научным вопросом, поэтому целью работы выбрано создание ГИС запасов и прогнозных ресурсов угля Кемеровской области.

Проблема, с которой связано исследование, заключается в том, что на данный момент в общем доступе отсутствуют географические карты и ГИС разрезов и шахт на территорию Кемеровской области, отсутствует технология дешифрирования нарушенных земель в результате добычи полезных ископаемых. Для достижения этой цели необходимо решить следующие задачи:

– выбрать космические снимки;
– выполнить тематическое дешифрирование угольных разрезов и шахт;
– определить масштабный ряд проекта;
– создать общегеографическую основу ГИС;
– создать атрибутивную таблицу тематических слоев.

Методы и материалы

Россия на 2022 год занимает лидирующее положение по величине запасов природного газа в мире, четвертое место по величине запасов угля и шестое по величине запасов нефти. Большие объемы производства требуют ведения эффективной статистической работы и обработки информации, поэтому основное внимание на горнодобывающих производствах уделяют созданию и ведению ГИС, позволяющих собирать, хранить, анализировать данные о запасах и прогнозных ресурсах полезных ископаемых [1–3].

Технологии космического мониторинга позволяют эффективно отслеживать различные аспекты промышленности. Аэрокосмическая информация, как правило, представляется в виде данных со спутников дистанционного зондирования Земли (ДЗЗ). За последнее время было запущено множество таких спутников, наиболее примечательными и известными из которых являются спутники миссий Landsat и Sentinel. Данные спутники обладают высококачественной съемочной аппаратурой и высокоточными сенсорами, способными улавливать изменения в видимом и инфракрасном спектре длин волн.

Анализ аэрокосмической информации дает возможность создавать электронные карты местности с учетом актуальных изменений на исследуемых территориях, что, в совокупности с цифровыми моделями рельефа (ЦМР), картографической и атрибутивной информацией, обеспечит мониторинг, оценку динамики и прогнозирование состояния объекта в целом [4].

Кузнецкий угольный бассейн – один из крупнейших угледобывающих районов в России, находящийся на территории Кемеровской области и частично на территориях Новосибирской области и Алтайского края. В 20-х годах XX века он стал энергетической базой СССР. В 2022 году общий объем экспорта угля из региона составил 230 млн. тонн, из них в страны Евросоюза было отгружено 36,3 млн. тонн (около 29 %) [5].

В административном плане Кузбасс почти полностью расположен в пределах Кемеровской области, за исключением Завьяловского и Доронинского районов (Новосибирская область), удельный вес которых по добыче угля невелик. Площадь бассейна составляет 26,7 тыс. км^2.

Общегеологические запасы углей до глубины 1 600 м оценены более чем в 700 млрд т, из них пригодных для коксования – 270 млрд. т (для сравнения: за-

пасы коксующихся углей в Донецком бассейне – 25 млрд. т, в Печорском бассейне – 9 млрд. т).

По данным министерства угольной промышленности Кузбасса, на 01.01.2022 г. в Кузбассе работает 152 угледобывающих и перерабатывающих предприятия:

– 58 шахт;

– 36 разрезов;

– 56 обогатительных фабрик и установок.

По количеству месторождений в собственности лидируют предприятия: АО «СУЭК-Кузбасс», ПАО «Кузбасская Топливная Компания» и АО «УК Кузбассразрезуголь». На их долю приходится 62 % всех месторождений. Также в этой отрасли работают такие предприятия, как АО «САЛЕК», ООО «Разрез Кийзасский», АО «Шахта Заречная», ОАО «Междуречье», ООО «Ресурс» [6].

На начальном этапе работы создания ГИС запасов и прогнозных ресурсов Кемеровской области происходит сбор исходных картографических и статистических данных, определяется масштабный ряд проекта. Также требуется определить структуру и содержание базы данных ГИС.

Для ГИС запасов и прогнозных ресурсов угля Кемеровской области выбраны уровни масштабного ряда: 1:10 000–1:100 000, 1:100 000–1:300 000, 1:300 000–1:1 000 000. Структура базы данных проектируемой ГИС представлена в табл. 1.

Таблица 1

Структура базы данных проектируемой ГИС

Слои	Название слоя	Тип локализации	Название полей слоя
Гидрография	Гидрография линейная	Линейный	Название Тип
	Гидрография площадная	Площадной	Название Тип
Населенные пункты	Населенные пункты	Точечный	Название Тип Численность населения
	Городские округа	Площадной	Название Площадь
Пути сообщения	Автомобильные дороги местного значения	Линейный	Название Тип
	Автомобильные трассы федерального значения	Линейный	Название Тип
	Железные дороги	Линейный	Название Тип
Границы	Граница Кемеровской области	Линейный	Тип
	Границы административных районов	Линейный	Тип

Слои	Название слоя	Тип локализации	Название полей слоя
Разрезы	Разрезы	Площадной	Название Предприятие Обеспеченность балансовыми запасами (лет) Добыча в год (млн т)
Шахты	Шахты	Площадной	Название Предприятие Обеспеченность балансовыми запасами (лет) Добыча в год (млн т)
Рельеф	Снимки SRTM в формате GeoTIFF с разрешением 90 метров		

Данные об угледобывающих предприятиях должны содержать актуальную информацию о предприятии, его собственнике, марке добываемого угля, балансовых запасах и о годовом объеме добычи. Общее количество тематических объектов: 26 разрезов, 18 шахт. Фрагмент базы данных тематического слоя ГИС отображен на рис. 1.

	Название	Способ добычи	Марки угля	Балансовые запасы	Объем добычи	Собственник предприятия
1	Заречный угольный разрез	Открытый	ДГ	80,000	1,600	СУЭК Кузбасс
2	Первомайский угольный разрез	Открытый	Д	520,000	15,000	СДС-Уголь
3	Черниговский угольный разрез	Открытый	Д	220,000	9,000	СДС-Уголь
4	ОАО "Шахта Ольжерасская-Новая"	Подземный	ГЖО	210,000	1,800	ОАО «Южный Кузбасс»
5	Краснобродский угольный разрез	Открытый	Т, СС, КС, КО,1	336,874	9,000	ОАО «УК «КУЗБАССРАЗРЕЗУГОЛЬ»
6	Калтанский угольный разрез	Открытый	Т	166,500	3,500	ОАО «УК «КУЗБАССРАЗРЕЗУГОЛЬ»
7	Кедровский угольный разрез	Открытый	СС	70,000	3,000	ОАО «УК «КУЗБАССРАЗРЕЗУГОЛЬ»
8	Моховский угольный разрез	Открытый	Д	41,408	7,000	ОАО «УК «КУЗБАССРАЗРЕЗУГОЛЬ»
9	Талдинский угольный разрез	Открытый	Д	336,874	9,000	ОАО «УК «КУЗБАССРАЗРЕЗУГОЛЬ»
10	Сибиргинская шахта	Подземный	ОС	65,000	1,200	ОАО "Южный Кузбасс"

Рис. 1. Фрагмент базы данных тематического слоя ГИС

Рассмотрим марки угля на рисунке. Они подразделяются на основные и промежуточные. К основным относятся бурые (Б), длиннопламенные (Д), газовые (Г), жирные (Ж), коксовые (К), отощенно-спекающиеся (ОС), тощие (Т), антрациты (А), к промежуточным – газовые жирные (ГЖ), коксовые жирные (КЖ), коксовые вторые (К2), слабоспекающиеся (СС).

На территории Кемеровской области преимущественно добывается уголь марок Г, Д, Ж, ГЖ [7].

На следующем этапе создания ГИС производится дешифрирование разрезов и шахт на спутниковых снимках и их векторизация.

В качестве источника данных были выбраны космические снимки со спутника Landsat 8, расположенные на сайте USGS. Основным критерием отбора служил процент покрытия территории облаками, равный 20 %.

Для получения снимка в естественных цветах была применена комбинация каналов 5-4-3 данных Landsat 8 [8].

Метод классификации – это процесс автоматизированного подразделения всех пикселов снимка на группы (классы) с использованием кластерного анализа. Существует два вида классификаций: классификация без обучения и классификация с обучением.

Классификации без обучения – распределение пикселов изображения происходит автоматически, на основе анализа статистического распределения яркости пикселов. При классификации с обучением происходит сравнение значения яркости каждого пиксела с эталонами, в результате чего каждый пиксел относится к наиболее подходящему классу объектов. При выборе любого из способов, изображения автоматически разделяются на классы.

Независимо от того, какой способ выбран для решения задач дешифрирования, автоматическая классификация включает несколько этапов.

При работе выбран способ классификации с обучением. Первый этап заключается в определении, какие классы объектов будут выделены в результате выполнения всей процедуры. Как правило, выделяют виды растительности, сельскохозяйственные культуры, породы леса, гидрографические объекты и т. д.

На втором этапе для каждого из классов объектов выбираются типичные для него пикселы, то есть формируется обучающая выборка. Обязательным условием выполнения этой процедуры является наличие на снимке эталонов, т.е. фрагментов изображения, однозначно относящихся к своему классу объектов. Процедура создания обучающей выборки реализуется выбором в пределах изображения эталонного объекта участков в несколько пикселов.

Третий этап – вычисление параметров, спектрального образа каждого из классов, сформированного в результате набора эталонных пикселов. Набор параметров зависит от алгоритма, который предполагается использовать для классификации [9–11].

Для дешифрирования и векторизации разрезов на снимке использовался метод автоматизированного дешифрирования алгоритмом управляемой классификации Maximum Likelihood в программе Erdas Imagine 2015. Этот метод показал себя наиболее информативным по сравнению с другими, представленными в программе. При Maximum Likelihood не захватывались большие площади пикселов. Для проведения классификации были созданы объекты интересов дешифрирования, содержащие спектральные характеристики объектов. Задавая их, определяется, какие объекты нужно выделить в отдельные классы. Объекты интересов представлены на рис. 2 [12].

Class #	>	Signature Name	Color	Red	Green	Blue	Value	Order	Count	Prob.	P	I	H	A	FS
1	▶	Coal		0.407	0.035	0.589	8	8	40703	1.000	✔	✔	✔	✔	
2		Forest		0.667	0.788	0.707	1	9	9219	1.000	✔	✔	✔	✔	
3		Fields 1		0.707	0.167	0.604	2	10	2006	1.000	✔	✔	✔	✔	
4		River		0.000	0.000	0.128	3	11	1010	1.000	✔	✔	✔	✔	
5		Fields 2		0.939	0.642	0.914	4	12	9949	1.000	✔	✔	✔	✔	
6		Fields 3		0.950	0.639	0.889	5	13	13614	1.000	✔	✔	✔	✔	
7		Fields 4		0.585	0.048	0.436	6	14	2053	1.000	✔	✔	✔	✔	

Рис. 2. Объекты интересов

После формирования обучающей выборки, получен результат дешифрирования в растровом виде. На следующем этапе проводилась его векторизация в программе QGIS, результат которой представлен на рис. 3.

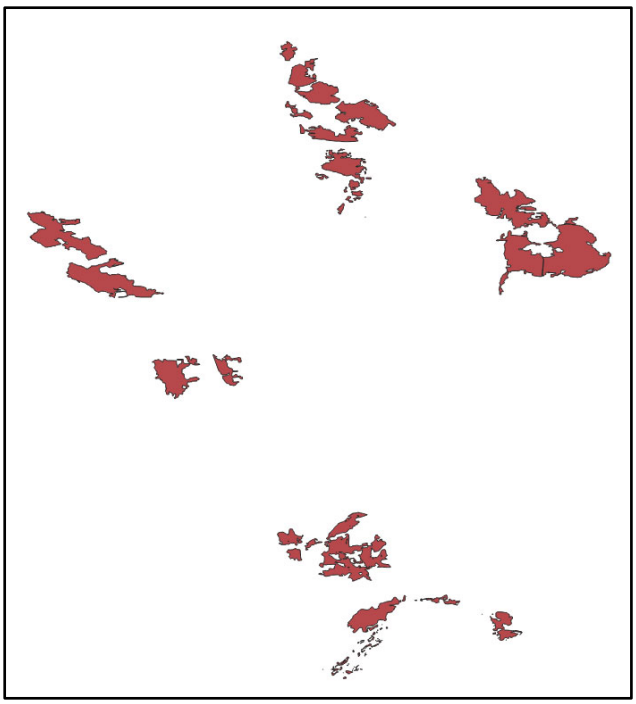


Рис. 3. Угольные разрезы и шахты, векторизованные в программе QGIS

Непосредственная обработка картографической информации происходит на основном этапе технологического процесса. Она включает в себя: определение масштабного ряда проекта, от которого будет зависеть изменение детальности изображения при переходах между масштабными уровнями; генерализацию исходных данных, чтобы обозначить степень детализации того или иного масштабного уровня; оформление, определяющее стили отображения данных; выбор условных знаков; правила подписывания картографических объектов. На заключительном этапе создания картографического сервиса осуществляется контроль результатов путем проверки слоев на корректность отображения, а также формирование рабочего набора, предназначенного для использования в геосервисах [13–15].

Результаты

Результаты работ по созданию геоинформационной системы запасов и прогнозных ресурсов угля Кемеровской области:

– выбраны космические снимки со спутника Landsat 8 с сайта USGS;
– выполнено тематическое дешифрирование угольных разрезов и шахт;
– определен масштабный ряд проекта;
– создана общегеографическая основа ГИС;
– создана атрибутивная таблица тематических слоев.

Результат работы представлен на рис. 4.

Рис. 4. ГИС запасов и прогнозных ресурсов угля Кемеровской области

Заключение

В ходе работы собрана информация о разрезах и шахтах Кемеровской области, описан порядок работ при дешифрировании нарушенных земель. Используя эти данные была создана мультимасштабная картографическая основа, на основе которой будет создан геопортал «Горнодобывающая промышленность Кемеровской области».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Лурье И. К. Геоинформационное картографирование: Учебник для вузов. – М.: Издательство КДУ, 2008. - 424 с.

2. Ковальчук А. К. Основы геоинформационных систем. – М.: Издательство «Рудомино», 2009. – 206 с.

3. Берлянт А. М. Геоинформационное картографирование. – М.: Наука, 1997. – 64 с.

4. Чадра А. М., Гош С. К. Дистанционное зондирование и географические информационные системы: учебник для вузов. – М.: Техносфера, 2008. – 312 с.

5. Звонарев И. Н., Сидоренко А. В., Староверов Л. Д., Фомичев В. Д. Геология СССР. Т. 14. Западная Сибирь (Алтайский край, Кемерово, Новосибирская, Омская и Томская области). Ч. 1. Геологическое описание. – М.: Недра, 1967. – 664 с.

6. Справка о состоянии и перспективах использования минерально-сырьевой базы Кемеровской области – Кузбасса на 01.09.2022 г. – ФГБУ «ВСЕГЕИ», 2022. – 15 с.

7. Ольховатенко В. Е. Инженерная геология угольных месторождений Кузнецкого бассейна: монография. – Томск : Издательство Томского архитектурно-строительного университета, 2014. – 150 с.

8. Керимов И. А., Эзирбаев Т. Б. Использование мультиспектральной съемки при наблюдении за состоянием лесного покрова Земли // Геология и геофизика Юга России. – 2022. – Т. 12. – № 3. – С. 182-194.

9. Шихов А. Н., Герасимов А. П., Пономарчук А. И., Перминова Е. С. Тематическое дешифрирование и интерпретация космических снимков среднего и высокого пространственного разрешения: учебное пособие. – Пермь, 2020. – 191 с.

10. Бузина Д. А., Коновалов В. Е., Рыбникова Л. С., Рыбников П. А. Особенности дешифрирования объектов горнопромышленных территорий на аэрофотоснимках и космических снимках // Агротехнологии XXI века: стратегия развития, технологии и инновации: Материалы Всероссийской научно-практической конференции, Пермь, 16–18 ноября 2021 года / Федеральное государственное бюджетное образовательное учреждение высшего образования «Пермский государственный аграрно-технологический университет имени академика Д. Н. Прянишникова». – Пермь: ИПЦ Прокростъ, 2021. – С. 349-353.

11. Новикова И. О. Современные программные комплексы и технологии для обработки данных ДЗЗ и создания тематических геопорталов // Гео-Сибирь. – 2009. – Т. 4. – № 1. – С. 57-59.

12. Попов И. П., Левитская Т. И., Радченко Т. А. Обработка спутниковых снимков в программном комплексе envi для мониторинга состояния растительного покрова // – Екатеринбург : Издательство Уральского университета, 2022. — С. 147-150.

13. Карпик А. П. Методологические и технологические основы геоинформационного обеспечения территорий: Монография. – Новосибирск: СГГА, 2004. – 260 с.

14. Гуров А. А., Осипов С. В., Ивакина Е. В. Ландшафтное картографирование горнопромышленных территорий и их природного окружения / // Вестник Воронежского государственного университета. Серия: География. Геоэкология. – 2022. – № 2. – С. 47-59.

15. Лубнин Д. С. Геопорталы и современные отечественные средства их создания // Приложение к журналу Известия вузов. Геодезия и аэрофотосъемка. Сборник статей по итогам научно-технической конференции. – 2010. – № 3. – С. 98-102.

УДК 528.9
DOI 10.33764/2618-981X-2023-6-93-97

М. А. Карасюк[1], С. Ю. Кацко[1], И. П. Кокорина[2]*

Геоинформационное обеспечение геологического исследования Курганской области

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Институт систематики и экологии животных СО РАН, г. Новосибирск, Российская Федерация
* e-mail: s.katsko@ssga.ru

Аннотация. В статье рассматривается использование геоинформационных систем в геологических исследованиях на примере создания карты общей минерализации подземных вод для цифрового эколого-географического атласа Курганской области. Авторы описывают проблему отсутствия в открытом доступе геоинформационных систем геологического профиля и предлагают разработать цифровую карту общей минерализации первого от поверхности водоносного комплекса в масштабе 1:1 250 000, используя свободную кроссплатформенную геоинформационную систему QGIS. Результаты исследования могут быть полезны для дальнейшего изучения геологии и экологии Курганской области.

Ключевые слова: карта минерализации, геологическое строение, полезные ископаемые

M. A. Karasyuk[1], S. Yu. Katsko[1], I. P. Kokorina[2]*

Geoinformation Support for Geological Research of the Kurgan Region

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Institute of Systematics and Ecology of Animals, Novosibirsk, Russian Federation
* e-mail: s.katsko@ssga.ru

Abstract. The article discusses the use of geographic information systems (GIS) in geological research, using the example of creating a map of the general mineralization of groundwater for the digital ecological-geographical atlas of the Kurgan region. The authors describe the problem of the lack of open access GIS systems of a geological profile and propose to develop a map of the general mineralization of the first water-bearing complex from the surface. The authors used the free cross-platform GIS system QGIS and created a digital map on a scale of 1:1 250 000. The research results can be useful for further study of the geology and ecology of the Kurgan region.

Keywords: mineralization map, geological structure, mineral resources

Введение

В настоящее время в геологических исследованиях широко используются геоинформационные системы [1, 2]. При этом в Зауралье нет обобщенной картографической базы эколого-географической информации, что является проблемой, которую предлагается решить в настоящем исследовании.

Целью исследования является разработка карты общей минерализации подземных вод для цифрового эколого-географического атласа Курганской области.

Для достижения поставленной цели необходимо решить следующие задачи:

– изучить геологию, тектонику и полезные ископаемые картографируемой территории;

– выбрать программное обеспечение;

– создать картографическую основу проектируемой геоинформационной системы геологического строения Курганской области;

– создать карту общей минерализации первого от поверхности водоносного комплекса Курганской области;

– разработать атрибутивную таблицу тематических слоев.

Методы и материалы

Территория Курганской области находится в пределах Урало-Монгольского геосинклинального складчатого пояса, который в России является единственным поясом, полностью завершившим геосинклинальное развитие в начале мезозоя. В южных и восточных районах пояса в неоген-четвертичное время проявились орогенные процессы. В пределах пояса расположена Западно-Сибирская плита с мезозойско-кайнозойским чехлом – поле развития юрско-неогеновых отложений в пределах Западно-Сибирской низменности [3–5].

Территория Курганской области расположена на площади развития Нижневартовско-Петропавловской подпровинции Западно-Сибирской провинции бассейна пластовых вод. Западная часть входит в состав Западно-Тобольского бассейна Восточно-Предуральской группы бассейнов пластовых вод; восточнее реки Тобол развиты Восточно-Тобольский и Петуховский бассейны Ишимской группы бассейнов пластовых вод. Граница между ними проходит по линии поверхностного водораздела рек Тобол и Ишим.

В вертикальном разрезе слоистой системы бассейнов стока пластовых вод выделяют три гидродинамические зоны: весьма затрудненного, затрудненного и активного водообмена. В верхнюю зону активного водообмена входят континентальные и морские водоносные отложения палеоцена – нижнего эоцена, в том числе водоносный комплекс аллювиальных отложений долин рек Тобол, Исеть, Миасс, их притоков, а также аллювиальные отложения древних речных долин, образующие единый водоносный комплекс с отложениями олигоцена. Уровень подземных вод – 0,5–3,5 м, на более высоких участках – до 10 м. Водоносные горизонты средней и нижней гидродинамических зон залегают на глубинах от 100 до 250 м и более на востоке.

Минерализация подземных вод четвертичных аллювиальных отложений изменяется от 0,4 до 13 г/л. В долине р. Тобол для аллювиального комплекса характерно большое развитие солоноватых и соленых вод.

По распределению минерализации подземных вод в этом горизонте территория делится на два района: западный район – минерализация до 1,5 г/л; восточный район – минерализация до 10 г/л. Увеличение к востоку минерализации и изменение химического состава связано с ослаблением питания и общим затуханием гидродинамической активности. По направлению к востоку гидрокарбонатно-сульфатные воды сменяются солоноватыми хлоридно-гидрокарбонатными и гидрокарбонатно-хлоридными. Сплошное распространение соленых вод с минерализацией более 3 г/л отмечено в восточных районах. В долинах граница проходит по р. Тобол, на водораздельных пространствах она смещается к западу.

Кроме региональной изменчивости качества подземных вод, для палеоцен-нижнеэоценового водоносного горизонта проявляется вертикальная гидрохимическая зональность, выражающаяся в увеличении минерализации с глубиной [6, 7].

Минерально-сырьевая база Курганской области представлена запасами 21 вида полезных ископаемых. Наиболее значимую роль играют разрабатываемые месторождения глин, строительного песка, урана, песчано-гравийных пород, строительного камня, лечебных грязей, подземных минеральных и пресных вод. Территориальным балансом запасов общераспространенных полезных ископаемых Курганской области учтено 267 месторождений.

Курганская область относится к Зауральскому урановорудному району и является одной из трех уранодобывающих провинций России. Выявлены Далматовское, Добровольное, Хохловское месторождения и ряд рудопроявлений урана в других районах. Прогнозные ресурсы урана оцениваются в 120–130 тыс. т [7, 8].

Для создания проекта предпочтение отдано программному обеспечению QGIS, так как это свободная, кроссплатформенная геоинформационная система, имеющая большое количество подключаемых модулей.

Цифровая карта выполнена в системе координат WGS84 зона 41 в масштабе 1 : 1 000 000 и содержит следующие слои: гидрография линейная; гидрография площадная; населенные пункты; автомобильные дороги; железные дороги; границы административных районов, Курганской области, государственная граница РФ; рельеф; растительность и грунты; геология; тектоника; подземные воды; полезные ископаемые.

Структура базы данных проектируемой ГИС представлена в табл. 1.

Таблица 1

Структура базы данных

Группа слоев	Название слоя	Тип
Гидрография	Гидрография линейная	линейный
	Гидрография площадная	площадной
Населенные пункты	Населенные пункты	точечный
Пути сообщения	Автомобильные дороги	линейный
	Железные дороги	линейный
Границы	Граница Курганской области	линейный
	Границы административных районов	линейный
	Государственная граница РФ	линейный
Рельеф	Рельеф	площадной
Растительность и грунты	Растительность и грунты	площадной
Геология	Геология	площадной
Тектоника	Тектоника	площадной
Подземные воды	Подземные воды	площадной
Полезные ископаемые	Полезные ископаемые	точечный

Результаты

Можно выделить следующие результаты работы:

– изучены геология, тектоника и полезные ископаемые картографируемой территории;

– выбрано программное обеспечение;

– создана картографическая основа проектируемой геоинформационной системы геологического строения Курганской области;

– создана карта общей минерализации первого от поверхности водоносного комплекса Курганской области;

– разработана атрибутивная таблица тематических слоев.

Результаты работы представлены на рис. 1, 2.

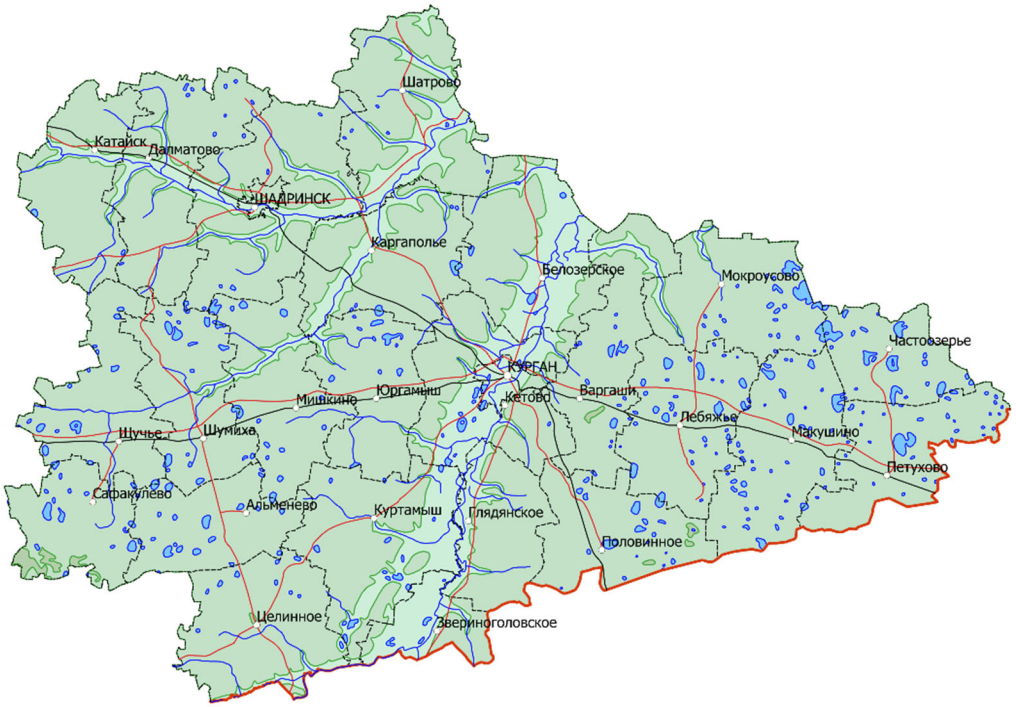


Рис. 1. Картографическая основа проектируемой ГИС

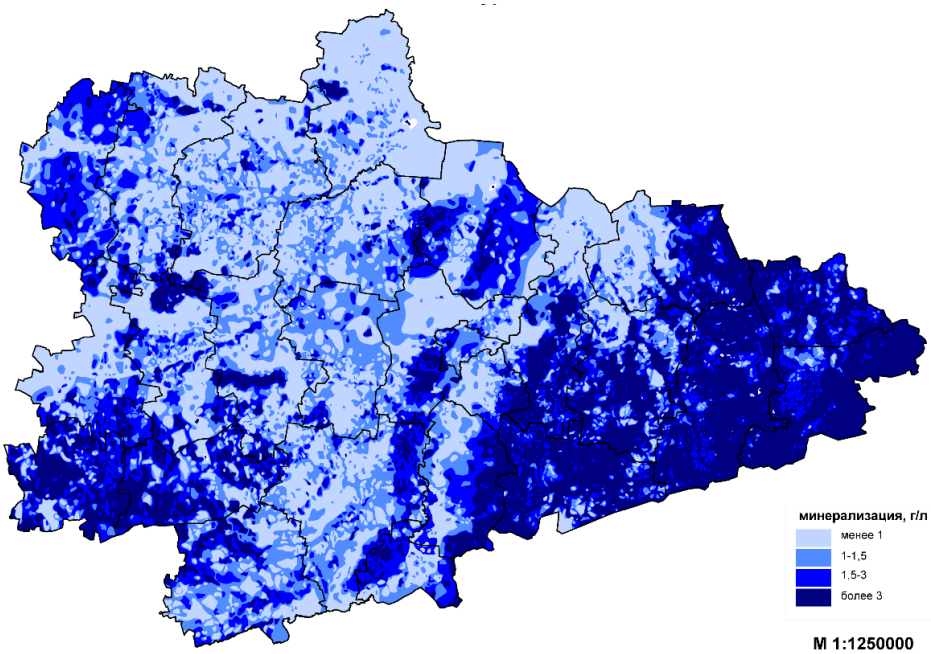


Рис. 2. Карта общей минерализации первого от поверхности водоносного комплекса Курганской области

Заключение

В ходе работы собрана информация о геологическом строении Курганской области. Разработанные картографическая основа и тематическая карта минерализации подземных вод в дельнейшем будут использованы для создания ГИС эколого-географического атласа Курганской области. Работая с этой ГИС, специалисты смогут проводить анализ геологической информации и сведений о полезных ископаемых на территории Курганской области.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кацко С. Ю., Ильин Д. А., Карасюк М. А. Разработка веб-ГИС «Отложения ордовикского периода северо-востока Горного Алтая» // Вестник СГУГиТ. Т. 27, № 6. – Новосибирск: СГУГиТ, 2022. – С. 131-140. – DOI 10.33764/2411-1759-2022-27-6-131-140.

2. Кокорина И. П., Карасюк М. А., Ильин Д. А. Картографическое обеспечение исследований на геологических разрезах горного Алтая // Регулирование земельно-имущественных отношений в России: правовое и геопространственное обеспечение, оценка недвижимости, экология, технологические решения. Сборник материалов V национальной научно-практической конференции. Ч. 2. – Новосибирск: СГУГиТ, 2022. – С. 51-56.

3. Науменко Н. И., Завьялова О. Г., Акимова Т. Г. География Курганской области: Краеведческое пособие. – Курган: КГУ, 2019. – 276 с.

4. Коровко А. В., Двоеглазов Д. А., Кузовков Г. Н. Государственная геологическая карта Российской Федерации. Масштаб 1 : 200 000. Издание второе. Серия Среднеуральская. Лист O-41-XXXII. Объяснительная записка. – Москва : МФ ВСЕГЕИ, 2015. – 274 с.

5. Завьялова О. Г., Коваль А. Е. Региональное природопользование (на примере Курганской области): Учеб. пособие. – Курган: Курганский гос. ун-т, 2008. – 198 с.

6. Объяснительная записка к атласу специализированных гидрогеологических карт первого от поверхности водоносного комплекса по территории Курганской области в масштабе 1: 200 000. – В. Пышма : АООТ «Средне-Уральская геологоразведочная экспедиция», 1995. – 35 с.

7. Недропользование – Департамент природных ресурсов и охраны окружающей среды Курганской области. – URL: http://www.priroda.kurganobl.ru/3580.html (дата обращения 02.11.2022).

8. Буданов Н. Д. Особенности геологического строения и гидрогеологическая карта Урала. – Свердловск: Типография изд-ва «Уральский рабочий», 1970. – 80 с.

УДК 338.45.01
DOI 10.33764/2618-981X-2023-6-98-103

А. С. Карпызин[1], О. В. Грицкевич[1]*

Исследование ресурсного обеспечения этапов жизненного цикла наукоемкой продукции

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: andrejka4600@gmail.com

Аннотация. Данная статья посвящена исследования ресурсного обеспечения наукоемкой продукции на разных этапах ее жизненного цикла. Был проведен анализ литературы в сфере ресурсного обеспечения высокотехнологичной продукции. Поставлена цель исследования – подтверждение теории методических рекомендаций по ресурсному обеспечению этапов жизненного цикла наукоемкой продукции для повышения эффективности процесса: исследования – производства. Практическая значимость исследования – полученные результаты и выводы по исследованию можно будет применить в разработке локальной методики предприятия для оптимизаций распределения ресурсов на каждом этапе жизненного цикла продукта, а также для проведения мероприятий по созданию и увеличению конкурентоспособности продукции на рынке.

Ключевые слова: жизненный цикл, наукоемкая продукция, управление, ресурсы

A. S. Karpyzin[1], O. V. Grickevich[1]*

Study of Resource Support for the Stages of the Life Cycle of High Technology Products

[1] Siberian State University of Geosystem and Technologies, Novosibirsk, Russian Federation
*e-mail: andrejka4600@gmail.com

Abstract. This article is devoted to the study of resource provision of science-intensive products at different stages of its life cycle. An analysis of the literature in the field of resource provision of high-tech products was carried out. The purpose of the study is to confirm the theory of methodological recommendations on the resource provision of the stages of the life cycle of science-intensive products to improve the efficiency of the process: research - production. The practical significance of the study - the results and conclusions of the study can be applied in the development of a local enterprise methodology for optimizing the allocation of resources at each stage of the product life cycle. And also for carrying out activities to create and increase the competitiveness of products in the market.

Keywords: life cycle, high technology products, management, resources

Введение

Отечественные компании сталкиваются с проблемами при производстве наукоемкой продукции из-за быстрого роста инновационных технологий. Также это связано с тем, что развитие той или иной отрасли зависит от эффективного ресурсного обеспечения предприятия.

Высокотехнологичным предприятиям необходима организационная структура, обеспечивающая быструю разработку и реализацию стратегий в условиях

ускоряющихся технологических изменений, коротких жизненных циклов продуктов и глобальной конкуренции. Стимулирование инновационной деятельности за счет развития инновационного потенциала требует постоянных инвестиций в научно-исследовательские и опытно-конструкторские работы (НИОКР).

Инновационная продукция разрабатывается и производится не только за счет инвестиций в НИОКР, но и благодаря эффективному распределению всех доступных ресурсов, которыми владеет компания (материальных, временных, кадровых и т.д.).

Целью данного исследования является теоретическое обоснование методических рекомендаций по ресурсному обеспечению каждого этапа жизненного цикла наукоёмкой продукции для повышения эффективности процесса: исследования – производство.

К задачам исследования относится: изучение литературных источников по ресурсному обеспечению предприятий наукоёмкой продукции, обобщение теоретических и практических материалов по данному направлению, разработка дальнейших подходов к развитию методики ресурсного обеспечения на различных этапах жизненного цикла наукоёмкой продукции.

Методы и материалы

Для получения теоретических данных использовались: системный подход, поиск, обзор и анализ тематической информации по направлениям менеджмент качества, управление жизненным циклом предприятия, управление разработкой наукоемкого продукта.

Проведя анализ литературных источников, рассмотрена основная теория в области ресурсного обеспечения наукоемкой продукции.

Наукоемкая продукция – это подмножество продуктов, которые предполагают применение современных научных, технологических и технических знаний для полезных целей и часто требуют значительных инвестиций в НИОКР [1, 2].

Жизненный цикл наукоемкой продукции включает в себя следующие этапы: маркетинговые исследования; проектирование продукта, включая прикладные (ПрИ) и фундаментальные (ФИ) исследования; производство; реализация; обслуживание; утилизация. Управление жизненным циклом наукоемкой продукции имеет большое значение в обеспечении эффективной работы всех субъектов, включенных в производство. На рис. 1 представлен жизненный цикл наукоемкой продукции.

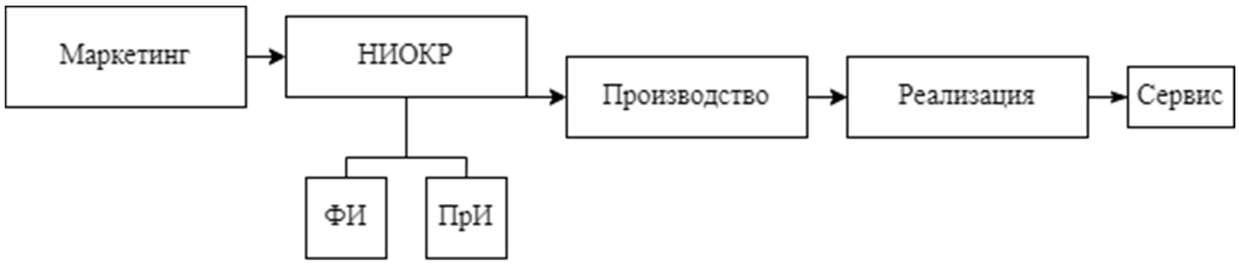


Рис. 1. Этапы жизненного цикла высокотехнологичной продукции

На всех этапах жизненного цикла наукоемкой (в том числе не высокотехнологичной) продукции большое внимание уделяется стратегии маркетинга, для внедрения и продвижения продукции на рынке. На основании теории Теодора Левина, 1965г. о концепции жизненного цикла товара, выделяется четыре этапа развития, для каждого из которых существует собственная стратегия (рис. 2) [3].

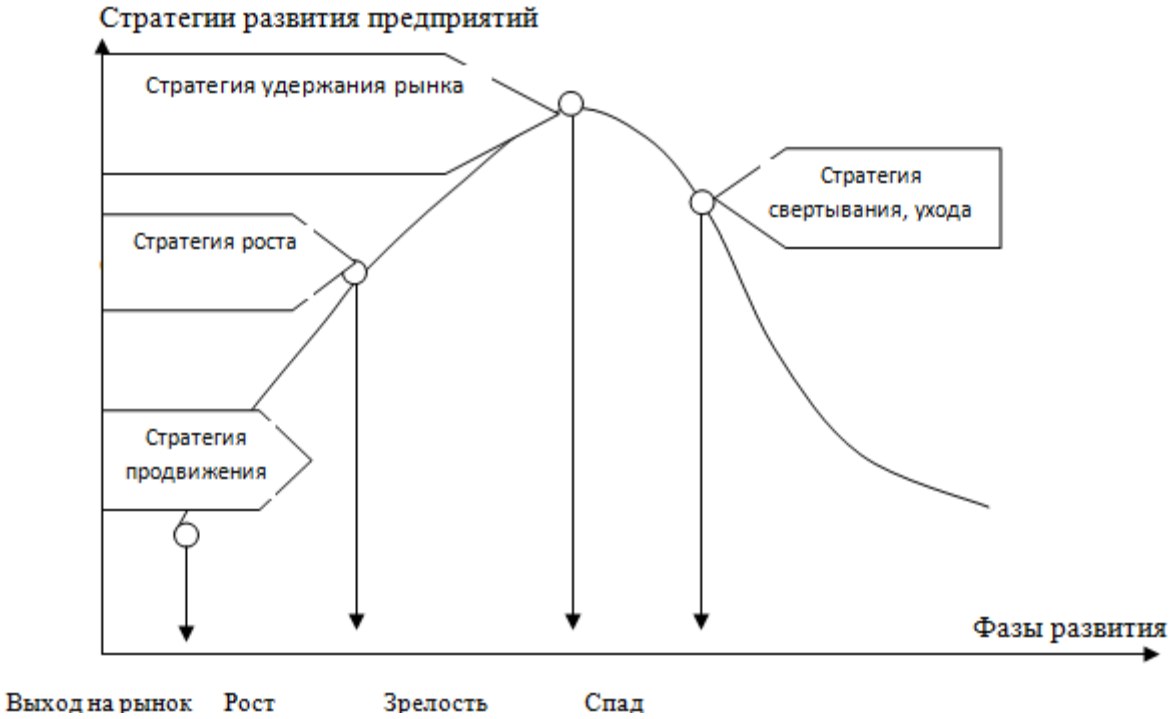


Рис. 2. Контрольные точки стратегической эффективности

Этап 1. Стратегия продвижения, внедрение и продвижение на рынке. Необходимость инвестирования в продвижение товара.

Этап 2. Стратегия роста продукта. Методика на расширение (увеличение) выпускаемой продукции, повышение доли на рынке.

Этап 3. Стратегия удержания. Направление на обслуживание выпускаемой продукции.

Этап 4. Стратегия свертывания. Предполагает стратегию ухода данного вида товара с рынка.

Подход по управлению жизненным циклом продукции, с точки зрения управления качеством продукции и в соответствии с международной организацией по стандартизации (ГОСТ Р ИСО 9004), содержит 11 стадий [4]:

– маркетинговые исследования рынка производства наукоёмкой продукции;
– материально-техническое снабжение подразделений предприятий;
– подготовка производства;
– производство наукоёмкой продукции;
– контроль и испытания продукции;
– упаковка и хранение продукции;
– реализация и распределение наукоёмкой продукции;

– монтаж и эксплуатация произведенной продукции;

– техническая помощь и обслуживание;

– утилизация продукции.

Данный подход является универсальным, применяется при управлении разными видами наукоёмкой продукции.

Обсуждение

Эффективность использования ресурсов производства – это соотношение стоимости товаров и затрат на их производство. Эффективность измеряется как отношение результатов, полученных на выходе, к ресурсам, затраченным на входе. Для характеристики эффективности использования ресурсов применяется система показателей, затрагивающих отдельные виды используемых ресурсов.

Основные показатели эффективности использования ресурсов: рентабельность активов, анализ их оборачиваемости; производительность труда; качество продукции; фондовооруженость; фондоотдача; материалоемкость [5, 6].

Для реализации экономического планирования основной деятельности организации следует применять метод ресурсной оценки. Это может вызвать трудности, так как реализация наукоемкой продукции может повлечь за собой ресурсные затраты, возникающие из-за уникальности работ, проводимых на инновационном производстве. Анализ теоретических методов ресурсной оценки позволит определить общий перечень рекомендаций по структурированию процедуры ресурсной оценки наукоемких проектов [7].

При проведении ресурсной оценки существует ряд важных элементов, которые будут рассмотрены далее.

Общие элементы: основные аспекты наукоемких проектов и НИОКР, термины и определения, этапы жизненного цикла наукоемкой продукции и границы между этими этапами.

Этапы и виды работ: конспектирование характеристик деятельности, характерных для проектирования, подготовки и производства, этапов жизненного цикла и их характеристика.

Для каждого типа ресурсов расчет стоимости можно описать следующим образом [8].

Ключевой показатель эффективности производства рассчитывается по формуле (1):

$$Э = \frac{P}{З}, \quad (1)$$

где Э – эффективность деятельности предприятия; Р – результат производственной деятельности; З – затраты на производство.

Финансовые ресурсы отражают сумму затрат, вложенных в наукоемкий проект. Обычно включаются в планы реализации проекта.

С помощью показателя оборачиваемости оборотных средств просчитывается эффективность использования оборотных активов компании. Для расчета используется формула (2):

$$O_{ос} = \frac{B}{C_{оа}}, \quad (2)$$

где $O_{ос}$ – оборачиваемость оборотных средств; В – выручка от реализации продукции, работ или услуг; $C_{оа}$ – стоимость всех оборотных активов, которыми может распоряжаться компания.

Временные ресурсы выражаются в днях (планируемые сроки запуска и окончания в рамках каждой стадии жизненного цикла наукоемкого проекта).

Трудовые ресурсы оценивают, насколько эффективно используется труд работников. Коэффициент производительности труда показывает количество трудозатрат в пересчете на единицу продукции и рассчитывается по следующей формуле (3):

$$П_{тр} = \frac{П_{п}}{C_{ч}}, \quad (3)$$

где $П_{тр}$ – производительность труда; $П_{п}$ – продукция, произведенная за определенный период (год, квартал); $С_{ч}$ – среднесписочная численность сотрудников за этот же период.

Материальные ресурсы включают в себя общую стоимость оборудования, материалов, сырья, комплектующих и т.д. Коэффициент эффективности использования сырья рассчитывается по формуле (4);

$$M_{е} = \frac{M_{з}}{T}, \quad (4)$$

где $M_{з}$ – материальные затраты на выпуск товара; Т – объем произведенной продукции.

Информационные активы оцениваются исходя из стоимости программного обеспечения, экспертизы и баз данных [9].

Метод ресурсной оценки направлен на оценку ресурсов, используемых при разработке и производстве наукоемкой продукции. Использование метода позволяет получить обоснованные оценки допустимых затрат ресурсов в результате выполнения конкретных работ в рамках наукоемкого проекта.

Для внедрения ресурсного метода оценки требуется: время выполнения наукоемкого проекта; данные о специфике научной работы; цели и задачи, про-

водимые в рамках НИОКР; перечень основных работ, выполняемых при конкретном этапе; финансовые показатели эффективности НИОКР; обоснованные значения нормативов стоимости и стоимости ресурсов, необходимых для выполнения работ [10].

Заключение

Таким образом, получив необходимые теоретические данные о ресурсном обеспечении наукоемкой продукции, можно разработать локальную методику прогнозирования ресурсного обеспечения на разных этапах жизненного цикла, включая индивидуальную возможность анализа всех видов ресурсов, используемых на производстве**.**

Метод прогнозирования позволит получить представление о максимальных затратах ресурсов, требующихся для реализации отдельных видов работ, а также при проведении мероприятий, обеспечивающих эффективное использование этих ресурсов.

При дальнейшем выборе конкретного продукта можно воспользоваться прямыми методами расчета себестоимости ресурсов и методами, основанными на информации об аналогах (если такие имеются). В результате будет сформирована комплексная оценка затрат ресурсов, необходимых для реализации проекта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Терентьева З.С. Предпринимательство в наукоемких производствах: управление портфелем наукоемкой продукции с учетом согласованности этапов ее жизненного цикла // Гуманитарный вестник (МГТУ им. Н.Э. Баумана). 2013. № 6. С. 1-8.
2. Ершова И.В., Гамберг А.Е., Кузнецова Н.А.. Управление разработкой наукоемкого продукта : учеб. пособие. Екатеринбург: Издательство Уральского Университета, 2018. С. 120.
3. Ансофф И. Стратегическое управление: учебное пособие. М.: Экономика, 2010. С. 519.
4. ГОСТ Р ИСО 9004-2001 Системы менеджмента качества. Рекомендации по улучшению деятельности (с Изменением N 1); М: Стандартинформ, 2005. С. 52.
5. Туккель И.Л., Сурина А.В., Культин Н.Б. Управление инновационными проектами : учеб. пособие. СПб.: БХВ-Петербург, 2011. С. 396.
6. Широкова, Г. В. Жизненный цикл организации : учеб. пособие. СПб.: Издательство Санкт-Петербургского университета, 2015. С. 450.
7. Баумгартен, Л.В. Маркетинг предприятия : учебное пособие. М.: ИНФРА-М, 2016. С. 216.
8. Голубев А.А. жизненный цикл инновации и ресурсное обеспечение инновационной деятельности // Современные проблемы науки и образования. 2015. № 2-2. С. 1-7
9. Дробышева Л.А. Экономика, маркетинг, менеджмент : учеб. пособие. М.: Дашков и К, 2016. С. 152.
10. Скворцов А.В., Схиртладзе А.Г., Чмырь Д.А. Автоматизация управления жизненным циклом продукции: учеб. пособие. М.: Академия (Academia), 2017. С. 512.

УДК 528
DOI 10.33764/2618-981X-2023-6-104-110

К. Г. Киндикбаев [1]*

Методика создания планово-высотного обоснования на месторождении «Каражыра»

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: kindikbaev00@mail.ru

Аннотация. Целью работы является описание методики создания планово-высотного обоснования, предназначенной для мониторинга границ расширения загрязнения радионуклидами на месторождении «Каражыра», находящегося на территории Семипалатинского испытательного ядерного полигона. Создание данного обоснования возможно наземными и спутниковыми способами. Результатом работы стала двухступенчатая схема геодезического обоснования для координатного обеспечения процесса межевания земельных участков месторождения «Каражыра».

Ключевые слова: угольное месторождение «Каражыра», планово-высотное обоснование

K. G. Kindikbaev [1]*

Methodology for Creating a Planned High-Rise Substantiation at the Karazhyra Field

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: kindikbaev00@mail.ru

Annotation. The purpose of the work is to describe a methodology for creating a planned high-rise substantiation designed to monitor the boundaries of the expansion of radionuclide contamination at the Karazhyra field located at the territory of the Semipalatinsk nuclear test site. The creation of this substantiation is possible by ground and satellite methods. The result of the work was a two-stage scheme of geodetic justification for the coordinate support of the process of surveying the land plots of the Karazhyra deposit.

Keywords: Karazhyra coal deposit, planned high-altitude justification, radionuclide contamination

Введение

Особенностью угольной продукции месторождения «Каражыра» является тот факт, что верхний слой почвы, а также грунтовые воды загрязнены техногенными радионуклидами, которые образовались вследствие проводимых ранее ядерных испытаний. Поэтому при проведении горных, геологоразведочных и строительных работ, а также разработке данного месторождения непосредственно в районах расположения карьеров происходит подъем вместе с пылью и радионуклидов, которые затем распространяются ветром на значительные расстояния [1 – 4].

Реализованные полезные ископаемые перевозятся за пределы полигона, что распространяет радионуклиды на большие расстояния [5, 6].

В данный момент в Республике Казахстан происходит постепенный перевод территории полигона в народно-хозяйственный оборот с учетом фактического уровня загрязнения окружающей среды. В связи с этим актуальным является ведение непрерывного мониторинга уровня загрязнения, а также определение динамики расширения его границ с последующим отображением полученной информации на межевых планах [7 – 10].

В связи с этим возникает научно-техническая задача, связанная с координатным обеспечением фактических границ загрязнения земельных участков на горнорудном месторождении. Для ее решения необходимо создавать соответствующее геодезическое обеспечение на данной территории принимая за внимание постоянное радионуклидное воздействие на исполнителей.

В связи с этим разработка методики создания планово-высотного обоснования на загрязненной территории угольного месторождения «Каражыра» и последующего ведения различных геодезических работ для целей мониторинга загрязнения техногенными радионуклидами является актуальной научно-технической задачей, имеющей социальное и практическое значение.

Методы и материалы

Пункты сети планово-высотного обоснования на месторождении должны быть расположены в местах с минимально возможным уровнем радионуклидного загрязнения, а также в местах, где не проводились подземные ядерные взрывы, чтобы не повлиять на стабильность положения заложенных пунктов сети. Пункты должны закладываться путем бурения, чтобы свести к минимуму контакт с радионуклидами, а при наличии скальных выходов – путем установки скальных марок [11 – 13].

На месторождении «Каражыра» необходимо построить двухступенчатую схему геодезического обоснования (табл. 1). Создание данного обоснования производится наземными способами, а также с использованием технологий глобальной навигационной спутниковой системы (ГНСС).

Вследствие большой разрушенности пунктов государственной геодезической сети, а также значительного расстояния до базовой станции, которое составляет 135 км, расположенной в г. Семей, для реализации данной схемы требуется создание опорной межевой сети. Плотность точек на 1 кв. км должна составлять не менее одной точки при величине среднего квадратического отклонения взаимного положения смежных пунктов сети, не превышающей 5,0 см. Определение положения пунктов опорной межевой сети производится с использованием ГНСС оборудования. Осуществляется привязка к не менее чем к двум исходным пунктам государственной или местной геодезической сети в дифференциальном режиме. Измерения на пунктах опорной межевой сети выполняются статическим методом [14 - 16].

Наземным способом определяют координаты границ добычи угля, границ отвалов вскрышных пород, а также границ загрязненных земельных участков путем решения обратных линейно-угловых засечек или способом полярных коор-

динат [17 – 19]. В табл. 1 представлена двухступенчатая схема использования геодезического обоснования для обеспечения межевания.

Таблица 1

Двухступенчатая схема использования геодезического обоснования для обеспечения межевания

Категории геодезического обоснования	Методы создания обоснования	Особенности закрепления пунктов
Сеть активных базовых станций или базовых станций на пунктах триангуляции	1) ГНСС; 2) Тахеометры.	– используют сохранившие пункты полигонометрии, триангуляции; – плотность пунктов обоснования на 50–200 км^2 составляет 1 пункт
Опорная межевая сеть	1) ГНСС (лучевой способ); 2) Тахеометры.	– один пункт координатной системы фиксируется на расстоянии 20–40 км^2; – пункты сети располагаются на стенах или углах административных зданий и жилых домов, а также на опорах ЛЭП и вершинах сопок; – закрепляются на поверхности земли наземными центрами характерных точек границ земельного участка; – дополнительное координирование на местности твердых точек

Результаты

Результатом работ стало созданное геодезическое обоснование для координатного обеспечения процесса межевания земельных участков месторождения «Каражыра» (рис. 1).

Определение положения пунктов сети определялось способом полярных координат. На ближайших пунктах (рис. 2) устанавливался тахеометр, строился угол от стороны разбивочной сети и фиксировалось направление на местности точками. Затем в полученном направлении откладывалось расстояние и фиксировалось положение разбиваемой точки от которых велась сьемка мест взятия проб на отвалах (рис. 3 –5). Значения расстояния и горизонтального угла находились из решения обратной геодезической задачи.

Рис. 1. Двухступенчатая схема геодезического обоснования угольного месторождения «Каражыра»

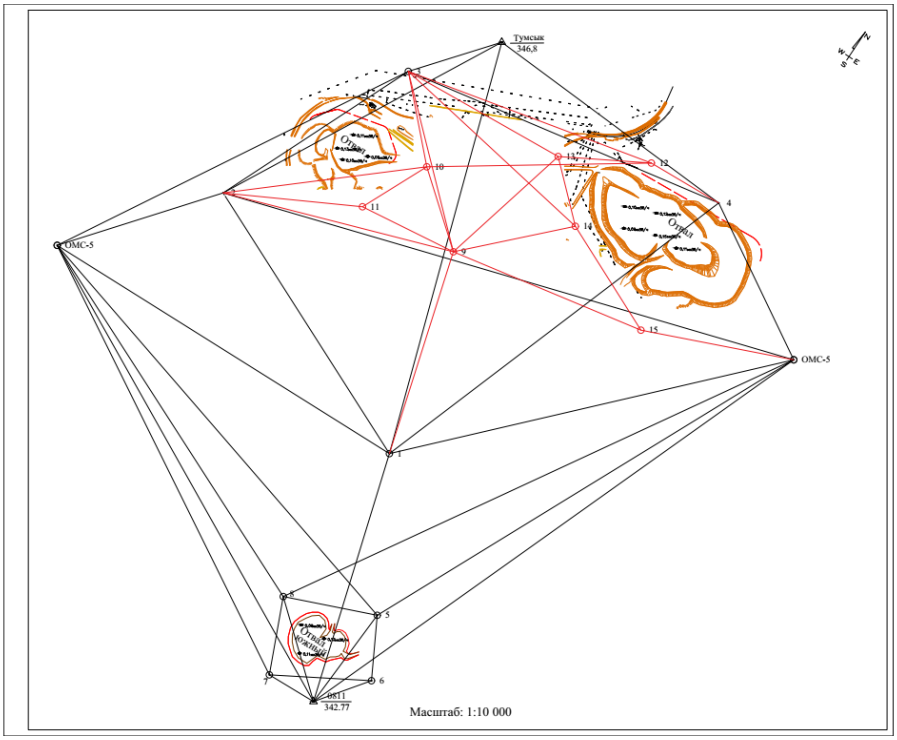


Рис. 2. Двухступенчатая схема геодезического обоснования отвалов угольного месторождения «Каражыра»

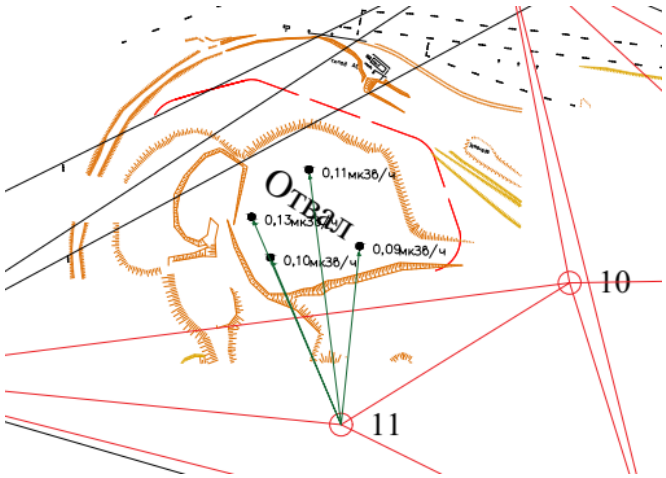


Рис. 3. Определение координат мест взятий проб радионуклидов на восточном отвале

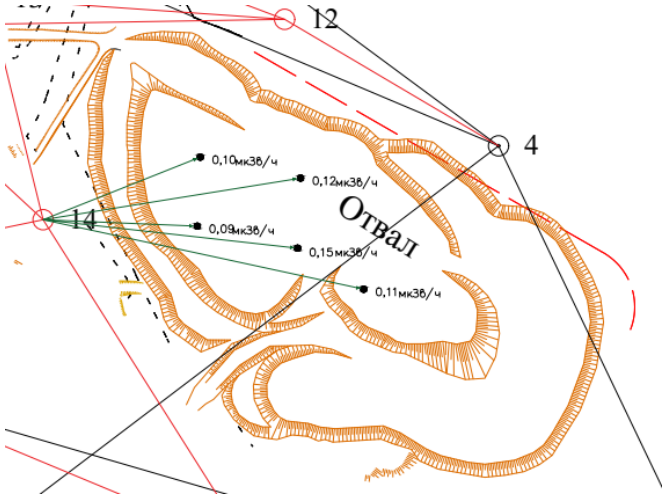


Рис. 4. Определение координат мест взятий проб радионуклидов на западном отвале

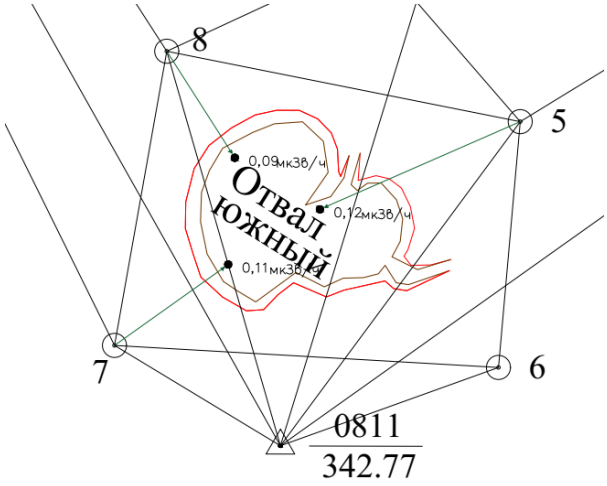


Рис. 5. Определение координат мест взятий проб радионуклидов на южном отвале

Заключение

В результате созданное обоснование определяет координаты границ добычи угля, а также границ расширяющегося отвала вскрышных пород для обозначения расширения границ загрязнения.

Также, со временем границы загрязнения земель будут постепенно увеличиваться вследствие факторов как возрастания объемов добычи и перевозок угля. В связи с этим, в дальнейшем возникнет необходимость разработки планово-высотного обоснования и создания межевых планов в районе угольного месторождения «Каражыра».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Актуальные вопросы радиоэкологии Казахстана : Монография / С.Н. Лукашенко – Павлодар. Дом печати, 2010. –343 с.
2. Геодезическое обеспечение государственного кадастра недвижимости / Е. И.Аврунев. – Новосибирск: СГГА, 2011. – 143 с.
3. Государственный кадастр недвижимости: учебник / А. А. Варламов, С. А. Гальченко. — М.: КолосС, 2012. –542 с.
4. Кадастровая деятельность: учебник / А. А.Варламов, С. А.Гальченко, Е. И.О.Аврунев. — М.:Форум Инфра–М, 2015. — 256 с.
5. Местные системы координат: учебник / А. П.Герасимов. –М.: Экзамен, 2009. – 324 с.
6. Кудеринов С.М., Какимов А.К., Кудеринова Н.А., Чигаева Ж.Е., Исабекова К.С. «Межевание земель, прилегающих к Семипалатинскому испытательному ядерному полигону» // Интерэкспо Гео-Сибирь. 2016. Т. 3. № 2. С. 219-224.
7. Исабекова К.С., Кудеринов С.М., Кудеринова Н.А. «Учет влияния розы ветров при межевании земель, прилегающих к угольному месторождению «Каражыра»» // Вестник СГУГиТ. 2021. Т. 26. № 4. С. 108-123.
8. Земельный кадастр: М.: Колос. 1979.–463 с.
9. Закон о радиационной безопасности [Электронный ресурс] / Электрон.дан. – М., 1998. – Режим доступа: СПС КонсультантПлюс . – Загл. с экрана.
10. Земельный кодекс Республики Казахстан [Электронный ресурс] / Электронные текстовые данные – Режим доступа: https://online.zakon.kz/document/?doc_id=1040583. – Загл. с экрана.
11. Кудеринов С.М., Исабекова К.С., Уставич Г.А., Кудеринова Н.А. «Особенности загрязнения техногенными радионуклидами частного сектора г. Семей» // Интерэкспо Гео-Сибирь. 2022. Т. 4. С. 184-191.
12. Радионуклиды и тяжелые металлы в окружающей среде Восточно–Казахстанской области и перспективы производства функциональных продуктов питания: монография / А.К.Какимов.– М. : Алматы, 2013. – 218 с.
13. Исследование степени накопления америция–24 и цезия–137 в пробах почвы на территории, прилегающих к СИЯП /А.К. Какимов, Б.Ж.Ахметов, Н.А. Кудеринова // ГЕО–Сибирь–2010 :сб. материалов VI Междунар. науч. конгр., 19–29 апр. 2010 г. – Новосибирск :СГГА, 2014. – Т. 2, ч. 2. – С. 63– 63.
14. Влияние розы ветров на хозяйственную деятельность на землях, прилегающих к СИЯП /А.К.Какимов, Я.Г.Пошивайло, Б.Ж.Ахметов, Н.А. Кудеринова, М.А. Минаева//ГЕО–Сибирь–2013 : сб. материалов VIII Междунар. науч. конгр., 19–29 апр. 2013 г. – Новосибирск : СГГА, 2013. – Т. 2, ч. 2. – С. 24– 28.

15. Исабекова К.С., Уставич Г.А., Кудеринова Н.А. «Совершенствование методики создания геодезического обоснования для территорий, загрязненных радионуклидами» // Интерэкспо Гео-Сибирь. 2020. Т. 3. № 2. С. 142-149.

16. Сборник нормативных актов по регулированию земельных отношений Республики Казахстан [Электронный ресурс] / Электрон.дан. – М., 1998. – Режим доступа: СПС КонсультантПлюс . – Загл. с экрана.

17. Особенности межевания земель Семейского региона Восточно–Казахстанской области / С.М.Кудеринов, А. К. Какимов, Н.А.Кудеринова, К.С.Исабекова // ГЕО–Сибирь–2017 : сб. материалов Междунар. науч. конгр., 19–29 апр. 2017 г. – Новосибирск :СГГА, 2017. – Т. 1, ч. 1. – С. 81– 84.

18. Радиоэкологическая обстановка территорий, прилегающих к Семипалатинскому испытательному полигону / Н. А.Кудеринова, А. К.Какимов, С. М.Кудеринов, Ж. З., Толеубекова, К.С.Исабекова //ГЕО–Сибирь–2015 : сб. материалов Междунар. науч. конгр., 13–25 апр. 2015 г. – Новосибирск :СГУГиТ, 2015– Т. 2, ч. 1. – С. 200– 206. //

19. Радиологические последствия проведения ядерных испытаний на полигонах мира / В. А.Логачев, Л.А.Логачева //Научно–технический журнал «Вестник» НЯЦ РК. – 2008. – №3 – С. 7–17.

УДК 57.087
DOI 10.33764/2618-981X-2023-6-111-117

М. А. Козлов[1]*, *А. Н. Поликанин*[1]

Биометрические системы, применяемые для контроля доступа в организациях

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
*e-mail: lfmisok@gmail.com

Аннотация. В статье поднимается вопрос контроля доступа, рассмотрены биометрические системы, которые способны ускорить процесс доступа. Ввод пароля требует определенного количества времени, например, из-за неправильного ввода, неправильной раскладки, более того уверенность в том, что определенный человек работает под своей учетной записью, а не его коллега, отсутствует. Аутентификация в системе по биометрическим признакам увеличивает уверенность в санкционированном доступе определенного пользователя, в нашем исследовании мы рассмотрим эффективность различных биометрических систем по нескольким параметрам, и выясним возможность применения таких систем на предприятиях. В данный момент широко используются биометрические системы, основанные на изображении лица, отпечатках пальцев, характеристик голоса, сетчатке глаза. Применены методы экспертной оценки и стоимостных регрессионных зависимостей для выявления оптимального вида биометрической системы и конкретного продукта, среди рассмотренных.

Ключевые слова: биометрия, аутентификация, биометрические системы

M. A. Kozlov[1]*, *A. N.Polikanin*[1]

Biometric Systems Used for Access Control in Organizations

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: lfmisok@gmail.com

Annotation. The article raises the issue of access control, considers biometric systems that can speed up the access process. Entering a password requires a certain amount of time, for example, due to incorrect input, incorrect layout, moreover, there is no confidence that a certain person works under his account, and not his colleague. Authentication in the system by biometric features increases confidence in the authorized access of a certain user, in our study we will consider the effectiveness of various biometric systems in several parameters, and find out the possibility of using such systems in enterprises. Currently, biometric systems based on facial images, fingerprints, voice characteristics, and the retina of the eye are widely used. The methods of expert evaluation and cost regression dependencies are applied to identify the optimal type of biometric system and a specific product, among those considered.

Keywords: biometrics, authentication, biometric systems

Введение

В современном мире обрабатывается колоссальное количество информации, поэтому вопрос обеспечения ее безопасности является актуальной задачей любой организации. При повышении требований к безопасности информационной системы возникает проблема снижения скорости доступа.

Классические пароли требуют определенного количества времени из-за неправильного ввода, неправильной раскладки, при этом отсутствует уверенность в том, что под учетной записью работает пользователь, а не его коллега. Данная проблема может быть решена при использовании аутентификации по биометрическим признакам. Анализ литературы позволил установить, что наиболее широкое распространение получили такие способы биометрической идентификации личности как идентификация по отпечатку пальца, распознаванию лица, радужной оболочке глаза, сетчатке глаза [4-8].

Цель работы заключается в выявлении биометрической системы, наиболее подходящей для внедрения в организации.

Для достижения поставленной цели были решены следующие задачи:

1) установить перечень характеристик биометрических систем;

2) оценить коэффициенты весомости показателей качества биометрических систем экспертным методом;

3) установить оптимальный программно-аппаратный продукт, основанный на биометрической аутентификации, методом стоимостных регрессионных зависимостей.

Методы и материалы

Для проведения исследований выбраны следующие характеристики биометрических систем: вероятность ложного недопуска (FRR); доля транзакций верификации подлинного лица, которые будут ошибочно отвергнуты; вероятность ложного допуска; доля транзакций верификации "самозванца", которые будут ошибочно приняты (FAR). EER (Equal Error Rate) — величина, которая характеризует уровень ошибок биометрического метода, при котором значения FAR и FRR равны [1]. Чем меньше этот параметр, тем точнее система. Значение соответствующих характеристик, рассчитанных с применением методов математической статистики, приведены в табл. 1 [2]. Данные характеристики были приведены на основании анализа литературных источников.

Таблица 1

Средние значения FAR, FRR, ERR для наиболее популярных методов биометрической идентификации

Вид системы	FAR, %	FRR,%	Err ,%
Отпечаток пальца	0,0010	0,60	0,130
Распознавание лиц	0,1100	2,50	0,900
Радужна оболочка глаза	0,0010	0,12	0,067
Сетчатка глаза	0,0001	0,40	0,110

Для оценки степени согласованности мнений экспертов произведен расчет коэффициентов вариации v_i по следующей формуле:

$$v_i = \frac{100\sigma_i}{R_i}, \quad (1)$$

где σ_i - среднеквадратическое отклонение по каждому единичному показателю; R_i - среднее арифметическое значение ранга каждой биометрической системы; R_{ij} - ранг каждого единичного показателя качества.

Оценка среднеквадратического отклонения по каждому единичному показателю качества производилась по формуле:

$$\sigma_i = \sqrt{\frac{\sum_{j=1}^{m} (\bar{R}_i - R_{ij})^2}{m-1}}. \quad (2)$$

Расчет коэффициента конкордации W производили по формуле:

$$W = \frac{12 \sum_{j=1}^{n} (S_i - \bar{S})^2}{m^2 (n^3 - n) - m \sum_{j=1}^{m} F_j}. \quad (3)$$

Показатель одинаковости F_j рассчитывался по следующей формуле:

$$F_j = \sum_{j=1}^{u} (t_g^3 - t_g), \quad (4)$$

где S_i - сумма ранговых оценок всех экспертов по каждому показателю; $\bar{S}$ -средняя арифметическая сумма рангов для всех показателей; n – количество биометрических систем; u – количество оценок с одинаковыми рангами у каждого привлекаемого эксперта; t_g – число одинаковых рангов в каждой g -ой оценке у каждого эксперта [9].

Результаты

Значимость биометрических систем и значения коэффициентов весомости характеристик биометрических систем оценивали экспертным методом (методом рангов) с привлечением пяти экспертов. В качестве экспертов привлекали профильных специалистов информационно-технической службы, результаты оценок представлены в табл. 2.

Результаты расчетов по оценке согласованности мнений экспертов приведены в табл. 3.

Значения коэффициентов вариации, полученных при экспертизе систем по отпечатку пальцев, радужной оболочке глаза и распознаванию лица, находятся в диапазоне от 10 до 33 %, что свидетельствует о средней степени согласованности результатов экспертной оценки. Значение коэффициента вариации для системы

по сетчатке глаза превышает критическое значение, что свидетельствует о низкой степени согласованности мнений экспертов. Рассчитанное значение коэффициента конкордации (табл. 3) свидетельствует о низкой согласованности мнений экспертов, в силу того, что эксперты имеют разные должности, разное образование, стаж работы и возраст.

Таблица 2

Результаты экспертизы

Вид системы	Начальник ИТ-службы	Сетевой инженер	Инженер ИТ-службы	Инженер второй линии	Инженер первой линии	Сумма оценок
Отпечаток пальцев	2	3	2	3	2	12
Распознавание лица	3	4	4	4	2	17
Радужная оболочка глаза	4	2	3	2	4	15
Сетчатка глаза	4	2	2	1	4	13

Таблица 3

Результаты расчетов при проведении экспертной оценки

Вид системы	σ_i	v_i	S_i	F_j	W
Отпечаток пальцев	0,55	11,41	12	6	0,23
Распознавание лица	0,85	25,00	17	6	
Радужная оболочка	0,5	16,67	15	-	
Сетчатка глаза	1,34	51,53	13	12	

На основании данных табл. 3 произведена оценка коэффициентов весомости для рассмотренных биометрических систем (табл. 4).

Таблица 4

Значения коэффициентов весомости

Биометрическая система	Коэффициент весомости, %
Отпечаток пальцев	21,05
Изображение лица	29,82
Радужная оболочка глаза	26,31
Сетчатка глаза	22,80

Таким образом, по результатам экспертной оценки установлено, что биометрическая система, основанная на распознавании лица, является наиболее оптимальной. По мнению экспертов, применение биометрической системы, основанной на отпечатках пальцев, сопряжено с постоянными ошибками сканирова-

ния вследствие недостаточной чистоты рук для считывания отпечатка и низкой степени гигиеничности.

Рассмотрим представленные на рынке продукты, основанные на распознавании лица: Face Station 2 (Suprema, Китай) [11], FaceDepot 7A (ZKteco, Китай) [12], DS-K1T331W (Hikvision, Китай) [13], ASI7223X-A (dahua, Китай) [14], их характеристики представлены в табл. 5.

Таблица 5

Выбранные продукты

Характеристики	Face Station 2	FaceDepot 7A	DS-K1T331W	ASI7214X
Скорость распознавания, с	1,0	1,0	0,2	0,2
Скорость сравнения, шаблонов /секунду	3000	2000	1000	2000
Количество шаблонов лиц	До 900 000 шаблонов	До 10 000 шаблонов	До 10 000 шаблонов	До 100 000 шаблонов
Журнал событий	5 млн событий	100000 событий	150000 событий	300000 событий
Разрешение камеры, mp	2	2	2	2
Наличие инфракрасной подсветки	есть	нет	нет	есть
Стоимость, руб	От 134 500	От 67 266	От 14 359	От 47 214

Для определения оптимального продукта применяли метод стоимостных регрессионных зависимостей [10]. Уравнение линейной регрессионной зависимости имеет следующий вид:

$$\lg\frac{Scp}{S_i} = \Sigma m_i \lg(\frac{P_{ik}}{Pcp}), \tag{5}$$

где m_i - коэффициенты весомости, рассчитываются методом наименьших квадратов.

$$M_1 = \frac{\sum(y_k * x_{1k}) * \sum x_{1k}^2 - \sum(y_k * x_{2k}) * \sum(x_{2k} * x_{1k})}{\sum x_{1k}^2 * \sum x_{2k}{}^2 - \sum(x_{2k} * x_{1k})^2}, \tag{6}$$

$$M_2 = \frac{\sum(y_k * x_{2k}) * \sum x_{1k}^2 - \sum(y_k * x_{1k}) * \sum(x_{2k} * x_{1k})}{\sum x_{1k}^2 * \sum x_{2k}{}^2 - \sum(x_{2k} * x_{1k})^2}, \tag{7}$$

где x – значение показателя качества; y – стоимость.

Интегральные показатели качества I_k рассчитывали по следующей формуле:

$$I_k = \frac{S_{cp}}{S_i} * \prod \left(\frac{P_{ik}}{P_{cp}}\right)^{m_i}, \quad (8)$$

где S – стоимость, P - значение показателя.

Результаты расчетов представлены в табл.6.

Таблица 6

Результаты вычислений интегральных показателей

M_1	M_2	S_{cp}, руб	I_1	I_2	I_3	I_4
0,49	0,29	65834	2,05	1,35	3,62	2,15

На основании проведенных расчетов (табл. 6) установлено, что максимальное значение интегрального показателя характерно для продукта DS-K1T331W, что свидетельствует о наивысшем качестве данного объекта по сравнению с остальными рассмотренными программно-аппаратными комплексами, по цене и заявленным характеристикам.

Заключение

Применение биометрической системы, основанной на изображении лица, требует сканирования лица для внесения его в базу данных. Так как значения являются биометрическими персональными данными, перед использованием необходимо получить письменное согласие субъекта на обработку персональных данных в соответствии с ФЗ-152 «О персональных данных» [3]. Таким образом, в настоящей работе выбраны характеристики биометрических систем такие как FAR, EER, FRR. На основании значений установленных характеристик проведена экспертная оценка четырех биометрических систем. Установлено, что система, основанная на распознавании лица, ускоряет процесс аутентификации, не требует сложных манипуляций, как в случае с отпечатком пальцев, и наиболее оптимальная по цене.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2008 г. N 403-ст : введен впервые : дата введения 2009-01-01 / разработан научно-исследовательским институтом биометрической техники Московского государственного технического университета имени Н.Э.Баумана (НИИ БМТ МГТУ им.Н.Э.Баумана) – Москва, Стандартинформ 2019. 48 с.

2. Михайлов А. А. Основные параметры биометрических систем / А.А. Михайлов, А.А Колосков Ю.И. Дронов // Алгоритм безопасности. - 2015. – № 5. - С. 61.

3. Российская Федерация. Законы. О персональных данных : Федеральный закон №152-ФЗ : [принят Государственной думой 27 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года].

4. Багаев, Е. С. Современные биометрические системы безопасности / Е. С. Багаев // Вестник магистратуры. — 2014. — № 6. — С. 21-25.

5. Фролова Е. Ю. Идентификация человека по биометрическим данным обзор современных технологий / Е. Ю. Фролова, Ю. А. Колышкова // Северно-Кавказский юридический вестник – 2022. – Т. 1. – № 3. – С. 167–174.

6. Нечаева В.С. Идентификация отпечатков пальцев в биометрической системе безопасности / В. С. Нечаева // Вестник магистратуры – 2021. – № 5-3. – С. 65–66.

7. Базанов П.В. Биометрическая система идентификации человека по изображениям лица / П. В. Базанов // Вестник Московского университета – 2006. – № 1. – С. 49–55.

8. Маркелов К.С. Идентификация и верификация личности – комплексная биометрическая информационная технология / К. С. Маркелов // International Journal of open information technologies – 2015. – № 3. – С. 12–17.

9. Романов В.Н. Квалиметрия : учебное пособие / В.Н. Романов, Ю.А. Орлов, М.П. Ромодановская, Д.Ю. Орлов ; Владимирский государственный университет. – Владимир : ВлГУ, 2017. – 135 с.

10. Подольская М. Н. Квалиметрия и управление качеством : практикум / М. Н. Подольская ; Тамбовский государственный технический университет. – Тамбов : ТГТУ, 2011. – 96 с.

11. Suprema : [сайт] . – Москва. 2015 – . – URL: https://supremainc.ru/products/biometricheskoe-oborudovanie/facestation-2 (дата обращения: 03.03.2023). – Текст : электронный.

12. ZKTeco : [сайт] . – Москва, 2017 – . – URL: https://zkteco-store.ru/shop/zkteco-facedepot-7a-id (дата обращения: 03.03.2023). – Текст : электронный.

13. Hikvision : [сайт] . – Москва, 2020 – . – URL: https://hikvision.ru/product/ds_k1t331w (дата обращения: 03.03.2023). – Текст : электронный.

14. Dahuasecurity : [сайт] . – Москва, 2022 – . – URL: https://www.dahuasecurity.com/ru/products/All-Products/Access-Control/AI/Standalone/ASI7223X-A-V1-T1 (дата обращения: 03.03.2023). – Текст : электронный.

УДК 621.384.3
DOI 10.33764/2618-981X-2023-6-118-124

*П. С. Кривошеев[1], Т. Н.Хацевич[1]**

Разработка широугольных инфракрасных объективов

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: khatsevich@rambler.ru

Аннотация. Актуальность темы определяется потребностями оптико-электронного приборостроения в расширении отечественной элементной базы широкоугольных инфракрасных объективов для матричных приемников излучений мегапиксельного формата. Целью работы является представление результатов разработки трех светосильных широкоугольных инфракрасных объективов с угловыми полями от 60 до 90 °. Работа построена на использовании методов технической оптики и компьютерного моделирования оптических систем. Схемное решение инфракрасного светосильного широкоугольного объектива включает квазиафокальную двухкомпонентную систему с угловым увеличением менее 1 крата и силовой компонент. Первая отрицательная линза объектива выполняется из германия, остальные – из халькогенидного стекла. Относительная оптическая сила силового компонента лежит в диапазоне от 0,40 до 0,45. При указанных угловых полях в объективе обеспечивается телецентрический ход главных лучей в пространстве изображений и высокое качество изображений при сопряжении с мегапиксельными приемниками LWIR диапазона спектра.

Ключевые слова: тепловизионная система, широкоугольный ИК-объектив, телецентрический ход лучей

*P. S. Krivosheev[1], T. N. Khatsevich[1]**

Design of Wide-Angle Infrared Objective Lens

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: khatsevich@rambler.ru

Abstract. The relevance of the research is defined by the need of optical electronic design field in Russia in expanding the range of elements of wide-angle objective lens for full-format matrix radiation receivers. The aim of study is to present the results of design of three high-aperture wide-angle infrared lenses with angular fields from 60 to 90 °. The study is based on the use of technical optics methods and computer modeling of optical systems. The design of the infrared high-aperture wide-angle lens includes a quasi-focal two-component system with an angular magnification of less than 1x and a power component. The first negative lens of the objective is made of germanium, the rest lenses are made of chalcogenide glass. The relative optical power of the power component lies in the range from 0.40 to 0.45. For angular fields from 60 to 90 ° the lens provides a telecentric path of the main rays in the image space and high image quality when paired with full-format receivers of LWIR spectrum range.

Keywords: infrared imaging system, wide-angle infrared lens, telecentric ray path

Введение

Актуальность разработки инфракрасных объективов для тепловизионных систем подтверждается многочисленными публикациями по тематике тепловизионной аппаратуры, расширением номенклатуры объективов для тепловизион-

ных приборов и систем, представленных на сайтах и в каталогах предприятий-производителей [1–4]. Однако широкоугольные объективы для обзорных тепловизионных систем представлены в ограниченном количестве. Разработка и появление на рынке неохлаждаемых мегапиксельных матричных приемников излучений спектрального диапазона от 8 до 14 мкм (LWIR диапазон) [5] является стимулом для поиска технологичных схемных решений широкоугольных инфракрасных объективов, поскольку совместно с такими приемниками большие значения угловых полей могут быть достигнуты при приемлемом масштабе изображения и диаметре входного зрачка, что позволяет решать задачи обнаружения и распознавания мелких объектов в широком угловом поле обзора.

Целью работы является представление результатов разработки светосильных широкоугольных инфракрасных объективов с угловыми полями от 60 до 90 °. Работа построена на использовании методов технической оптики и компьютерного моделирования оптических систем.

Методы и материалы

В широкоугольных оптических системах рекомендуется обеспечивать не ортоскопический, а линейный закон построения изображений [6], называемый часто F-Theta законом. Поэтому требуемое значение фокусного расстояния объектива, соответствующее заданному угловому полю, при равных линейных размерах чувствительной площадки приемника излучений, получается несколько больше, чем в ортоскопических объективах. Так, превышение фокусного расстояния для углового поля по диагонали кадра, равного 60 °, составляет 10 %, равного 90 ° – около 30 %. При равных относительных отверстиях объективов соответственно возрастают диаметры входных зрачков в 1,1 и 1,3 раза. Согласно [7], дальность решения зрительных задач пропорциональна квадрату относительного отверстия и фокусному расстоянию объектива. Таким образом, применение в широкоугольной тепловизионной системе F-Theta объектива при прочих равных условиях способствует повышению дальности обнаружения и распознавания объектов, или повышает вероятность обнаружения более мелких объектов.

Разработка широкоугольных светосильных объективов осушествлялась в соответствии с принципиальной схемой, использованной ранее для разработки сверхширокоугольных светосильных объективов видимого диапазона спектра [8]. В состав принципиальной схемы включается двухкомпонентная афокальная система галилеевского типа, обращенная отрицательным компонентом 1 к пространству предметов и имеющая угловое увеличение менее 1 крата или близкое к нему, и расположенный за ней силовой компонент 3 (рис. 1). Расстояние между компонентами 2 и 3 принимается близким к фокусному расстоянию компонента 3, что способствует обеспечению телецентрического хода главных лучей наклонных пучков лучей в пространстве изображений.

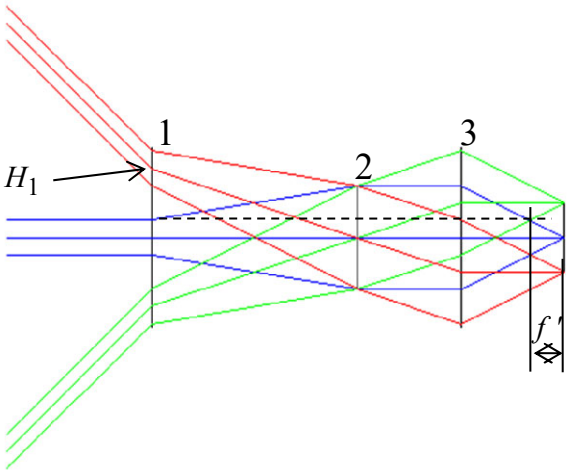


Рис. 1. Принципиальная схема для разработки широкоугольного объектива

Исследование условия устранения хроматизма увеличения в принципиальной схеме, показанной на рис. 1, позволило выявить, что на хроматизм увеличения оказывают влияние оптические силы компонентов 1 – 3 и коэффициенты средней дисперсии материалов компонентов 1 и 3. Коэффициент средней дисперсии компонента 2 оказывает влияние на хроматизм положения. Если принять, что в принципиальной схеме компоненты 1 – 3 являюся однолинзовыми, то для коррекции хроматизма увеличения должно соблюдаться условие:

$$\nu_1 / \nu_3 = H_1 / f', \qquad (1)$$

где ν_1, ν_3 – коэффициенты средней дисперсии материалов компонентов 1 и 3 сответственно; H_1 – высота второго параксиального луча на компоненте 1; f' – фокусное расстояние объектива.

При угловом увеличении афокальной системы, состоящей из компонентов 1, 2, менее 1 отношение ν_1/ν_3 получается больше 1. Иными словами, отрицательный компонент 1 должен быть изготовлен из материала, имеющего коэффициент средней дисперсии в рабочем спектральном диапазоне больше, чем коэффициент средней дисперсии материала положительного коэффициента 3.

Полученное соотношение объясняет, почему при расчете оптических систем широкоугольных объективов в диапазоне спектра от 8 до 14 мкм с помощью методов компьютерного проектирования для первого отрицательного компонента объектива в результате оптимизации методом перебора материалов выбирается германий, имеющий наибольший коэффициент средней дисперсии среди материалов, прозрачных в LWIR диапазоне спектра. В качестве материала остальных компонентов объектива могут быть использованы халькогенидные стекла, селенид цинка или германий.

Результаты моделирования оптических систем широкоугольных объективов, приведенные в следующем разделе, подтверждают, что проектирование компонентов 1 – 3 в виде двух или трех линз при наличии двух асферических поверхностей в системе является достаточным для приемлемого уровня коррекции аберраций.

Результаты

Результаты разработки трех оптических систем объективов с угловыми полями 70, 80 и 90 ° приведены в табл. 1. Объективы ориентированы на сопряжение с перспективной мегапиксельной матрицей формата 1920×1080 (пиксель 15×15 мкм). Оптические оси объективов показаны вертикальными. Все объективы являются телецентрическими, имеют относительное отверстие 1 : 1,2. В них соблюдается закон построения, близкий к линейному. Оптические системы содержат по две асферических преломляющих поверхности. В качестве примера на рис. 2 приведена оптическая схема объектива 80FTT1,2/1920×1080×15.

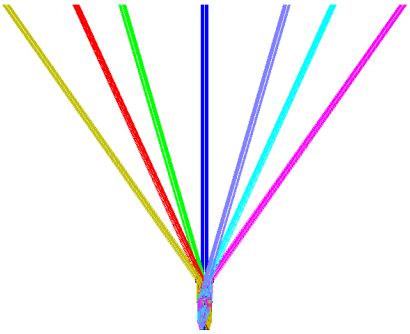
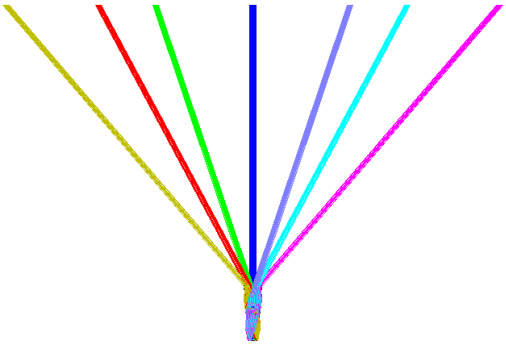
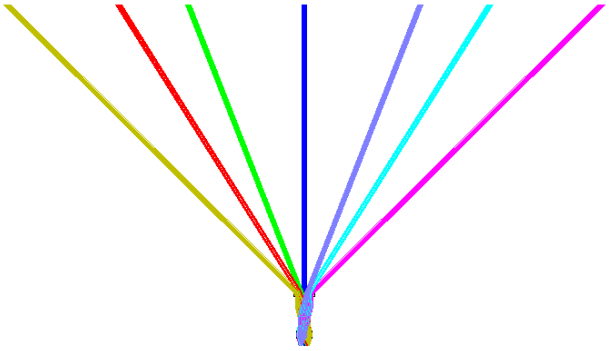
Объектив, схема которого приведена на рис. 2 а, имеет фокусное расстояние 24 мм и обеспечивает угловое поле 70х39 ° (80 ° по диагонали). Предусмотрено выполнение линз объектива из двух материалов: германия и халькогенидного стекла, при этом первая отрицательная линза – из германия. Это обеспечивает относительный хроматизм увеличения в пределах всего поля не более 0,015 %. Распределение энергии в изображении осевой точки в пределах квадратной площадки со стороной 15 мкм, приведенное на рис. 2 б, иллюстрирует согласование качества изображения, формируемое объективом, с характеристиками приемника излучений формата 1920×1080 с размером пикселя 15х15 мкм. Сечения частотно-контрастной характеристики (ЧКХ), приведенное на рис. 2 в, демонстрирует постоянство качества изображения по полю. Отступление от F-Theta закона (рис. 2 г) не превышает 2 %.

Качество изображения в объективах 70FTT1,2/1920×1080×15 и 90FTT1,2/1920×1080×15 (табл. 1) близко к 80FTT1,2/1920×1080×15.

Структурный анализ разработанных оптических систем показал, что компоненты 1 и 2 (рис. 1) выполняются из двух линз, а компонент 3 – из двух или трех, при этом относительная оптическая сила компонента 3 находится в диапазоне от 0,40 до 0,45, а компоненты 1 и 2 в ходе оптимизации и балансировки аберраций оптической системы трансформируется из афокальной в оптическую систему с малой положительной оптической силой.

Таблица 1

Характеристики оптических систем объективов

Условное обозначение	Иллюстрация углового поля по диагонали кадра	$\frac{D}{L}$	n/a	Масса, г
70FTT1,2/1920×1080×15		$\frac{62}{183}$	6/2	480
80FTT1,2/1920×1080×15		$\frac{67}{197}$	7/2	670
90FTT1,2/1920×1080×15		$\frac{67}{191}$	7/2	620

Примечание:
условное обозначение объектива: первые цифры – угловое поле по диагонали кадра; FT – F-Theta закон построения изображения; T – телецентрический; формат кадра x размер пикселя, мкм;
$\frac{D}{L}$ – в числителе наибольший диаметр линз объектива, в знаменателе – длина вдоль оптической оси, мм;
n/a количество линз в объективе / из них асферических.

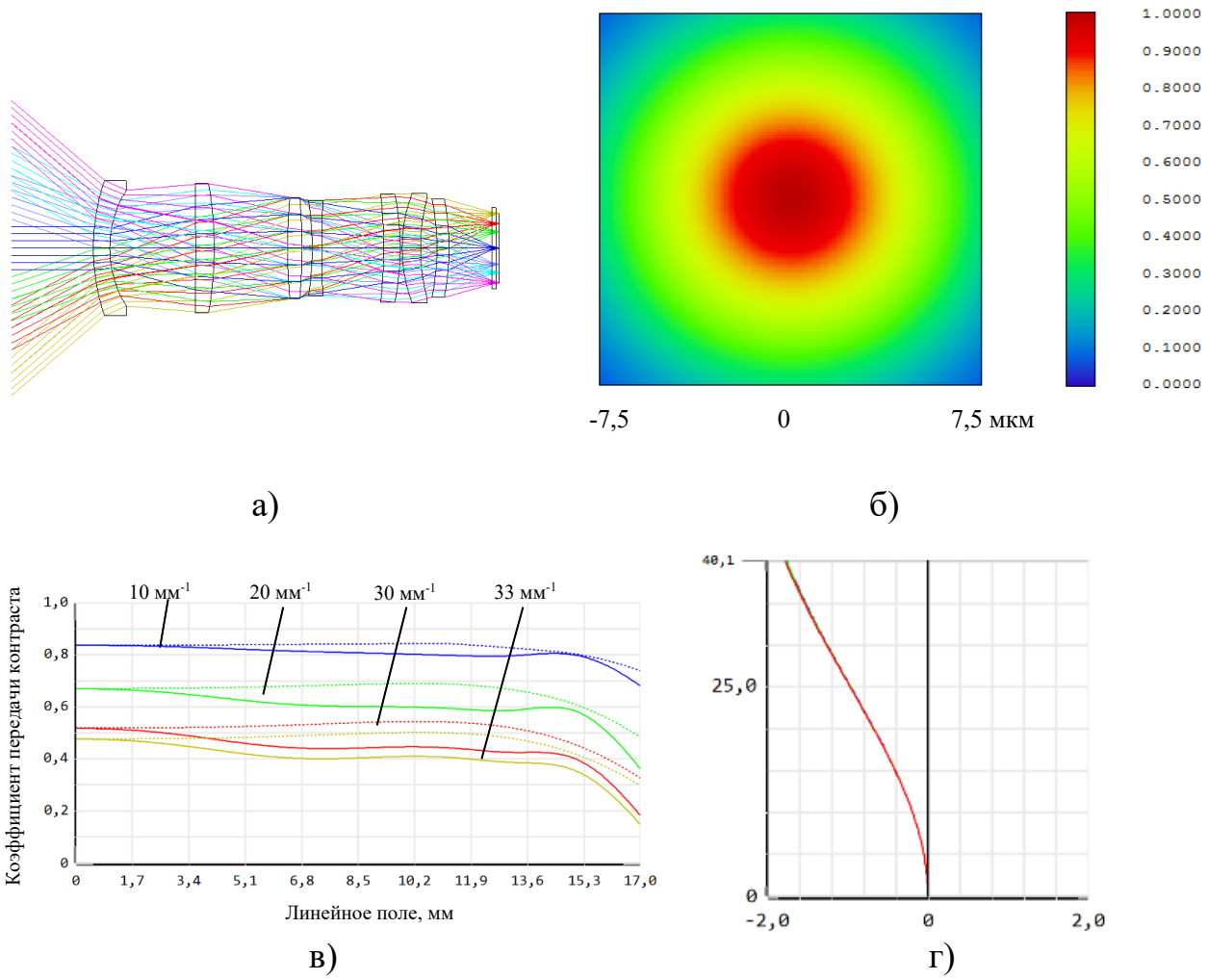


Рис. 2. Объектив 80FTT1,2/1920×1080×15: а) оптическая схема с ходом лучей; б) распределение энергии в изображении точки в квадрате со стороной 15 мкм; в) сечения ЧКХ по полю изображения; г) дисторсия F-Theta

Обсуждение

Если сравнить разработанные объективы с объективами известного производителя инфракрасной оптики [9], то при равных фокусных расстояниях в них реализуются в два раза большие угловые поля, соответствующие наибольшей стороне чувствительной площадки приемника излучений, но разработанные объективы проигрывают аналогам по массо-габаритным характеристикам. Однако для их применения в тепловизионных системах, устанавливаемых на стационарных площадках или подвижных носителях, последнее не является препятствием. Сравнение с известной оптической схемой широкоугольного инфракрасного объектива [10] показывает, что разработанные объективы сопоставимы с указанным объективом по такому показателю, как относительная длина объектива.

Заключение

Схемное решение инфракрасного светосильного широкоугольного объектива, содержащее двухкомпонентную систему с угловым увеличением в зрачках

менее 1 крата, и силовой компонент, отличающееся тем, что первая отрицательная линза системы выполняется из материала с наибольшим коэффициентом средней дисперсии, а относительная оптическая сила силового компонента лежит в диапазоне от 0,40 до 0,45, позволяет при угловых полях от 60 до 90 ° обеспечить телецентрический ход главных лучей в пространстве изображений и высокое качество изображений при сопряжении с перспективными мегапиксельными приемниками LWIR диапазона спектра.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Волков В. Г. Современные тенденции в разработках инновационных тепловизионных объективов и проблемные вопросы их промышленного производства / В. Г. Волков, Е. А. Моисеев, Ю. С. Митрофанова, Б. Н. Сеник // Фотоника, 2018, № 1. – С. 94–105.

2. Кульчицкий Н. А. Матричные фотоприемные устройства ИК-диапазона: «постпандемические» тенденции развития. Часть II. / Н. А. Кульчицкий, А. В. Наумов, В. В. Старцев. // Фотоника, 2020, т. 14; № 4. С. 320–330.

3. Астрон. Тепловизионные системы. Неохлаждаемые тепловизионные системы [Электронный ресурс] – Режим доступа: https://astrohn.ru/thermal-imaging-systems/uncooled-thermal-imaging-systems/ (дата обращения: 22.05.2023).

4. Pranav Wani, Kashif Usmani, Gokul Krishnan, Timothy O'Connor, Bahram Javidi. Lowlight object recognition by deep learning with passive three-dimensional integral imaging in visible and long wave infrared wavelengths // Optics Express, 17 Jan. 2022, Vol. 30, No. 2. – P. 1205–1218.

5. DLE1920 a-Si detector [Электронный ресурс] – Режим доступа: https://www.dalithermal.com/productinfo/749159.html (дата обращения: 22.05.2023).

6. Русинов М.М. Техническая оптика. – Л.: Машиностроение, Ленингр. отд-ние, 1979. – 488 с.

7. Тымкул В.М. , Тымкул Л.В., Фесько Ю.А., Поликанин А.Н. Дальность действия тепловизионных систем. Ч.I. Методика расчета // Автометрия, 2014, Т.50, № 4. – С. 96–101.

8. Абрамкина Д.Е., Хацевич Т.Н. Оптические системы особоширокоугольных объективов для цифровых камер // Интерэкспо ГЕО-Сибирь. XVI Междунар. науч. конгр., 18 июня – 8 июля 2020 г., Новосибирск : сб. материалов в 8 т. Т. 6 : Магистерская научная сессия «Первые шаги в науке». – Новосибирск : СГУГиТ, 2020. № 1. – С.3-10.

9. Thermal Imaging Lenses Catalog. LWIR/MWIR.Ophir 2023. pdf [Электронный ресурс] – Режим доступа: https://www.ophiropt.com/infrared, для зарегистрированных пользователей/ (дата обращения: 02.03.2023).

10. Пат. RU 2385475 Российская Федерация. Светосильный широкоугольный объектив для инфракрасной области спектра (варианты) / Хацевич Т.Н., Терешин Е.А.; патентообладатель: Институт физики полупроводников СО РАН. – № 2008132637/28; заявл. 07.08.2008; опубл. 27.03.2010, бюл. № 9. – 12 с.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-125-128

О. О. Крупко[1], А. В. Шабурова[1]*

Исторические аспекты оценки эффективности инвестирования в информационную безопасность предприятия

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: olesyakrupko4@gmail.com

Аннотация. Предмет исследования: проблема недофинансирования и избыточного финансирования информационной безопасности на предприятиях. Цели исследования: краткий обзор истории инвестирования в информационную безопасность; описание ключевых технологических и методологических изменений в области информационной безопасности; разбор экономических и финансовых аспектов инвестирования в информационную безопасность; объяснение, как оценивается эффективность инвестирования в информационную безопасность на предприятии; описание современных инструментов и методик оценки эффективности инвестирования в информационную безопасность; обзор технологических инноваций в информационной безопасности; разбор технических аспектов инвестирования в информационную безопасность; описание лучших практик и приведение примеров успешного инвестирования в информационную безопасность; анализ факторов, определяющих успех инвестирования в информационную безопасность на предприятии.

Ключевые слова: информационная безопасность, эффективность инвестирования, оценка инвестирования

O. O. Krupko[1], A. V. Shaburova[1]*

Historical Aspects of Evaluating the Effectiveness of Investments in Information Security of an Enterprise

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: olesyakrupko4@gmail.com

Abstract. Subject of research: the problem of underfunding and excessive financing of information security at enterprises. Research objectives: a brief overview of the history of investing in information security; description of key technological and methodological changes in the field of information security; analysis of economic and financial aspects of investing in information security; explanation of how the effectiveness of investing in information security at the enterprise is evaluated; description of modern tools and techniques for evaluating the effectiveness of investing in information security; overview of technological innovations in analysis of technical aspects of investing in information security; description of best practices and examples of successful investment in information security; analysis of factors determining the success of investing in information security at the enterprise.

Keywords: information security, investment efficiency, investment evaluation

Введение

Сегодня информационная безопасность (ИБ) является одним из ключевых факторов, обеспечивающих стабильное и эффективное функционирование предприятий. Но, невзирая на то, что инвестирование в ИБ становится все более ак-

туальным, многие компании и сейчас не могут понять, как оценить эффективность собственных инвестиций в эту область. В данной статье будут рассмотрены исторические аспекты оценки эффективности инвестирования в ИБ на предприятии.

Исторический обзор инвестирования в информационную безопасность предприятия

Начиная с 2000-х годов ИБ становится важнейшей частью функционирования предприятий, обеспечивая всестороннюю защиту конфиденциальной корпоративной информации от неправильного использования и несанкционированного доступа. Примерно к 2010 году сильно возросло число кибератак и утечек данных, проблема обеспечения защиты информации стала одной из важнейших для бизнеса. В это время многие предприятия начали осознавать важность инвестирования в ИБ.

Таким образом главным вопросом ведения бизнеса остается оценка эффективного инвестирования в информационную безопасность для обеспечения необходимого уровня защищённости данных [1].

В соответствии с [2], управление рисками ИБ позволяет идентифицировать риски, оценить вероятность и последствия этих рисков, способствует проведению систематического мониторинга процесса управления рисками.

Оценка эффективности инвестирования в ИБ на предприятии является сложной задачей, так как она включает в себя не только экономические и финансовые аспекты, но и технические.

Экономические и финансовые аспекты инвестирования в информационную безопасность предприятия

Оценка экономической эффективности инвестирования в ИБ на предприятии должна учитывать затраты на обеспечение безопасности информации и снижение рисков.

Современные инструменты и методики оценки эффективности инвестирования в ИБ на предприятии включают в себя анализ затрат, рисков и результатов внедрения. Одним из наиболее распространенных инструментов является методика ROI (Return on Investment), которая позволяет оценить экономическую эффективность инвестирования в ИБ на предприятии [3].

В работе [4] управление финансовыми затратами на обеспечение информационной безопасности представлено как процесс, входными данными которого являются стоимость активов и коэффициент дисконтирования, а выходными – возможный ущерб при реализации угрозы и оптимизация затрат.

Технические аспекты инвестирования в информационную безопасность предприятия

Важным аспектом при инвестировании в ИБ на предприятии является технический аспект. В статье [5] рассмотрена особенность российского подхода в отношении инвестирования в ИБ, в которой выделяют пять основных ступеней:

аудит, обнаружение рисков, оценка их уровней, разработка мероприятий управления рисками и дальнейший мониторинг.

Современные технические средства для обеспечения безопасности информации на предприятии включают в себя системы мониторинга, системы защиты от вирусов и злоумышленников, системы защиты от DDoS-атак, системы защиты от утечки данных и другие. Оценка технических аспектов инвестирования в ИБ на предприятии позволяет определить не только эффективность инвестиций, но и рациональность выбора технических средств для обеспечения безопасности информации.

В [6, 7] рассмотрены математические модели, позволяющие найти оптимальный уровень вложения средств в информационную безопасность

Согласно результатам аудита защищенности информационных систем, проведенного компанией Positive Technologies [8], важнейшей проблемой защищенности ресурса является не его уязвимость, а источник угроз, характеризующихся человеческим фактором

Методика инвестирования ИБ, которую предлагают авторы [9], содержит структуру, описывающую возможности применения теории управления инвестициями в ИБ.

Примеры оценки эффективности инвестирования в информационную безопасность предприятия

Примером оценки эффективности инвестирования в ИБ на предприятии может служить компания Target [10], которая в 2013 году стала жертвой кибератаки. В результате кибератаки украдены данные о 40 миллионах клиентов компании. Компания потратила около 250 миллионов долларов на улучшение своих систем безопасности и компенсацию ущерба клиентам. Однако, после улучшения систем безопасности, компания смогла увеличить свою прибыль на 40 % за год.

Другим примером может служить компания Equifax [11], которая также стала жертвой кибератаки в 2017 году. Компания потратила около 1,4 миллиарда долларов на восстановление после кибератаки, но утверждает, что инвестирование в ИБ было выгодным, так как компания смогла сохранить свою репутацию и клиентскую базу.

Заключение

В данной статье были рассмотрены исторические аспекты оценки эффективности инвестирования в ИБ на предприятии. Оценка эффективности инвестирования в ИБ на предприятии имеет множество аспектов, которые должны быть учтены при принятии решений. Важно учитывать, как финансовые, так и технические аспекты, а также риски и потенциальные угрозы, которые могут возникнуть.

Как показывают примеры компаний Target и Equifax, инвестирование в ИБ может оказаться выгодным, даже если компания стала жертвой кибератаки. В то же время, отсутствие адекватных мер по защите информации может привести к серьезным последствиям и значительным убыткам для компании.

Таким образом, оценка эффективности инвестирования в ИБ на предприятии является сложным и многогранным процессом, который требует комплексного подхода и профессиональных знаний. Правильно спланированные и выполненные инвестиции в ИБ могут привести к повышению эффективности и прибыльности предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бедрань А. Оценка эффективности инвестиций в информационную безопасность / А. Бедрань // Мудрый Экономист. – 2011. – № 16. – С. 15.

2. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 2011-12-01. - М. : Стандартинформ, 2011. - 51 с.

3. Успенская О. А. Использование механизма бизнес-диагностики для анализа эффективности проектов оптимизации системы управления предприятием / О. А. Успенская // Научные труды Вольного экономического общества России. – 2010. – № 137. – С. 488-493.

4. Козунова С. С. Система управления информационном безопасностью предприятия / С. С. Козунова // Евразийский Союз Ученых. – 2016. – № 7. – С. 22-23.

5. Жаринова С. С. Модель эффективности инвестиций в информационную безопасность предприятия / С. С. Жаринова, А. А. Бабенко // Моделирование экономических процессов современной России: отчет о научно-исследовательской работе. В 5 ч. Ч. 4. Разработка микроэкономических моделей. – Волгоград : Волгогр. науч. изд-во, 2014. - С. 88-112.

6. Ажмухамедов И. М. Оценка экономической эффективности мер по обеспечению информационной безопасности / И. М. Ажмухамедов, Т. Б. Ханжина // Вестник Астраханского государственного технического университета. Серия: Экономика. – 2011. – № 1. – С. 4-9.

7. Курило А. П. , Милославская Н. Г. , Сенаторов М. Ю. , Толстой А. И. / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 1-е изд. – Москва : Горячая линия – Телеком, 2013. – 244 с.

8. PT Application Inspector повысил защищенность продуктов «Открытого кода» // Positive Technologies : [сайт]. – URL: https://www.ptsecurity.com/ru-ru/ (дата обращения: 26.03.2023).

9. Козунова С. С. Методика инвестирования информационной безопасности организации / С. С. Козунова, А. А. Бабенко // NBI-technologies. – 2017. – № 4. – С. 11-14.

10. Target уточнил число пострадавших от кибератаки. – Текст : электронный // New Retail : [сайт]. – URL: https://new-retail.ru/novosti/retail/target_utochnil_chislo_postradavshikh_ot_kiberataki/ (дата обращения: 26.05.2023).

11. Бюро кредитных историй Equifax сообщило о краже данных 143 млн клиентов – Текст : электронный // РБК : [сайт]. – URL: https://www.rbc.ru/technology_and_media/08/09/2017/59b1e9b39a79471642f7f07d (дата обращения: 26.05.2023).

УДК 004.421.5
DOI 10.33764/2618-981X-2023-6-129-136

В. Е. Кудряшов[1], А. Н. Фионов[1,2]*

Метод генерации случайных компонент в системе NTRU

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: vadkud@inbox.ru

Аннотация. В современном мире безопасность информации зависит от защищенности криптосистем. И в последние годы замечен стремительный рост количества исследовательских работ в области квантовой криптографии. Ведется активное создание первых прототипов квантовых компьютеров и процессоров (существуют идеи реализации на оптических системах, где в роли кубита выступает фотон). Такие устройства значительно превосходят классические компьютеры по скорости обработки операций. Например, задача факторизации больших целых чисел решима за реальное время с использования алгоритма Шора на квантовом компьютере. Это делает небезопасными многие современные системы криптографической защиты информации (RSA, DH, ECDSA, ЭЦП). Поэтому необходимо уже сейчас задумываться о криптографических системах защиты информации, которые будут сохранять свою стойкость даже к атакам с квантовых компьютеров. Одна из таких систем-претендентов – NTRU. В данной статье она рассмотрена более детально, а также предложен метод генерации случайных компонент для ее реализации.

Ключевые слова: шифрование, RSA, квантовый компьютер, NTPU, постквавовая криптография, информационная безопасность

V. E. Kudryashov[1], A. N. Fionov[1, 2]*

The Method of Generation of Random Components in NTRU System

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: vadkud@inbox.ru

Abstract. In the modern world, the security of information depends on the security of cryptosystems. And in recent years, there has been a rapid increase in the number of research papers in the field of quantum cryptography. An active creation of the first prototypes of quantum computers and processors is underway (there are ideas for implementation on optical systems, where a photon plays the role of qubit). Such devices are significantly superior to classical computers in terms of processing speed. For example, the problem of factorization of large integers can be solved in real time using Shor's algorithm on a quantum computer. This makes many modern systems of cryptographic information protection (RSA, DH, ECDSA, EDS) insecure. Therefore, it is necessary now to think about cryptographic information protection systems that will remain resistant even to attacks from quantum computers. One such candidate system is NTRU. In this article, it is considered in more detail, and a method for generating random components for its implementation is also proposed.

Keywords: encryption, RSA, quantum computer, NTPUEncrypt, post-quantum cryptography, information secuirity

Введение

Криптосистема NTRU относится к методам криптографии, основанной на решетках. Криптография на решетках – подход к построению алгоритмов асимметричного шифрования с использованием задач теории решеток, то есть задач оптимизации на дискретных аддитивных подгруппах, заданных на множестве [4]. Вместе с другими методами постквантовой криптографии она считается перспективной из-за способности квантового компьютера расшифровывать широко используемые системы асимметричной криптографии, основанные на двух типах задач теории чисел: задачах целочисленной факторизации и задачах дискретного логарифмирования. Сложность алгоритмов взлома, построенных на решетках, чрезвычайно высока, лучшие алгоритмы могут решить эту задачу с трудом за экспоненциальное время.

Постквантовая криптография на решетках основана на труднорешаемых как для квантовых, так и для классических компьютеров задачах на решетках, таких как:

- нахождение кратчайшего вектора;
- нахождение идеального кратчайшего вектора;
- нахождение кратчайшего независимого вектора;
- поиск короткого целого решения.

NTRU был изобретен в 1996 году и представлен миру на конференции CRYPTO. Причиной, послужившей началом разработки алгоритма в 1994 году, стала статья, в которой говорилось о легкости взлома существующих алгоритмов на квантовых компьютерах, которые, как показало время, не за горами. Система полностью отвечает стандартам IEEE P1363 в соответствии со спецификациями решетчатой криптографии с открытым ключом [5].

В отличие от RSA или El Gamal, NTRU работает не над кольцом вычетов по модулю целого числа N, а над кольцом многочленов (полиномов), приводимых по модулю. Например, множество полиномов для работы NTRU можно задать так:

$$(Z / 7Z)[x] / (x^4 - 1), \tag{1}$$

где Z – множество целых чисел.

Из формулы (1) можно понять, что это множество многочленов, приводимых по модулю ($x^4 - 1$); у которых коэффициенты – целые числа, приводимые по модулю 7 [6].

Для реализации алгоритма задаются 6 парамтеров: N, p, q, d, d_f, d_g. Задаются также 3 призвольных набора многочленов, отвечающих принципу (1): L_f, L_g, L_r.

Рассмотрим метод генерации открытого и секретного ключей:

1. Из набора L_f выбирается произвольный многочлен f степени $(N - 1)$, который имеет d_f «1» и $(d_f - 1)$ «-1» (остальные «0») в качестве коэффиентов. Выбираться продолжается до тех пор, пока не будет получен многочлен, который имеет инверсии:

$$f_p = f^{(-1)} \ mod(p, x^n - 1), \tag{2}$$

$$f_q = f^{(-1)} \ mod(p, x^q - 1). \tag{3}$$

2. Из набора L_g выбирается произвольный многочлен g степени $(N - 1)$, который имеет d_g «1» и d_g «-1» (остальные «0») в качестве коэффиентов.

3. Открытый ключ вычисляется по формуле:

$$h = p * g \otimes f_q \ mod(q, x^n - 1). \tag{4}$$

4. Секретный ключ – это пара полиномов $(f; f_p)$.

Рассмотрим процесс шифрования сообщения:

1. Представляем отправляемое сообщение в виде полинома m степени $(N - 1)$.

2. Из набора L_r выбираем произвольный многочлен r степени $(N - 1)$, который имеет d «1» и d «-1» (остальные «0») в качестве коэффиентов. Полином называется «ослепляющим».

3. Зашифрованное сообщение вычисляется по формуле:

$$c = r \otimes h + m \ mod(q, x^n - 1). \tag{5}$$

Рассмотрим процесс расшифрования сообщения:

1. Вычисляем полином a по формуле:

$$a = c \otimes f \ mod(q, x^n - 1). \tag{6}$$

2. Переводим многочлен a в канонический вид по модулю q.

3. Расшифрованное сообщение вычисляется по формуле:

$$m = a \otimes f_p \ mod(p, x^n - 1). \tag{7}$$

Работу алгоритма расшифрования можно проверить, если подставить в формулу (6) формулу (5). Тогда мы получим a, равное:

$$a = m \otimes f \ mod(p, x^n - 1). \tag{8}$$

В результате преобразования формулы (7) с учетом формулы (8) получим:

$$m = m \otimes f \otimes f_p \ mod(p, x^n - 1). \tag{9}$$

Применив к формуле (9) формулу (2), получим $m = m$.

Рассмотрев весь алгоритм работы NTRU, можно выделить проблему генерации случайных полиномов с ограничениями по количеству опередлнных ко-

эффициентов. Это шаги 1-2 в алгоритмах генерации ключей и шаг 2 в алгоритме шифрования. Можно сформулировать следующую цель: разработать метод генерации «случайных» компонент для реализации алгоритма NTRU.

Методы и материалы

Перед тем как перейти к предложенному методу генерации случайных полиномов, вспомним, как работает арифметичекое кодирование.

Например, у нас есть алфавит A = {a; b; c}. Процесс кодирования/декодирования можно представить в виде схемы (рис. 1), где P – распределение вероятностей, а Q – распределение кумулятивных вероятностей.

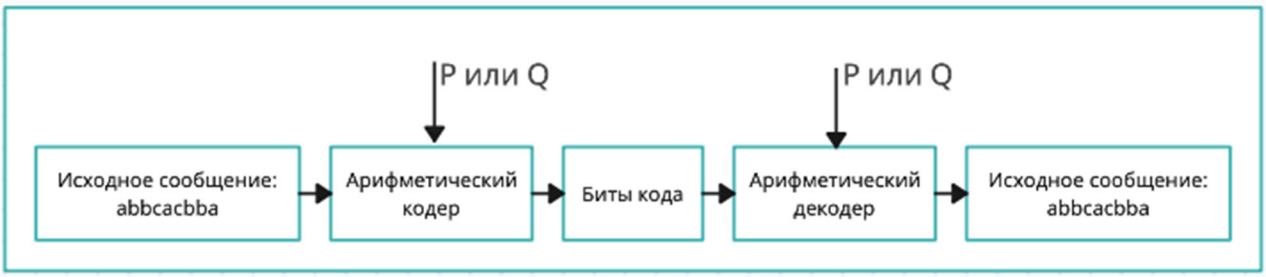


Рис. 1. Процес кодирования/декодирования

Предположим, у нас стоит задача закодировать сообщение (0 1 0 -1 1). Заменим буквы в алфавите A на нужные нам коэффициенты {-1; 0; 1}. Распределение вероястностей можно увидеть в табл. 1 [7]. То есть если в схему из рис. 1 передать алфавит A с распределением вероятностей из табл. 1, то мы сможем закодировать и однозначно декодировать исходное сообщение из нашей задачи.

В схеме (рис. 1) заменим арифметический кодер/декодер на омофонный. Омофонное кодирование представляет собой вид рандомизации сообщений, в котором буква источника заменяется специальными символами (омофонами), выбираемыми случайным образом так, чтобы сделать кодовую последовательность неотличимой от последовательности равновероятных и независимых нулей и единиц [8].

При посимвольном омофонном кодировании для каждого символа сообщения выбирается соответствующий ему интервал и производится омофонное кодирование этого интервала. Основная идея арифметического кодирования заключается в том, что кодирование интервала на каждом шаге не производится [9]. Вместо этого на интервале, соответствующем первому символу сообщения, рассматривается новое распределение символов алфавита источника, в котором выбирается интервал, соответствующий второму символу сообщения и т.д. Иными словами, каждый последующий символ сообщения сужает текущий интервал до интервала, соответствующего этому символу. В результате получается интервал, соответствующий всему сообщению. Для рандомизации сообщения необходимо произвести омофонное кодирование этого заключительного интервала [10]. Для обозначения описанного метода далее в тексте будет использо-

ваться аббревиатура АКРИ (арифметическое кодирование с разделением интервала).

Таблица 1

Распределение вероятностей

	0	1	0	-1	1	
p_{-1}	1	1	1	1	0	0
p_0	2	1	1	0	0	0
p_1	2	2	1	1	1	0
N	5	4	3	2	1	0
q_{-1}	0	0	0	0	0	0
q_0	1	1	1	1	0	0
q_1	3	2	2	1	0	0

Дело в том, что омофонный кодер гарантирует на выходе получение полностью случайной кодовой последовательности. Благодаря этому свойству, можно получить случайные коэффициенты полинома из случайной последовательности бит при задании кумулятивного распределения вероятностей (количества «-1», «0» и «1») для декодера АКРИ [11]. А случайную последовательность бит можно получить из генератора случайных бит (рис. 2).

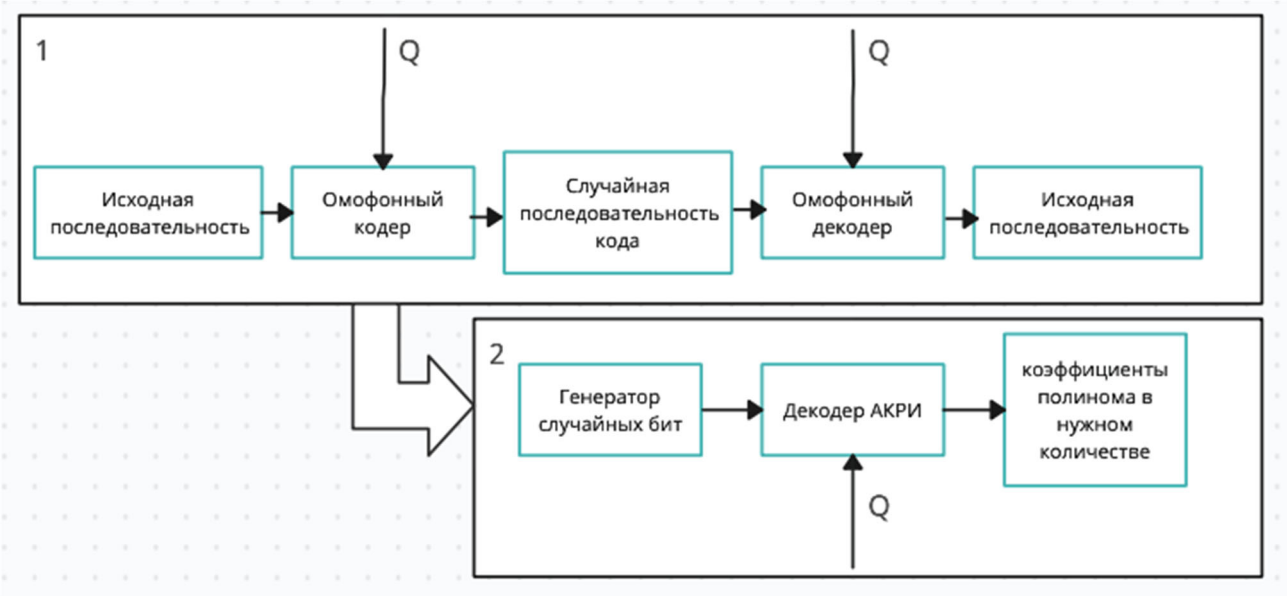


Рис. 2. Алгоритм генерации случайных коэффициентов заданного количества

Результаты

Попробуем сгенерировать необходимые нам наборы коэффициентов для многочленов f, g и r по рекомендуемым входным параметрам NTRU для максимального уровня стойкости ($N = 503$, $d_f = 155$, $d_g = 100$, $d = 65$) [7].

На рис. 3 показан результат работы программы для первого полинома *f*, который имеет всего 503 элемента, из них 155 «1», 154 «-1» и остальные «0». Т.е. мы в результате получаем готовый случайный полином с нужным количеством «0», «1» и «-1»: $-x^{501}+x^{500}-x^{499}-x^{497}$ …-1. Также программа считает, сколько случайных бит понадобилось извлечь из входной последовательности. Для полинома *f* это 798 случайных бит. Скорость работы программы меньше 1 секунды.

```
MacBook-Air-Vadim:~ kite$ ./genntru 503 155 154
6549ce9721ae61a473375ad19850296c881a57f1b4719656ade609f8b680882ad3ad4bdaa1860139e79a
b26075182dea936f7c1068db9d28e707909231472bdb83311ad30f43d645a1e1925af94b7e4f8caee0e8
6fa279659bdac88c9849b8c2cf4d16899bf78a858c01b0b5c6987e8cb8ac84270c86f588146cd7036ac7
c662
0 -1 1 -1 0 1 0 -1 1 0 -1 0 0 -1 1 1 1 -1 0 0 -1 0 -1 0 1 -1 1 1 -1 0 1 0 -1 -1 0 0
1 0 0 1 0 -1 -1 1 1 0 0 1 0 1 0 0 -1 1 -1 -1 -1 0 0 1 0 1 0 -1 0 1 0 1 0 -1 -1 1 1 -
1 -1 1 1 1 0 0 0 1 1 1 -1 -1 0 1 0 -1 -1 0 0 0 1 -1 0 1 1 1 0 1 1 0 0 0 -1 1 -1 0 0
-1 0 0 0 1 -1 0 1 0 0 0 0 0 1 -1 0 0 1 -1 0 -1 0 1 0 1 0 0 0 0 1 0 1 1 -1 1 -1 0 0 1
 1 -1 0 -1 -1 -1 0 1 1 0 -1 -1 -1 0 1 1 0 0 1 0 0 0 0 -1 -1 -1 0 -1 -1 -1 -1 1 0 -1
0 1 0 0 0 0 -1 1 1 0 1 1 -1 -1 1 1 0 1 1 0 1 0 -1 1 1 1 1 0 -1 0 0 1 0 -1 0 1 1 0 0
0 0 0 -1 -1 -1 0 1 -1 1 -1 -1 0 -1 0 1 1 1 -1 0 -1 1 1 1 0 0 1 1 1 0 0 0 -1 1 -1 0 -
1 0 1 1 -1 -1 -1 0 1 -1 -1 -1 -1 0 -1 0 -1 -1 0 1 -1 0 0 1 0 0 1 0 0 0 0 0 1 0 -1 0
1 1 0 0 -1 1 1 0 -1 0 1 -1 1 1 0 -1 1 0 0 -1 1 0 -1 1 1 -1 -1 0 1 0 0 1 -1 0 0 0 -1
1 -1 1 1 1 -1 -1 1 1 -1 0 0 -1 -1 -1 0 -1 0 0 0 -1 0 1 -1 1 0 -1 -1 0 0 -1 0 0 1 1 1
 -1 1 1 -1 0 -1 0 -1 1 1 0 -1 1 0 -1 1 -1 -1 0 0 1 1 1 1 1 0 0 1 0 1 1 -1 -1 0 0 0 -
1 0 1 -1 0 -1 -1 0 1 0 1 1 1 1 1 -1 1 0 -1 -1 0 -1 0 -1 -1 -1 1 0 -1 1 0 -1 -1 1 0 1
 -1 -1 -1 -1 0 0 -1 -1 -1 1 0 -1 0 1 1 0 -1 -1 0 0 0 0 -1 1 -1 -1 0 0 0 0 0 -1 1 0 -
1 -1 0 -1 0 1 0 -1 0 -1 -1 0 -1 -1 1 1 1 1 1 0 1 1 -1 1 0 0 -1 0 -1
bits = 798
```

Рис. 3. Случайные коэффициенты для полинома *f* в нужном количестве

На рис. 4, 5 показаны результаты работы программы для полиномов *g* и *r* соответсвенно.

```
MacBook-Air-Vadim:~ kite$ ./genntru 503 100 100
cf4d16899bf78a858c01b0b5c6987e8cb8ac84270c86f588146cd7036ac7c6620f32d152e57a9420ec26
a12cb8f9f000bd5d26c77401b8c097b0e938d46d0a5a28a80b156726f11ee6ac1aef5c563693aa4056a9
e8de861c44ec66b4642d5e8c
1 -1 0 -1 -1 -1 1 0 0 0 0 0 0 -1 0 -1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 -1 0 0 0 0 1 1
 0 0 0 -1 0 -1 0 1 0 1 1 0 0 -1 -1 0 0 0 0 0 1 0 1 0 -1 0 0 0 0 0 0 0 -1 0 0 0 0 0 0
 0 -1 0 0 0 1 0 -1 1 0 0 0 0 0 0 0 -1 0 1 0 0 1 0 0 -1 -1 1 0 0 0 1 -1 1 0 1 0 0 1 0
 0 0 0 1 0 1 1 0 -1 0 -1 1 0 0 1 0 -1 0 -1 0 0 -1 0 0 -1 0 0 -1 0 0 0 0 0 1 -1 0 0 0 0
 -1 0 0 0 0 0 -1 -1 0 1 -1 0 -1 0 0 0 0 0 1 0 -1 0 0 0 0 0 -1 0 1 -1 0 1 0 -1 0 0 1 1
-1 0 0 -1 0 0 0 0 1 1 0 0 0 0 0 1 0 0 1 0 -1 0 1 0 1 0 0 0 -1 -1 0 0 1 -1 0 0 -1 1 1
 -1 1 0 0 1 0 0 1 -1 0 0 0 -1 1 0 0 -1 -1 -1 0 0 -1 0 0 0 1 1 -1 0 0 1 0 -1 1 0 1 0
0 0 -1 -1 0 0 1 0 0 0 1 0 1 0 -1 1 0 1 0 -1 0 -1 1 0 -1 0 1 0 0 -1 0 0 0 0 0 0 0 1 0
 1 -1 0 0 0 1 0 -1 1 0 0 1 0 0 1 -1 0 0 1 0 0 0 0 -1 0 0 0 0 0 0 -1 1 0 0 0 0 0 0 0 0
0 1 0 -1 0 1 -1 0 0 0 0 0 1 0 0 1 -1 0 -1 0 0 -1 0 0 0 0 0 0 1 0 0 -1 0 1 1 1 0 1 1
0 -1 0 -1 1 0 0 1 0 1 0 0 1 0 0 0 -1 -1 0 -1 1 1 -1 0 0 1 -1 0 0 0 0 0 0 -1 -1 0 0 0
 -1 0 0 1 -1 0 1 -1 0 1 1 0 1 -1 0 0 0 -1 0 1 0 1 0 -1 0 0 0 -1 -1 0 0 1 0 0 0 0 0 -
1 -1 1 0 1 -1 -1 -1 -1 -1 0 0 0 0 0 1 0 0 0 -1 0 0 1 0 0 0 0 -1 0 -1 0 -1 0 -1 0 1 1
 -1 0 1 1 0 1
bits = 693
```

Рис. 4. Случайные коэффициенты для полинома *g* в нужном количестве

```
MacBook-Air-Vadim:~ kite$ ./genntru 503 65 65
9e7c1d2333be6b3925da298edf424a511fbb8b571aace82a55daa2ee3ed7c6623552538d4387991fdd55
4b0eff4842998df6dc64ea69ccca06439b53c26d078dcdb8b3c06827ee17063c618305f4b477da939d68
e5cc53cf451593c64b99c0d2
0 0 0 0 1 0 -1 0 0 0 0 0 0 0 -1 0 0 0 -1 -1 0 0 0 0 0 0 0 -1 1 0 1 0 0 0 0 0 0 0 0
 0 0 0 0 -1 -1 0 1 0 -1 1 -1 0 0 0 0 0 0 0 0 0 0 0 -1 0 0 0 0 -1 0 1 1 0 0 0 0 -1 0
0 0 0 0 0 -1 0 0 0 0 -1 0 0 -1 0 0 1 0 0 0 1 0 0 0 1 -1 1 -1 0 0 0 0 1 0 0 0 0 -1 0
0 0 0 0 0 0 0 0 0 0 0 0 1 -1 0 1 0 0 -1 0 0 0 1 0 1 0 0 0 0 0 1 1 0 1 0 1 0 -1 1 0 1
 0 -1 1 0 0 0 0 0 0 -1 0 0 -1 0 0 0 -1 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 1 0
 0 0 0 0 0 -1 0 -1 0 0 0 0 0 -1 1 0 0 0 0 1 0 0 0 -1 -1 0 0 0 0 0 0 0 0 0 0 0 1 0 0
0 0 0 0 0 1 -1 0 0 0 0 0 0 0 0 -1 1 0 0 0 1 0 0 -1 0 0 -1 0 0 0 0 -1 0 -1 0 0 0 0 0 0
0 0 0 0 0 0 0 -1 0 0 0 0 0 0 1 -1 0 0 1 0 0 0 0 0 0 0 0 -1 0 0 0 0 1 0 1 -1 1 0 0 0 0
0 0 0 -1 -1 1 1 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 -1 1 0 0 -1 0 -1 0
 0 0 0 0 0 0 -1 0 0 0 -1 1 0 0 0 0 -1 1 -1 0 0 -1 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0
1 0 0 0 -1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 -1 1 1 0 0 0 0 0
0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 1 -1 0 -1 0 0 0 0 0 0 -1 0 1 1 0 0 0 0 0 -1 -1 0 0 0
 0 0 1 0 -1 0 1 1 0 -1 0 -1 -1 0 0 0 0 -1 -1 0 0 0 0 -1 1 -1 0
bits = 551
```

Рис. 5. Случайные коэффициенты для полинома *r* в нужном количестве

Заключение

Появление квантовых компьютеров ставит под угрозу безопасность всей информации, защищемой методами классической криптографии (RSA, ЭЦП, Эль-Гамаль, DH) [12]. Необходимо уже сейчас задумываться о системах защиты (например NTRU), которые будут стойки к атакам с подобных устройств. Одна из сложностей реализации системы NTRU залючается в том, что несколько раз нужно из набора многочленов выбрать «произвольный» многочлен с заданным во входных параметрах количеством определенных коэффициентов. В данной статье предложен метод генерации случайных компонент для системы NTRU, который позволяет это решить. Метод основан на свойстве арифметического кодирования с разделением интервала (АКРИ) получить в результате полностью случайную закодированную последовательность кода.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Буковшин, В.А., Чуб, П.А., Черкесова, Л.В., Короченцев, Д.А., Поркшеян, В.М. Анализ современных постквантовых алгоритмов шифрования / В.А. Буковшин – Научное обозрение №4: Технические науки, 2005. – 128 с.

2. Дрон, К.К. О перспективах совместного использования методов квантовой и классической криптографии / К.К Дрон. – Вестник Хакасского государственного университета им НФ Катанова. – 2018. – № 24. – С. 8-11.

3. Кузьмин, Т. В. Криптографические методы защиты информации / Т.В. Кузьмин. – Москва: Огни, 2013. – 192 с.

4. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. NTRU: A Ring Based Public Key Cryptosystem. In Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267–288.

5. Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch. NTRU Prime: reducing attack surface at low cost. / D.J. Bernstein – URL: https://eprint.iacr.org/2016/461.pdf (дата обращения: 15.10.2020).

6. Авдошин, С. Дискретная математика. Модулярная алгебра, криптография, кодирование [Текст] / С. Авдошин – Москва: СИНТЕГ, 2016. – 260 с.

7. Fionov A. Universal homophonic coding // 2001 IEEE International Symposium on Information Theory (ISIT 2001). – Washington, DC, USA, June 24-29, 2001. – P. 116.

8. Jendal H. N., Kuhn Y. J. B., Massey J. L. An information-theoretic treatment of homophonic substitution // Advances in Cryptology Eurocrypt- 89. – Berlin: Springer-Verlag, 1990. – P. 382–394 (Lecture Notes in Computer Science; V. 434).

9. Rissanen J. J., Langdon G. G. Arithmetic coding // IBM J. Res. Dev. – 1979. – V. 23, No2. – P. 149–162.

10. Фионов А. Н. Эффективный метод рандомизации сообщений на основе арифметического кодирования. – 1997. – Т. 4, No 2. – С. 51–74.

11. Fionov A. Random number generation via homophonic coding [Text] // 2000 IEEE International Symposium on Information Theory (ISIT 2000). – Sorrento, Italy, June 25–30, 2000. – P. 354.

12. Хоффман, Л. Дж. Современные методы защиты информации / Л. Дж. Хоффман – СПб: Питер**,** 2014. – 264 с.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-137-143

Е. А. Кузнецова[1], А. Н. Фионов[1]*

Обработка данных, полученных с сцинтилляционного экрана

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: elizaveta.kuznetsova04@mail.ru

Аннотация. Данная статья посвящена обработке данных, полученных с сцинтилляционного экрана. В работе использовались методы и материалы, описанные в книге В.В. Смалюк «Диагностика пучков заряженных частиц в ускорителях». В работе были исследованы различные методы обработки данных, полученных с сцинтилляционного экрана, включая алгоритмы для определения энергии и угла вылета частиц. Были получены результаты, подтверждающие эффективность предложенных методов обработки данных. В заключении подчеркивается, что данная работа может быть использована в качестве основы для дальнейшего развития методов обработки данных в области оптики.

Ключевые слова: диагностика, пучки частиц, сцинтилляционного экрана

E. A. Kuznetsova[1], A. N. Fionov[1]*

Processing of data received from the scintillation screen

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: elizaveta.kuznetsova04@mail.ru

Abstract. This article is devoted to the processing of data obtained from the scintillation screen. The methods and materials described in V.V. Smalyuk's book «Diagnostics of charged particle beams in accelerators» were used in the work. Various methods of processing data obtained from the scintillation screen were investigated, including algorithms for determining the energy and angle of departure of particles. The results confirming the effectiveness of the proposed data processing methods were obtained. In conclusion, it is emphasized that this work can be used as a basis for further development of data processing methods in the field of optics.

Keywords: diagnostics, particle beams, scintillation screen

Введение

Сцинтилляционный экран – это устройство, используемое в различных областях науки, включая оптику, физику, медицину и другие. Он используется для обнаружения и измерения различных типов излучения, таких как заряженные частицы, фотоны и электроны. В качестве материала для экрана используются различные сцинтилляционные кристаллы, которые преобразуют энергию частиц в световые вспышки.

Одной из главных задач при работе с сцинтилляционными экранами является обработка данных, получаемых от них. Обработка этих данных может быть трудоемкой задачей, особенно когда необходимо анализировать большое количество данных. Кроме того, точность измерений зависит от правильной обработки данных.

Для обработки данных, полученных с сцинтилляционного экрана, можно использовать различные методы, такие как методы фильтрации, преобразования Фурье, методы машинного обучения и другие. Каждый из этих методов имеет свои преимущества и недостатки и может быть применен в зависимости от конкретной задачи.

В данной работе будет рассмотрен метод обработки данных, основанный на использовании оптических камер и программного обеспечения. Данный метод был применен для обработки данных, полученных с сцинтилляционного экрана. Далее в статье будет описано подробное описание метода, а также результаты экспериментов, проведенных с его помощью.

Методы и материалы

Для обработки данных, полученных с сцинтилляционного экрана, использовалась программная обработка изображений. Для сбора данных была использована камера, которая устанавливалась на определенном расстоянии от экрана. Изображения и видео с камеры загружались в программу для получения контура вспышки.

Для разработки программы использовался язык программирования Python, а также ключевые библиотеки OpenCV, NumPy и pyqtgraph. Программа позволяет автоматически обрабатывать изображения и видео, полученные с камеры, и выводить на экран график распределения вспышек на сцинтилляционном экране.

Одной из ключевых особенностей программы является возможность автоматического определения момента возникновения вспышки на экране. Для этого был использован алгоритм, который автоматически определяет пороговое значение яркости и срабатывает, когда это значение превышается. Кроме того, программа также позволяет ручное управление процессом съемки, что дает пользователю большую гибкость в проведении экспериментов.

Для анализа данных использовались методы обработки изображений, в том числе фильтрация, выделение контуров, определение координат центра вспышки и расчет интенсивности свечения. Результаты обработки данных выводились на экран в виде графиков.

Для регистрации траекторий частиц, которые проходят через люминесцентный экран, используются камеры, установленные в ускорителе частиц. Камеры устанавливаются с разных сторон экрана под разными углами, чтобы обеспечить наиболее полное покрытие экрана и зафиксировать как можно больше проходящих частиц [2]. Камеры должны быть чувствительны к свету, излучаемому экраном, и передавать сигналы на приемник для обработки данных. Для достижения наилучшего качества изображения камеры могут быть синхронизированы с ускорителем частиц. Важно также учитывать, что установка камер может повлиять на детектируемый сигнал и способность экрана регистрировать прохождение частиц, поэтому необходимо тщательно выбирать места установки камер и проводить калибровку системы для оптимальной работы. Камеры могут быть оснащены оптическими системами, такими как объективы, фильтры и затворы, чтобы обеспечить наилучшее качество изображения.

Обсуждения

Для измерения поперечного распределения плотности пучка частиц используется оптико-электронный прибор – ПЗС-матрица (рис. 1). ПЗС-матрица используется для получения изображения поперечного распределения плотности пучка в диагностике пучков частиц [3]. Этот оптико-электронный прибор состоит из двумерного массива полупроводниковых ячеек, размером от 5 до 20 мкм, разделенных слоем диэлектрика от подложки из поликристаллического кремния. К ячейкам прикладывается напряжение от внешнего источника, которое формирует электрическое поле. Положительное напряжение на электродах создает потенциальную яму, в которую направляются возбужденные фотонами электроны из валентной зоны. В этой потенциальной яме заряд сохраняется до момента считывания.

Чем интенсивнее световой поток в течение экспозиции, тем больше электронов накапливается в потенциальной яме, и тем выше заряд данной ячейки. Для считывания накопленного заряда поликремневые затворы должны выполнить роль сдвиговых регистров таким образом, чтобы они образовали конвейерную цепочку вдоль одной оси [4]. Поочередная активация регистров позволяет последовательно считывать заряд из каждой ячейки матрицы и формировать двумерное изображение.

В настоящее время CCD-приборы широко используются в цифровой фотографии как параллельно-последовательные преобразователи массива сигналов фоточувствительных элементов [5].

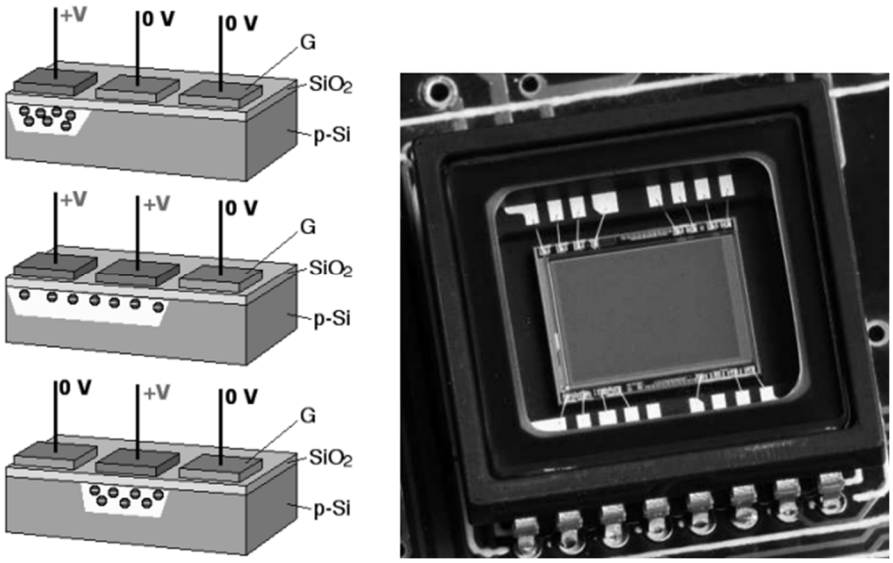


Рис.1. ПЗС-матрица: а- принцип работы; б- внешний вид

Результаты

Для регистрации вспышек была разработана программа, реализованная на языке программирования Python (рис. 2) [6]. Python является интерпретируемым языком программирования, который обладает многими преимуществами для

научных исследований. Python имеет обширную стандартную библиотеку, а также множество сторонних библиотек, таких как OpenCV, Numpy и PyQt5, которые содержат множество полезных инструментов для научных исследований [7].

OpenCV (Open Source Computer Vision Library) – это библиотека с открытым исходным кодом для обработки изображений и компьютерного зрения. Она предоставляет множество инструментов для работы с изображениями, включая их загрузку, обработку, анализ и визуализацию. OpenCV написана на языке программирования C++, но имеет интерфейсы для других языков, включая Python [8].

PyQt5 – это библиотека на языке программирования Python, которая используется для создания графических пользовательских интерфейсов. Она содержит множество инструментов для создания элементов управления, окон, диалогов, меню и других элементов пользовательского интерфейса. PyQt5 основана на Qt, кроссплатформенном фреймворке для разработки программного обеспечения на языке программирования C++. PyQt5 обладает множеством возможностей для создания мощных и удобных пользовательских интерфейсов и позволяет создавать кроссплатформенные приложения, которые могут работать на различных операционных системах, включая Windows, macOS и Linux.

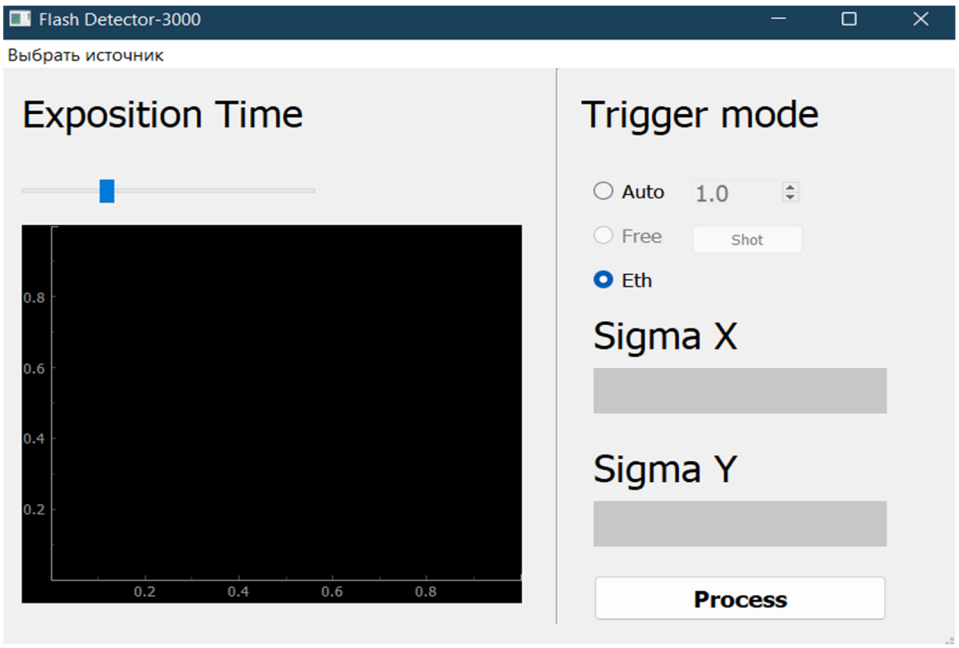


Рис. 2. Окно Flash Detector-3000

Данная программа обладает тремя основными источниками работы (рис. 2). В первую очередь, она предназначена для анализа отдельных изображений световых пучков. Во-вторых, программа способна распознавать световые пучки на видеозаписи, загруженной в программу [1]. И, наконец, она позволяет распознавать световые вспышки в режиме реального времени.

Для реализации данных функций, в программе используется набор инструментов, основанных на алгоритмах обработки изображений и компьютерного

зрения. Одним из ключевых инструментов, на котором базируется программа, является библиотека OpenCV. Данная библиотека предназначена для работы с изображениями и видео, а также содержит в себе множество алгоритмов для обнаружения и распознавания объектов на изображениях.

В качестве тестовой фотографии была выбрана фотография вспышки, возникшей на экране (рис.3).

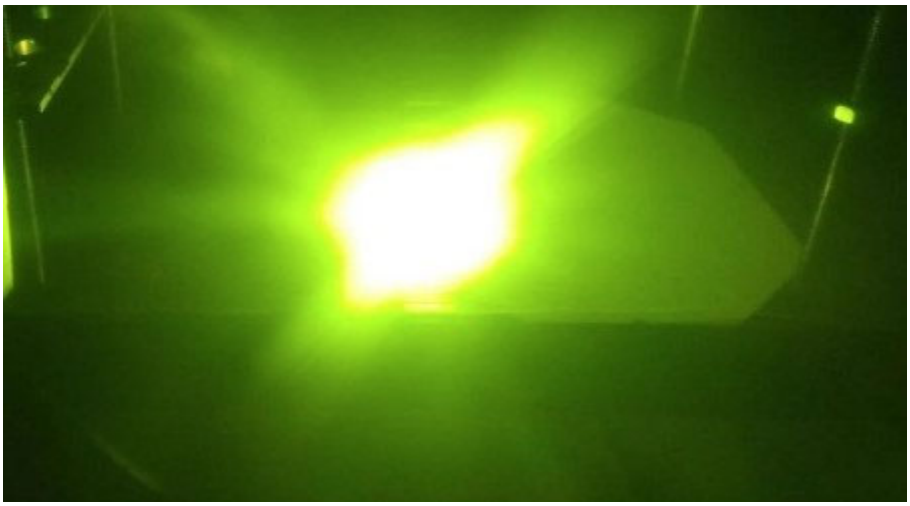


Рис. 3. Тестовая вспышка

При нажатии на кнопку «Process» происходит запуск программы, после чего пучок света полученный на изображении распознается и выводится на график, также отображается sigma x и sigma y в соответствующих полях окна программы, которые отображают верхнюю границу по x и y на графике (рис. 4).

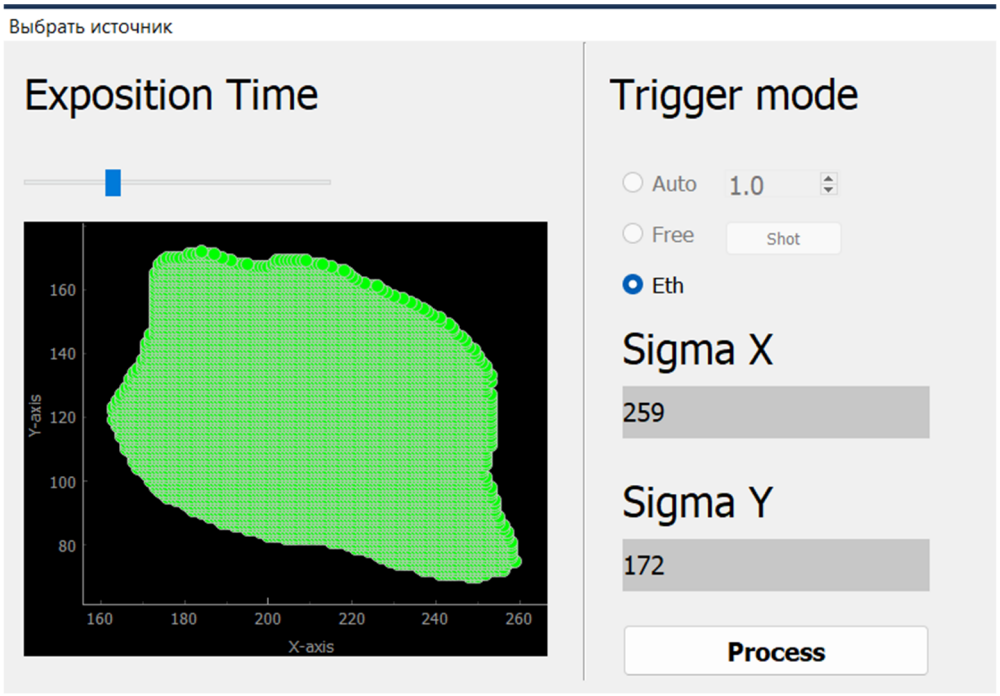


Рис. 4. Окно программы с демонстрацией режима «изображение»

Заключение

В данной работе были рассмотрены методы обработки данных, полученных с сцинтилляционного экрана, а также разработана программа для автоматической обработки изображений и видео с камеры. Целью работы было определение свойств пучков заряженных частиц на основе данных, полученных с экрана. Была рассмотрена актуальность и значимость обработки данных сцинтилляционных экранов. Важность этой работы заключается в возможности получения более точных результатов и более полного анализа пучков заряженных частиц. В ходе эксперимента была разработана программа на языке программирования Python, которая позволяет автоматически обрабатывать изображения и видео, полученные с камеры. Программа была протестирована на сцинтилляционном экране, и были проведены различные эксперименты для проверки ее эффективности и точности.

Результаты эксперимента показали, что разработанная программа успешно выполняет обработку данных, полученных с сцинтилляционного экрана. Она позволяет автоматически обнаруживать вспышки на экране, делать соответствующие снимки и проводить обработку изображений для определения координат пучков заряженных частиц. Программа также предоставляет возможность ручного управления процессом съемки, что позволяет исследователям гибко настраивать параметры эксперимента. Она позволяет анализировать данные и строить графики, отображающие зависимость координат вспышек от времени.

В заключение, разработанная программа для обработки данных, полученных с сцинтилляционного экрана, оказалась эффективной и точной в определении свойств пучков заряженных частиц. Она позволяет автоматически обрабатывать изображения и видео, полученные с камеры, и предоставляет удобные инструменты для анализа и визуализации данных. Эта программа может быть полезна для исследователей в области оптики, физики высоких энергий и других областей, где требуется обработка данных с сцинтилляционных экранов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванов, А. Б. Разработка алгоритмов распознавания вспышек на сцинтилляционном экране [Текст] / А. Б. Иванов, В. Г. Петров // Вестник Московского университета. Серия 3: Физика, астрономия. - 2019. - Т. 6. - С. 65-71.

2. Козлов, В. А. Применение методов машинного обучения для распознавания вспышек на сцинтилляционном экране [Текст] / В. А. Козлов, С. В. Смирнов // Физика и техника полупроводников. - 2021. - Т. 55, № 2. - С. 245-249.

3. Сидоров, Д. В. Разработка программы для автоматического считывания данных с сцинтилляционного экрана [Текст] / Д. В. Сидоров, Е. В. Никитина // Материалы IV Международной научно-технической конференции "Современные проблемы инженерии и информационных технологий". - 2022. - С. 101-105.

4. Федоров, Н. В. Применение библиотеки OpenCV для обработки изображений с сцинтилляционного экрана [Текст] / Н. В. Федоров, А. И. Иванов // Труды Международной научно-практической конференции "Информационные технологии и системы". - 2020. - С. 214-219.

5. Чернышев, С. Г. Программное обеспечение для сшивки изображений с сцинтилляционного экрана [Текст] / С. Г. Чернышев, О. А. Корнилова // Современные технологии в науке и образовании. - 2018. - Т. 1, № 5. - С. 111-116.

6. Python [Электронный ресурс]. - URL: https://www.python.org/ (дата обращения: 02.05.2023).
7. OpenCV [Электронный ресурс]. - URL: https://opencv.org/ (дата обращения: 02.05.2023).
8. PyQt5 [Электронный ресурс]. - URL: https://pypi.org/project/PyQt5/ (дата обращения: 02.05.2023).

УДК 539.1.03
DOI 10.33764/2618-981X-2023-6-144-147

Е. А. Кузнецова[1], А. Н. Фионов[1,2]*

Технические вопросы построения сцинтилляционного экрана

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: elizaveta.kuznetsova04@mail.ru

Аннотация. Для проведения диагностики пучка используются сцинтилляционные датчики (люминофоры). Люминофоры уже более ста лет служат средством диагностики ионизирующего излучения. Были рассмотрены основные свойства люминофоров и определен наиболее оптимальный люминофор для диагностики – им является Chomax. Данная диагностика проводится для создания синхротронного испытательного комплекса. Синхротронный комплекс испытательный предназначен для генерации интенсивных протонных и ионных пучков, и их транспортировки к облучательным портам. Целью данной статьи является расчет параметров потерь от одного типа частиц к другим. Расчет параметров проводится с помощью формулы Бете-Блоха. По итогам статьи было определено соотношение для дальнейшей диагностики пучков ионов.

Ключевые слова: люминофор, пучки ионов, сцинтилляционный экран

E. A. Kuznetsova[1], A. N. Fionov[1, 2]*

Technical Aspects of Building a Scintillation Screen

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: elizaveta.kuznetsova04@mail.ru

Abstract. Scintillation sensors (phosphors) are used to diagnose the beam. Phosphors have been used as a diagnostic tool for ionizing radiation for more than a hundred years. Earlier, the main properties of phosphors were considered and the most optimal phosphor for diagnostics was determined – it is Chomax. This diagnosis is carried out to create a synchrotron test complex. The synchrotron test complex is designed to generate intense proton and ion beams and transport them to irradiation ports. The purpose of this work is to calculate the parameters of losses from one type of particle to another. The parameters will be calculated using the Bethe-Bloch formula. Based on the results of the work, the ratio for further diagnosis was determined.

Keywords: luminophore, ion beams, scintillation screen

Введение

Люминофоры уже более ста лет служат средством диагностики ионизирующего излучения. Люминофорами называются химические вещества в виде пигментов или порошков, преобразующие лучистую энергию, которую они поглощают, в световое излучение [1]. Производство люминофоров строится, в основ-

ном, на базе цинка – это его сульфиды и сульфаты, а также на базе алюминия — это алюминаты редкоземельных металлов [2]. Сцинтилляционный экран - это устройство для регистрации и измерения энергии ионизирующих излучений, таких как гамма-лучи, рентгеновские лучи и частицы высокой энергии. Он состоит из сцинтиллятора - материала, который при взаимодействии с частицами или фотонами выделяет световые фотоны или электроны, также называемые "сцинтилляциями" [3]. Были рассмотрены основные свойства люминофоров и определен наиболее оптимальный люминофор для диагностики – им является Chomax. Данная диагностика проводится для создания синхротронного испытательного комплекса [4]. Синхротронный комплекс испытательный (СКИ) предназначен для генерации интенсивных протонных и ионных пучков, и их транспортировки к облучательным портам (ОП).

Методы и материалы

Существуют специфичные средства диагностики пучка, но в данном случае будет использоваться сцинтилляционный датчик, либо просто люминофор. Выглядит он следующим образом: имеется поперечное сечение камеры и в определённом месте имеется сильфон (вакуумно-плотная трубка, которая имеет свойство сжиматься и разжиматься) и имеется экран на который нанесен сцинтилляционный материал, и есть привод, который вводит ионы в камеру, и пучок, попадая в экран, теряет часть энергии, что приводит к высвобождению этой энергии в виде светового излучении [5]. Потери энергии описываются по формуле Бете - Блоха. Формула Бете – Блоха – формула для удельной ионизационной потери энергии при прохождении заряженных частиц через вещество.

Удельная потеря энергии $\frac{dE}{dx}$ описывается формулой:

$$\frac{dE}{dx} = 4\pi E_e r_e^2 \frac{n_e Z_0^2}{\beta^2}\left(\frac{1}{2} ln \frac{2E_e \gamma^2 \beta^2 E_{\max}}{I^2} - \beta^2\right), \quad (1)$$

где $E_e = m_e c^2 \simeq 0{,}51$ МэВ – энергия покоя электрона; $n_e = \frac{\rho N_A Z}{A}$ – плотность электронов в веществе (N_A – число Авогадро, Z – атомный номер, A – атомная масса, ρ – плотность); Z_0 – заряд частиц пучка в единицах заряда протона; $r_e = 2{,}818 \cdot 10^{-15}$ м – классический радиус электрона; $\beta = \frac{v}{c}$ и $\gamma = \frac{1}{1 - \beta^2}$ – релятивистские параметры частиц пучка; $I \simeq 13{,}5 \cdot Z$ эВ — средний потенциал ионизации вещества. E_{max} – максимальная энергия, которую может передать частица пучка электрону вещества, показанная в формуле:

$$E_{\max} = \frac{2E_e \beta^2 E^2}{E_0^2 + E_e^2 + 2E_e E}, \quad (2)$$

где E_0 – энергия покоя и $E = \gamma E_0$, E – полная энергия частиц пучка. Для тяжелых частиц (протонов и ионов) $E_{max} = 2E_e\beta^2\gamma^2$, для ультрарелятивистских электронов и позитронов ($\gamma \gg 1$, $\beta = 1$) $E_{max} = \gamma E_e = E$.

Формула Бете-Блоха была выведена для тяжелых частиц – протонов и ионов [6]. Для легких частиц – электронов и позитронов – формула расчета удельной потери энергии на ионизацию, встречающаяся в литературе, содержит дополнительные члены:

$$\frac{dE}{dx} = 2\pi E_e r_e^2 \frac{n_e}{\beta^2}[ln\frac{(\gamma-1)E_e^2\beta^2\gamma^2}{2I^2} - (\frac{2}{\gamma} - 1 + \beta^2)ln2 + \frac{1}{\gamma^2} + \frac{1}{8}(1-\frac{1}{\gamma})^2]. \quad (3)$$

У СКИ есть набор элементов, которые она производит и диагностику которых надо выполнять. Основной вопрос – это радиационная стойкость веществ. В Институте ядерной физики СО РАН имеется протонный ускоритель Тандем-БНЗТ (Тандем-БНЗТ), на котором будет проводится испытание радиационной стойкости Chomax [7].

Проблема в том, что на СКИ используются тяжелые ионы, а на Тандем – БНЗТ протоны, и необходимо посчитать параметры потерь от одного типа частиц к другим. Нужно взять из частиц ионов ту, которая вносит больше всего радиационных потерь в люминофор, и самую тяжелую (большой заряд и маленькая скорость) [8].

Результаты

Используя формулу Бета-Блоха (формула (1)) проанализировали и посчитали в каком соотношении находится доза, потерянная протонами на 2 мэВ пучке Тандем - БНЗТ и те параметры пучка, которые есть у СКИ ПЗ [9]. Исходя из формулы (1) получаем выражение:

$$-\frac{dT}{dx} \sim A\frac{z^2}{\gamma^2}N, \quad (4)$$

при условии γ↑ , $\frac{dT}{dx}$↓; z↑ , $\frac{dT}{dx}$↑. (табл. 1).

Таблица 1

Сводная характеристика

Частицы	Z	N	γ,(N_eV)	$\frac{dT}{dx}$
Bi	-50	10^8	$3{,}5\cdot10^{-3}$	$AN_1\frac{2500}{12\cdot25\cdot10^{-6}} = 200AN_1\cdot10^{-6}$
P	-1	10^{11}	$7{,}5\cdot10^{-3}$	$AN_2\frac{1}{56\cdot25}10^6 = 0{,}018AN_2\cdot10^6$

Частицы	Z	N	γ,(N_eV)	$\frac{dT}{dx}$
Ag	-25	10^8	$3{,}5\cdot10^{-3}$	$AN_3\frac{625}{12\cdot25}10^6 = 50AN_3\cdot10^6$
$P_{бнзт}$	-1	N_0	$1{,}8\cdot10^{-3}$	$AN_0\frac{1}{9\cdot24}10^6 = 0{,}3AN_0\cdot10^6$

$$Ag:\frac{N_3}{N_0}\cdot\frac{50\cdot10^6}{0{,}3\cdot10^6}=1\rightarrow N_0=N_3\cdot324\cdot50=1{,}5\cdot10^{10},$$

$$Bi:\frac{N_1}{N_0}\cdot\frac{200\cdot10^6}{0{,}3\cdot10^6}=1\rightarrow N_0=N_1\cdot3\cdot24\cdot200=6\cdot10^{10},$$

$$p:\frac{N_2}{N_0}\cdot\frac{0{,}018\cdot10^6}{0{,}3\cdot10^6}=1\rightarrow N_0=N_2\frac{3\cdot24}{56{,}25}=5{,}78\cdot10^9,$$

$$Ag:\frac{N_3}{N_0}\cdot\frac{50\cdot10^6}{0{,}3\cdot10^6}=1\rightarrow N_0=N_3\cdot324\cdot50=1{,}5\cdot10^{10}.$$

Если $N_0 = 10^{12}$, то один выстрел ионов у Bi равен 17 выстрелам протонов, у p равен 170 выстрелам протонов, у Ag равен 50 выстрелам протонов. Зная параметры пучка ионов, вычислили соотношения для протонов [10].

Заключение

В данной статье были рассчитаны соотношения ионов к протонам для дальнейшего проведения испытаний для диагностики пучков, необходимых для разработки СКИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Борн, М.Э. Основы оптики / М.Э. Борн. – Москва: Наука, 1973. – 215 с.
2. Булина, Н. А. Детонационное напыление гидроксиапатита на имплантат из титанового сплава / Н. А. Булина. – Москва: Материалы, 2021. – 169 с.
3. Бутслов, М.М. Электронно-оптические преобразователи и их применение в научных исследованиях / М.М. Бутслов. – Москва: Наука, 1978. – 225 с.
4. Бутслов, М. М. Электрофоретические люминесцентные экраны для ЭОП / М. М. Бутслов. — Москва: Наука, 1976. - 231 с.
5. Глобус, М. Е. Неорганические сцинтилляторы / М. Е. Глобус. – Харьков: Акта, 2000. – 174 с.
6. Казянкин, О. Н. Неорганические люминофоры / О. Н. Казянкин. – Москва: Химия, 1975. – 246 с.
7. Калашникова, В. И. Сцинтилляционные счетчики / В. И. Калашникова. – Москва: Наука, 1966. – 279 с.
8. Михайлов, М.М. Термостабилизирующие покрытия BaTiO3, синтезированные методом детонационного напыления, Технология поверхностей и покрытий / М.М. Михайлов. – Москва, 2017. – 192 с.
9. Пустоваров, В.Д. Люминесценция твердых тел / В. Д. Пустоваров. – Екатеринбург: Издательство Уральского университета, 2017. — 272 с.
10. Соболева, Н. А. Фотоэлектронные приборы / Н. А. Соболева. – Москва: Высшая школа, 1974. – 219 с.

УДК 004
DOI 10.33764/2618-981X-2023-6-148-152

Н. С. Кукушкина[1]*, *Е. Ю. Воронкин*[1]

Исследование возможности применения мультиагентных систем для организации работы технической поддержки внутри организации

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: prostomatika@mail.ru

Аннотация. В статье представлено исследование возможности применения мультиагентных систем для организации работы технической поддержки внутри организации. Описана актуальность проблемы и необходимость ее решения путем постановки цели, определения задач и выбора методики. Проведен обзор литературы и изучены уже существующие подходы к организации работы технической поддержки. Приведено обоснование выбора конкретной методики решения. Представлены основные понятия, используемые в ходе описания исследования. Статья представляет собой исследование, которое рассматривает возможность применения мультиагентных систем для улучшения работы технической поддержки внутри организации.

Ключевые слова: мультиагентные системы, анализ, агент, бизнес-организации, заявка, исследование

N. S. Kukushkina[1]*, *E. Yu. Voronkin*[1]

Research of the Possibility of Using Multi-Agent Systems for Organizing the Work of Technical Support Within the Organization

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: prostomatika@mail.ru

Annotation. The article presents a study of the possibility of using multi-agent systems to organize the work of technical support within an organization. The relevance of the problem and the need to solve it by setting goals, defining tasks and choosing a methodology are described. To achieve this goal, a methodology for analyzing existing solutions was chosen. A review of the literature was carried out and existing approaches to organizing the work of technical support were studied. The rationale for choosing a specific solution methodology is given. The main concepts used in the course of the description of the study are presented. The article considers the possibility of using multi-agent systems to improve the work of technical support within an organization.

Keywords: multi-agent systems, analysis, agent, business organizations, application, research.

Введение

В настоящее время бизнес-организации сталкиваются с ростом количества заявок технической поддержки на различные продукты и услуги. Некоторые из этих заявок могут быть повышенного спроса и требовать мгновенного или быстрого решения. Оптимизация распределения таких заявок может быть важной задачей для организации, и мультиагентные системы представляют собой полезный инструмент для решения подобных проблем.

Цель анализа: определение возможности применения мультиагенстных систем для распределения клиентских обращений к специалистам технической поддержки внутри организации.

Для решения поставленной цели были выявлены ряд задач:

– дать понятия основным терминам;

– провести анализ возможности применения мультиагентных систем в исследуемой области.

Мультиагентная система – это совокупность двух или более агентов, которые взаимодействуют друг с другом для достижения общей цели. Каждый агент в мультиагентной системе обладает своим набором знаний, умений и правил поведения, которые позволяют ему решать определенные задачи и совместно работать с другими агентами для достижения общего результата [1– 3].

Любой агент обладает следующими свойствами:

1. активность – то есть каждый агент способен к организации и реализации действии (в соответствии с внутренним алгоритмом функционирования);
2. автономность – относительная независимость от окружающей среды;
3. целенаправленность – наличие собственных источников мотивации (у каждого агента присутствует некоторая цель, для достижения которой он функционирует) [4–6].

Как было отмечено выше, у каждого агента существует цель. Группу агентов, имеющих одинаковую цель, объединяют в класс агентов.

На рис. 1 представлено 2 варианта построения схемы программного продукта:

4. традиционная схема построения программной системы;
5. схема, базирующаяся на мультиагентных системах.

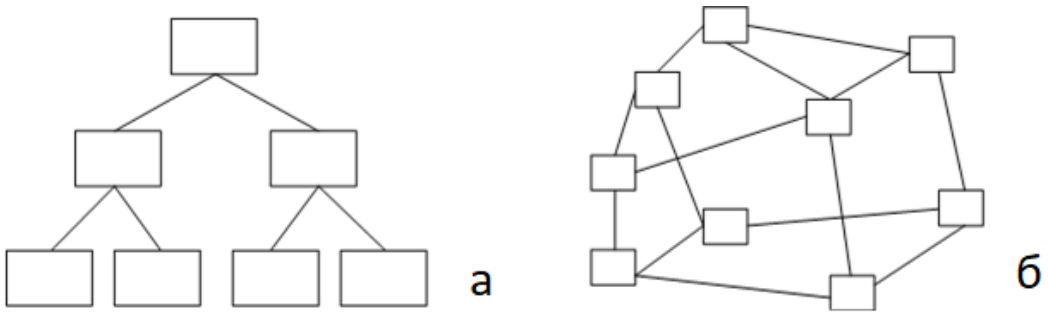


Рис. 1. Традиционная схема построения программной среды (а)
и мультиагентная система (б)

Каждый агент в мультиагентной системе выполняет свою задачу, основываясь на информации, полученной от других агентов. Такой подход к решению задач называется распределенным интеллектом. Каждый агент в мультиагентной системе является автономным и способен принимать решения на основе своих

знаний и опыта. Однако, чтобы достичь общей цели, агенты должны обмениваться информацией и координировать свои действия.

Для обмена информацией между агентами используются различные протоколы и алгоритмы, такие как протоколы передачи сообщений, распределенные базы данных и механизмы согласования. Кроме того, для эффективной координации действий агентов могут использоваться различные методы, такие как механизмы распределения задач, аукционы и коалиции. [7– 9].

В технической поддержке мультиагентные системы могут использоваться для автоматизации процесса обработки заявок от пользователей. Каждый агент может иметь свою область компетенции, например, один агент может решать проблемы с аппаратным обеспечением, а другой – с программным обеспечением.

На рис. 2 представлен пример схемы мультиагентной системы для организации поддержки внутри организации.

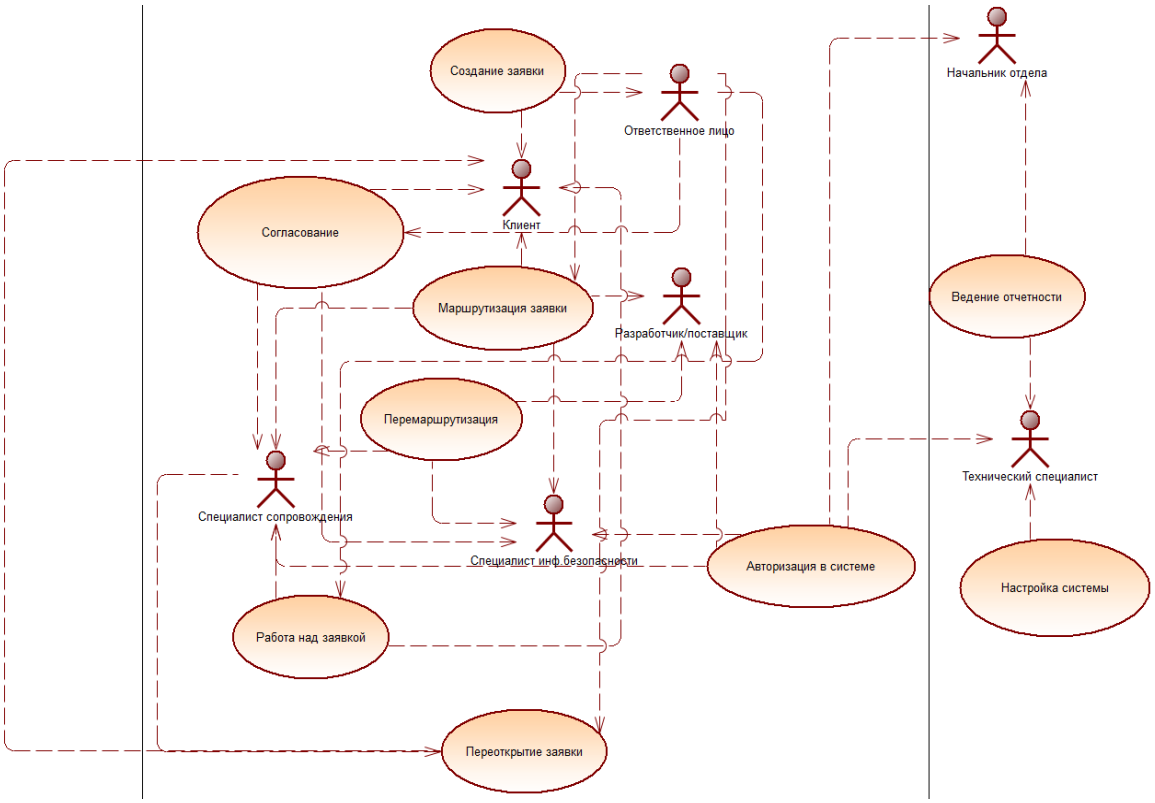


Рис. 2. Пример схемы мультиагентной системы для организации поддержки внутри организации

Результаты

Мультиагентные системы могут быть последовательно применены к различным задачам технической поддержки и оптимизировать процесс обслуживания клиентов в организации.

Они могут помочь автоматизировать процесс управления заявками, оптимизировать распределение задач, повысить скорость реакции на запросы клиентов и улучшить качество обслуживания.

Ниже приведены возможности, которые могут быть реализованы с помощью мультиагентных систем при распределении заявок технической поддержки:

– автоматическое распределение заявок: мультиагентные системы могут автоматически распределять заявки между различными техническими специалистами на основе различных критериев, таких как навыки, опыт, доступность и загруженность. Это позволит быстро и эффективно отвечать на запросы клиентов и улучшить качество обслуживания;

– мониторинг выполнения: мультиагентная система может мониторить выполнение задач технической поддержки, уведомлять о возможных задержках и перераспределять заявки, чтобы обеспечить эффективное выполнение задач вовремя;

– поддержка коммуникации: мультиагентные системы могут обеспечить коммуникацию между людьми, которые работают над решением проблемы клиента, и автоматически уведомлять о статусе решения проблемы;

– оптимизация использования ресурсов: мультиагентные системы могут рассчитывать оптимальную нагрузку на различных специалистов технической поддержки, что позволит улучшить распределение нагрузки и повысить эффективность выполнения задач;

– улучшение качества обслуживания: мультиагентные системы позволяют усовершенствовать процесс обслуживания клиентов, уменьшать ожидание ответа на запросы, решать проблемы быстрее и улучшать доверие клиентов к организации [10–14].

Выводы

Исследование показало, что мультиагентные системы могут быть эффективным инструментом для управления заявками технической поддержки внутри организации. Они позволяют автоматизировать процессы обработки заявок, ускорить время реакции на проблемы и повысить качество обслуживания клиентов.

В рамках исследования были определены основные термины, связанные с мультиагентными системами, такие как агент, мультиагентная система, активность, автономность и т.д. Это позволило установить общий язык для дальнейшего обсуждения темы.

Также были решены поставленные задачи:

– даны понятия основным терминам;

– проведен анализ возможности применения мультиагентных систем в исследуемой области.

Также был проведен анализ возможности применения мультиагентных систем в исследуемой области. Были выявлены преимущества и недостатки такого подхода, а также определены основные задачи, которые могут быть решены с помощью мультиагентных систем. В результате исследования было установлено, что мультиагентные системы могут быть полезным инструментом для управления заявками технической поддержки внутри организации, что может положительно сказаться на репутации и результатах деятельности компании.

Данный подход применим при разработке системы маршрутизации заявок внутри организации, а также является наиболее оптимальным решением.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Expert Systems : монография / Cornelius T. Leondes – Academic Press, 2001. – 1947 с. – ISBN 978-0124438804 – Текст : непосредственный.
2. Make Your Own Neural Network : учебное пособие / Tariq Rashid – CreateSpace Independent Publishing Platform, 2016. – 222 с. – ISBN 978-1530826605 – Текст : непосредственный.
3. Базы данных и знаний : монография / Никитина Т. П. – Ярославль : Изд-во ЯГТУ, 2003. – ISBN 5-230-20603-9 – Текст : непосредственный.
4. Введение в мультиагентные технологии : [сайт]. – URL: http://www.kg.ru/technology/multiagent/ (дата обращения: 20.12.2022). – Текст: электронный.
5. Использование продукционной модели представления знаний при проектировании экспертной системы : статья в сборнике статей / БЕЛЯКОВ Е.А. – Хабаровск : Тихоокеанский государственный университет, 2014. – 307 с. – ISBN 978-5-7389-1491-1 – Текст : непосредственный.
6. Использование нейросетевых технологий для построения экспертных систем: статья в сборнике статей / Варламов О.О., Чибирова М.О., Хадиев А.М. [и др.]. – Москва : Общество с ограниченной ответственностью "Международный центр науки и образования", 2018. – 83 с. – Текст : непосредственный.
7. Интеллектуальные системы : монография / Курейчик В. М, Сороколетов П. В. – Москва : ООО Издательская фирма "Физико-математическая литература", 2007. – 295 с. – ISBN 5-9221-0096-3 – Текст : непосредственный.
8. Особенности экспертных систем и оправданность их применения в реальных проектах : статья в сборнике статей / Петрунина И. Н. – Москва : Общество с ограниченной ответственностью "Интернаука", 2017. – 155 с. – Текст : электронный.
9. Разработка экспертных и обучающих систем на основе принципов искусственного интеллекта : статья в сборнике статей / Суконщиков А. А. – Вологда : Вологодский политехнический институт, 1997. – 248 с. – Текст : непосредственный.
10. Разработка пользовательских интерфейсов : монография / Дженифер Тидвелл – Москва : Питер, 2011. – ISBN 978-5-459-00434-2 – Текст : непосредственный.
11. Нейросетевая экспертная система на основе прецедентов для решения проблем абонентов сотовой связи : монография / Малыхина М. П., Бегман Ю. В. – Краснодар : ООО "Издательский Дом-Юг", 2011. – 150 с. – ISBN 978-5-91718-132-5 – Текст : непосредственный.
12. Тестирование экспертных систем при эксплуатации и сопровождении : монография / Фатхи В. А., Фатхи Д. В. – Ростов-на-Дону : ГОУ РГАСМ, 2008. – 81 с. – ISBN 978-5-89071-160-1 – Текст : непосредственный.
13. Теория и методы решения многовариантных неформализованных задач выбора : монография / Лазарсон Э. В. – Старый Оскол : ООО «Тонкие наукоемкие технологии», 2018. – 240 с. – ISBN 978-5-94178-042-6 – Текст : непосредственный.
14. Человеко-машинное взаимодействие. Теория и практика разработки интерфейса человек - компьютер : монография / Матасова Ю. А – Новосибирск : Новосибирская гос. акад. водного трансп., 2008. – 73 с. – Текст : непосредственный.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-153-159

А. А. Литвяков[1]*, *И. Н. Карманов*[1]

Оценка риска нарушения конфиденциальности информации с использованием лазерных систем разведки

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: mr.go_old@mail.ru

Аннотация. Статья посвящена исследованию потенциальных угроз и уязвимостей нарушения конфиденциальности информации с использованием лазерных систем разведки на основе банка данных угроз Федеральной Службы технического и экспортного контроля. В статье проводится анализ возможных угроз и уязвимостей, связанных с применением лазерных систем разведки, включая возможность несанкционированного доступа к конфиденциальным данным, перехвата информации, нарушения конфиденциальности передачи данных и других аспектов информационной безопасности. Базируясь на банке данных угроз Федеральной Службы технического и экспортного контроля, выделяются определенные категории угроз и уязвимостей. В заключении статьи предлагаются рекомендации по предотвращению и минимизации рисков нарушения конфиденциальности информации с использованием лазерных систем разведки.

Ключевые слова: лазерные системы разведки, угрозы, уязвимости, конфиденциальная информация, информационная безопасность

A. A. Litvyakov[1]*, *I. N. Karmanov*[1]

Assessment of the Risk of Violating the Confidentiality of Information Using Laser Reconnaissance Systems

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: mr.go_old@mail.ru

Abstract. The article is devoted to the study of potential threats and vulnerabilities of breaking confidential information using laser reconnaissance systems based on the threat data bank of the Federal Service for technical and export control. The article analyzes possible threats and vulnerabilities associated with the use of laser reconnaissance systems, including the possibility of unauthorized access to confidential data, interception of information, violation of the confidentiality of data transmission and other aspects of information security. Based on the threat data bank of the Federal Service for technical and export control, certain categories of threats and vulnerabilities are distinguished. In conclusion, the article offers recommendations for preventing and minimizing the risks of breaching confidential information using laser reconnaissance systems.

Keywords: laser reconnaissance systems, threats, vulnerabilities, confidential information, information security

Введение

С развитием технологий лазерные системы разведки становятся все более распространенным средством хищения конфиденциальной информации. Такие системы представляют шанс реализации потенциальных угроз и уязвимостей,

связанных с нарушением конфиденциальности передачи данных, несанкционированным доступом и перехватом информации.

Цель данной статьи – провести исследование потенциальных угроз и уязвимостей нарушения конфиденциальной информации с использованием лазерных систем разведки на основе банка данных угроз Федеральной Службы технического и экспортного контроля (БДУ ФСТЭК). БДУ ФСТЭК является руководством, разработанным ФСТЭК России, и содержит рекомендации и требования по обеспечению информационной безопасности в различных сферах деятельности.

В данной статье проводится анализ возможных угроз и уязвимостей, связанных с применением лазерных систем разведки, на основе БДУ ФСТЭК. Были выделены основные категории угроз и уязвимостей и проведена оценка. Затем, на основе анализа, предложены рекомендации по предотвращению и минимизации рисков нарушения конфиденциальной информации при использовании лазерных систем разведки.

Методы и материалы

Осуществить перехват речевой информации внутри помещений возможно с помощью лазерных средств акустической разведки, используя дистанционное лазерно-локационное зондирование объектов, обладающих свойствами, которые позволяют их использовать в качестве потенциальных источников закрытой речевой информации. Такими объектами могут быть, например, оконные стекла и другие виброотражающие поверхности [2].

Данный метод основывается на использовании лазерных лучей для измерения вибраций, возникающих на поверхности этих объектов в ответ на звуковые волны, создаваемые голосом людей внутри помещения. Измеренные вибрации преобразуются обратно в звуковые волны, что позволяет перехватывать и записывать речевую информацию [1].

На рис. 1 представлена схема утечки речевой информации с использованием лазерных систем разведки.

На сегодняшний день существует множество различных систем лазерной акустической разведки, которые позволяют перехватывать звуковую информацию на расстоянии от нескольких десятков метров до нескольких километров. Например, система SIPE LASER 3-DA SUPER [3] включает в себя гелий-неоновый лазер, блок фильтрации шумов, головные телефоны, аккумулятор и штатив для установки оборудования.

Для наведения лазерного излучения на нужное окно используется телескопический визир, а специальная оптическая насадка позволяет регулировать угол расходимости светового пучка [7]. Система обеспечивает высокое качество перехвата речевой информации на расстоянии до 250 метров [3].

Из современных систем лазерной акустической разведки особое внимание стоит обратить на следующие модели [3]:

– «Икар» (Icar) – это система, разработанная компанией «Лазерный инженеринг» (Laser Engineering) [3], которая может обнаруживать и идентифициро-

вать звуки, создаваемые различными видами вычислительной техники, на расстоянии до 2 км. Она использует технологию измерения времени задержки отраженных звуковых волн, чтобы определить расстояние до источника звука;

– «акула» (Akula) – это система, разработанная компанией «Российская электронная техника» (Russian Electronic Technology), которая использует лазерное излучение для обнаружения и анализа звуковых волн на расстоянии до 2 км. Она может использоваться для обнаружения и идентификации транспортных средств, определения местоположения стрелков и детектирования звуковых сигналов в акустических областях;

– «комплекс-24» (Complex-24) – это система, разработанная компанией «Технологии лазерной микрообработки» (Laser Microprocessing Technologies), которая может обнаруживать звуковые сигналы на расстоянии до 5 км. Она использует лазерное излучение для измерения времени задержки отраженных звуковых волн, чтобы определить расстояние до источника звука.

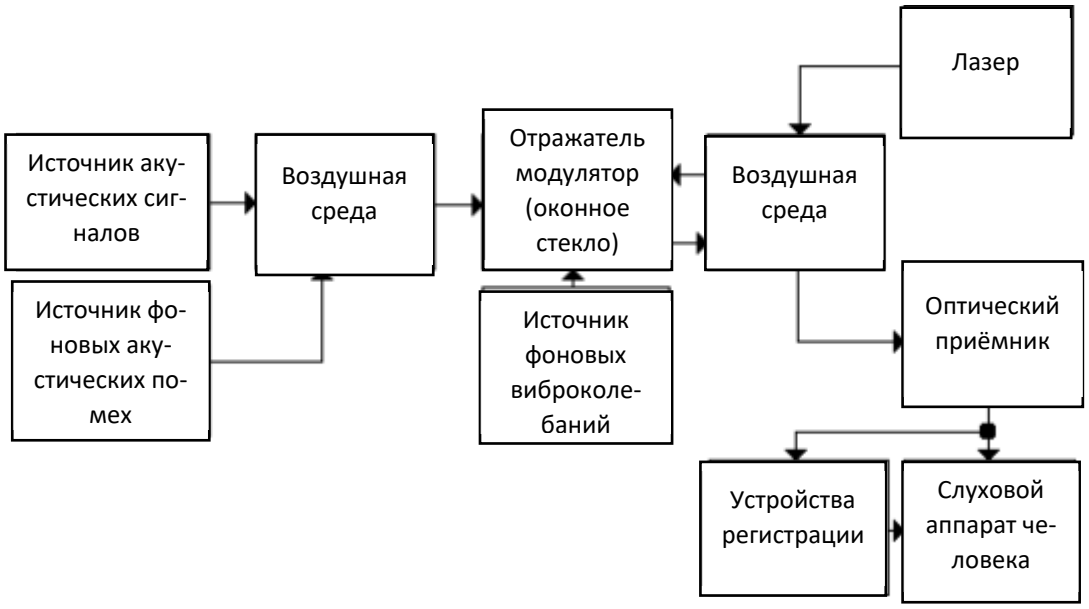


Рис. 1. Обобщенная схема утечки информации по оптико-акустическому каналу

Другим примером является лазерное устройство НРО150 [3], которое также использует гелий-неоновый лазер в качестве передатчика, а также блок компенсации помех и кассетное устройство магнитной записи в составе приемника. Это устройство обладает дальностью ведения разведки до 1000 метров [3].

Однако, устройства лазерной акустической разведки сталкиваются с высокими требованиями к помехоустойчивости, так как качество перехватываемой информации напрямую зависит от уровня фоновых шумов, помеховых вибраций отражателя-модулятора, а также ослабления лазерного излучения в атмосфере и фоновой оптической засветки при приеме отраженного от объекта сигнала [4].

Для оценки риска нарушения конфиденциальности информации с использованием лазерных систем разведки, на основе БДУ ФСТЭК, были выделены угрозы, представленные в табл. 1. [5].

Согласно ГОСТ Р 58771-2019 «Спецификация системы управления информационной безопасностью», уровень риска вычисляется с учетом следующих показателей: ценности ресурса, уровня угрозы и степени уязвимости. С увеличением значений этих параметров риск возрастает. Таким образом, формулу можно представить в следующем виде [10]:

$$R = AV \times EF \times ARO, \quad (1)$$

где AV (Asset Value, AV) – ценность актива (ресурса). Указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 – минимальная стоимость ресурса, 2 – средняя стоимость ресурса и 3 – максимальная стоимость ресурса [10]; *EF* (Exposure Factor, *EF*) – уровень угрозы (мера уязвимости ресурса к угрозе). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 – минимальная мера уязвимости (слабое воздействие), 2 – средняя (ресурс подлежит восстановлению), 3 – максимальная (ресурс требует полной замены после реализации угрозы) [10]; *ARO* (Annual Rate of Occurrence, *ARO*) – уровень (оценка вероятности реализации угрозы) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая) [10].

Таблица 1

Угрозы безопасности информации

Угроза	Наименование угрозы	Потенциал нарушителя	Последствия реализации угрозы	Качественный показатель риска (*ARO*)
УБИ. 132	Угроза получения предварительной информации об объекте защиты	Средний	Нарушение конфиденциальности	3
УБИ. 139	Угроза преодоления физической защиты	Средний	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	3
УБИ. 187	Угроза несанкционированного воздействия на средство защиты информации	Средний	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	3

Угроза	Наименование угрозы	Потенциал нарушителя	Последствия реализации угрозы	Качественный показатель риска (*ARO*)
УБИ. 203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Средний	Нарушение конфиденциальности	3
УБИ. 080	Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети	Средний	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	2
УБИ. 085	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	Средний	Нарушение конфиденциальности	2
УБИ.111	Угроза передачи данных по скрытым каналам	Средний	Нарушение конфиденциальности	3

Таким образом, можно рассчитать качественный показатель риска представленных угроз: в случае использования лазерной системы разведки, вероятность реализации каждой из угроз возрастает до максимального значения – показатель *ARO* = 3. Исключением являются УБИ 80 и УБИ 85, так как хоть и при использовании лазерной системы разведки существует вероятность считывания сигналов компьютера или звуков нажатия клавиш, однако такие данные довольно сложно расшифровать и использовать.

Результаты

В табл. 2 представлены результаты вычислений качественного показателя риска. С учетом максимальных значений расчета, наивысший показатель равен 27 пунктам. График качественного значения показателя риска приведен на рис. 2.

Из рис. 2 видно, что большинство угроз имеет средний уровень риска и выше. Это говорит о том, что применение мер по снижению рисков хищения конфиденциальной информации с использованием лазерных систем разведки является оправданным и необходимым.

Таблица 2

Расчет качественного значения риска

Угроза	Показатель *AV*	Показатель *EF*	Значение риска *R*
УБИ. 132	1	2	6
УБИ. 139	2	2	12
УБИ. 187	2	3	27
УБИ. 203	2	3	18
УБИ. 080	3	3	18
УБИ. 085	3	3	18
УБИ.111	3	3	27

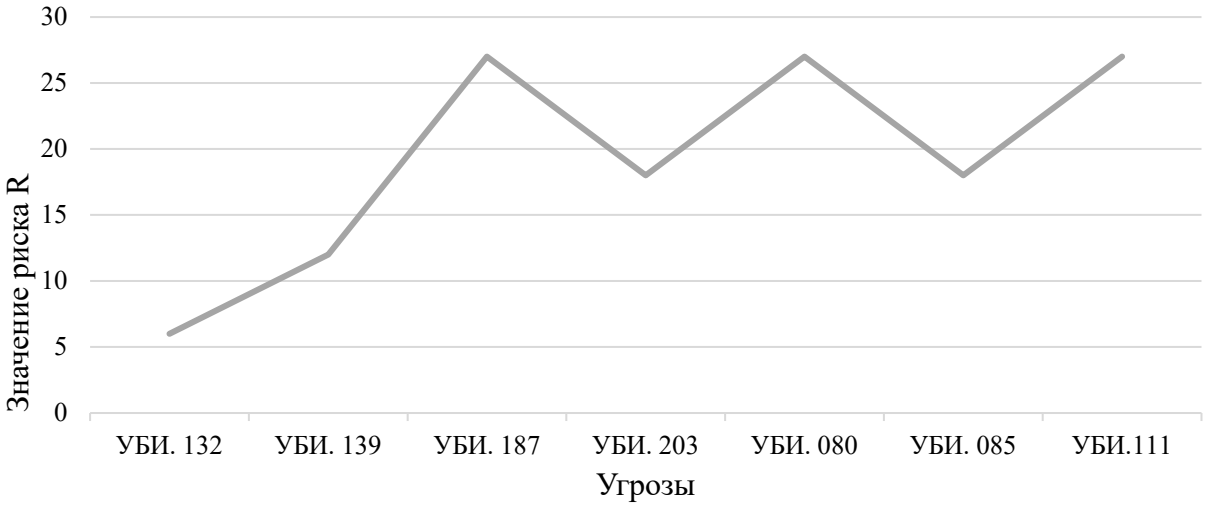


Рис. 2. График качественного значения показателя риска

Заключение

В ходе исследования была проведена качественная оценка рисков утечки конфиденциально информации по акустооптическому каналу. По результатам оценки стало ясно, что применение мер по снижению представленных рисков является оправданным, необходимым и окупаемым.

Для того, чтобы снизить риск утечки информации по акустооптическому каналу рекомендуется:

– ограничить доступ к зонам, где может быть применена лазерная система разведки;

– использовать специальные средства защиты, такие как экранирующие устройства или оптические фильтры;

– проводить регулярные проверки на наличие утечек конфиденциальной информации с помощью специального оборудования;

– обучать персонал правильной процедуре обращения с конфиденциальной информацией и предоставлять инструкции по использованию специальных устройств защиты;

– организовывать регулярное техническое обслуживание и проверку на наличие возможных уязвимостей и угроз в системах безопасности [6].

Благодарности

Авторы выражают благодарность Федеральной службе по техническому и экспортному контролю за предоставленные данные и информацию, необходимые для проведения исследования и написания данной статьи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ярочкин В.И. Технические каналы утечки информации. – М.: ИПКИР, 1994. – 102 с.

2. Лаврухин Ю.Н. Проблемы технической защиты конфиденциальной информации / Ю.Н. Лаврухин // Информация и безопасность: материалы межрегиональной научно-практической конференции. – Вып.2. – Воронеж: ВГТУ, 2002. – С. 14–16.

3. Андрианов В.И., Бородин В.А., Соколов А.В. Шпионские штучки и устройства для защиты объектов и информации. Справочное пособие. – СПб.: Лань, 1998. – 272 с.

4. Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. М.: РЦИБ Факел, 2008. 256 с.

5. Официальный сайт банка данных угроз ФСТЭК России. – [Электронный ресурс] –Режим доступа: https://bdu.fstec.ru/threat (дата обращения 24.04.2023).

6. Управление рисками по ITIL [Электронный ресурс]. – Режим доступа: https://www.itexpert.ru/rus/ITEMS/77-33/ (дата обращения 22.04.2023).

7. Зайцев А.П. Технические средства и методы защиты информации: учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. - М.: ГЛТ , 2012. - 616 с.

8. Учаев Д.Ю., Брумштейн Ю.М., Ажмухадедов И.М., Князева О.М., Дюдиков И.А. Анализ и управление рисками, связанными с информационным обеспечением человеко-машинных АСУ технологическими процессами в реальном времени // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2. – С. 82–97.

9. Методический документ. "Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021) – [Электронный ресурс] – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения 26.04.2023)

10. Национальный стандарт Российской Федерации «Менеджмент риска. Технологии оценки риска» ГОСТ Р 58771-2019 (введен 01.03.2020) [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200170253 (дата обращения 27.09.2021).

УДК 004.93
DOI 10.33764/2618-981X-2023-6-160-164

Е. К. Малютин[1], Г. В. Попков[1,2]*

Анализ эффективности программ распознавания образов

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: shuklinaa@list.ru

Аннотация. В статье проведен анализ некоторых программ, соответствующих тематике статьи. Выбранные программы были исследованы. Их функции и специализация была проверена экспериментальным путем, позволяя изучить эффективность их технических характеристик для сравнения и анализа. Также были проведены мероприятия по объединению целей их изначальных алгоритмов. В связи с различной темой выбранных для экспериментального анализа программ к ним применялся разный подход. Дополнительно были выявлены их сильные и слабые стороны, позволяя на основе этих данных построить новую тропу, ведущую хоть и не по-новому, но относительно свободному пути, который на основе объединения и взаимного дополнения позволит упростить взаимодействие и расширить возможности как для собственника информации, так и для владельца программы.

Ключевые слова: распознавания образов, IOS, Android, программа, сравнение эффективности

E. K. Malyutin[1], G. V. Popkov[1,2]*

Analysis of the effectiveness of image recognition programs

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: shuklinaa@list.ru

Abstract. The article analyzes some programs, corresponding to the subject of the article. Selected programs were researched. Their functions and specializations have been experimentally tested, allowing the effectiveness of their technical characteristics to be studied for comparison and analysis. Activities were also carried out to combine the goals of their original algorithms. Due to the different topics chosen for the experimental analysis of the programs, a different approach was applied to them. Additionally, their strengths and weaknesses were identified, allowing, on the basis of these data, to build a new path leading, although not in a new way, but in a relatively free way, which, based on association and mutual complementation, will simplify interaction and expand opportunities, both for the owner of information, and for the owner of the program.

Keywords: image recognition, IOS, Android, program, efficiency comparison

Введение

Для защиты личной информации человек придумывал, придумывает и будет придумывать все более совершенные методы, в том числе в области защиты информации.

В настоящее время защита персонифицированной информации имеет тенденцию роста, так как в современных реалиях злоумышленники становятся изощреннее в обманных методах сбора информации, что представляет опасность как для общества, так и для отдельного индивида.

Самые уязвимые места – это мобильные устройства, доступ к которым, можно получить самым прямым и быстрым способом, а обладая им, легко управлять всеми сферами жизни современного человека. Это вынуждает каждого иметь действенный способ защиты информации. Однако каждый способ основан на распознавании образов, что выражается как в числовом коде, так и в биометрических данных [1].

Анализ публикаций на эту тему показывает, что их количество невелико, а из опубликованных большинство являются описанием преимуществ или метода работы программы.

В связи с этим целью статьи является сравнительный анализ возможностей и технической обеспеченности программ на базе IOS и Android для дополнительной защиты персонифицированной информации.

Анализ проведен по следующим критериям: вариативность, скорость обработки и эффективность.

Методы и материалы

Программы, основанные на образах, создаются и улучшаются для постоянного увеличения уровня защищенности. Основными методами защиты информации в этих программах являются: числовой пароль, отпечаток пальца и биометрический снимок лица.

В настоящее время многие пользователи персональных устройств, заинтересованные в безопасности личной информации, используют для защиты отпечаток пальца или лица. Операционные системы (ОС) персональных устройств предоставляют базовый уровень подобной защиты, однако, защитить персонифицированную информацию они не в силах. Для создания многоуровневой защиты используются дополнительные программы, обеспечивающие более высокий уровень защищенности и возможность выборочной защиты информации. Для оценки любой биометрической системы используют два параметра:

– FAR (False Acceptance Rate) – коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе;

– FRR (False Rejection Rate) – коэффициент ложного отказа, т.е. отказ в доступе зарегистрированному пользователю системы [2, 3].

Данные параметры получают расчетным путем, в основе которого лежит метод математической статистики. Чем ниже значение, тем выше точность распознавания. Средние значения FAR и FRR представлены в табл. 1.

Эти данные не являются абсолютными, однако позволяют выбрать в настоящее время наиболее эффективный метод защиты информации для персональных устройств из доступных методов. На главных ОС современности программы дополнительной защиты распознают лица своих владельцев в режиме реального

времени минимум по 80 узловым точкам. Примером являются программы: «IObit Applock» с платформы Android и «BioID» на базе IOS [4, 5].

Таблица 1

Средние значения FAR и FRR для распространенных способов биометрической идентификации

Способ биометрической идентификации	FAR, %	FRR, %
Отпечаток пальца	0,001	0,6
Распознавание лица 2D	0,1	2,5
Распознавание лица 3D	0,0005	0,1

«IObit Applock» является уникальной программой для дополнительной защиты персонифицированных данных по желанию пользователя.

Особенность этой программы заключается в возможности создания индивидуального ключа-образа на основе воображения (рис. 1) [4]. Уровень защиты информации при данном методе признан наивысшим, так как возможность кражи такого ключа исключена. Однако его сложность так же является высокой, так как созданный таким методом ключ уникален и должен быть повторен в точности.

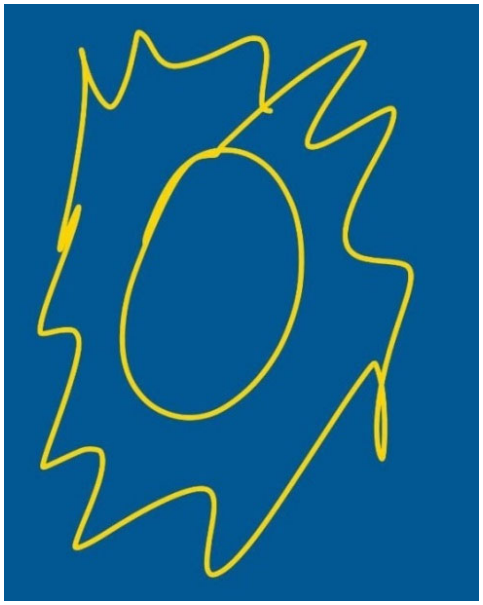


Рис. 1. Пример индивидуального ключа-образа

«BioID» является инновационным продуктом интеллектуального творчества, способным к распознаванию глаз для частично прикрытых лиц (рис. 2) [5]. Такой алгоритм распознавания позволяет увеличить уровень защищенности, при уменьшении объема обрабатываемой информации, что соответствует современным реалиям, позволяя получить доступ к защищенной информации в общественных местах быстро и безопасно.

Рис. 2. Пример периокулярного распознавания

Результаты

В результате выполненных исследований на основе изучения тематической информации из технической литературы был проведен сравнительный анализ по следующим критериям: вариативность, скорость обработки и эффективность.

Сравнение проводилось на основе заявленных разработчиком данных, а также экспериментально рассчитанных в лабораторных условиях значения. Преимущества программы в критериях будет показано знаком «+», если она уступает – знаком «–», преимущества их квалификации минимизирует ущерб от недостатков – знаком «+/–». Результаты представлены в табл. 2.

Таблица 2

Преимущества характеристик программ защиты персональных данных

Критерии	IObit Applock	BioID
Вариативность	+	-
Скорость обработки	-	+/-
Эффективность	+/-	+/-

В ходе проведенной работы было выявлено, что программа IObit Applock имеет весь спектр способов защиты информации, возможных для персональных устройств, а именно: PIN-код, отпечаток пальца, биометрию лица и графический пароль, который так же представлен в виде произвольного рисунка. Тогда как BioID специализируется на биометрическом снимке лица, однако его уровень осведомленности позволяет проводить аутентификацию по ограниченной площади лица, что способствует более высокой степени защиты информации и минимизации FRR [6, 7].

В лабораторных экспериментах проведены подсчеты скорости обработки образа для получения доступа пользователя к информации. Эксперимент показал, что программе IObit Applock требуется не более 1,5 секунд на обработку поступающего образа для аутентификации, однако, в случае произвольного графического пароля временной диапазон увеличивается пропорционально сложности и точности воспроизведения последнего, что приводит к высокой степени защиты персональных данных. Временные показатели программы BioID имеют диапазон от 1 секунды (при полном доступе к биометрии лица, без внешнего вмешательства) до 5 секунд (при частичном сокрытии и плохой освещенности) [8].

Критерий эффективности был исследован по уровню сложности системы защиты. Проанализировав IObit Applock и BioID, можно утверждать, что первый имеет самый высокий уровень безопасности, так как произвольный графический пароль повторить или взломать невозможно. Однако, остальные способы аутентификации IObit Applock равны, а в случае с биометрией лица BioID уступают, из-за чего критерий эффективности для каждой программы равнозначен, так как у каждой есть преимущественная черта, на которой она специализируется.

Заключение

Сравнительный анализ характеристик рассмотренных программ позволяет сделать вывод о том, что преимущество в области спецификации и метод, на который делает акцент данная программа, обладают большей самостоятельной эффективностью в защите персональных данных. Так же следует отметить, что метод периокулярного распознавания программы BioID является очень эффективным для защиты как персональных данных, так и самого мобильного устройства. Однако проблема угрозы конфиденциальной информации остается не решенной окончательно, так как кражи личных данных продолжаются и в настоящее время не только не намечается спад, а заметен рост краж с последующей публикацией в общественном доступе или с целью шантажа. Одним из возможных путей решения данной проблемы является синтез преимуществ программ распознавания образов, используемых для защиты персональных данных, подобные тем, что рассмотрены выше. Таким образом, в дальнейшем исследовании полученные данные и результаты сравнительного анализа, будут использованы для синтеза новой программы, которая, объединив преимущества других, сможет решать более широкий спектр задач при высокой скорости и большей эффективности [9, 10].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Царев А.Г. Принципы и методы автоматического распознавания образов // Труды Международного симпозиума «Надежность и качество» – Пенза, 2010. – Т.1. – С. 56 – 58.

2. Растригин Л. А., Эренштейн Р. Х. Метод коллективного распознавания: учебник. Москва: Энергоиздат, 2006. 80 с.

3. Потапов А.С. Распознавание образов и машинное восприятие: учебник. Санкт-Петербург: Политехника, 2019. – 548 с.

4. Разработчик программы IObit Applock. URL: http://www.spsoftmobile.com/ (дата обращения: 28.03.2023).

5. Разработчик программы BioID. URL: http://www.bioid.com/ (дата обращения: 28.03.2023).

6. Фу К. Структурные методы в распознавании образов: учебник. Москва: Мир, 2005. – 144 с.

7. Мазуров В.Д. Комитеты систем неравенств и задача распознавания // Кибернетика – Москва, 2004. – № 2. – С. 140-146.

8. Айзерман М.А., Браверман Э.М., Розоноэр Л.И. Метод потенциальных функций в теории обучения маши: учебное пособие. Москва: Наука, 2018. – 264 с.

9. Журавлев Ю.И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики – Москва, 2015. – № 33. – С. 5-68.

10. Горбань А., Россиев Д. Нейронные сети на персональном компьютере: учебник. Новосибирск: Наука, 2016. – 278 с.

УДК 004.056
DOI 10.33764/2618-981X-2023-6-165-170

Е. Б. Маркелова[1], А. В. Троеглазова[1]*

Оценка факторов, оказывающих влияние на реализацию угроз информационной безопасности

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Markelova-EB2021@sgugit.ru

Аннотация. Важнейшим этапом разработки и совершенствования защищенной системы электронного документооборота является выявление угроз информационной безопасности, а также факторов, оказывающих влияние на их реализацию. Математическая оценка значимости влияния этих факторов необходима для построения эффективной системы защиты информации, обрабатываемой в системе электронного документооборота. Целью данной работы является математическая оценка факторов, оказывающих влияние на реализацию угроз безопасности информации, обрабатываемой в системе электронного документооборота, методом дробного факторного планирования эксперимента. Оценка рисков была произведена для группы угроз, реализуемых в государственной организации внутренним нарушителем с низким потенциалом, и изучено влияние факторов несанкционированного доступа к аутентификационной информации, устаревших антивирусных баз и отсутствия запрета на запуск исполняемых файлов от имени пользователей. Рассмотренный подход может быть применим и к автоматизированной системе, и к системам обработки информации без использования средств автоматизации.

Ключевые слова: угрозы информационной безопасности, система электронного документооборота, оценка вероятности, факторное планирование эксперимента

E. B. Markelova[1], A. V. Troeglazova[1]*

Assessment of Factors Influencing the Implementation of Information Security Threats

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: Markelova-EB2021@sgugit.ru

Abstract. The most important stage in the development and improvement of a secure electronic document management system is the identification of threats to information security, as well as factors that affect their implementation. A mathematical assessment of the significance of the influence of these factors is necessary to build an effective system for protecting information processed in an electronic document management system. The purpose of this work is a mathematical assessment of the factors influencing the implementation of threats to the security of information processed in the electronic document management system using the method of fractional factorial planning of the experiment. The risk assessment was carried out for a group of threats implemented in a government organization by an insider with low potential and the impact of factors of unauthorized access to authentication information, outdated anti-virus databases and the absence of a ban on running executable files on behalf of users was studied. The considered approach can be applied both to an automated system and to information processing systems without the use of automation tools.

Keywords: information security threats, electronic document management system, probability assessment, factorial planning of experiment

Введение

Для создания в организации защищенного электронного документооборота необходимо обеспечить аутентификацию пользователей и разделение прав доступа к электронным документам, подтвердить авторство документов в системе электронного документооборота, реализовать важнейшие свойства информации (конфиденциальность, целостность, доступность) за счет обеспечения юридической значимости электронных документов [1]. Наиболее распространенными угрозами, реализуемыми при эксплуатации систем электронного документооборота, являются угроза неправомерного ознакомления с информацией, угроза несанкционированного копирования информации, угроза внедрения кода или данных, угроза распространения «почтовых червей», угроза заражения компьютера при посещении неблагонадежных сайтов, угроза несанкционированной модификации защищаемой информации, «кража» учетной записи доступа к сетевым сервисам, угроза приведения системы в состояние «отказ в обслуживании» (DOS), угроза утраты носителей информации [2, 3].

Важнейшим этапом разработки и совершенствования системы защиты информации, обрабатываемой в системе электронного документооборота, является выявление и количественная оценка факторов, оказывающих влияние на реализацию угроз информационной безопасности. В литературе описаны различные методы – как качественные, так и количественные [4-6], широкое распространение среди которых получил метод факторного планирования эксперимента [5-8].

Цель настоящей работы заключается в математической оценке факторов, оказывающих влияние на реализацию угрозы безопасности информации, обрабатываемой в СЭД, методом дробного факторного планирования эксперимента.

Методы и материалы

Модель угроз безопасности информации, обрабатываемой в системе электронного документооборота, составлена в соответствии с требованиями Методического документа «Методика оценки угроз безопасности информации» (утв. ФСТЭК от 5 февраля 2021 г.) [9] и на основании банка угроз [10]. Оценку рисков выполняли для группы угроз, реализуемых в государственной организации внутренним нарушителем с низким потенциалом, что приводит к нарушению конфиденциальности, целостности и доступности информации [10]:

– УБИ.074 – угроза несанкционированного доступа к аутентификационной информации;

– УБИ.086 – угроза несанкционированного изменения аутентификационной информации;

– УБИ.088 – угроза несанкционированного копирования защищаемой информации;

– УБИ.152 – угроза удаления аутентификационной информации;

– УБИ.167 – угроза заражения компьютера при посещении неблагонадёжных сайтов;

– УБИ.168 – угроза «кражи» учётной записи доступа к сетевым сервисам;

– УБИ.172 – угроза распространения «почтовых червей»;

– УБИ.191 – угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

Процесс оценки вероятности реализации угроз методом дробного факторного планирования эксперимента представлен на рис. 1 [5, 6].

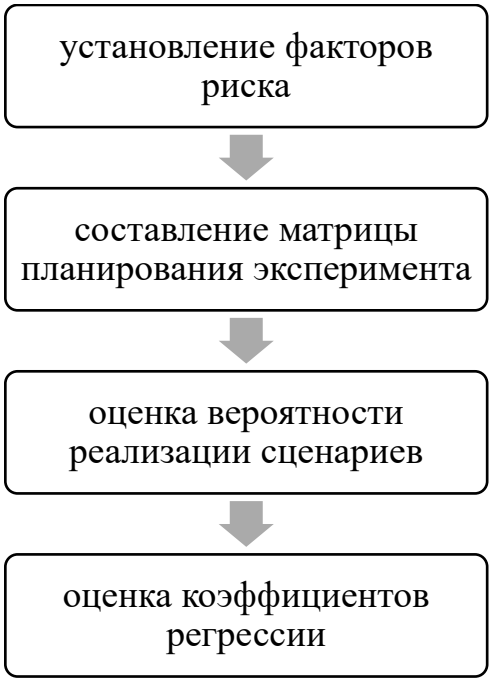


Рис. 1. Процесс оценки вероятности реализации угроз методом дробного факторного планирования эксперимента

Математическая модель реализации угрозы информационной безопасности для дробного факторного эксперимента может быть представлена в виде линейной регрессионной зависимости:

$$Y = b_0 + \sum_{i=1}^{k} b_i X_i + \sum_{i,j=1}^{k} b_{ij} X_i X_j + \ldots + \sum_{i,j,n=1}^{k} b_{ijn} X_i X_j X_n , \quad (1)$$

где Y – вероятность реализации угрозы; X_i – значения факторов; b_0 – свободный член; b_i – коэффициент линейного воздействия факторов; b_{ij} – коэффициент взаимодействия факторов; b_{ijn} – коэффициент n-го взаимодействия факторов; i, j, n – номер фактора.

Факторы X_i могут принимать только одно из двух значений: минус 1 – если рассматриваемый фактор не оказывает влияния на реализацию угрозы; плюс 1 – если реализация угрозы зависит от наличия или отсутствия рассматриваемого фактора. Коэффициенты регрессии определяются по формуле:

$$b_j = \frac{\sum_{i-1}^{N} X_{ij} Y_i}{N}. \quad (2)$$

Количество реализуемых сценариев (экспериментов) в факторном дробном эксперименте определяется по следующей формуле:

$$N = 2^{k-p}, \quad (3)$$

где N – количество сценариев (экспериментов); k – количество рассматриваемых факторов; p – целое положительное количество факторов, выведенных путем замены незначимых взаимодействий.

Значения вектор-столбца X_0 во всех сценариях приняты равными +1, поэтому p=1. При условии рассмотрения влияния четырех факторов на реализацию угроз информационной безопасности количество сценариев (экспериментов) составляет 8.

Вероятность реализации угроз для каждого сценария (Y_{ij}) оценивается экспертным методом (метод непосредственного оценивания) по шкале от 0,00 до 1,00. Метод предполагает присваивание объектам экспертизы (каждому сценарию) баллов каждым экспертом, при этом наиболее значимому объекту (сценарию) присваивается наибольшее количество баллов согласно установленной шкале. Вероятность реализации угроз для каждого сценария (Y_i) оценивается как среднее арифметическое значение оценок сценариев каждым из четырех экспертов.

Результаты

В качестве причин реализации угрозы несанкционированного доступа к аутентификационной информации (УБИ.074 [10]) можно назвать следующие:

1) небрежность персонала в информационном измерении;

2) устаревшие антивирусные базы;

3) отсутствие запрета на запуск исполняемых файлов от имени пользователей;

4) возможность управления функционированием антивирусного программного обеспечения от имени пользователей.

Матрица планирования эксперимента, составленная для восьми сценариев реализации угроз информационной безопасности, представлена в табл. 1.

Результаты оценки вероятности реализации угроз информационной безопасности экспертным методом представлены в табл. 2.

На основании результатов оценки вероятностей реализации угрозы (табл. 2) для восьми сценариев, представленных в табл. 1, была произведена оценка коэффициентов регрессии по формуле (2). Для четырехфакторного планирования эксперимента уравнение регрессии:

$$Y = 0,669 + 0,064X_1 + 0,076X_2 + 0,171X_3 + 0,019X_4 + 0,001X_1X_2 - 0,019X_1X_3 + 0,009X_2X_3 . \quad (4)$$

Таблица 1

Матрица планирования эксперимента

N	X_0	X_1	X_2	X_3	X_4	X_1X_2	X_1X_3	X_2X_3	Y_i
1	+	–	–	–	–	+	+	+	Y_1
2	+	+	–	–	+	–	–	+	Y_2
3	+	–	+	–	+	–	+	–	Y_3
4	+	+	+	–	–	+	–	–	Y_4
5	+	–	–	+	+	+	–	–	Y_5
6	+	+	–	+	–	–	+	–	Y_6
7	+	–	+	+	–	–	–	+	Y_7
8	+	+	+	+	+	+	+	+	Y_8

Таблица 2

Результаты оценки вероятности реализации угроз
методом непосредственного оценивания

N	Ранги, присвоенные экспертами R_{ij}				$\sum_{i=1}^{n} R_{ij}$	Y_i
	1	2	3	4		
1	0,30	0,30	0,30	0,40	1,30	0,33
2	0,50	0,50	0,50	0,60	2,10	0,53
3	0,40	0,60	0,50	0,50	2,00	0,50
4	0,50	0,70	0,60	0,70	2,50	0,63
5	0,80	0,70	0,80	0,60	2,90	0,73
6	0,70	0,80	0,80	0,80	3,10	0,78
7	0,85	1,00	0,90	0,70	3,45	0,86
8	1,00	1,00	0,95	1,00	3,95	0,99

Каждый коэффициент регрессии играет определенную роль в установлении актуальности угрозы несанкционированного доступа к аутентификационной информации. Так, превышение свободным членом b_0 значения 0,50 свидетельствует об актуальности рассматриваемой угрозы и значимости влияния каждого из четырех рассмотренных факторов на реализацию угрозы информационной безопасности. Третий фактор, отсутствие запрета на запуск исполняемых файлов от имени пользователей, вносит наибольший вклад в реализацию угрозы информационной безопасности и усиливает негативное действие второго фактора (устаревших антивирусных баз) и ослабляет действие первого фактора (небрежность персонала в информационном измерении). Наименьшее влияние на реализацию угрозы оказывает четвертый фактор – возможность управления функцио-

нированием антивирусного программного обеспечения от имени пользователей. Результаты оценки коэффициентов регрессии позволяют осуществлять непрерывный мониторинг выявленных факторов риска.

Заключение

Таким образом, методом дробного факторного эксперимента проведена математическая оценка факторов, оказывающих влияние на угрозу несанкционированного доступа к аутентификационной информации. Было изучено влияние следующих факторов: небрежность персонала в информационном измерении, устаревшие антивирусные базы, отсутствие запрета на запуск исполняемых файлов от имени пользователей, возможность управления функционированием антивирусного программного обеспечения от имени пользователей. Применение рассмотренного подхода позволяет оценить вероятные риски на основе анализа результатов экспертной оценки вероятности реализации угрозы для восьми сценариев.

Методика может быть одинаково применима и к автоматизированной информационной системе, и к системам обработки информации без использования средств автоматизации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Булдакова Т.И., Глазунова Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота // Доклады ТУСУРа. – 2012. – № 1 (25), часть 2. – С. 52-56.
2. Заводцев И.В., Борисов М.А., Бондаренко Н.Н., Мелешко В.А. Моделирование угроз безопасности информации и определение их актуальности для информационных систем объектов информатизации федеральных органов исполнительной власти // Computational nanotechnology. – 2022. – № 1, Т. 9. – С. 106-114.
3. Майстренко В.А., Безродных О.А., Дорохин Р.А. Методика определения актуальных угроз безопасности информации в медицинской информационной системе // Омский научный вестник. – 2021. – № 5 (179). – С. 74-79.
4. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. – 2014. – № 4 (7). – С. 49-54.
5. Белов В.М., Белкин С.А. Оценка вероятности угрозы заражения компьютерным вирусом на основе факторного планирования эксперимента // Информационное противодействие угрозам терроризма. – 2014. – № 23. – С. 55–61.
6. Плетнев П.В., Белов В.М., Зубков Е.В., Крыжановская О.А. К вопросу об определении угроз и рисков информационной безопасности с использованием сценарного подхода и факторного планирования эксперимента // Вестник СибГУТИ. – 2016. – № 4. – С. 12-18.
7. Ильченко Л.М., Брагина Е.К., Егоров И.Э., Зайцев С.И. Расчет рисков информационной безопасности телекоммуникационного предприятия // Открытое образование. – 2018. – Т. 22. – № 2. – С. 62-70.
8. Котенко Д.А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования. – автореферат дисс. на соиск. ученой степени канд.технич.наук. – СПб, 2010. – 18 с.
9. Методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК 05.02.2021 г.).
10. Банк данных угроз безопасности информации [сайт]. URL: https://bdu.fstec.ru/threat.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-171-174

К. А. Мартынов[1]*, *Н. Е. Карпова*[1]

Использование аппарата нейронных сетей для оценки разборчивости речи

[1] Самарский государственный технический университет, г. Самара, Российская Федерация
* e-mail: martyn987@mail.ru

Аннотация. В этой статье представлен всесторонний обзор того, как нейронные сети могут быть использованы для объективной оценки разборчивости речи. В статье объясняются традиционные субъективные методы, используемые для оценки разборчивости речи и связанные с ними ограничения. Вводится концепция нейронных сетей и то, как их можно обучить предсказывать показатели разборчивости речи на основе признаков, извлеченных из речевого сигнала. Описываются две популярные архитектуры нейронных сетей: сверточная нейронная сеть (CNN) и рекуррентная нейронная сеть (RNN), которые успешно использовались для оценки разборчивости речи. Освещаются факторы, которые могут повлиять на производительность системы оценки разборчивости речи на основе нейронных сетей. В целом, статья дает обширную информацию о потенциале нейронных сетей для улучшения оценки разборчивости речи и их применении в различных областях.

Ключевые слова: искусственные нейронные сети, глубокие нейронные сети, сверточная нейронная сеть, оценка разборчивости речи

K. A. Martynov[1]*, *N. E. Karpova*[1]

Using the Neural Network Apparatus to Assess Speech Intelligibility

[1] Samara State Technical University, Samara, Russian Federation
* e-mail: martyn987@mail.ru

Annotation. This article provides a comprehensive overview of how neural networks can be used to objectively assess speech intelligibility. The article explains the traditional subjective methods used to assess speech intelligibility and the associated limitations. The concept of neural networks and how they can be trained to predict speech intelligibility indicators based on features extracted from a speech signal is introduced. Two popular neural network architectures are described: convolutional neural network (CNN) and recurrent neural network (RNN), which have been successfully used to assess speech intelligibility. The factors that can affect the performance of a speech intelligibility assessment system based on neural networks are highlighted. In general, the article provides extensive information about the potential of neural networks to improve the assessment of speech intelligibility and their application in various fields.

Keywords: artificial neural networks, deep neural networks, convolutional neural network, speech intelligibility assessment

Введение

Разборчивость речи является важнейшим аспектом общения, который относится к способности слушателя понимать произносимые слова. Точная оценка

разборчивости речи необходима в различных областях, включая аудиологию, логопедию и телекоммуникации. Традиционно оценка разборчивости речи проводилась с помощью субъективных методов, что может отнимать много времени и приводить к ошибкам [1, 8, 9]. Однако с недавними достижениями в области глубокого обучения нейронные сети стали многообещающим подходом к объективной оценке разборчивости речи. В этой статье рассматривается, как нейронные сети можно использовать для оценки разборчивости речи.

Методы машинного обучения

Нейронные сети – это вычислительные модели, основанные на структуре и функциях человеческого мозга. Они состоят из взаимосвязанных узлов или нейронов, которые выполняют простые операции над входными данными и передают выходные данные следующему слою нейронов. Выходные данные последнего слоя нейронов обеспечивают прогнозирование сети. Процесс обучения нейронной сети включает в себя настройку весов соединений между нейронами, чтобы свести к минимуму разницу между выходными данными сети и базовыми метками истинности.

Чтобы оценить разборчивость речи, нейронную сеть можно обучить на наборе данных образцов речи с соответствующими показателями разборчивости. Набор данных может быть получен с помощью субъективных тестов, в которых слушатели оценивают образцы речи на основе их способности понимать произносимые слова. Нейронная сеть обучена предсказывать оценку разборчивости на основе признаков, извлеченных из речевого сигнала.

Одной из самых популярных архитектур нейронных сетей, используемых для оценки разборчивости речи, является сверточная нейронная сеть (CNN) (рис. 1). CNN обычно используются в задачах обработки изображений, а также показала многообещающие результаты в обработке речи. В CNN входной речевой сигнал сначала преобразуется в спектрограмму, которая представляет собой двумерное представление частотного содержания речевого сигнала с течением времени. Затем CNN учится извлекать соответствующие характеристики из спектрограммы, которые используются для прогнозирования показателя разборчивости [5].

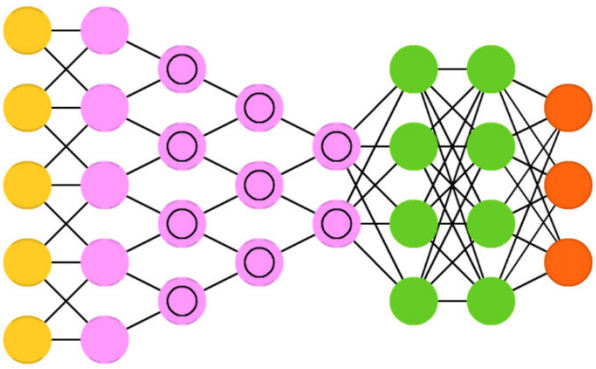


Рис. 1. Сверточная нейронная сеть

Производительность системы оценки разборчивости речи на основе нейронной сети зависит от нескольких факторов, таких как качество обучающего набора данных, выбор архитектуры нейронной сети и метод извлечения признаков. Кроме того, на производительность нейронной сети может влиять фоновый шум и акцент говорящего. Поэтому важно тщательно спроектировать обучающий набор данных и архитектуру нейронной сети для достижения наилучшей производительности.

Обучение и достоверность реализованной нейронной сети

Обучение сверточной нейронной сети происходит на спектрограммах в логарифмическом виде из аудиозаписи мужского голоса с наложенным белым шумом (рис. 2, рис. 3).

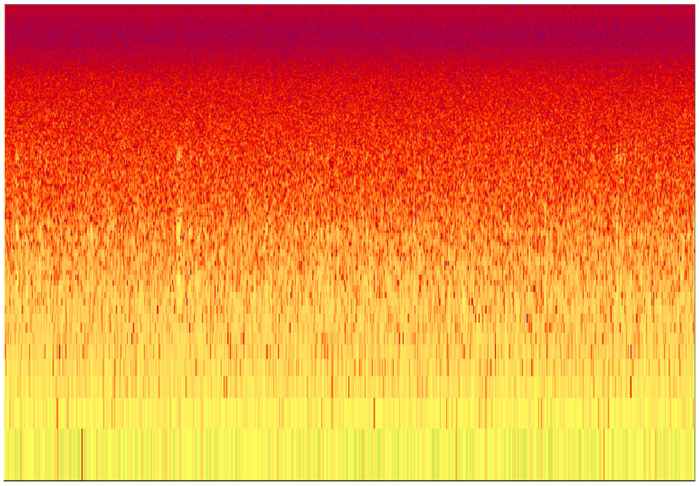


Рис. 2. Спектрограмма из аудиозаписи

```
0.6636
Epoch 4996/5000
110/110 [==============================] - 1s 7ms/step - loss: 1.1527 - accuracy: 0.4209 - val_loss: 2.1001 - val_accuracy:
0.8182
Epoch 4997/5000
110/110 [==============================] - 1s 7ms/step - loss: 1.2951 - accuracy: 0.4324 - val_loss: 2.1113 - val_accuracy:
0.8636
Epoch 4998/5000
110/110 [==============================] - 1s 7ms/step - loss: 1.2793 - accuracy: 0.2818 - val_loss: 1.1710 - val_accuracy:
0.7182
Epoch 4999/5000
110/110 [==============================] - 1s 7ms/step - loss: 1.2919 - accuracy: 0.4000 - val_loss: 1.1290 - val_accuracy:
0.9182
Epoch 5000/5000
110/110 [==============================] - 1s 7ms/step - loss: 1.1904 - accuracy: 0.4455 - val_loss: 1.8576 - val_accuracy:
0.8818

: model.evaluate_generator(generator=test_set, steps=22)

: [1.6221108436584473, 0.27272728085517883]
```

Рис. 3. Точность распознавания разборчивости речи на 4996-5000 эпохе

Проверку достоверности произведем с помощью меры точности (precision) [6]. Результаты процесса обучения введем в TensorBoard, это инструмент для визуализации показателя точности на каждой итерации эпохи (рис. 4), можем увидеть, что средняя достоверность 0,789 [7].

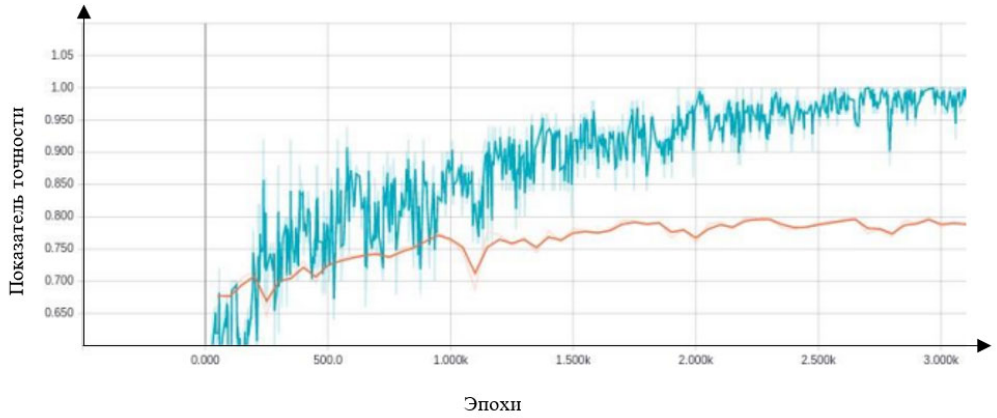


Рис. 4. Доля корректных прогнозов (accuracy): синий график – обучение, оранжевый – проверка

Заключение

В заключение можно сказать, что нейронные сети продемонстрировали большой потенциал в объективной оценке разборчивости речи. Способность точно оценивать разборчивость речи может иметь значительные последствия в различных областях, включая аудиологию, логопедию и телекоммуникации. С дальнейшими достижениями в области глубокого обучения можно ожидать появления более сложных моделей нейронных сетей, которые могут еще больше повысить эффективность оценки разборчивости речи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Акустическая экспертиза каналов речевой коммуникации. Монография / Дидковский В. С., Дидковская М. В., Продеус А. Н. – Киев, 2008. 420.

2. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М.: Гелиос АРВ, 2017. – 336 с.

3. ОЗИ Практикум ВМ Алефиренко, ЮВ Шамгин, БГУИР 2004 (Лаб практикум).

4. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. – М.: ГЛТ, 2016. – 280 с.

5. J. Turian et al. Word representations: A simple and general method for semi-supervised learning. Proceedings of the 48th Annual Meeting of the Association for Computational Linguistics, с. 384-394, 2010.

6. В. Д. Чабаненко. Модификации метода стохастического градиентного спуска для задач машинного обучения с большими объемами данных. Master’s thesis, Московский государственный университет имени М.В. Ломоносова, 2016.

7. Google Research Team. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. arXiv:1603.04467 [cs.DC], 2016.

8. Партыка, Т.Л. Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2016. – 432 с.

9. Петров, С.В. Информационная безопасность: учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – М.: АРТА, 2016. – 296 с.

10. Семененко, В.А. Информационная безопасность: учебное пособие / В.А. Семененко. – М.: МГИУ, 2017. – 277 с.

УДК 796:616
DOI 10.33764/2618-981X-2023-6-175-181

А. Д. Меньшикова[1], Г. В. Симонова[1]*

Спортивная и медицинская диагностика посредством анализа выдыхаемого воздуха газоанализатором HEALTHMONITOR

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: shtork00@inbox.ru

Аннотация. На сегодняшний день измерительные системы для определения качественного и количественного состава малых газовых примесей имеют важное значение в различных областях деятельности человека. Анализ состава выдыхаемого воздуха в последнее время все чаще используется как способ мониторинга состояний метаболизма при различных заболеваниях. Основными преимуществами данного метода является неинвазивность, безболезненность и простота в исполнении для пациента и исследователя. По данным литературы изучение образцов выдыхаемого воздуха различными методами показало корреляцию между концентрацией некоторых летучих органических соединений и определенными заболеваниями. Анализ рынка аппаратов для медицинской и спортивной диагностики показывает необходимость в коммерчески доступных и простых в эксплуатации устройств неинвазивного мониторинга состояния метаболизма. В статье рассмотрены методы газоанализа, которые могут быть использованы для данных целей. Показаны отличительные особенности и преимущества атомно-эмиссионной спектроскопии на примере газоанализатора HEALTHMONITOR.

Ключевые слова: газоанализ, атомно-эмиссионная спектроскопия, медицинская диагностика

A. D.Menshikova[1], G. V.Simonova[1]*

Sports and Medical Diagnostics Through the Analysis of Exhaled Air By the Gas Analyzer HEALTHMONITOR

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: shtork00@inbox.ru

Abstract. To date, measuring systems for determining the qualitative and quantitative composition of small gas impurities are important in various fields of human activity. Analysis of the composition of exhaled air has recently increasingly used as a way to monitor metabolic conditions in various diseases. The main advantages of this method are non-invasiveness, painlessness and ease of execution for the patient and researcher. According to the literature, the study of exhaled air samples by various methods showed a correlation between the concentration of certain volatile organic compounds and certain diseases. Analysis of the market of devices for medical and sports diagnostics shows the need for commercially available and easy-to-use devices for noninvasive monitoring of metabolic conditions. The article discusses the methods of gas analysis that can used for these purposes. The distinctive features of the atomic emission spectroscopy method presented on the example of the HEALTHMONITOR gas analyzer.

Keywords: gas analysis, atomic emission spectroscopy, medical diagnostics

Введение

Анализ человеческого дыхания – это новая и перспективная методика, так как позволяет эффективно контролировать биохимические процессы и неинвазивна, что делает технологию доступной и безопасной. В результате метаболических процессов в организме образуются летучие органические соединения. Эти вещества проходят через кровоток, участвуют в альвеолярном обмене и впоследствии появляются при выдохе.

В нормальных условиях концентрация определенных соединений в тканях или жидкостях человека определяется их ролью в метаболических процессах и, как правило, колеблется в небольших пределах. Однако при патологии метаболический профиль может резко измениться.

Контролируя эти показатели ежедневно/еженедельно, можно определить индивидуальную норму, идентифицировать проблемы в работе организма, отравления, вирусные или бактериальные инфекции и т. д.

Целью данной работы является поиск наиболее эффективного метода спортивной и медицинской диагностики.

Задачей данной работы является проведение сравнительного анализа существующих методов диагностики.

Анализ рынка аппаратов для медицинской и спортивной диагностики пациентов показывает необходимость в коммерчески доступных и простых в эксплуатации устройств неинвазивного мониторинга состояний метаболизма особенно при диабете, заболеваниях легких и желудочно-кишечного тракта (ЖКТ). При инвазивном методе диагностики и мониторинга требуется ежедневный многократный забор капиллярной крови, что особенно проблематично при проведении такой манипуляции больным детям, либо необходимы болезненные эндоскопические процедуры (при заболеваниях легких и ЖКТ) [1]. Поэтому потребность в разработке новых, не инвазивных, дистанционных технологий детектирования следов биомаркеров с высокой экономической эффективностью и большим социально значимым эффектом является, несомненно, актуальной задачей.

HEALTHMONITOR – это высокотехнологичный газоанализатор, который позволяет определять перечисленные выше параметры и проанализировать летучие органические соединения, содержащиеся в выдыхаемом человеком воздухе [2], что позволит получить глубокое понимание состояния различных биохимических процессов в организме человека.

Основные принципы работы газоанализатора HEALTHMONITOR

В основе созданного газоанализатора лежит хорошо известный физический принцип: спектр каждого химического соединения уникален и имеет свои индивидуальные интенсивные характеристические линии.

В основе лежит оригинальная технология эмиссионной спектроскопии, использующая излучения тлеющего разряда. Данная технология является уникальной и не имеет аналогов в мире. Способ детектирования малых примесей атомов и молекул в воздухе или газовой пробе основан на спектральном анализе линий

высокочастотного емкостного тлеющего разряда при пониженном давлении с нормировкой на спектр эмиссии опорной пробы для выделения спектральных групп пиков и полос, характерных для примесных компонентов [2].

Использование данной технологии обеспечивает возможность определения качественного и количественного состава малых газовых примесей в воздухе в режиме реального времени, а также проводить непрерывную фиксацию и анализ газовой пробы с высокой точностью и чувствительностью измерения.

Поскольку измерения примесей в пробе производятся с использованием эмиссионного излучения, становится ненужным использование многопроходных ячеек поглощения пробного лазерного излучения. Кроме того, высокая селективность предложенного метода сочетается с широким спектральным диапазоном детектируемых спектров, которые охватывают практически все газообразные примеси в анализируемой пробе [3]. Регистрация эмиссионного спектра газовой примеси происходит на «нулевом световом фоне» в отличие от регистрации спектра поглощения этой примеси, которая производится в условиях сильной засветки фотоприемника пробным лазерным излучением. Это позволяет достичь большего соотношения сигнал/шум, чем в случае с использованием спектроскопии поглощения пробного лазерного излучения [4].

Устройство для реализации заявленной технологии состоит из разрядной трубки с высокочастотным емкостным генератором тлеющего разряда в условиях низкого давления в сочетании со спектрометром видимого диапазона волн с возможностью расшифровки и интерпретации спектров [5].

Пробоотборная часть также включает стеклянный капилляр, производимый компанией [5], который обеспечивает понижение давления воздуха в разрядной ячейке до крайне малых значений в диапазоне от 40 Па до 94 Па. Новизна применяемого капилляра в совокупности с возможностями снятия спектра раз в миллисекунду позволяет использовать капилляр как аналог дорогостоящей полимерной разделительной колонки.

Дополнительную очистку системы осуществляет встроенный насос, который обеспечивает удаление остатков воздуха от предыдущего теста из патрубков системы, не допуская его застоя. Помимо насоса откачки, третью ступень очистки обеспечивают ультрафиолетовые светодиоды, захватывающие пробоотборную зону газоанализатора, где отсутствует самоочищающийся тлеющий разряд. Управление системами газоанализатора производится микроконтроллером [6, 7].

Новизна представленного решения заключается не только в аппаратном комплексе, но и способе анализа данных.

Полученные спектрограммы газовоздушной смеси подвергаются не только классическому спектральному анализу, но и анализу с использованием нейросетевых технологий. Использование нейросетевого анализа было включено в общий процесс аналитики для расширения возможностей газоанализатора и ускорения исследовательского процесса. В настоящее время использование нейросетей является достаточно тривиальной задачей, например, они широко используются для целей идентификации личности. В созданном газоанализаторе нейросе-

тевые алгоритмы используются для анализа газовых примесей (химических соединений) в анализируемых пробах (выдох человека, проба газовоздушной смеси из какого-либо промышленного технологического процесса и пр.). Использование нейросетевых алгоритмов позволяет анализировать не только наличие конкретных газовых соединений в анализируемой пробе, но и получать и анализировать общий “рисунок” спектра. Ниже представлены спектры органических соединений бутана и ацетона (по вертикали определяется интенсивность свечения спектра, по горизонтали длина волны), зафиксированных на газоанализаторе HEALTHMONITOR (рис. 1).

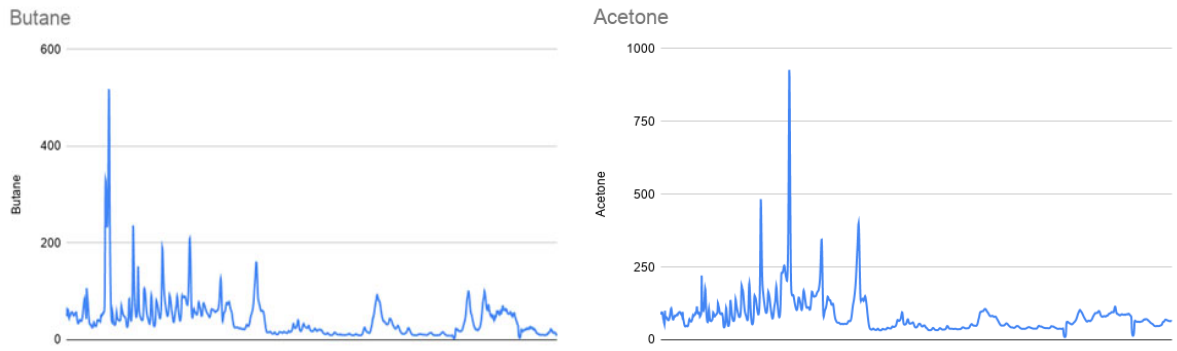


Рис. 1. Спектры органических классов веществ

Анализ существующих методов

Все существующие сопоставимые методы газоанализа, в основном, можно разделить на три группы:

Электрохимические методы, основанные на отличии степени адсорбции различных газов к поверхности микрочипа. Данный тип газоанализаторов широко распространен в силу своей относительно невысокой стоимости, однако имеет существенные ограничения, поскольку: не является универсальным, датчики производятся для одного выбранного газа (один газ - один датчик); теряют чувствительность и селективность в процессе эксплуатации требуется постоянная замена датчиков, являющихся, по сути, расходным материалом, и их калибровка [8, 9].

Методы, основанные на измерении отношения массы к заряду ионов детектируемых веществ или отличии их диффузионных свойств. Эта группа методов включает в себя: масс-спектрометрию, газовую хроматографию, масс-спектрометрию, совмещенную с газохроматографическим разделением. Недостатками технических решений, реализующих указанные методы, являются: высокая стоимость, необходимость использования сложного и громоздкого оборудования; необходимость наличия больших объемов сверхчистых газов-носителей в сменяемых баллонах высокого давления; техническая сложность реализации в конкретных изделиях; высокие требования к квалификации операторов, работающих на данном оборудовании. Кроме того, как правило, процесс измерения занимает достаточно много времени в связи с необходимостью сбора газовой

пробы (образцов), их транспортировкой, хранением и подготовкой к анализу. В качестве еще одного недостатка можно указать отсутствие мобильности у оборудования данных типов, поэтому приходится осуществлять пробоотбор на месте и транспортировать пробы в стационарную лабораторию [10, 11].

Методы, основанные на различии спектров поглощения исследуемых газов от спектров воздуха. Известны технические решения с использованием спектров поглощения: фотоакустическая спектроскопия; диодно-лазерная спектроскопия поглощения. Недостатком этих достаточно известных технических решений является использование в их конструкции дорогих лазерных источников света, состоящих из лазеров накачки или перестраиваемых в широком спектральном диапазоне диодных лазеров и громоздких многопроходных ячеек поглощения. Зачастую, эти методы требуют использование криогенных температур, необходимых для функционирования источников излучения или детекторов. В случае использования спектроскопии поглощения, большое количество паров воды, повсеместно присутствующих при заборе газовой пробы, оказывает негативное влияние на чувствительность и точность измерений, поскольку газопропускание многопроходных ячеек поглощения резко снижается вследствие конденсации паров на оптических окнах. Использование нагреваемых ячеек неудобно в практике и требует большого расхода электроэнергии. Кроме того, большое количество линий воды в регистрируемых спектрах представляет серьезную проблему для их расшифровки и корректной интерпретации [12, 13].

На основе проведенного анализа были сделаны выводы о преимуществе применяемой в газоанализаторах HEALTHMONITOR эмиссионной спектроскопии тлеющего разряда по сравнению с другими выше перечисленными методами, заключающемся в том, что не требуется применение сверхвысокого вакуума и криогенных температур. К тому же эмиссионная спектроскопия в видимом диапазоне длин волн малочувствительна к наличию паров воды в анализируемой пробе в силу отсутствия сильных линий воды в этом диапазоне и имеет высокую спектральную селективность и универсальность.

Заключение

HEALTHMONITOR предлагает простые и дешевые решения на основе использования свечения слаботочного газового разряда в рабочей прокачиваемой ячейке с воздухом и молекулами биомаркеров, что позволяет с высокой точностью идентифицировать газовый состав среды, в которой происходит разряд, по известным спектральным базам.

Метод прост в реализации, не нуждается в использовании газа носителя, не требует дорогих расходных материалов и допускает создание компактных устройств, пригодных, в том числе для применения в домашних условиях.

Газоанализатор соответствует уровню технического развития нашей страны, что делает возможным реализацию производства на базе отечественных промышленных мощностей.

В рамках данной работы планируются дальнейшие исследования использования спектроскопии тлеющего разряда в воздухе в видимом диапазоне спектра

для медицинской и спортивной диагностики, а также организация серийного производства газоанализатора.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Анализ рынка «Спорт и здоровье 2.0» // HealthNet: [сайт]. – URL: https://healthnet.academpark.com/media/analitika/analiz-rynka-sport-i-zdorove-2-0/ (дата обращения: 13.04.2023)

2 Способ хроматографического анализа смесей веществ и газовый хроматограф : пат. 2018821 C1 Рос. Федерация, МПК G01N 30/40. № 5007268/25 ; заявл. 02.10.1991 ; опубл. 30.08.1994 / В. Г. Березкин, А. Б. Урин, Е. Ю. Сорокина [и др.]. – EDN FCVDHX (дата обращения: 13.04.2023)

3 Способ выполнения анализа газовых смесей : пат. 2470290 C1 Рос. Федерация, МПК G01N 30/00. № 2011119457/28 ; заявл. 13.05.2011 ; опубл. 20.12.2012 / А. М. Хисматулина, О. Ф. Верещагина, Е. В. Коровицкая [и др.]; заявитель Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Дальневосточный федеральный университет» (ДВФУ). – EDN UVNWMM (дата обращения: 13.04.2023)

4 Лебедев, А. Т. Масс-спектрометрия в органической химии : учебное пособие / А. Т. Лебедев. – 2-е изд., перераб. и доп. – Москва : Техносфера, 2015. – 704 с. – ISBN 978-5-94836-409-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/110953 (дата обращения: 24.11.2022). – Режим доступа: для авториз. пользователей

5 Мотт, Ж. Хроматографические методы анализа смесей / Ж. Мотт, М. Тэйлор // Нефтегазовые технологии. – 2008. – № 7. – С. 78–80. – EDN KWEOCH (дата обращения: 13.04.2023)

6 ГОСТ 30324.0-95. Изделия медицинские электрические. – М. : Стандартинформ, 2009. – 140 с. – Текст : непосредственный.

7 ГОСТ Р 50444. Приборы, аппараты и оборудование медицинские. Общие технические требования. – М. : Стандартинформ, 2020. – 28 с. – Текст : непосредственный.

8 Способ хроматографического анализа газовых смесей: а. с. 181375 A1 СССР, МПК G01N 30/34. № 1004230/26-25 / Л. А. Галкин, С. М. Гуревич ; заявл. 21.04.1965 ; опубл. 15.04.1966. – EDN TKOCRR (дата обращения: 13.04.2023)

9 Жебентяев, А. И. Аналитическая химия. Хроматографические методы анализа : учебное пособие / А. И. Жебентяев. – Минск : Новое знание, 2013. – 206 с. – ISBN 978-985-475-553-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/64909 (дата обращения: 24.03.2023). – Режим доступа: для авториз. пользователей

10 Вялых, И. А. Автоматический газовый хроматографический анализ: теоретическте основы и аппаратурное оформление : учебное пособие / И. А. Вялых, А. Г. Шумихин. – Пермь : ПНИПУ, [б. г.]. – Ч. 1. – 2008. – 290 с. – ISBN 9789-5-88151-971-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/160936 (дата обращения: 24.03.2023). – Режим доступа: для авториз. пользователей;

11 Гуськова, В. П. Хроматографические методы разделения и анализа : учебное пособие / В. П. Гуськова, Л. С. Сизова. – 2-е изд., испр. и доп. – Кемерово : КемГУ, 2015. – 148 с. – ISBN 978-5-89289-888-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/72028 (дата обращения: 24.03.2023). – Режим доступа: для авториз. пользователей

12 Конюхов, В. Ю. Хроматография : учебник / В. Ю. Конюхов. – Санкт-Петербург : Лань, 2022. – 224 с. – ISBN 978-5-8114-1333-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/210989 (дата обращения: 24.03.2023). – Режим доступа: для авториз. пользователей

13 Краснокутская, Е. А. Спектральные методы исследования в органической химии : учебное пособие / Е. А. Краснокутская, В. Д. Филимонов. – Томск : ТПУ, [б. г.]. – Часть II : ЯМР-спектроскопия, масс-спектрометрия. – 2013. – 88 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/45172 (дата обращения: 24.03.2023). – Режим доступа: для авториз. пользователей

УДК 528.71
DOI 10.33764/2618-981X-2023-6-182-185

Н. Г. Нестеров[1], А. В. Чуваков[1]*

Стеганографический метод защиты информации в графическом файле формата GIF

[1] Самарский государственный технический университет, г. Самара, Российская Федерация
*e-mail: nesterovnikita0906@gmail.com

Аннотация. В данной статье исследуем, как можно улучшить стеганографию путем включения невзаимозаменяемых токенов (NFT) в изображения GIF, чтобы обеспечить дополнительный уровень защиты конфиденциальной информации. Стеганография — это метод сокрытия конфиденциальной информации в другом файле или носителе без изменения ее видимого содержимого. Изображения в формате GIF (Graphics Interchange Format) обычно используются в качестве носителей для стеганографических сообщений из-за простоты их передачи и широкого распространения в Интернете.

Ключевые слова: технологии NFT (Non-Fungible Token), стеганография, изображение GIF, авторские права, невзаимозаменяемый токен

N. G. Nesterov[1], A. V. Chuvakov[1]*

Steganographic Method of Protecting Information in a GIF Graphic File

[1] Samara State Technical University, Samara, Russian Federation
*e-mail: nesterovnikita0906@gmail.com

Annotaion. In this article, we explore how steganography can be improved by including non-fungible tokens (NFTs) in GIF images to provide an additional layer of protection for sensitive information. Steganography is a method of hiding sensitive information in another file or medium without changing its visible content. GIF (Graphics Interchange Format) images are commonly used as media for steganographic messages due to their ease of transmission and wide distribution on the Internet.

Keywords: technologies NFT (Non-Fungible Token), steganography, GIF image, copyright, non-fungible token

Введение

С ростом распространенности кибератак потребность в безопасных методах передачи информации стала первостепенной. Стеганография позволяет передавать конфиденциальную информацию по скрытым каналам, не привлекая к ней внимания. Скрывая информацию в изображениях GIF, можно передавать сообщения незамеченными для перехватчиков. Однако с появлением NFT (Non-Fungible Token) теперь можно усовершенствовать стеганографические методы и обеспечить дополнительный уровень безопасности [1, 2]. NFT – это уникальные цифровые активы, которые хранятся в блокчейне. Каждый NFT уникален и не может быть воспроизведен или обменен на другой токен. NFT становятся все более популярными для различных приложений, включая цифровое искусство, предметы коллекционирования и игры [3].

Стеганографические методы

Существует несколько стеганографических методов, которые могут использоваться для защиты информации в графическом файле GIF, включая:

– метод Least Significant Bit (LSB) – этот метод заключается в том, чтобы заменить наименее значимый бит каждого пикселя в изображении на биты информации, которую нужно скрыть. Данные скрываются в младших разрядах каждого пикселя, что делает их почти незаметными для человеческого глаза. Этот метод является одним из самых простых и широко используемых методов стеганографии в изображениях;

– метод маскировки – в этом методе используется маска, которая накладывается на изображение для скрытия данных. Это делается путем замены определенных цветовых пикселей на другие цвета, которые представляют биты информации. Таким образом, данные могут быть скрыты в маске, которая используется для скрытия их в изображении;

– метод частотного преобразования – в этом методе данные скрываются в высокочастотных компонентах изображения. Данные могут быть встроены в компоненты, такие как дискретное косинусное преобразование (DCT) или вейвлет-преобразование. Этот метод обычно используется в JPEG-изображениях, но также может быть применен к GIF-изображениям.

– метод встраивания NFT-элементов – этот метод заключается в встраивании информации в изображение, используя NFT-элементы. Это делается путем сокрытия метаданных NFT в младших разрядах каждого пикселя или путем встраивания самого NFT в изображение. Этот метод может быть использован для передачи конфиденциальной информации, такой как ID токена, информация о владельце, история транзакций и т.д. [4, 5].

В данной статье исследуются два метода усиления стеганографии с помощью NFT-элементов в GIF-изображениях: сокрытие метаданных NFT в младших разрядах каждого пикселя и встраивание самого NFT в изображение. Оба метода могут использоваться для передачи конфиденциальной информации в GIF-изображениях.

Методы встраивания NFT элементов

Путем включения элементов NFT в изображения GIF можно повысить безопасность стеганографии. Один из методов заключается в сокрытии метаданных NFT в младших разрядах каждого пикселя. В этом методе метаданные NFT (например, ID токена, информация о владельце, история транзакций и т.д.) могут быть сокрыты в младших разрядах каждого пикселя в GIF-изображении. Данные могут быть сокрыты с использованием метода Least Significant Bit (LSB), путем замены наименее значимого бита каждого пикселя на биты метаданных NFT. Это позволяет сохранить визуальное качество изображения, при этом скрытая информация остается защищенной от нежелательных глаз [5, 6].

Данный метод предлагает усиленную стеганографию с использованием NFT-элементов в GIF-изображениях. Такой подход может быть использован в

различных областях, таких как в электронной коммерции, где GIF-изображения могут быть использованы для передачи информации о товарах и услугах, а также в медицинских областях, где GIF-изображения могут быть использованы для передачи конфиденциальной информации о пациентах [7].

Другой метод включает встраивание NFT в само изображение GIF. В этом методе сам NFT может быть встроен в GIF-изображение. Для этого необходимо определить определенный участок изображения, который будет использоваться для встраивания NFT. В этом участке можно использовать определенные пиксели для представления битов информации NFT. После встраивания NFT в изображение оно может быть сохранено в формате GIF и передано получателю [7].

Этот метод также предоставляет усиленную стеганографию с использованием NFT-элементов в GIF-изображениях. Этот подход может быть использован в качестве дополнительного слоя защиты, что делает его особенно полезным для передачи конфиденциальной информации, такой как ID токена, информация о владельце, история транзакций и т.д. [4].

Оба этих метода демонстрируют возможности усиленной стеганографии в GIF-изображениях с использованием NFT-элементов. В данной статье будет произведено сравнение этих методов на основе критериев, таких как качество изображения, стойкость к атакам и скорость встраивания/извлечения данных [8].

Сравнение методов

Для сравнения двух методов рассмотрены следующие критерии: качество изображения, стойкость к атакам и скорость встраивания/извлечения данных.

Качество изображения. Оба метода позволяют сохранить качество изображения на высоком уровне. Однако, при использовании метода встраивания NFT в изображение, может потребоваться выделить определенную область изображения, что может повлиять на общее качество изображения.

Стойкость к атакам. Метод сокрытия метаданных NFT в младших разрядах каждого пикселя имеет более высокую стойкость к атакам, чем метод встраивания самого NFT в изображение. Это связано с тем, что второй метод может быть подвержен атакам, которые могут изменять выбранный участок изображения и портить данные NFT.

Скорость встраивания/извлечения данных. Метод сокрытия метаданных NFT в младших разрядах каждого пикселя обычно требует больше времени на встраивание и извлечение данных, так как данные должны быть встроены в каждый пиксель. Метод встраивания самого NFT в изображение, в свою очередь, может быть выполнен быстрее, так как данные NFT могут быть легко встроены в определенный участок изображения [9].

Исходя из этих критериев, можно сделать вывод, что оба метода имеют свои преимущества и недостатки в зависимости от конкретной ситуации, в которой они могут быть использованы. Например, метод сокрытия метаданных NFT в младших разрядах каждого пикселя может быть полезен в случае, когда стойкость к атакам является приоритетной задачей. Метод встраивания самого NFT в изображение может быть более подходящим в случае, когда необходимо

быстро встроить данные NFT в изображение и сохранить высокое качество изображения [9, 10].

Заключение

В заключение можно сказать, что включение элементов NFT в стеганографию в изображениях GIF обеспечивает дополнительный уровень безопасности для защиты конфиденциальной информации. Встраивая метаданные NFT в LSB каждого пикселя или создавая уникальный NFT для представления изображения GIF, можно передавать сообщения скрытно и безопасно. Однако стеганографию, усиленную NFT, следует использовать в сочетании с другими мерами безопасности, чтобы обеспечить максимальную защиту конфиденциальной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Луговой В. Е. Non-Fungible Token (NFT). В сборнике: информационные технологии, системный анализ и управление (ИТСАУ-2021). Ростов-на-Дону – Таганрог, 2021. С. 173-175.

2. Тройнин Р. А., Корниленко О. И., Денисенко В. В. Обзор технологии NFT, ее структура и особенности. Инновации. Наука. Образование. 2022. № 52. С. 515-520.

3. Анненко А. И., Кочетков П. С. Правовая природа NFT с точки зрения права интеллектуальной собственности. В сборнике: дни науки факультета права НИУ «Высшая школа экономики». Сборник докладов VI Ежегодной научно-практической конференции. Москва, 2022. С. 95-100.

4. Ванцовская А. А. Цифровое искусство на блокчейне и NFT-рынок. StudNet 2021. Т. 4 № 7. С. 25.

5. Петрова А. Цифровое искусство на примере NFT. Проблемы распределения прав при обращении NFT на блокчейн-платформах. В сборнике: Правовая защита интеллектуальной собственности: проблемы теории и практики. Сборник материалов X Международного юридического форума (IP Форум). 2022. С. 312-316.

6. Исааков Г. Н., Соколова Е. С. В сборнике: Молодежь в науке 2023. Сборник статей Международного научно-исследовательского конкурса. г. Петрозаводск, 2023. С. 179-183.

7. Лаптева И. Е. Применение технологии NFT в области создания цифрового контента. Академическая публицистика. 2022. № 6-1. С. 126-139.

8. Зобов А. NFT-токены: Правовой статус и их роль в IP. В сборнике: Правовая защита интеллектуальной собственности: проблемы теории и практики. Сборник материалов X Международного юридического форума (IP форум). 2022. С. 234-237.

9. Мисиченко Н. Ю., Асанов А. Р. Особенности технологии (NFT). В сборнике: Теория и практика менеджмента: состояние и перспективы. Сборник материалов международной научно-практической конференции профессорско-преподавательского состава, молодых ученых и студентов. Ростовский государственный экономический университет (РИНХ). 2022. С. 75-81.

10. Чикалова Ю. А. NFT и криптоискусство, влияние технологии NFT на арт-рынок. Инновации. Наука. Образование. 2021. № 48. С. 2659-2663.

УДК 681.7
DOI 10.33764/2618-981X-2023-6-186-190

И. А. Нищаков[1], В. С. Ефремов[1]*

Разработка тепловизионного коллиматорного прицела

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: ivanyso@yandex.ru

Аннотация. Основная проблема существующего прицельно-приборного оснащения подразделений сухопутных войск и частей специального назначения заключается в существенном отставании технических характеристик существующих оптико-электронных средств наблюдения, разведки и прицеливания. В ведущих зарубежных странах проводятся активные работы, направленные на модернизацию существующей и создание новой экипировки для военнослужащих. Одной из важных задач является снижение ее стоимости и внедрение в процесс серийного производства новых технологий, часть которых весьма дорогостояща. При этом их применение также требует значительных затрат. Задачей исследования является поиск схемного решения прицельного устройства, объединяющего преимущества коллиматорного прицела и тепловизионного прибора. Методами исследования являются: методы расчета и анализа оптических систем, автоматизированные методы проектирования. Вывод: предложено схемное решение нового прицельного устройства, обеспечивающего возможность одновременного наблюдаения сцены в видимом и в инфракрасном диапазонах.

Ключевые слова: прицел, тепловизор, коллиматорный прицел

I. A. Nishchakov[1], V. S. Efremov[1]*

Engineering of the Thermal Reflex Sight

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: ivanyso@yandex.ru

Abstract. The main problem of the existing sighting and instrument equipment of ground forces units and special purpose units is a significant lag in the technical characteristics of the existing optical-electronic means of surveillance, reconnaissance and aiming. In leading foreign countries, active work is being carried out aimed at modernizing the existing and creating new equipment for military personnel. One of the important tasks is to reduce its cost and introduce new technologies into the mass production process, some of which are very expensive. At the same time, their use also requires significant costs.The objective of the study is to find a schematic solution of a sighting device that combines the advantages of a collimator sight and a thermal imaging device. The research methods are: methods of calculation and analysis of optical systems, automated design methods. Conclusion: a schematic solution of a new sighting device is proposed, which provides the possibility of simultaneous observation of the scene in the visible and infrared ranges.

Keywords: scope, thermal vision, reflex sight

Введение

Основная проблема существующего прицельно-приборного оснащения подразделений сухопутных войск и частей специального назначения заключается в существенном отставании технических характеристик существующих оп-

тико-электронных средств наблюдения, разведки и прицеливания [1]. В ведущих зарубежных странах проводятся активные работы, направленные на модернизацию существующей и создание новой экипировки для военнослужащих. Одной из важных задач является снижение ее стоимости и внедрение в процесс серийного производства новых технологий, часть которых весьма дорогостояща. При этом их применение также требует значительных затрат.

Обзор существующих устройств

Прицел по патенту RU 2682988 (год публикации 2019) [2] содержит коллиматорный и тепловизионный каналы. Устройство прицела поясняется схемой, приведенной на рис. 1.

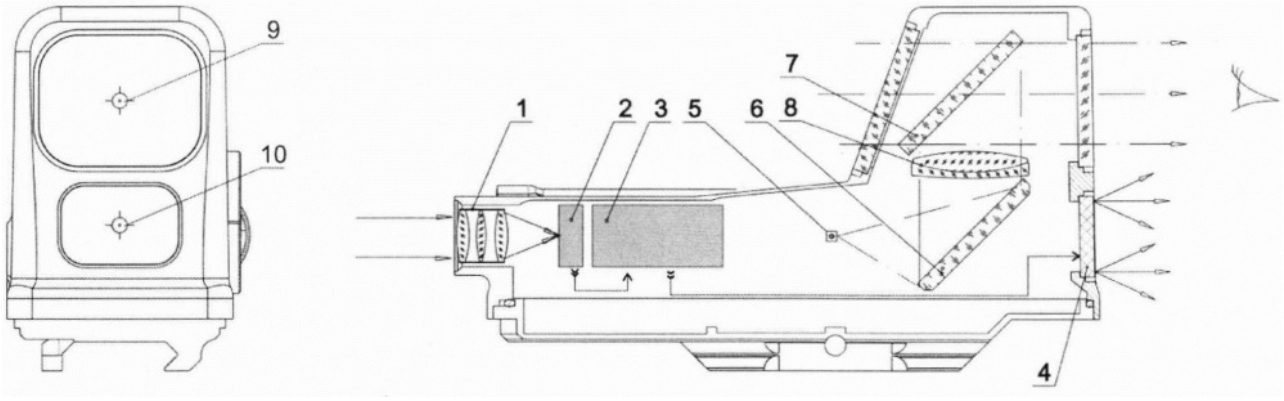


Рис. 1. Схема из патента RU 2682988:

1 - инфракрасный объектив, 2 - фотоприемное устройство, 3 - блок обработки изображения, 4 – дисплей, 5 - устройство формирования оптической прицельной марки, 6 - зеркало, 7 - светоделительная пластина или призма для направления изображения марки в глаз наблюдателя, 8 - линза или группа линз для перевода светового потока от марки в параллельные пучки, 9 - окно коллиматорного канала с оптической прицельной маркой, 10 - дисплей тепловизионного канала с электронной прицельной маркой

Коллиматорный тепловизионный прицел, содержащий коллиматорный канал в видимом диапазоне спектра, отличается из аналогов тем, что для одновременного наблюдения в двух спектральных диапазонах дополнительно содержит в одном корпусе инфракрасный объектив и фотоприемное устройство в виде матрицы микроболометров в фокальной плоскости объектива с областью чувствительности не менее 0,8 и не более 17 мкм, блок обработки сигнала и формирования электронной прицельной марки и матричный дисплей разрешением не менее 324x256 пикселей, причем оптическая ось коллиматорного канала и направление на дисплей параллельны с отклонением не более 15 градусов [2].

Недостатком данного технического решения является необходимость стрелка отвлекаться от наблюдения в видимом канале для работы с тепловизионным каналом.

Схемное решение устройства

Для устанения недостатка устройства, приведенного выше на рис. 1, предложена новая структурная схема и вариант компоновки устройства. Структурная схема предложенного устройства представлена ниже на рис. 2, а вариант компоновки устройства – на рис. 3.

Преложенное схемное решениие включает в себя следующие модули: излучатель, обьектив тепловизионный, обьектив коллиматорного канала, видеоконтрольное устройство (дисплей), блок обработки изображения, устройство преобразования изображения, усилитель, предусилитель, фотоприемное устройство, блок питания, источник питания.

Совмещение изображений видимого и инфракрасного диапазонов осуществляется путём проецирования микродисплея тепловизионного модуля в поле зрения коллиматорного прицела.

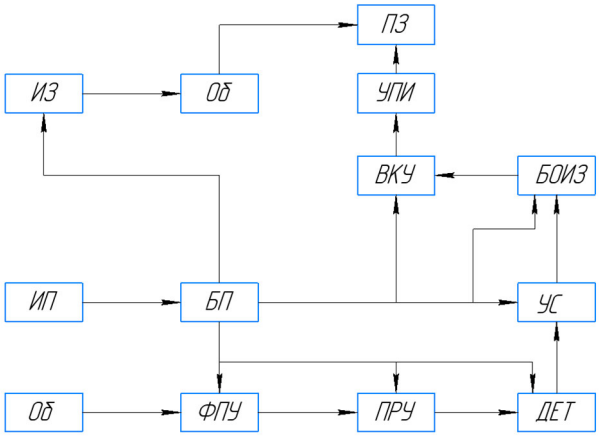


Рис. 2. Структурная схема устройства:

ИЗ – излучатель, Об – обьектив, ПЗ – поле зрения, ВКУ - видеоконтрольное устройство (дисплей) БОИЗ – блок обработки изображения, УПИ – устройство преобразования изображения, УС - усилитель, ДЕТ – детектор, ПРУ – предусилитель, ФПУ – фотоприемное устройство, БП – блок питания, ИП – источник питания.

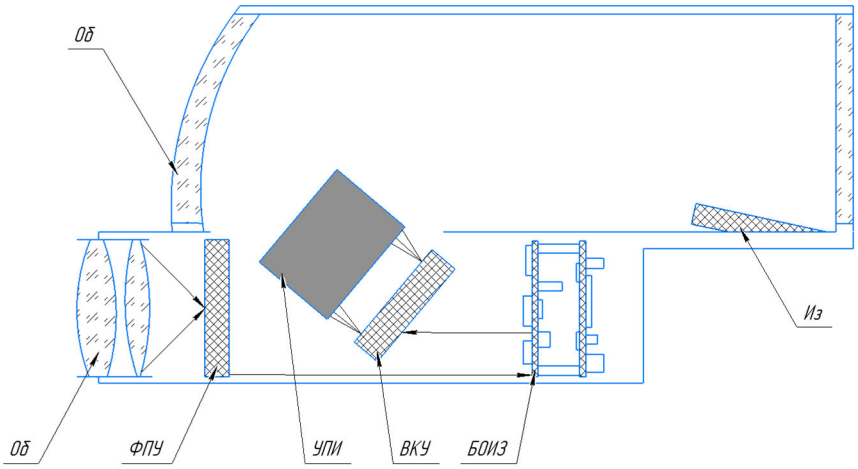


Рис. 3. Вариант компоновки устройства

Проверочный расчёт объектива

По выбраннному ФПУ GWIR 0203X1A на основе оксида ванадия [3] с разрешением 384x288 и размером пиксела 20x20 мкм по методике [4] был произведен энергетический расчёт, на основании которого выбран диаметр входного зрачка объектива: не менее 50 мм. В [5] был выбран объектив с требуемым диаметром входного зрачка и относительным отверстием 1:1,2, оптическая схема которого с ходом лучей приведена на рис. 4. Совместно с вышеуказанным приемником объектив обеспечивает поле зрения в пространстве предметов 9,6°. На рис. 5 приведен график дисторсии объектива, на рис. 6 – графики функции концентрации энергии в геометрическом приближении, без учета дифракции.

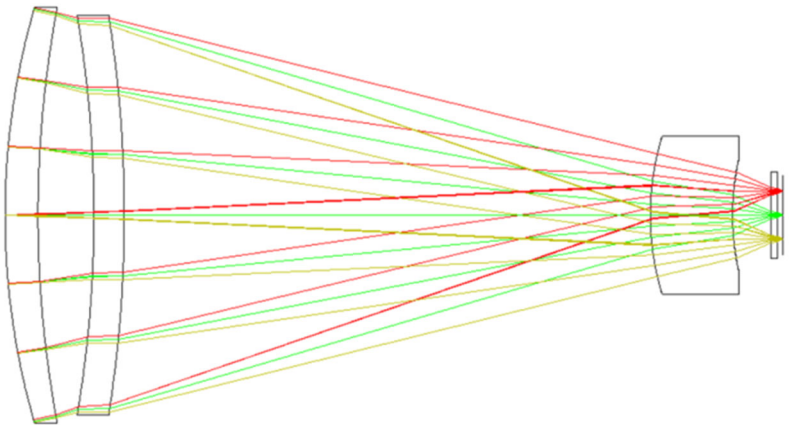


Рис. 4 . Оптическая схема объектива тепловизионного модуля

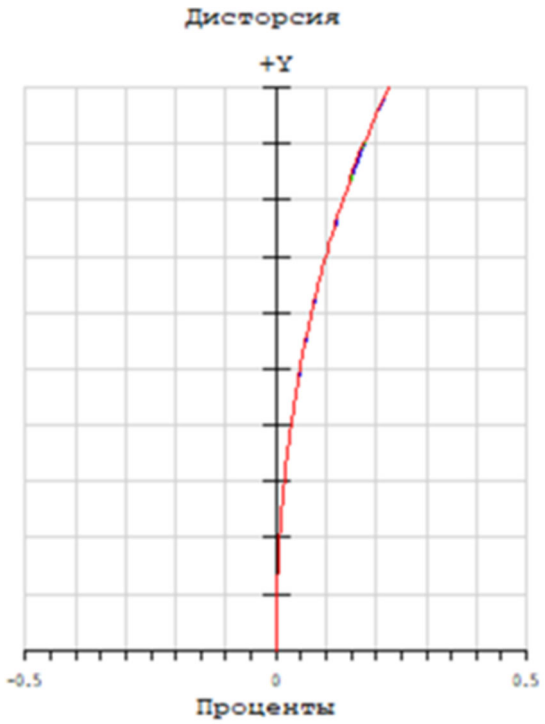


Рис. 5. График дисторсии объектива

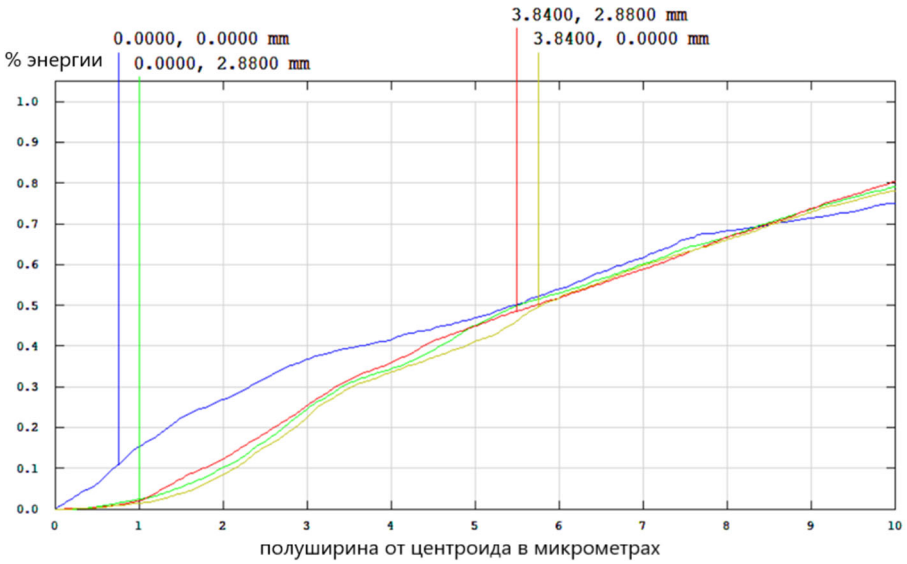


Рис. 6. График концентрации энергии

Дисторсия не превышает 0,3 %. На квадратной площадке размером 20×20 мм уровень концентрации энергии для различных точек поля составляет от 75 до 80 %, что характеризует высокую степень коррекции геометрических аберраций в оптической системе объектива и возможность его применения в разрабатываемом устройстве [6].

Заключение

Вывод: предложено схемное решение нового прицельного устройства, обеспечивающего возможность одновременного наблюдаения сцены в видимом и в инфракрасном диапазонах спектра.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Комбаров М. С., Кузнецов М. М. Современные оптико-электронные средства наблюдения, разведки и прицеливания для стрелкового оружия нормального калибра Интерэкспо Гео-Сибирь, 2017. – С. 104–107.

2. Пат. RU2682988 Российская Федерация, МПК F41G 1/00. Коллиматорный тепловизионный прицел ; № 2017113935 ; заявл. 21.04.2017; опубл. 25.03.2019 / Старцев В. В. ; заявитель и патентообладатель: АО «Оптико-механическое конструкторское бюро «Астрон». – 10 с. – Текст : непосредственный

3. НПК фотоника [Электронный ресурс] / НПК фотоника.–Режим доступа: https://www.npk-photonica.ru/. – Загл. с экрана. (дата обращения 10.05.2023).

4. Криксунов Л.З. Справочник по основам инфракрасной техники. – М.: Сов. радио, 1978. – 400 с.

5. Хацевич Т. Н. Компьютерные методы проектирования оптических систем : учебник для обучающихся по направлению подготовки 12.04.02 Оптотехника (уровень магистратуры). – Новосибирск : СГУГиТ, 2022. – 156 с..

6. Запрягаева Л.А., Свешникова И.С. Расчет и проектирование оптических систем: учебник для вузов. – Москва: Логос – 2000.

УДК 004.056.5
DOI 10.33764/2618-981X-2023-6-191-196

А. Р. Пашинин[1], В. В. Селифанов[1,2], П. А. Звягинцева[2,3], Е. А. Плахотникова[3],*

Экспертиза модели угроз безопасности информации для информационных систем

[1] Новосибирский государственный технический университет, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[3] Управление ФСТЭК России по Сибирскому федеральному округу, г. Новосибирск, Российская Федерация
*e-mail: a.pashinin@internet.ru

Аннотация. Основой работы является разработка автоматизированного программного средства для проведения экспертизы модели угроз безопасности информации, разрабатываемых для различных информационных систем, обрабатывающих данные на соответствие требованиям нормативным правовым актам и нормативно методической документации, инициированных Постановлением Правительства, ФСБ России и ФСТЭК России. В данной работе большое внимание уделяется реализации алгоритма построения модели угроз и созданию программного обеспечения, так как на данный момент нет аналогов данному приложению, а проверка документов оператором занимает большое количество времени. Основным продуктом в результате работы с разработкой автоматизированного средства является приложение, которое позволяет существенно сократить временные расходы за счет автоматизации процессов. Также разработанное программное обеспечение уменьшает количество ошибок, связанных с человеческим фактором.

Ключевые слова: модель угроз, государственная информационная система, экспертиза модели угроз, угрозы, защита информации

A. R. Pashinin[1], V. V. Selifanov[1,2], P. A. Zvyagintseva[2,3], E. A. Plakhotnikova[3]*

Expertise of the Information Security Threat Model for Information Systems

[1] Novosibirsk State Technical University, Novosibirsk, Russian Federation
[2] Siberian State University of Geosystems and Technologies, г. Novosibirsk, Russian Federation
[3] The Office of the Federal service for technical and export control in the Siberian Federal District, Novosibirsk, Russian Federation
*e-mail: a.pashinin@internet.ru

Abstract. The basis of the work is the development of an automated software tool for the expertise of information security threat models developed for various information systems that process data for compliance with the requirements of regulatory legal acts and regulatory methodological documentation initiated by the Decree of the Government, the Federal security service and the Federal service for technical and export control. In this work, much attention is paid to the implementation of the algorithm for building a threat model and the creation of software, since at the moment there are no analogues to this application, and the verification of documents by the operator takes a lot of time. The main product as a result of working with the development of an automated tool is an application that allows you to significantly reduce time costs by automating processes. Also, the developed software reduces the number of errors associated with the human factor.

Keywords: threat model, state information system, threat model expertise, threats, protection of information

Введение

Для любых информационных систем, так или иначе подлежащих защите, необходимо разрабатывать и актуализировать модель угроз, что является требованием соответствующих нормативных правовых документов [1, 2, 3].

Модель угроз содержит описание информационной системы и ее структурно-функциональные характеристики, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможные уязвимости информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации [3, 4], и разрабатывается в соответствии с методическими документами ФСТЭК России [5, 6].

Обязательным требованием для модели угроз государственных информационных систем является проведение государственной экспертизы документов и их согласование с ФСТЭК России и ФСБ России [6]. Это весьма трудоемкая работа, при этом сроки проведения ограничены 10 рабочими днями. Все это требует автоматизации процессов экспертизы. Задачей настоящей работы является разработка программного средства для автоматизации процессов экспертизы моделей угроз.

Разрабатываемое программное средство должно решить данные проблемы и уменьшить временные затраты на проведение экспертизы модели угроз за счет автоматизации процессов, позволив в условиях ограниченного времени на проведение экспертизы модели угроз составить заключение и позволить оператору проверить документ быстрее с минимизацией ошибок, связанных с человеческим фактором.

Требования к модели угроз для проведения экспертизы

Корректное создание модели угроз требует выявления актуальных угроз, так как именно они влияют на устанавливаемые средства защиты информации (далее – СЗИ).

Анализ требований к модели угроз [3-8], опыт работы, накопленный в Управлении ФСТЭК России по Сибирскому федеральному округу, показывает, что для проведения экспертизы достаточным условием будет оценка правильности определения класса защищенности, объекта воздействия и технологий, используемых для обработки информации, возможных негативных последствий от реализации угроз безопасности информации и их источника. Определяется вид нарушителей, их категории и уровень возможностей, а также совокупность тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность [10, 11 – 13]. При оценке возможности реализации угрозы должны присутствовать: объект воздействия, источник угрозы, способ реализации, возможные негативные последствия.

Указанная последовательность действий детально описана в Методике определения угроз безопасности информации [6] и хорошо алгоритмизируется. Программное обеспечение включает стандартные пункты методики [6], необходимые для сохранения общего вида стандартной модели угроз.

В ходе оценки угроз безопасности информации определяются информационные ресурсы, компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям.

Разработка программного средства на базе алгоритма для автоматизированного проведения экспертизы модели угроз

Для решения поставленной задачи было разработано программное обеспечение для проведения экспертизы модели угроз безопасности информации в информационных системах и ориентировано как на операторов, специалистов по защите информации, так и неопытных пользователей.

По результатам работы с программным обеспечением выдается отчет с базовым заполнением документа, актуальными угрозами и подобранными для них тактиками, и соответствующими им типовыми техниками, предлагаемые ФСТЭК России и матрицей MITRE ATT&CK [8 – 9].

Программное обеспечение включает в себя девять диалоговых окон:

1) начальная страница;
2) определение класса защищенности;
3) определение объектов воздействия;
4) выбор видов риска;
5) негативные последствия, после выбора риска;
6) определение нарушителя;
7) выбор источника угрозы;
8) возможность реализации угрозы безопасности информации;
9) завершение работы программы. Формирование и сохранение отчета.

Для начала необходимо выбрать уровень значимости информации и масштаб системы (рис. 1).

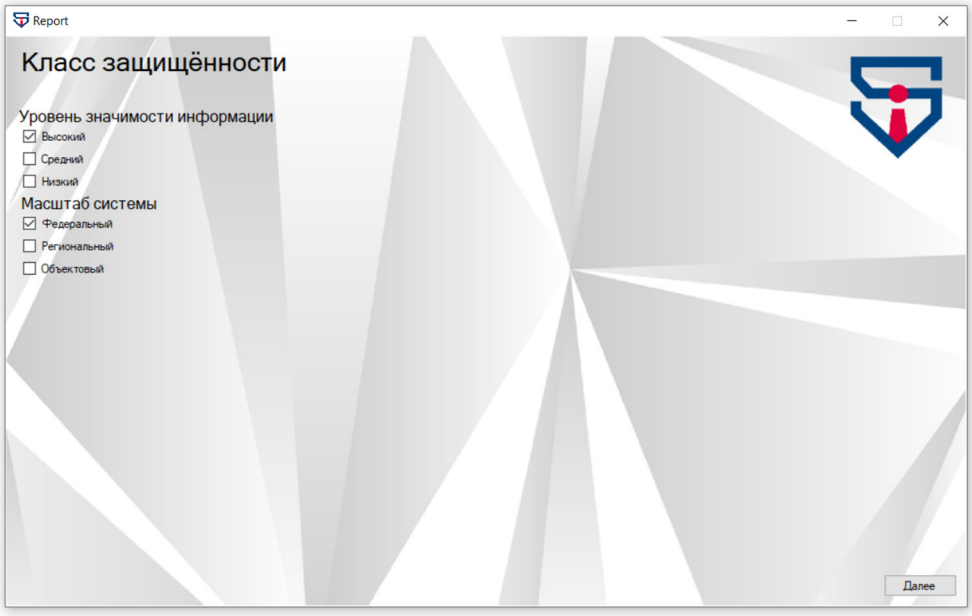


Рис. 1. Определение класса защищенности

Далее программа предложит выбор из списка объектов воздействия (рис. 2).

Рис. 2. Выбор объектов воздействия

Следующим этапом выбирается источник угроз и формируется список возможных угроз. Оператор выбирает угрозы, актуальные для конкретной системы и исключая лишние из проверяемой модели угроз (рис. 3).

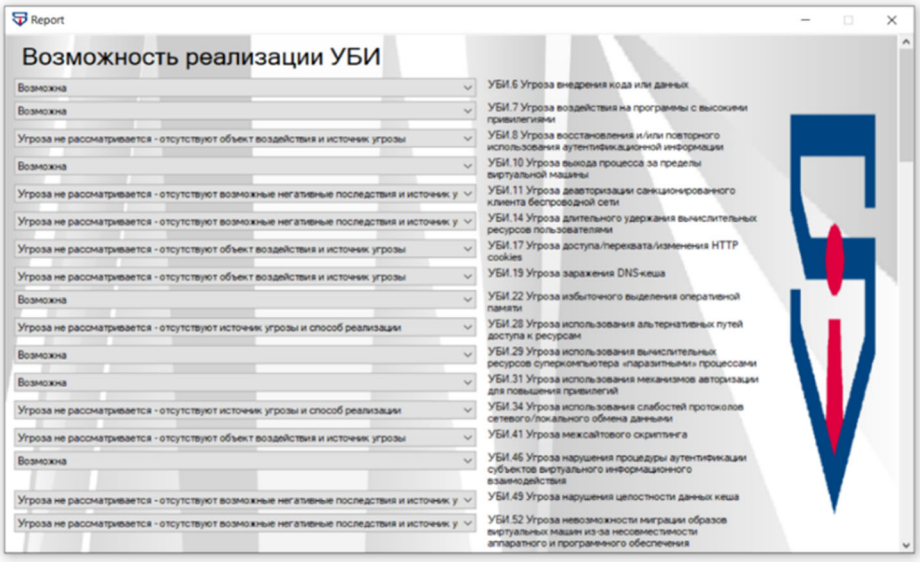


Рис. 3. Выбор объектов воздействия

Время заполнение отчета индивидуально и зависит от списка актуальных угроз, так как при заполнении отчета заполняются и таблицы с тактиками и соответствующими им типовыми техниками, используемыми для построения сценариев реализации угроз безопасности информации по методике ФСТЭК России и матрице MITRE ATT&CK [8 – 9]. Выбор тактик и техник осуществляется по

методическому документу «Методика оценки угроз безопасности информации» с помощью приложения 11, с перечнем основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации [4], а также с помощью матрицы MITRE ATT&CK. В MITRE было выделено двенадцать тактических задач (тактик), которые приходится решать нарушителю и из которых складывается сценарий. В ATT&CK из публично доступных отчетов об инцидентах и исследованиях угроз компьютерной безопасности выделяются общие Тактики, Техники и Процедуры. Также используются публично доступные исследования новых техник, схожих с уже известными поведениями, и потому регулярно обновляются.

Заключение

В процессе работы было разработано программное обеспечение для создания модели угроз безопасности информации информационных систем. Данный продукт позволяет существенно сократить временные расходы за счет автоматизации процессов и уменьшить количество ошибок, связанных с человеческим фактором, поскольку все данные уже внесены в программу, и нельзя пропустить или не указать важные характеристики.

Приложение может использовать любая организация, которая занимается построением или проведением экспертиз модели угроз безопасности информации информационных систем. Благодаря универсальности, ее используют как для проведения экспертизы, так и для разработки самой модели угроз. программа служит хорошим помощником и помогает существенно сократить время на выполнение поставленных задач.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и защите информации» URL: https://docs.cntd.ru/document/901990051 (дата обращения: 15.02.2022 г.).

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных». URL: https://docs.cntd.ru/document/901990046 (дата обращения: 15.02.2023 г.).

3. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 5.05.2023 г.).

4. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методический документ. Методика оценки угроз безопасности информации» URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2169-informatsionnoe-soobshchenie-fstek-rossii-ot-15-fevralya-2021-g-n-240-22-690 (дата обращения: 5.05.2023 г.).

5. Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» URL: https://docs.cntd.ru/document/420285955 (дата обращения: 15.02.2023 г.).

6. Методика определения угроз безопасности информации: методич. материал - Москва, ФСТЭК, 2021. - 83 с. URL: https://docs.cntd.ru/document/607749876 (дата обращения: 13.06.2023 г.).

7. Методический документ. Утвержден ФСТЭК России от 11 февраля 2014 года «Меры защиты информации в государственных информационных системах» URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 15.02.2023 г.).

8. Интернет-ресурс «Банк данных угроз безопасности информации». URL: https://bdu.fstec.ru (дата обращения: 3.05.2022 г.).

9. Интернет-ресурс Матрица MITRE ATT&CK, адрес URL: https://attack.mitre.org (дата обращения: 3.02.2023 г.);

10. Хабр. О моделировании угроз. URL: https://habr.com/ru/company /cloud4y/blog/350228/ (дата обращения: 10.06.2022 г.).

11. Степанов В.А. Моделирование угроз безопасности информации по новой методике ФСТЭК, используя средства автоматизации Информационные технологии. Проблемы и решения. 2021. № 4 (17). С. 95-101.

12. Дорошенко И.Е. Вопросы описания возможных сценариев угроз при разработке моделей угроз безопасности информации. /Дорошенко И.Е., Максудов М.О., Селифанов В.В.// Интерэкспо Гео-Сибирь. 2021. Т. 7. № 1. С. 16-21.

13. Стариковская Н.А. Разработка модели угроз для государственной информационной системы. / Стариковская Н.А., Слепухина Ю.В.// Материалы Афанасьевских чтений. 2022. № 2 (39). С. 36-41.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-197-202

Д. С. Пельц[1], А. В. Шабурова[1]*

Построение защищенного канала связи для системы видеоконференцсвязи в органах местного самоуправления

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: diana4ka-00@mail.ru

Аннотация. Предмет исследования**.** Проблема построения защищенных каналов связи для передачи конфиденциальной информации в информационных системах видеоконференцсвязи играет важную роль в организации защиты информации в органах местного самоуправления. Потребность в использовании систем видеоконференцсвязи в муниципалитетах с течением времени становится все более необходимой. Особенно важно в информационных системах такого типа при шифровании канала связи сохранить качество изображение, скорость звука и другие технические характеристики. В данной статье проведено исследование влияния средств криптографической защиты на пропускную способность канала передачи данных. Цели исследования. Определение влияния шифрования канала связи сертифицированными средствами криптографической защиты на его пропускную способность с последующим внедрением защищенной системы видеоконференцсвязи в органы местного самоуправления при использовании собственных технических средств. Методология**.** В процессе исследования проблемы шифрования каналов для систем видеоконференцсвязи использовались сравнительный методы и метод тестирования. Результаты. В ходе исследования был проведен сравнительный анализ открытого канала передачи данных системы видеоконференцсвязи и защищенного сертифицированными средствами криптографической защиты информации. В процессе эксперимента по выбранным техническим критериям были сняты показатели передачи информации по открытому и закрытому каналам связи. По результатам было выявлено минимальное расхождение значений открытого и закрытого каналов системы видеоконференцсвязи. Выводы. Сделан вывод о том, что шифрование каналов связи информационной системы ВКС сертифицированными средствами криптографической защиты информации не сказывается на технических характеристиках каналов передачи данных, но позволяет предотвратить утечку конфиденциальной информации в органах местного самоуправления.

Ключевые слова: защищенный канал связи, система видеоконференцсвязи, средства криптографической защиты информации

D. S. Pelts[1], A. V. Shaburova[1]*

Definition of the Characteristics of the Unmanned Aviation System when Carrying out Search and Rescue Operations in Wetted Areas

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: diana4ka-00@mail.ru

Abstract. Subject researches. The problem of building secure communication channels for transmitting confidential information in videoconferencing information systems plays an important role in organizing information protection in local governments. The need for the use of video conferencing systems in municipalities is becoming more and more necessary over time. It is especially important

in information systems of this type to preserve image quality, sound speed and other technical characteristics when encrypting a communication channel. This article will study the effect of cryptographic protection on the throughput of a data transmission channel. Goals researches. Determination of the impact of the encryption of the communication channel by certified cryptographic protection means on its bandwidth, followed by the introduction of a secure VCS system to local governments using their own technical means. Methodology**.** In the process of studying the problem of channel encryption for videoconferencing systems, measuring, comparative methods and a testing method were used. Results**.** In the course of the study, a comparative analysis of the open data transmission channel of the videoconferencing system and the protected by certified cryptographic information protection was carried out. In the course of the experiment, according to the selected technical criteria, indicators of information transmission over an open and closed communication channel were taken. According to the results, the minimum discrepancy between the values of the open and closed channel of the videoconferencing system was revealed. Conclusions**.** It is concluded that the encryption of communication channels of the videoconferencing information system with certified means of cryptographic information protection does not significantly affect the technical characteristics of data transmission channels, but it helps to prevent the leakage of confidential information in local governments.

Keywords: secure communication channel, videoconferencing system, means of cryptographic information protection

Введение

В современное время значительно возросла актуальность систем видеоконференцсвязи в рабочем процессе органов местного самоуправления. Видеоконференцсвязь (ВКС) – это сеанс связи между двумя пользователями или группой пользователей, независимо от их месторасположения, при этом, участники видят и слышат друг друга согласно правилам, определяемым видом видеоконференции.

В качестве среды передачи данных может использоваться как сеть органов местного самоуправления, так и глобальная сеть интернет. Поэтому при проведении видеоконференции в муниципалитетах важную роль играют вопросы информационной безопасности, особенно при реализации связи с удаленными филиалами при помощи сети интернет. В связи с этим остро встал вопрос обработки в информационных системах ВКС не только общедоступной информации, но и информации ограниченного доступа [1, 12]. В данных условиях передача данных по открытым сетям недопустима, ведь даже минимальная утечка сведений может привести к утере информации ограниченного доступа, что накладывает определенные требования для обеспечения защищенности информации с точки зрения законодательства Российской Федерации [7 – 9, 11, 13].

Защиту информации в информационных системах ВКС можно разделить на следующие аспекты: защита аудиовизуальной информации из помещений; защита конечных точек и серверов от несанкционированного доступа; защита информации по каналам передачи связи между пользователями и серверами. Если первые два аспекта не вызывают вопросов и ничем не отличаются от защиты информации в иных информационных системах, то третий аспект требует дополнительного внимания. Это обусловлено тем, что системы ВКС не накапливают информацию, а ведут обработку информации в режиме реального времени, что

в свою очередь, накладывает определенные требования к скорости сетевого взаимодействия и качеству передаваемой информации.

Наиболее универсальным способом защиты информации по линиям связи смешанного типа, включающим в себя отрезки как внутри контролируемой зоны, так и вне ее, является шифрованием трафика между конечными оппонентами и (или) серверами. Так как рассматриваемая информационная система содержит конфиденциальную информацию, то средства криптографической защиты информации должны быть сертифицированы органами ФСБ (Приказ ФСБ России от 10.07.2014 N 378) [10].

Поэтому цель настоящей работы заключается в установлении влияния шифрования канала связи сертифицированными средствами криптографической защиты на его пропускную способность с последующим внедрением защищенной системы ВКС в органы местного самоуправления при использовании собственных технических средств.

Методы и материалы

Для реализации поставленной цели по защите, имеющейся ВКС применялось аппаратное шифрование каналов с использованием маршрутизаторов «Cisco ASA» (IPsec) и аппаратно-программный комплекс шифрования (АПКШ) защиты информации «ViPNetCoordinatorHW-1000» (рис. 1).

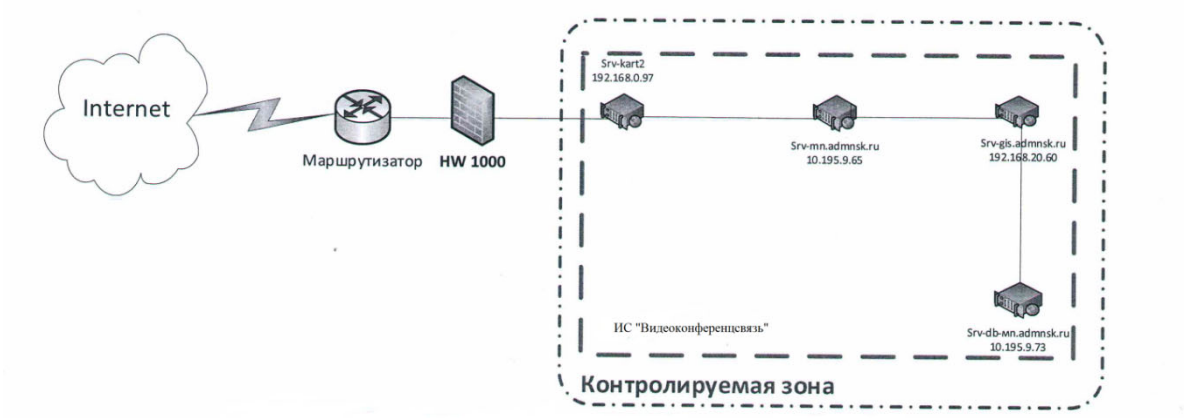


Рис. 1. Структурная схема ИС «Видеоконференцсвязь»

Эксперимент проводили с участием 20 пользователей системы ВКС, находящихся в равных условиях, таких как наличие одинаковых камер, типа подключения к системе, ширины канала, динамичности изображения т.д. Результаты были получены в течение 4 сеансов ВКС. В качестве критериев для сравнительного анализа каналов были приняты количество ошибок на порту, количество потерянных пакетов и скорость отправки и приема.

Результаты

В ходе построения и модернизации защищенного канала системы ВКС был проведен сравнительный анализ открытого и защищенного сертифицирован-

ными средствами криптографической защиты информации (СКЗИ) каналов передачи данных системы ВКС. Результаты, полученные экспериментальным методом, представлены в табл. 1 и 2.

Таблица 1

Анализ открытого канала передачи данных системы ВКС

Название критерия	Отправка				Прием			
	1	2	3	4	1	2	3	4
Скорость передачи данных, (кбит/сек)	403,1	982,4	4096	1024	1024	1024	4096	1024
Количество потерянных пакетов, %	0	0	0	0	0	0	0	0
Количество ошибок на порту	0	0	0	0	0	0	0	0

Таблица 2

Анализ защищенного канала передачи данных системы ВКС

Название критерия	Отправка				Прием			
	1	2	3	4	1	2	3	4
Скорость передачи данных, (Мбит/сек)	400,3	949,4	1024	985,8	1024	1024	1024	1024
Количество потерянных пакетов, %	0	1	0	0	0	0	0	0
Количество ошибок на порту	0	0	0	0	0	0	0	0

Сопоставив значения, представленные в табл. 1 и 2, можно сделать вывод о том, что канал передачи данных, зашифрованный сертифицированными СКЗИ, обладает меньшей пропускной способность на (1-3) %, чем открытый канал передачи данных. Это свидетельствует о том, что защищенный канал передачи данных не уступает по своим техническим характеристикам открытому каналу передачи данных, а также предотвращает возможную утечку конфиденциальной информации и защищает от несанкционированного доступа.

Обсуждение

С помощью внедрения системы ВКС в криптографическую сеть под управлением аппаратно-программного комплекса шифрования «ViPNetCoordinator HW-1000» появилась возможность объединить через интернет территориально распределенные локальные сети филиалов в единую сеть VPN. Данное решение определено рядом преимуществ аппаратно-программного комплекса шифрования «ViPNetCoordinatorHW-1000». В их число входят неограниченное количество узлов аудио и видеосвязи, возможность группирования как стационарных систем аудио- и видеосвязи, так и удаленных рабочих мест, оснащенных программными компонентами системы аудио- и видеосвязи; полноценная поддержка технологии виртуальных адресов в мультимедийных протоколах типа SIP, SCCP (CiscoSkinnyClientProtocol), H.323, обеспечение беспрепятственного прохождения защищенного трафика или в случаях противодействия интернет-провайдера.

Существенным фактором является наличие всех необходимых сертификатов ФСБ и ФСТЭК России [4, 5, 6]. Реализованные в СКЗИ обнаружение и предотвращение утечки информации, а также блокировка трафика сетевых приложений значительно повышают действенность фильтрации. Следует отметить, что созданные администратором правила разграничения трафика на основе команд протоколов HTTP(S) и FTP гарантируют эффективность контроля доступа пользователей в сеть интернет. А интегрированный детектор атак при обнаружении угрозы даст межсетевому экрану на криптошлюзе команду на создание временного правила для фильтрации трафика источника атаки, позволяющего активно и оперативно отражать нежелательный трафик, направленный на сеть органов местного самоуправления.

Заключение

Таким образом, в рамках проведенного исследования можно сделать вывод о том, что применение сертифицированного СКЗИ в системе ВКС не ведет к потере качества проведения видеоконференций в органах местного самоуправления, но позволяет объединить муниципалитеты в сегмент закрытой локально-вычислительной сети, включающий в себя разграничение пользователей на группы с правами доступа, которые соответствуют уровню доступа к сведениям, содержащим конфиденциальную информацию, а также успешно интегрировать систему закрытой ВКС в муниципалитеты [2, 3, 14].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Банк данных угроз безопасности информации // ФСТЭК России: официальный сайт – URL: https://bdu.fstec.ru/threat (дата обращения: 20.02.2023).

2. Болик, В. Н. О правомерности законодательных ограничений конституционного права на неприкосновенность частной жизни / В. Н. Болик // Законы России: опыт, анализ, практика. – 2015. – № 7. – С. 78-84.

3. Буркова, А. Ю. Локализация баз данных на территории Российской Федерации / А. Ю. Буркова. - 1. - Москва: Законодательство и экономика, 2015. – С. 54-57.

4. Выписка из перечня средств защиты информации, сертифицированных ФСБ России // Центр по лицензированию, сертификации и защите государственной тайны ФСБ России : официальный сайт: clsz.fsb.ru/clsz/certification.htm- (дата обращения: 20.02.2023).

5. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина – Москва: Форум, 2017. – 159 с.

6. Меры по обеспечению защиты персональных данных в организации // СерчИнформ: официальный сайт – URL: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/mery-po-obespecheniyu-zashchity-personalnyh-dannyh-v-organizacii/ (дата обращения: 28.02.2023).

7. Постановление правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» // Справочная правовая система КонсультантПлюс. - Режим доступа: по подписке (дата обращения: 06.03.2023).

8. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 10.03.2023).

9. Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 14.03.2023).

10. Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 14.03.2023).

11. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 16.04.2022).

12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 29.03.2023).

13. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения: 29.03.2023).

14. Яковец, Е. Н. Своеобразие состава защищаемой конфиденциальной информации/ Е.Н. Яковец // Право и кибербезопасность. – 2014. – № 2. – С. 51-58.

УДК 004.492
DOI 10.33764/2618-981X-2023-6-203-208

Д. Е. Пешков[1], А. В. Шабурова[1]*

Исследование программного обеспечения pon-роутера на предмет уязвимостей и программных закладок

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
*e-mail: peshkowdima@yandex.ru

Аннотация. Одной из важных задач в обеспечении информационной безопасности корпоративной и домашней сети является обеспечение безопасности и целостности данных в сети. Развитие сетевой инфраструктуры неизбежно связано с возникновением рисков информационной безопасности, связанных с сетевым оборудованием. Одной из сложнейших задач администрирования крупных корпоративных сетей является отслеживание и контроль версий сетевого оборудования для установки актуальных обновлений, если они имеются. Кибергруппировки все активнее используют атаки на цепочки поставки. Подделывая данные программного обеспечения или внедряя в него программные закладки, злоумышленники доводят до конечного пользователя уязвимое устройств. Пользователь же ничего не подозревает, получая устройства или обновления из легитимных источников. Поэтому необходимо выполнять сканирование программного обеспечения роутеров на предмет программных закладок.

Ключевые слова: целостность данных, программное обеспечение, атаки на цепочки поставки, программные закладки

D. E. Peshkov[1], A. V. Shaburova[1]*

Investigation of the Software of the Pon-Router for Vulnerabilities and Software Backdoors

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: peshkowdima@yandex.ru

Abstract. One of the important tasks in ensuring the information security of corporate and home networks is to ensure the security and integrity of data in the network. The development of network infrastructure is inevitably associated with the emergence of information security risks associated with network equipment. One of the most difficult tasks of the administration of large corporate networks is tracking and version control of network equipment to install up-to-date updates, if any. Cyber groups are increasingly using attacks on supply chains. By faking software data or introducing software bookmarks into it, attackers bring vulnerable devices to the end user. The user does not suspect anything, receiving devices or updates from legitimate sources.

Key words: data integrity, software, supply chain attacks, software backdoor

Введение

Распространение сетевых устройств в домашних и корпоративных сетях повлекло за собой повышения интереса злоумышленников к данному виду устройств и атак на них [1, 2]. И если пользователи зачастую выбирают устройство по красивой коробке, не проверяя присутствуют ли в нем какого-либо рода

уязвимости, то бизнес может просто не уследить за всем имевшимся оборудование в виду расширения мощностей. Вендоры же данного оборудования зачастую не стравляться с новыми вызовами, которые ставят перед ними злоумышленники. Устройства на момент выхода уже имеют встроенные уязвимости, которые злоумышленникам лишь нужно обнаружить. А если говорить не о новых устройствах, то данные уязвимости имеют и публичные рабочие эксплойты.

Данную проблему могло бы решить регулярное обновление программного обеспечения или микропрограммы устройств, но зачастую в жизненном цикле таких устройств такие события случаться лишь изредка. Этим и пользуются злоумышленники.

К данным проблемам последние несколько лет добавляться и новые. В последние несколько лет злоумышленники выполняют атаки на цепочку поставок [3]. Данный вид атаки нацелен на разработчиков программного обеспечения и поставщиков. Их основная цель – это получить доступ к исходным кодам, процессам сборки или механизмам обновления путем заражения допустимых приложений для распространения вредоносных программ [4]. Тем самым устройство поступает владельцу от легитимного источника, но с измененным исходным кодом.

В рамках статьи будет исследовано стандартное программное обеспечение роутера с внедренной программной закладкой [5].

Целью статьи является выявление возможных уязвимостей в программном обеспечении, и попытка обнаружить программную закладку в стандартном сетевом оборудовании [6].

Методика исследования

Для достижения поставленной цели необходимо произвести анализ программного обеспечения роутера и выявить все возможные уязвимости, в том числе программные закладки. Для данной задачи будет использован «The Firmware Analysis and Comparison Tool». Данный инструмент с открытым исходным кодом предназначен для автоматизации большей части процесса анализа встроенного программного обеспечения. Он распаковывает внутренние файлы программного обеспечения и выполняет анализ файлов.

После установки всех зависимостей, которые имеются у данного инструмента, и запуска «The Firmware Analysis and Comparison Tool» представляет собой веб-приложение с возможностью загрузки программного обеспечения. Помимо загрузки также иметься список всех выполненных загрузок и продвинутый поиск по загруженным файлам.

В качестве уязвимого программного обеспечения был выбран роутер D-Link DIR-620. Версия программного обеспечения DIR-620-1.3.0.bin была изменена для внедрения в нее программной закладки [7].

В качестве программной закладки был сгенерирован исполняемый файл линукс, который инициализирует подключение к удаленному ip-адресу. Программное обеспечение роутера было декомпилировано для внедрения в него программной закладки, после чего снова собрано.

Результаты

Основным способом выявления уязвимостей программного обеспечения является статический анализ. В данном способе все файлы программного обеспечения анализируются по очереди, и на основе найденной информации делается вывод о наличии той или иной уязвимости. Имея сигнатуры уязвимого кода, можно с достаточно большой точностью выявлять уязвимости в коде программного обеспечения.

Для данной работы по выявлению уязвимостей и программных закладок будет выбрана прошивка роутера D-LINK DIR-620 [8]. В данной прошивке присутствуют множественные уязвимости. Данная прошивка свободно распространяется и ее можно получить с сайта производителя.

Для внедрения программной закладки необходимо извлечь исходный код программного обеспечения и внедрить в него код программной закладки (рис. 1).

```
ubuntu@ubuntu:~/Diplom/firmware-mod-kit$ ./extract-firmware.sh ../DIR_620_1.3.0.bin
Firmware Mod Kit (extract) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake

Scanning firmware...

Scan Time:     2023-05-04 11:32:11
Target File:   /home/ubuntu/Diplom/DIR_620_1.3.0.bin
MD5 Checksum:  43fd5794b1aa97968a42bdccfb050be1
Signatures:    344

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0x47252455, created: 2011-12-07 13:33:45, image size: 90
oint: 0x8027F000, data CRC: 0x79AC8763, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "DIR_620"
64            0x40            LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2727584 bytes
983040        0xF0000         Squashfs filesystem, little endian, non-standard signature, version 3.1, size: 3564733 bytes, 883 inodes,
3:33:41

Extracting 983040 bytes of uimage header image at offset 0
Extracting squashfs file system at offset 983040
4587520
4587520
0
Extracting squashfs files...
Firmware extraction successful!
Firmware parts can be found in '/home/ubuntu/Diplom/firmware-mod-kit/fmk/*'
```

Рис. 1. Извлечение исходного кода программного обеспечения

Также для генерации программной закладки необходимо знать тип архитектуры программного обеспечения (рис. 2).

```
ubuntu@ubuntu:~/Diplom/firmware-mod-kit/fmk/rootfs$ file bin/busybox
bin/busybox: setuid ELF 32-bit LSB executable, MIPS, MIPS32 rel2 version 1 (SYSV), statically linked, stripped
```

Рис. 2. Тип архитектуры устройства

Из этого становиться известно, что программная закладка должна работать с архитектурой MIPS. Для генерации программной закладки был использован msfvenom (рис. 3). С помощью msfvenom был создан исполняемый файла backdoor в каталоге роутера rootfs/usr/bin/.

После перемещения данного эксплойта в код прошивки и установки автозапуска прошивка может быть обратно скомпилирована (рис. 4).

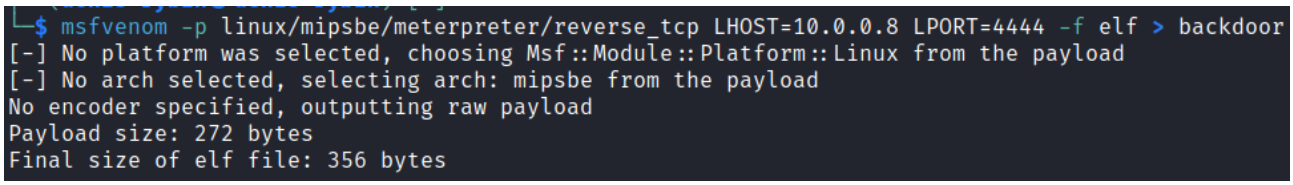


Рис. 3. Генерация программной закладки

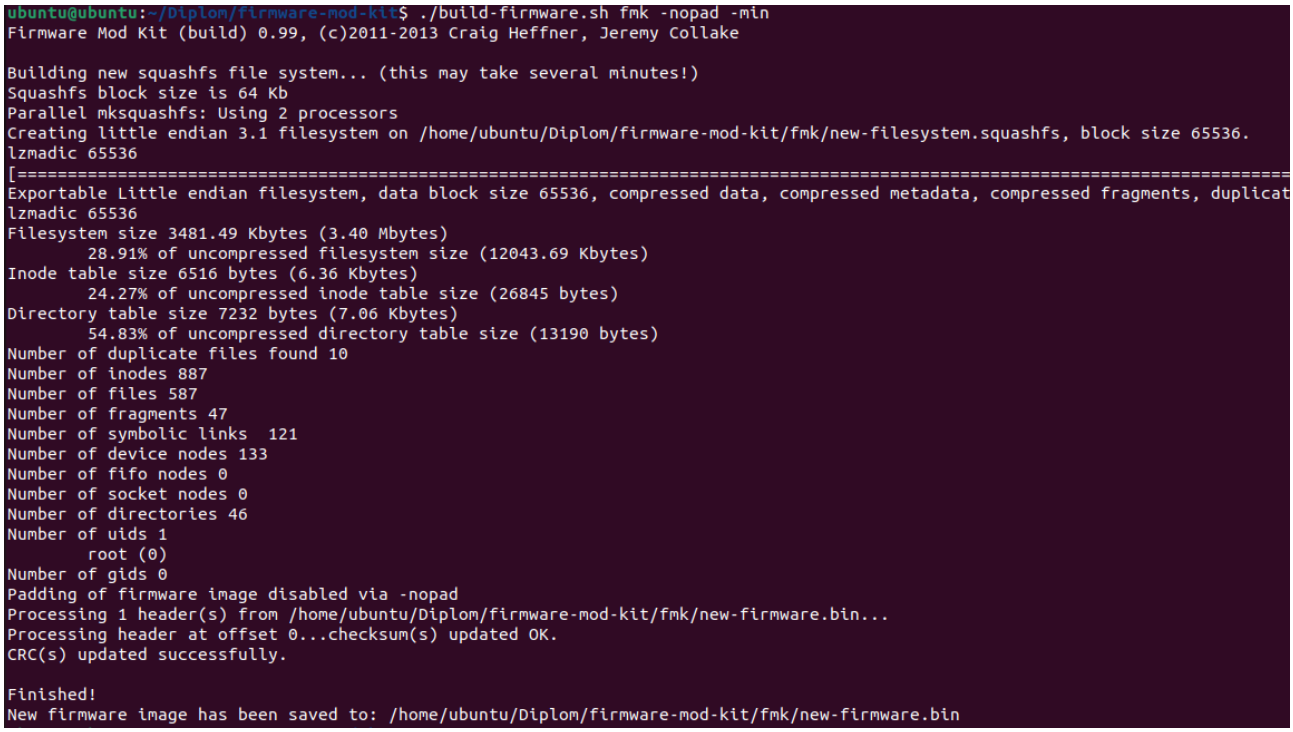


Рис. 4. Сборка прошивки с установленной программной закладкой

Этими действиями будет эмулирована прошивка с программными закладными устройствами, которая может присутствовать в каком-либо маршрутизаторе в сети дома или организации.

После подготовки уязвимого программного обеспечения можно переходить к этапу сканирования. Полученная прошивка была загружена и просканирована инструментом «The Firmware Analysis and Comparison Tool». В результате работы является отчет по разным модулям работы инструмента (рис. 5).

Однако несмотря на то, что найденные уязвимости являются критическими, программная закладка не была обнаружена инструментом. Таким образом данный инструмент должен быть существенно модернизирован и дополнен модулем поиска программных закладок.

BusyBox 1.19.2 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /bin/busybox Size: 472.65 KiB , Type: application/x-executable
Dnsmasq 2.55 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /usr/sbin/dnsmasq Size: 183.15 KiB , Type: application/x-executable
GNU Zebra 0.95a	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /usr/sbin/ripd Size: 392.68 KiB , Type: application/x-executable
Linux Kernel 2.6.21 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /uboot.lzma | //uboot.lzma~ Size: 2.60 MiB , Type: application/octet-stream
Point-to-Point Protocol daemon (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /sbin/pppd Size: 615.08 KiB , Type: application/x-executable
portable SDK for UPnP 1.3.1 (CRITICAL)	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /lib/libupnp.so Size: 245.93 KiB , Type: application/x-sharedlib
Pure-FTPd 1.0.34	router router - dir 620 test 2 backdoor (router) | /903533_unknown.bin | /13693.squashfs | /usr/sbin/pure-ftpd Size: 99.40 KiB , Type: application/x-executable

Рис. 5. Обнаруженные уязвимости

Заключение

Таким образом можно сделать вывод, что с поиском известных уязвимостей программные продукты справляться достаточно хорошо, однако для более сложных атак они еще не готовы.

Данную проблему можно решить ручным или поведенческим анализом прошивки, но тогда пострадает скорость и автоматизация процесса [9]. Также данные два способа занимают достаточно много времени и специалиста.

В данный момент ведется разработка инструмента по автоматизированному сканированию программного обеспечения роутера, который позволит в автоматическом режиме обнаруживать программные закладки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Яскевич В.И. Секьюрити. Организационные основы безопасности фирмы: учеб. пособие / В.И. Яскевич. М.: Ось-89, 2012. – 230 с.

2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М.: Книжный мир, 2012. – 352 с.

3. Милославская Н.Г. Визуализация процессов управления информационной // Научная визуализация. – 2017. – Том 9, № 5. – С. 117–136.

4. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения = Information protection. Information security monitoring. General provi-

sions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 июля 2021 г. N 656-ст : введен впервые : дата введения 2022-04-01 / подготовлен Федеральной службой по техническому и экспортному контролю (ФСТЭК России), обществом с ограниченной ответственностью "Центр безопасности информации" (ООО "ЦБИ"). Москва : Стандартинформ, 2021 – 10 с.

5. Федоров С.Е. Компьютерное моделирование и исследование систем автоматического управления: учебно-методическое пособие / Федоров С.Е. – Москва : Русайнс, 2020. – 92 с.

6. Мельников В.П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 2-е изд., стер. – М. : Academia, 2014. – 330 с.

7. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: учеб. пособие. – Волгоград: Изд-во ВолГУ, 2002. – 122 с.

8. Жарова А.К. Правовая классификация угроз и рисков в информационной сфере / А.К. Жарова // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2016. – № 7-8 (97-98). – С. 130-138.

9. Астахова Л.В. Кадровые проблемы построения системы управления информационной безопасностью на предприятии / Л.В. Астахова, Л.О. Овчинникова // Вестник УрФО. Безопасность в информационной сфере. – 2016. – № 3 (21). – С. 38-46.

УДК 004.91
DOI 10.33764/2618-981X-2023-6-209-215

О. А. Поликанина[1], А. Н. Поликанин[1] А. В. Шабурова[1]*

Методический подход для организации разграничений доступа к сведениям в информационной системе персональных данных

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Polikanina-OA2021@sgugit.ru

Аннотация. С 01 марта 2023 года вступили в силу изменения в Федеральный закон от 13.07.2015 №218-ФЗ «О государственной регистрации недвижимости» в части защиты персональных данных. Вопросы доступности, целостности и конфиденциальности персональных данных, обрабатываемых в информационной системе, становятся все более актуальными. В настоящее время общедоступные сведения и сведения ограниченного доступа, в том числе персональные данные, не разграничены между собой техническими и организационными средствами защиты. В статье авторы предлагают организовать защиту данных в зависимости от категории: «открытые», «ограниченного доступа», «закрытые». Деление на категории осуществляется в зависимости от степени тяжести ущерба, который может быть нанесен субъекту, в результате распространения сведений. Такой подход позволит избежать применения избыточных мер защиты «открытых» данных, вместе с тем организация защиты сведений ограниченного доступа потребует больших затрат, при этом количество пользователей, допущенных к обработке, будет значительно меньше.

Ключевые слова: персональные данные, информационная система персональных данных, сведения ограниченного доступа, разграничение прав доступа

O. A. Polikanina[1], A. N. Polikanin[1], A. V. Shaburova[1]*

Methodical Approach to Organize Access to Information in the Personal Data Information System

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: polikanina-olga@yandex.ru

Abstract. On March 1, 2023, amendments to the Federal Law of July 13, 2015 № 218-FZ “On State Registration of Real Estate” came into force regarding the protection of personal data. The issues of availability, integrity and confidentiality of personal data processed in the state information system are becoming more and more relevant. At present, public and restricted information, including personal data, is not separated from each other by technical and organizational means of protection. In the article, the authors propose to organize data protection depending on the category: “open”, “limited access”, “closed”. The division into categories is carried out depending on the severity of the damage that can be inflicted on the subject as a result of the dissemination of information. This approach will avoid the use of excessive measures to protect "open" data, however, the organization of the protection of restricted access information will be expensive, while the number of users allowed for processing will be much smaller.

Keywords: personal data, the personal data information system, restricted access information, access rights differentiation

Введение

С 01 марта 2023 года вступили в силу изменения в Федеральный закон от 13.07.2015 №218-ФЗ «О государственной регистрации недвижимости» (далее – Закон о недвижимости) в части защиты персональных данных (далее – ПДн).

Закон о недвижимости дополнен статьей 36.3 Правила внесения в государственный реестр недвижимости (далее – реестр недвижимости) записи о возможности предоставления ПДн правообладателя объекта недвижимости. ПДн владельца недвижимости (фамилия, имя, отчество, дата рождения) могут быть предоставлены третьим лицам только при наличии *согласия* правообладателя или лица, в пользу которого зарегистрированы ограничения права (обременения) объекта недвижимости.

Вместе с тем частью 6 статьи 36.3 Закон о недвижимости предусмотрено, что ПДн гражданина, независимо от наличия записи о возможности их предоставления, указываются в Выписке из реестра недвижимости по запросам нотариусов, правоохранительных органов, судебных приставов, арбитражных управляющих, судов, залогодержателей, иных лиц, указанных в законе [1].

В этой связи вопросы обеспечения доступности, целостности и конфиденциальности сведений, обрабатываемых в информационной системе персональных данных (далее – ИСПДн) Росреестра имеют большое практическое значение и становятся всё более актуальными [2].

В настоящее время все сведения реестра недвижимости защищаются одинаково, при этом при предоставлении сведений ограниченного доступа возникают ошибки информационной системы либо конкретного исполнителя, которые приводят к негативным последствиям, одним из которых является утечка ПДн в госсекторе [3,4,5].

Целью исследования является выработка методического подхода для организации разграничений доступа к сведениям в ИСПДн в зависимости от установленной категории данных. Для достижения поставленной цели в статье решены следующие задачи:

– проанализирован существующий порядок доступа к сведениям в ИСПДн;

– выполнена классификация данных, обрабатываемых в ИСПДн;

– выработан авторский подход к разграничению прав доступа к сведениям в ИСПДн в зависимости от категории обрабатываемых данных и должности исполнителя.

Методы и материалы

Законом о недвижимости установлено, что сведения реестра недвижимости предоставляются по запросам любых лиц и подлежат размещению на официальном сайте ведомства [6], за исключением сведений, доступ к которым ограничен федеральным законом, к таким сведениям относятся ПДн правообладателя объекта недвижимости.

В случае принятия решения о наложении запрета на выдачу сведений о защищаемых лицах и их близких, объектах государственной охраны и членах их семей сведения о таких лицах не предоставляются, за исключением случаев, предусмотренных федеральными законами либо указом Президента РФ [1].

Таким образом, законодательно сведения реестра недвижимости разделены на три группы: общедоступные, имеющие ограниченный доступ и запрещенные для выдачи.

В настоящее время порядок доступа к сведениям в ИСПДн не разграничен, пользователи с ролью Предоставление сведений имеют равный доступ ко всем данным. Авторизация пользователей при входе в ИСПДн осуществляется по паре логин/пароль или с использованием электронной подписи (далее – ЭП), что не гарантирует 100% достоверную идентификацию должностного лица. Иными словами, зная логин и пароль либо имея доступ к ЭП, любой сотрудник может войти в систему и получить доступ к информации, включая ПДн правообладателей объектов недвижимости.

Кроме того, пользователи с ролью Предоставление сведений технически могут формировать для выдачи любые сведения, как общедоступные, так и конфиденциальные, при этом сведения автоматически удостоверяются ЭП организации, а не конкретного должностного лица.

Обработка данных осуществляется в одинаковых условиях (помещениях) с использованием компьютеров, оснащенных одними и теми же техническими средствами защиты. Особая организация рабочих мест специалистов, обрабатывающих конфиденциальную информацию и запрещенные для выдачи сведения, отсутствует.

Существующий порядок доступа пользователей к сведениям в ИСПДн Росреестра представлен в табл. 1.

Таблица 1

Порядок доступа пользователей к сведениям в ИСПДн

Организация доступа пользователя	Общедоступные сведения	Сведения, ограниченного доступа	Сведения, на которые наложен запрет
Создание учетной записи (регистрация пользователя в системе)	+	+	+
Настройка ролей	+	+	+
Вход в систему Логин/пароль	+	+	+
Вход в систему ЭП на съемном носителей	+	+	+
Биометрическая идентификация			
Выделенное защищенное помещение			
Аттестованное АРМ пользователя			
Поиск запрашиваемой информации в БД только открытые данные	+	+	+
Поиск запрашиваемой информации в БД, включая сведения ограниченного доступа	+	+	+
Поиск запрашиваемой информации в БД, включая закрытые данные	+	+	+
Идентификация субъекта на получение запрашиваемых сведений		+	+
Предоставление сведений удостоверенных обезличенной ЭП организации	+	+	+

Организация доступа пользователя	Общедоступные сведения	Сведения, ограниченного доступа	Сведения, на которые наложен запрет
Предоставление сведений удостоверенных ЭП исполнителя			
Передача данных по защищенному каналу (криптографическому)	+	+	+

Таким образом, существующий порядок доступа в ИСПДн обеспечивает сотрудникам с ролью Предоставление сведений одинаковые права на просмотр, обработку и выдачу любых сведений реестра недвижимости, включая ПДн правообладателей объектов недвижимости.

Результаты

В связи с вступлением в силу Федерального закона от 14.07.2022 №266-ФЗ о внесении изменений в Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» [7] ПДн правообладателя объекта недвижимости исключены из общедоступных сведений, предоставляемых ранее по запросам любых лиц, следовательно, меры по защите ПДн должны быть усилены.

В предыдущих публикациях авторами было предложено разделить сведения реестра недвижимости на три категории: «открытые», «ограниченного доступа» и «закрытые» в зависимости от степени тяжести ущерба, который может быть нанесен субъекту в результате утечки данных [8].

Для дальнейшей организации защиты данных в зависимости от категории в первую очередь необходимо определить круг лиц, имеющих доступ к разным категориям сведений, в соответствии с занимаемой должностью. К «закрытым» сведениям разрешить доступ лиц не ниже начальника структурного подразделения. К сведениям «ограниченного доступа» могут быть допущены заместитель начальника и ведущие специалисты отдела. «Открытые» сведения доступны всем сотрудникам.

Авторский подход к разграничению прав доступа в зависимости от категории сведений и занимаемой должности представлен в табл. 2.

Таблица 2

Группы разграничения доступа

Должность	Шт. ед.	Открытые	Ограниченного доступа	Закрытые
Директор	1	+	+	+
Заместитель директора	1	+	+	+
Начальник отдела	1	+	+	+
Зам. начальника отдела	1	+	+	
Ведущий инженер	5	+	+	
Инженер 1 категории	4	+		
Инженер 2 категории	4	+		

Таким образом, чем выше уровень закрытости сведений, тем меньше сотрудников в организации должны быть допущены к их обработке, при этом персональная ответственность и занимаемая должность должны быть выше у лиц, осуществляющих обработку конфиденциальной информации, в том числе ПДн правообладателей объектов недвижимости.

Опираясь на авторский подход для организации разграничений доступа к сведениям, исходя из занимаемой должности, немало важным фактором является предложенное деление сведений на 3 категории: «открытые», «ограниченного доступа» и «закрытые».

Используя метод системного исследования функций объекта с целью поиска баланса между затратами и эффективностью [9], предлагаем доступ пользователей в ИСПДн разграничить по категориям сведений, предусмотрев дополнительные меры защиты при работе с конфиденциальными данными.

В целях достоверного распознавания должностного лица, имеющего права на работу со сведениями «ограниченного доступа» и/или «закрытыми», для входа в ИСПДн дополнительно применять биометрическую идентификацию и аутентификацию пользователя. Автоматизированное рабочее место пользователя необходимо обеспечить средствами защиты конфиденциальной информации от несанкционированного доступа. Проход в помещение, в котором ведется обработка ПДн, предоставить исключительно лицам, допущенным к работе со сведениями ограниченного доступа.

Поскольку Законом о недвижимости установлен круг лиц, которым могут быть предоставлены сведения «ограниченного доступа», исполнитель должен лично проверять полномочия заявителя, нести персональную ответственность за выдачу сведений надлежащему лицу, заверяя их своей ЭП.

Обработка «закрытых» данных должна осуществляться в специально оборудованном помещении на аттестованном компьютере, оснащенном средствами криптографической защиты. Доступ к «закрытым» данным должны иметь минимальное количество должностных лиц.

Предлагаемый подход к организации разграничений доступа к сведениям в ИСПДн Росреестра представлен в табл. 3.

Таблица 3

Организация разграничений доступа пользователей в ИСПДн в зависимости от категории данных

Организация доступа пользователя	Открытые	Ограниченного доступа	Закрытые
Создание учетной записи	+	+	+
Настройка ролей	+	+	+
Вход в систему Логин/пароль	+		
Вход в систему ЭП на съемном носителей		+	+
Биометрическая идентификация		+	+
Выделенное защищенное помещение			+
Аттестованное АРМ пользователя			+

Организация доступа пользователя	Откры-тые	Ограниченного до-ступа	Закры-тые
Поиск запрашиваемой информации в БД только открытые данные	+	+	+
Поиск запрашиваемой информации в БД, включая сведения ограниченного доступа		+	+
Поиск запрашиваемой информации в БД, включая закрытые данные			+
Идентификация субъекта на получение за-прашиваемых сведений		+	+
Предоставление сведений удостоверенных обезличенной ЭП организации	+		
Предоставление сведений удостоверенных ЭП исполнителя		+	+
Передача данных по защищенному каналу (криптографическому)		+	+

Предлагаемый подход к организации доступа в ИСПДн в зависимости от категории сведений позволит разграничить меры защиты информации и повысить эффективность защиты сведений ограниченного доступа, включая ПДн, обеспечив дополнительные организационно-технических мероприятий и персональную ответственность сотрудников за утечку данных, при этом количество пользователей, допущенных к обработке конфиденциальной информации, число автоматизированных рабочих мест и помещений, требующих применения дорогостоящих средств защиты, будет минимальным.

Заключение

Организация защиты данных реестра недвижимости в зависимости от установленной категории сведений: «открытые», «ограниченного доступа», «закрытые» имеет большое практическое значение и позволит:

1) избежать применения избыточных организационных мер и технических средств защиты «открытых» данных, доступ к которым имеет максимальное количество пользователей в организации, разрешенных для опубликования на официальном сайте ведомства, так как утечка таких сведений может нанести минимальный ущерб гражданину, юридическому лицу либо государству;

2) разрешить доступ к конфиденциальным данным должностным лицам, начиная от ведущего специалиста и выше, сократив количество пользователей, допущенных к обработке, поскольку организация защиты таких сведений потребует дополнительных мер, включая биометрическую идентификацию пользователей и больших затрат, а исполнители будут нести персональную ответственность за ненадлежащее предоставление и утечку сведений, включая ПДн правообладателей;

3) ограничить доступ к «закрытым» данным, разрешив их обработку минимальному числу лиц в организации, начиная от начальника структурного подразделения и выше, так как для организации защиты потребуется специально выделенное помещение с аттестованным АРМ пользователя, а в случае утечки «за-

крытых» данных должностные лица могут быть привлечены к ответственности вплоть до уголовной в зависимости от степени причиненного ущерба [10, 11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О государственной регистрации недвижимости [Электронный ресурс] : федер. закон от 13.07.2015 № 218-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс] : постановление Правительства Рос. Федерации от 01.11.2012 № 1119. Доступ из справ.-правовой системы «КонсультантПлюс».
3. Исследование уровня информационной безопасности в компаниях России за 2022 год [Электронный ресурс] // SearchInform: [сайт]. [2023]. URL: https://searchinform.ru/survey/global-2022/ (дата обращения 10.05.2023).
4. Исследование осведомленности и отношения государственных служащих к проблемам защиты персональных данных [Электронный ресурс] // SearchInform: [сайт]. [2022]. URL: https://searchinform.ru/survey/zaschita-persdannyh-v-gossektore-2021/ (дата обращения 10.05.2023).
5. Глобальное исследование уровня информационной безопасности в компаниях России и СНГ за 2021 год [Электронный ресурс] // SearchInform: [сайт]. [2021]. URL: https://searchinform.ru/survey/global-2021/ (дата обращения 10.05.2023).
6. Об установлении состава сведений, содержащихся в Едином государственном реестре недвижимости, подлежащих размещению на официальном сайте Федеральной службы государственной регистрации, кадастра и картографии в информационно-телекоммуникационной сети Интернет, и порядка их размещения [Электронный ресурс] : приказ Росреестра от 30.08.2021 № П/0375. Доступ из справ.-правовой системы «КонсультантПлюс».
7. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
8. Поликанина О.А., Поликанин А.Н., Шабурова А.В. Организация защиты персональных данных в государственных и муниципальных информационных системах // Интерэкспо Гео-Сибирь. 2022. Т.6. С. 197–203.
9. Никитина Е. Б. Функционально-стоимостный анализ [Электронный ресурс] : учеб. пособие // Пермский государственный национальный исследовательский университет: [сайт]. [2021]. URL: http://www.psu.ru/nauka/elektronnye-publikatsii/uchebnye-posobiya-i-metodicheskie-materialy/e-b-nikitina-funktsionalno-stoimostnyj-analiz (дата обращения 10.05.2023).
10. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Технические, организационные и кадровые аспекты управления информационной безопасностью: учеб. пособие для вузов. М. : Гор. линия–Телеком, 2013. 214 с.
11. Курило А. П., Милославская Н. Г., Сенаторов М. Ю. Основы управления информационной безопасностью : учеб. пособие для вузов. М. : Гор. линия–Телеком, 2013. 244 с.

УДК 528.942
DOI 10.33764/2618-981X-2023-6-216-223

А. А. Попов[1], П. Ю. Бугаков[1]*

Разработка прототипа геоинформационной системы для анализа инфраструктуры сервиса проката электросамокатов в городе Новосибирске

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: sashapopov9999@gmail.com

Аннотация. В последние годы электросамокаты стали очень популярными в крупных городах, так как они представляют собой удобное и экологически чистое средство передвижения. Сервисы проката электросамокатов также стали широко распространенными, и в различных городах открываются все больше и больше пунктов проката. Сервисы проката электросамокатов требуют определенной инфраструктуры, включая пункты проката, зоны парковки, зарядные станции и т.д. Оптимизация этой инфраструктуры может значительно повысить эффективность и удобство использования сервиса, а также улучшить безопасность и снизить нагрузку на окружающую среду. Специализированная ГИС с актуальной базой данных позволит обеспечить эффективный контроль состояния инфраструктуры с целью определения путей ее дальнейшего развития. В работе описана обобщенная концепция функционирования ГИС, описаны исходные данные ГИС, определен перечень задач, решаемых ГИС. Также представлен перечень функциональных возможностей ГИС для каждой отдельной группы пользователей и выполнена практическая реализация функциональных элементов геоинформационной системы.

Ключевые слова: геоинформационная система, инфраструктура, электросамокаты, QGIS, Open Street Map, интерактивная карта

A. A. Popov[1], P. Y. Bugakov[1]*

Development of a Prototype of Geoinformation System for Analyzing the Infrastructure of the Electric Scooter Rental Service in Novosibirsk

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: sashapopov9999@gmail.com

Abstract. In recent years, electric scooters have become very popular in large cities, as a convenient and environmentally friendly means of transportation. Electric scooter rental services also became widespread, and more and more rental points are opening in various cities. Electric scooter rental services require a certain infrastructure, including rental locations, parking areas, charging stations, etc. Optimization of this infrastructure can significantly increase the efficiency and usability of the service, as well as improve safety and reduce the burden on the environment. A specialized GIS with an up-to-date database will ensure effective monitoring of the state of the infrastructure in order to determine the ways of its further development. The paper describes a generalized concept of GIS functioning, describes the initial GIS data, defines a list of tasks solved by GIS. The list of GIS functionality for each individual user group is also presented and the practical implementation of the functional elements of the geoinformation system is carried out.

Keywords: geographic information system, infrastructure, electric scooters, QGIS, Open Street Map, interactive map

Введение

На данный момент электросамокаты набирают свою популярность среди населения, они разгружают общественный транспорт и снижают интенсивность использования личных автомобилей, что оказывает положительное влияние на загруженность дорог в городе и окружающую среду [1–3]. Вместе с тем использование электросамокатов приводит к ряду проблем, решение которых становится одной из приоритетных задач муниципальных служб. В данной работе рассматривается проблема, связанная с недостаточным уровнем развития инфраструктуры для электросамокатов на территории Новосибирска. Самокаты, размещенные на тротуарах, зачастую плохо припаркованы или просто оставлены на земле, занимают пространство, предназначенное для пешеходов. Из-за хаотично размещенных самокатов больше всего страдают люди с ограниченной подвижностью, которые не всегда могут их обойти [4, 5].

Геоинформационная система (ГИС) позволит на основе пространственного анализа данных оптимизировать размещение пунктов проката и зарядных станций, выявить популярные маршруты и зоны использования, а также оценить уровень безопасности на дорогах и тротуарах.

Проблемы инфраструктуры сервисов проката электросамокатов актуальны для многих городов. Разработка научно-методических основ создания ГИС для анализа этой инфраструктуры может привести к разработке более эффективных и удобных сервисов, которые будут способствовать развитию экологически чистых видов транспорта.

Цель данной работы – разработать прототип геоинформационной системы для анализа инфраструктуры сервиса проката электросамокатов на примере города Новосибирска. Исходя из цели работы, был составлен перечень задач, которые необходимо решить:

– описать обобщенную концепцию функционирования ГИС и определить исходные данные, необходимые для реализации системы;

– определить перечень задач, решаемых ГИС;

– определить перечень функциональных возможностей ГИС для всех групп пользователей;

– выполнить разработку прототипа геоинформационной системы.

Обобщенная концепция функционирования ГИС

Ранее в работах [6, 7] на основе результатов анализа предметной области была предложена схема структуры и выполнено описание обобщенной концепции геоинформационной системы для анализа инфраструктуры сервиса проката электросамокатов в городе Новосибирске. Предложенная схема структуры геоинформационной системы включает в себя 5 блоков, а именно:

Блок 1, отвечающий за отрисовку карты;

Блок 2, предназначенный для формирования пользовательского интерфейса;

Блок 3, отвечающий за сбор данных;

Блок 4, отвечающий за функции ГИС;

Блок 5, отвечающий за базу пространственных и атрибутивных данных.

Обобщенная концепция ГИС включает в себя описание трех этапов работ, которые необходимо выполнить для создания ГИС. Первый этап включает в себя работы по подготовке данных для ГИС. На этом этапе осуществляется сбор данных из открытых источников, которые в дальнейшем необходимо структурировать и подготовить к интеграции в систему. Второй этап отвечает за создание и настройку отображения карты с использованием данных, полученных на предыдущем этапе. На третьем этапе выполняется разработка функционала ГИС, а также отрисовка элементов пользовательского интерфейса для управления картой и выбора инструментария для решения задач пространственного анализа.

В качестве исходных данных для реализации ГИС необходимо использовать общие данные, а также специализированные семантические данные из предметной области, необходимые для решения поставленных перед ГИС задач.

Общие данные включают в себя:

– картографическую основу (векторные карты и космические снимки сверхвысокого разрешения);

– географические данные о районах и микрорайонах города;

– сведения о парковках;

– сведения о зонах и точках интереса в городе.

Картографическая основа взята из открытого источника OpenStreetMap, модуль которого встроен в программу QGIS. Данные по районам города, точках и зонах интереса, а также о парковках были взяты с сайта geofabrik.de, данный сервис предоставляет бесплатный доступ к векторным данным по разным территориям земного шара.

В качестве специализированных были использованы данные о перемещении самокатов по городу, предоставленные компанией WHOOSH [8]. На их основе были подготовлены тематические слои карты города Новосибирска, отображающие количество поездок на определенных участках города за месяц, а также дороги, требующие переоборудования для обеспечения безопасного передвижения электросамокатов.

Перечень задач, решаемых ГИС

Геоинформационная система для анализа инфраструктуры сервиса проката электросамокатов должна решать следующие задачи.

1. Сбор и хранение пространственных данных: система должна иметь возможность собирать, обрабатывать и хранить географические данные о территории, где функционирует сервис проката электросамокатов. Для этого могут использоваться специализированные ГИС-платформы, такие как ArcGIS, QGIS, GeoServer и другие.

2. Анализ инфраструктуры сервиса проката: система должна иметь возможность производить пространственный анализ инфраструктуры сервиса проката, включая расположение станций проката, количество электросамокатов на каждой станции, плотность расположения станций проката, количество поездок в

каждом отдельном районе, сравнение нескольких эпох данных. Для этого могут использоваться инструменты пространственного анализа, такие как расчет расстояний, плотности и прочие алгоритмы.

3. Прогнозирование спроса: система должна иметь возможность прогнозировать спрос на сервис проката электросамокатов в разных точках города. Для этого может использоваться моделирование с помощью методов машинного обучения или статистических методов.

4. Формирование рекомендаций: система должна иметь возможность формировать рекомендации по оптимизации инфраструктуры сервиса проката, такие как оптимизация расположения станций проката, оптимизация количества электросамокатов на каждой станции, определение дорог и площадок, требующих модернизацию. Для этого могут использоваться алгоритмы оптимизации и принятия решений.

Для решения этих задач могут быть использованы различные технологии и инструменты, включая базы данных географической информации, программное обеспечение для пространственного анализа, методы машинного обучения и оптимизации, а также визуализация результатов анализа с помощью интерактивных карт и диаграмм. Важно также обеспечить высокую точность и достоверность данных, используемых в системе, а также возможность оперативного обновления данных для актуального анализа инфраструктуры сервиса проката электросамокатов.

Схема функционирования ГИС для групп пользователей

Геоинформационная система для анализа инфраструктуры сервиса проката электросамокатов может использоваться разными группами пользователей в зависимости от их задач и целей [9]. С учетом этого был определен перечень функций, предоставляемых ГИС каждой группе пользователей.

Перечень функций ГИС для администрации ГИС, которая отвечает за анализ инфраструктуры сервиса проката электросамокатов, включает в себя сбор, обработку и управление данными, управление и обновление ГИС, обучение пользователей.

Для администрации города, заинтересованной в анализе инфраструктуры сервисов проката электросамокатов, перечень функций ГИС включает в себя сбор и обработку данных, визуализацию статистических данных и результатов пространственного анализа, обеспечивающего поддержку принятия решений, а также мониторинг и контроль текущего состояния сервисов проката электросамокатов.

Для администрации сервисов проката электросамокатов ГИС может рассматриваться как инструмент для мониторинга и управления операциями проката. Перечень функциональных возможностей может включать сбор, обработку и анализ данных; генерацию отчетов и рекомендаций по управлению и оптимизации проката.

Перечень функций ГИС для пользователя сервиса проката электросамокатов может включать в себя просмотр статистических данных и сведений о теку-

щем состоянии инфраструктуры города, отзывы и оценки. Пользователь может оставить отзыв и оценить качество сервиса, что поможет улучшить его работу в будущем.

Реализация прототипа геоинформационной системы

В качестве прототипа было рассмотрено несколько вариантов реализации системы:

Для создания первого варианта необходим сервис QGIS Cloud Free [10], который позволяет при помощи плагина, встроенного в основной клиент QGIS, загрузить карту на сервер. Главным минусом данного способа является отсутствие необходимого функционала, поскольку он доступен в платной подписке.

Во втором варианте карта может быть перенесена на сервер с помощью плагина QGIS2Web. Этот способ позволяет обойти платное ограничение функционала и самостоятельно реализовать необходимые функции. Из минусов такого решения, можно выделить увеличение времени на разработку, программирование необходимого функционала, а также его тестирование.

В качестве основного варианта, была выбрана ГИС-площадка QGIS с плагином QGIS2Web [11]. Исходные данные для реализации прототипа были взяты из следующих источников:

– с официального сайта приложения для проката электосамокатов [8];
– из открытых источников векторных геоданных [12];
– из статистических и литературных источников информации [13].

После сбора данные были структурированы и визуализированы средствами QGIS [14–16]. В результате были сформированы следующие слои (рис. 1):

– районы города;
– площадные зоны интереса в городе;
– точечные объекты интереса в городе;
– парковки;
– тематический слой, отображающий количество поездок электросамокатов за месяц.

После подготовки картографической основы в прототипе было необходимо реализовать тестовый функционал, позволяющий решать одну или несколько задач, поставленных перед ГИС. Для примера была создана функция, которая автоматически определяет среднее количество поездок по районам и высчитывает интенсивность движения самокатов по дорогам за месяц [14].

После выполнения данной функции создается новый слой, отображающий количество поездок самокатов за месяц (рис. 3).

Далее созданный слой сопоставляется со слоем зон и точек интереса. В результате работы алгоритма пространственного анализа формируется слой (рис. 4), показывающий текущую интенсивность движения самокатов и количество точек интереса.

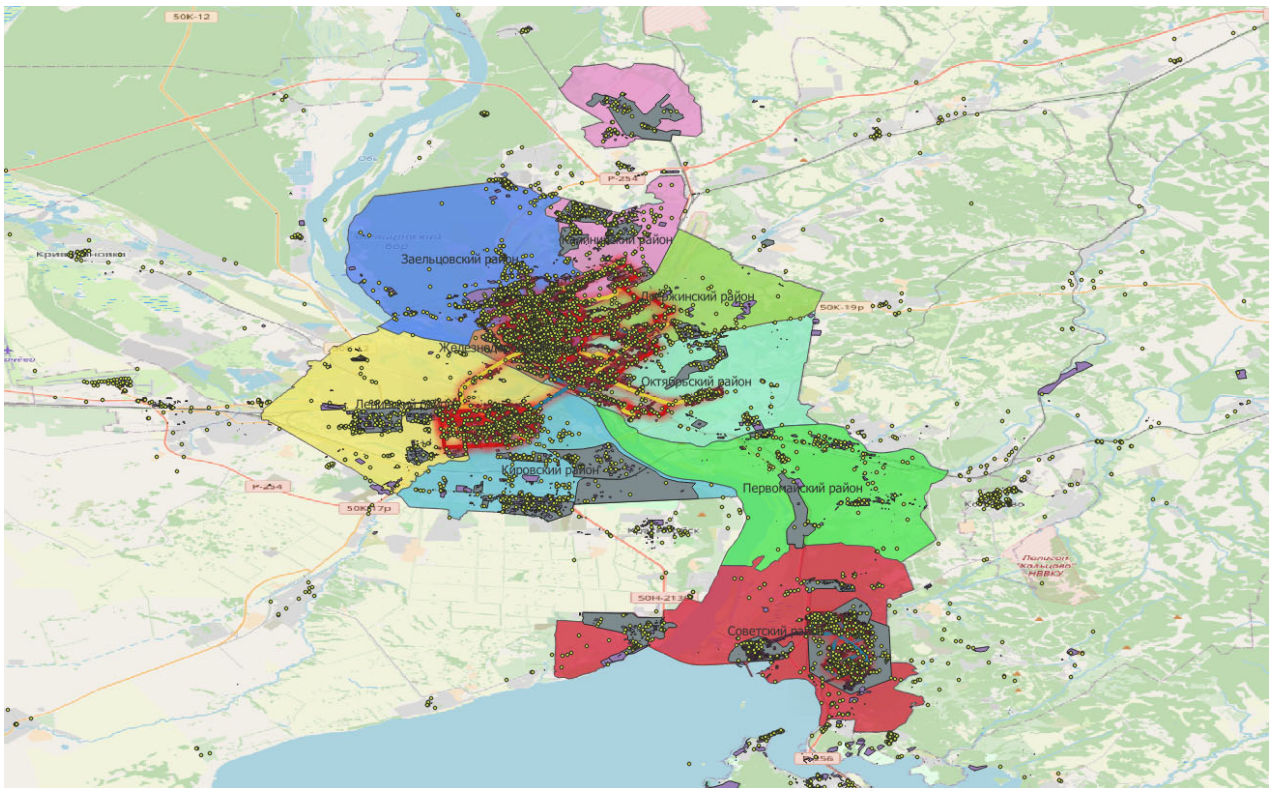


Рис. 1. Карта с отображением всех слоев

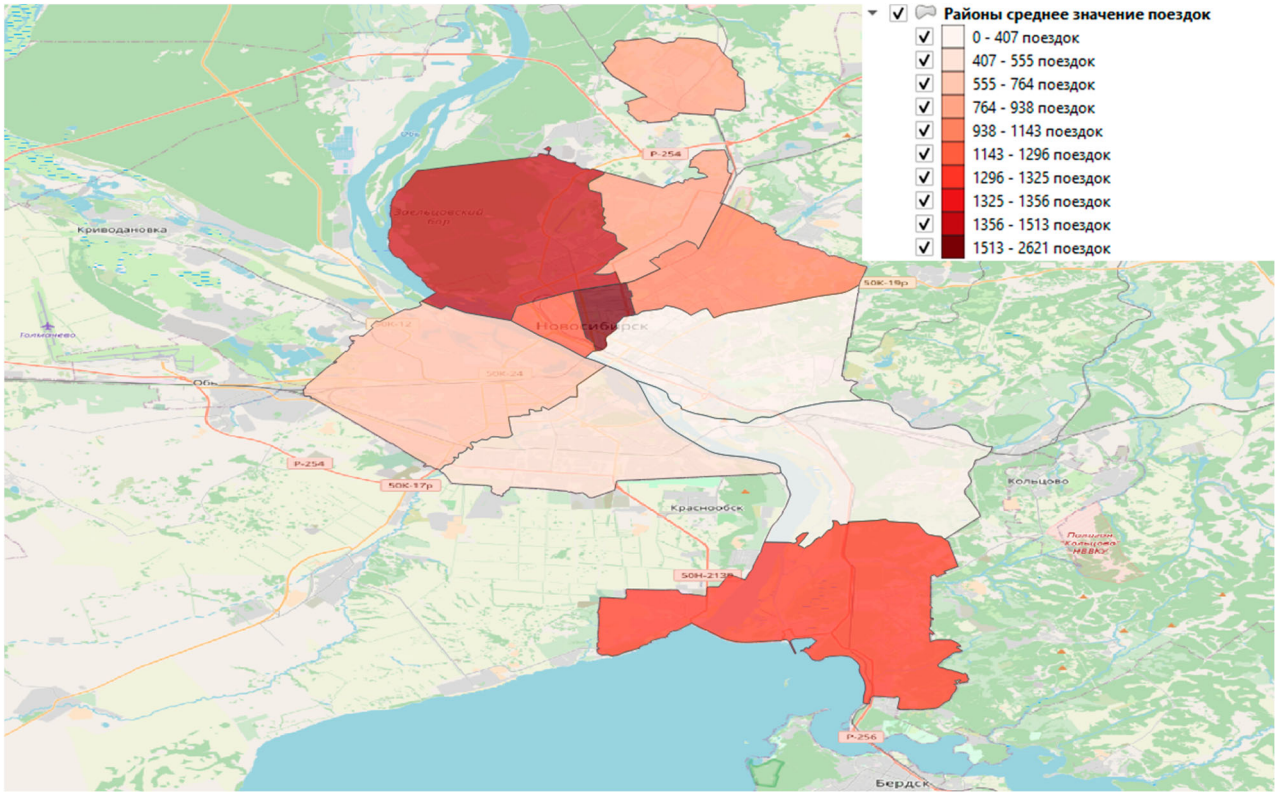


Рис. 3. Слой, отображающий количество поездок самокатов за месяц

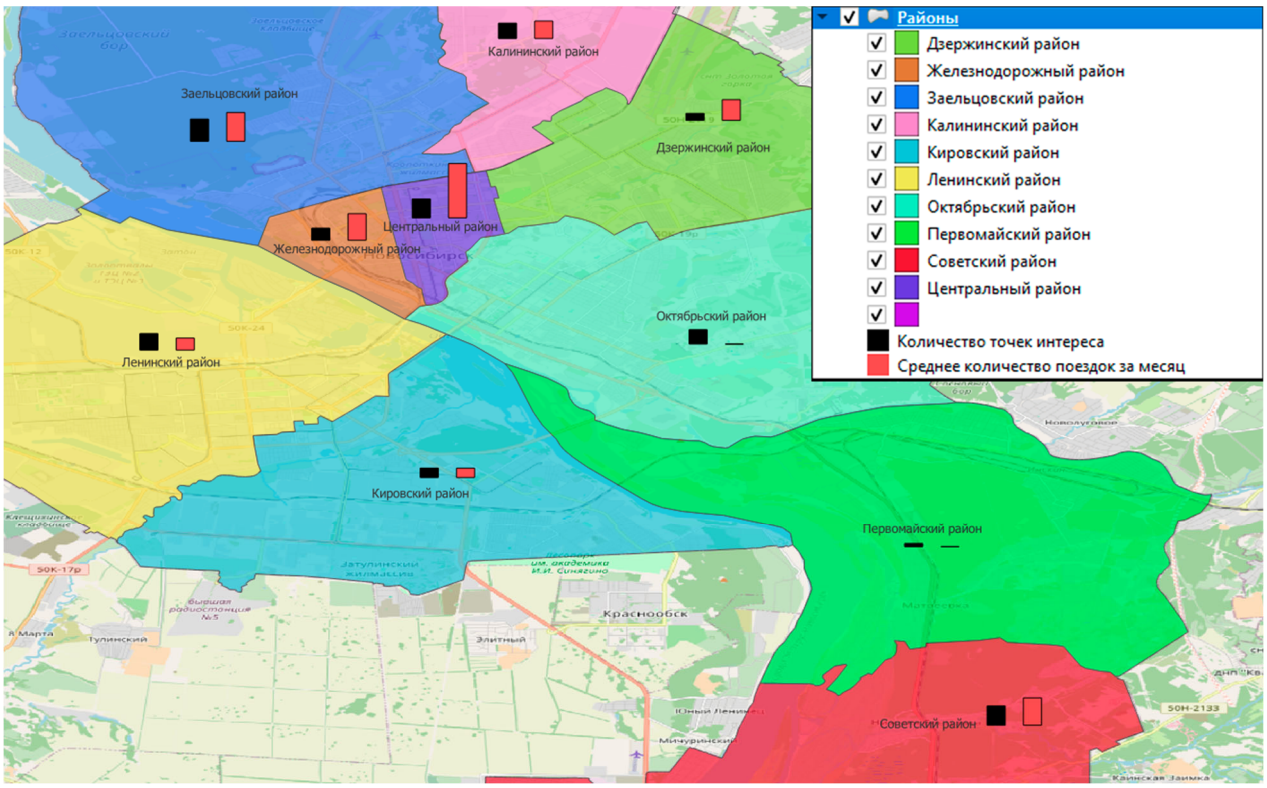


Рис. 4. Интенсивность движения электросамокатов

Заключение

Работа является актуальной, поскольку электросамокаты как полноценный вид транспорта появился достаточно недавно. Интенсивная эксплуатация электросамокатов, обусловленная появлением сервисов проката, вскрыла ряд проблем, требующих безотлагательного решения как со стороны муниципальных служб, так и со стороны коммерческих организаций, занимающихся сдачей электосамокатов в прокат.

Выполненная работа является частью методики создания ГИС для анализа инфраструктуры сервиса проката электросамокатов в городе Новосибирске. Созданный прототип геоинформационной системы рассматривается как способ апробации методики и может быть использован в дальнейшей разработке полнофункциональной геоинформационной системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 58680-2019. Оборудование спортивное на роликах. Самокаты. Требования безопасности и методы испытаний. - Официальное издание. М.: Стандартинформ, 2019 год.

2. Корчагин, Р. Е. Новая мобильность: как экотранспорт меняет каркас уличного движения / Р. Е. Корчагин // Логистика - евразийский мост: Материалы XVI Международной научно-практической конференции, Красноярск-Енисейск, 28 апреля – 01 2021 года. – Красноярск: Красноярский государственный аграрный университет, 2021. – С. 330-334.

3. Олейник, В. М. Понятие механического транспортного средства / В. М. Олейник // Стратегия научно-технологического развития - 2021: Сборник материалов Международной научно-практической конференции, Кемерово, 30 января 2021 года. – Кемерово: Общество с ограниченной ответственностью "Западно-Сибирский научный центр", 2021. – С. 120-124.

4. Злобина, Е. В. Самокат в современном мире / Е. В. Злобина, А. Г. Черепанов // Инновации. Наука. Образование. – 2021. – № 38. – С. 112-116.

5. Махарадзе, Н. С. Электротранспорт: популярность и опасность / Н. С. Махарадзе, А. В. Рудник // Актуальные вопросы юридической науки и практики : Материалы II Всероссийской научно-практической конференции со студенческим участием, Хабаровск, 28 мая 2021 года / Редколлегия: В.Е. Степенко (председатель) [и др.]. – Хабаровск: Тихоокеанский государственный университет, 2021. – С. 64-69.

6. Разработка концепции геоинформационной системы для анализа инфраструктуры сервиса проката электросамокатов в городе Новосибирске / Попов А.А., Бугаков П.Ю. // Материалы XVIII Международного научного конгресса ГЕО-Сибирь, Новосибирск 2022г. – СГУГиТ, 2022. – Том 6 С. 204-212

7. Разработка концепции геоинформационной системы для анализа инфраструктуры сервиса проката электросамокатов в городе Новосибирске / Попов А.А., Бугаков П.Ю. // Материалы Молодежной научно-практической конференции ИНЖЕНЕРНАЯ ГРАФИКА И ТРЕХМЕРНОЕ МОДЕЛИРОВАНИЕ, Новосибирск 2022г. – СГУГиТ, 2022. – С. 44-46

8. Whoosh data lab [Электронный ресурс]. – Режим доступа: https://whoosh-bike.ru/datalab

9. Лурье И.К. - Геоинформационное картографирование - М., КДУ – 2008

10. QGIS Cloud [Электронный ресурс]. – Режим доступа: https://qgiscloud.com

11. QGIS [Электронный ресурс]. – Режим доступа: https://qgis.org/en/site/

12. Карты районов [Электронный ресурс]. – Режим доступа: https://karta-raionov.ru/ru/novosibirskaya-oblast/novosibirsk/

13. Статистика электросамокатов [Электронный ресурс]. – Режим доступа: https://infopro54.ru/news/bolee-145-tysyach-novosibircev-vospolzovalis-uslugami-sheringa-samokatov-v-2021-godu/

14. Документация QGIS [Электронный ресурс]. – Режим доступа: https://docs.qgis.org/2.8/ru/docs/index.html

15. Лебедева, К. С. Алгоритм разработки геоинформационной системы для анализа велоинфраструктуры в Г. Новосибирск / К. С. Лебедева, П. Ю. Бугаков // Интерэкспо Гео-Сибирь. – 2021. – Т. 7. – № 2. – С. 107-113.

16. Научно-методические основы формализации процессов составления тематических карт для реализации в среде ГИС / С. С. Дышлюк, О. Н. Николаева, Л. А. Ромашова, С. А. Сухорукова // Известия высших учебных заведений. Геодезия и аэрофотосъемка. – 2011. – № 5. – С. 91-93.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-224-231

А. В. Ситская[1], В. В. Селифанов[1]*

Вопросы управления информационной безопасностью на объектах критической информационной инфраструктуры

[1]Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: AnSits@yandex.ru

Аннотация. На сегодняшний день главной проблемой в области обеспечения информационной безопасности – это грамотное управление информационной безопасностью на объектах критической информационной инфраструктуры, подрыв деятельности которой может привести к нарушению функционирования целой отрасли как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Главный метод управления информационной безопасностью является аудит. Организация должна проводить как внешний, так и внутренний аудит. Главным результатом данной статьи становятся рекомендации правильного управления информационной безопасностью на объектах критической информационной инфраструктуры. Чтобы получить наглядные результаты необходимо правильно провести аудит, следуя определенным правилам. В статье рассматривается цикл У. Э. Деминга, повсеместно используемый во всех сферах как метод проведения аудита. Главный принцип цикла «Plan-Do-Check-Act» или «планируй-реализуй-проверяй-действуй» наглядно показывает правильную организацию эффективного управления информационной безопасностью.

Ключевые слова: информационная безопасность, объект критической информационной инфраструктуры, цикл Деминга, цикл PDCA

A. V. Sitskaya[1], V. V. Selivanov[1]*

Issues of Information Security Management at Critical Information Infrastructure Facilities

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: AnSits@yandex.ru

Abstract. To date, the main problem in the field of information security is the competent management of information security at critical information infrastructure facilities, the undermining of which can lead to disruption of the functioning of an entire industry such as healthcare, science, transport, communications, energy, banking, fuel and energy complex, in the field of nuclear energy, defense, missile andspace, mining, metallurgical and chemical industries. The main method of information security management is auditing. The organization must conduct both external and internal audits. The main result of this article are recommendations for proper information security management at critical information infrastructure facilities. To get visual results, it is necessary to conduct an audit correctly, following certain rules. The article discusses the W. E. Deming cycle, which is widely used in all spheres as a method of conducting an audit. The main principle of the "Plan-Do-Check-Act" or "plan-implement-check-act" cycle clearly shows the correct organization of effective information security management.

Keywords: information security, critical information infrastructure facility, deming cycle, PDCA cycle

Введение

В настоящее время одним из наиболее острых вопросов стал вопрос обеспечения информационной безопасности (ОИБ). На ОИБ объектов критической информационной инфраструктур (КИИ) нацелено наиболее пристальное внимание. В первую очередь ИБ объектов КИИ – это безопасность информационных систем (ИС) стратегически важных для государства областей. Нарушение безопасности ИС предприятия одной из стратегических областей может не просто остановить на некоторое время предприятие, но и снизить эффективность работы целой отрасли как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Для регулирования ИБ на объектах КИИ были выпущены как Федеральные законы (187-ФЗ от 26 июля 2017 г. [1]), Постановления правительства (ПП РФ №127 от 08.02.2018г.[2], ПП РФ №162 от 17.02.2018г. [3]), так и приказы таких регуляторов как ФСТЭК России (Приказ ФСТЭК России №227 от 06.12.2017г. [4], Приказ ФСТЭК России №235 от 21.12.2017г. [5], Приказ ФСТЭК России №239 от 25.12.2017г. [6]), так и ФСБ России (Приказ ФСБ России №366 от 24.07.2018г. [7], Приказ ФСБ России №368 от 24.07.2018г. [8], Приказ ФСБ России №196 от 06.05.2019г. [9], Приказ ФСБ России № 281 от 19.06.2019г. [10], Приказ ФСБ России № 282 от 19.06.2019г. [11]). Однако слепое следование законодательству не говорит об эффективности построенной системы защиты информации (СЗИ) на предприятии. Для обеспечения и поддержания эффективности СЗИ необходимо, чтобы на предприятии была эффективно построена система управления информационной безопасностью (СУИБ), адаптированная под конкретную ИС и учитывающая специфику организации.

Цикл Деминга как эффективная СУИБ

Главной проблемой, затрудняющей повышение качества управления параметрами ИБ, является непостоянность параметров объекта управления и постоянное изменение требований к качеству регулирования в процессе работы [12]. Функционирование наиболее эффективной СУИБ хорошо иллюстрирует цикл У.Э. Деминга (PDCA), где главная мысль: «Plan-Do-Check-Act» или «планируй-реализуй-проверяй-действуй». При соблюдении такого подхода СЗИ будет наиболее эффективна и работоспособна, т.к. большая часть уязвимостей будет выявлена и устранена вовремя. Однако реализация данного цикла также требует усилий.

Один из основополагающих стандартов, касающихся аудита, ГОСТ Р ИСО 19011-2021[13], который различает следующие типы аудита:

– внутренний аудит 1-й стороны проводится самой организацией или от ее имени для внутренних целей [14]. Основанием для проведения такого аудита служит внутренний контроль принятых нормативных документов по защите информации (ЗИ);

– внешний аудит 2-й стороны проводится сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами от их имени [14];

– внешний аудит 3-й стороны (независимая оценка) проводится внешними независимыми коммерческими организациями, имеющими лицензии на осуществление аудиторской деятельности в области ОИБ [14]. В области ЗИ объектов КИИ такой аудит является неотъемлемой частью функционирования предприятия, утвержденный законодательством РФ, и именно такой аудит зачастую приносит наибольший результат по контролю функционирования СЗИ.

Также ГОСТ Р ИСО 19011-2021[13] предлагает схему последовательности действий для управления программой аудита, которая очень ярко иллюстрирует цикл Деминга в области аудита ИБ.

Аудит на всех этапах жизненного цикла СЗИ

На этапе планирования как СЗИ, так и аудита происходит разработка технического задания (для СЗИ) и разработка программы проведения аудита. Первичный аудит объекта КИИ должен представлять из себя процесс категорирования. На данном этапе аудит может быть, как внутренним 1-й стороны, так и внешним 3-й стороны.

Во время этапа планирования аудита должны быть рассмотрены и реализованы следующие пункты, согласно [13]:

– установить объем программы в соответствии с поставленными целями и известными ограничениями;

– определить внешние и внутренние проблемы, риски и возможности, которые могут повлиять на программу;

– обеспечить выбор групп аудита, обладающих необходимой компетентностью для проведения аудита, определив их обязанности ответственность и полномочия;

– разработать все необходимые процессы, включая процессы для координации и планирования всех аудитов в рамках программы, разработка целей аудита, области и критериев, определения методов аудита, подбор аудиторской группы, разработка внешних и внутренних процессов коммуникаций;

– и т.п.

Далее, согласно циклу Деминга идет «реализация». При реализации стоит обратить внимание, что согласно законодательству, объекты КИИ разделяются на «значимые» и «не значимые». При этом «значимым» объектам необходимо присвоить категорию, в соответствии с которой далее и будет осуществляться построение/ модернизация предприятия. «Не значимые» объекты не участвуют в автоматизации критических процессов, а значит не подлежат категорированию.

Схема последовательности действий управления программой аудита представлена на рис. 1.

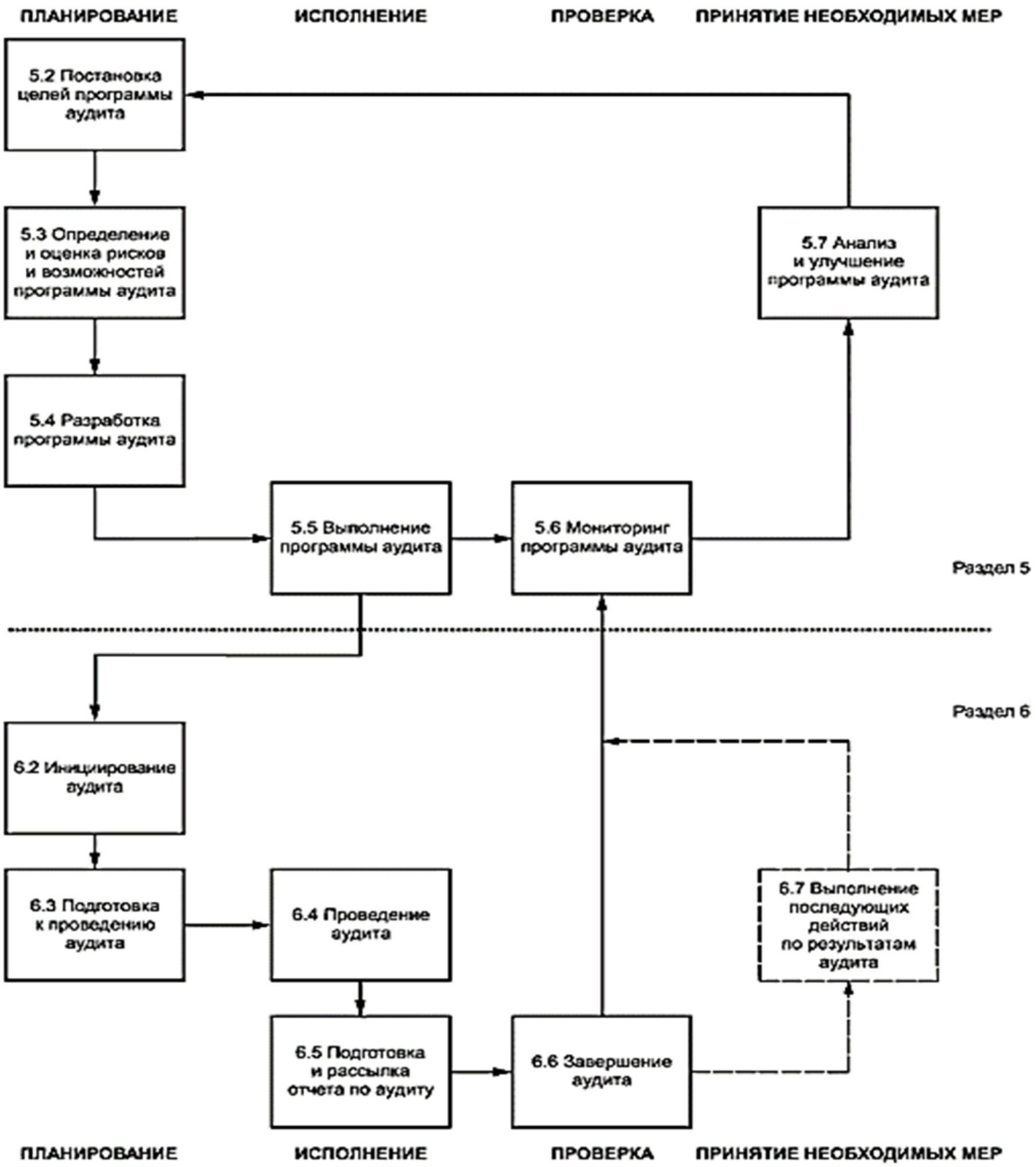


Рис. 1. Схема последовательности действий управления программой аудита [13]

Если при проведении аудита значимых объектов КИИ (ЗО КИИ) все достаточно понятно, аудитор в первую очередь обращает внимание на соблюдение законодательства, то при аудите не значимых объектов КИИ аудитор может не учитывать законодательство для ЗО КИИ, однако необходимо оценивать полноту выполнения субъектом КИИ обязанностей, возложенных на него частью 2 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». По решению субъекта КИИ, для обеспечения безопасности «не значимого» объекта КИИ может быть создана система безопасности, базирующаяся на требованиях для «зна-

чимых» объектов КИИ. В этом случае, в критерии аудита уже включаются все требования, характерные для безопасности «значимых» объектов КИИ [15].

При первичном аудите аудитору необходимо оценить полноту и достаточность реализации СЗИ. А для ЗО КИИ соответствующей категории значимости согласно Приказу ФСТЭК России №239 [6] определить, какие меры выполняются, а какие нет, затем понять, как и насколько полно они выполняются.

Результатом первичного аудита будет являться понимание того, какая часть обязательных мер по обеспечению безопасности ЗО КИИ уже реализована, а какая требует реализации в процессе создания/модернизации СЗИ.

На следующем этапе цикла производится улучшение методов проведения аудита, корректировка сроков проведения аудита. Далее с учетом всех результатов предыдущих этапов проводится аудит, результаты которого в полной мере будут отражать текущее состояние СУИБ предприятия.

Однако проведение аудита не гарантирует эффективность работы СЗИ предприятия. В процессе внешнего аудита отдельное внимание уделяется именно СУИБ. И после получения отчета по аудиторской проверке руководству организации стоит обратить пристальное внимание именно к разделу, посвящённому СУИБ. Ведь дальнейшие результаты по устранению недостатков всей СЗИ возлагаются именное на СУИБ.

Анализ функционирования СУИБ основан на следующем:

– результаты мониторинга ИБ и контроля мер ОИБ, который иллюстрирует эффективность проводимых внутренних аудитов организации силами сотрудников самой организации;

– сведения об инцидентах ИБ. В сведениях содержится информация об существующих инцидентах, а также как они были проработаны, как была скорректирована СЗИ для предотвращения аналогичных инцидентов;

– результаты проведения аудитов и самоконтроля ИБ. В результатах будет раскрыт вопрос эффективности и объективности проводимых мероприятий сотрудниками подразделения ИБ;

– данные об угрозах ИБ, возможных нарушителях ИБ и уязвимостях. Сведения определяют дальнейшую работу СУИБ, которую руководство может отслеживать;

– данные об изменениях внутри организации. В сведениях содержится вся информация о деятельности СУИБ в процессе жизненного цикла ИБ организации.

Для проведения анализа функционирования СУИБ, согласно [14] необходимы следующие мероприятия:

– анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению законодательства РФ и стандартов, договорным обязательствам организации;

– анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению и управлению ИБ, требованиям политики ИБ организации;

– оценку адекватности модели угроз ИБ организации существующим угрозам ИБ;

– оценку рисков в области ОИБ организации, включая оценку уровней остаточного и допустимого риска ИБ;

– проверку адекватности используемых мер ОИБ требованиям внутренних документов организации и результатам оценки рисков ИБ;

– анализ отсутствия разрывов в технологических процессах ОИБ, а также несогласованности в использовании защитных мер ИБ.

Для контроля и анализа деятельности СУИБ в организации руководство утверждается план мероприятий, в том числе совещаний на уровне руководства, на которых проводится анализ проблем ОИБ.

В целом по результатам анализа СУИБ со стороны руководства необходимо реализовать тактические или стратегические улучшения СУИБ [15].

К тактическим улучшениям СУИБ относят корректирующие или превентивные действия, связанные с пересмотром отдельных процессов СУИБ. Примеры решений по тактическим улучшениям, согласно [16]:

– пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;

– пересмотр процедур эксплуатации отдельных видов защитных мер;

– пересмотр процедур обнаружения и обработки инцидентов;

– уточнение описи информационных активов;

– пересмотр программы обучения и повышения осведомленности персонала;

– пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;

– пересмотр планов обработки рисков;

– вынесение санкций в отношении персонала;

– пересмотр процедур мониторинга ИБ и контроля защитных мер;

– пересмотр программ аудитов;

– корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;

– ввод новых или замена используемых защитных мер.

К стратегическим улучшениям СУИБ относят корректирующие или превентивные действия, связанные с пересмотром политик ИБ организации. Примеры решений по стратегическим улучшениям, согласно [16]:

– уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ организации БС РФ;

– изменение в области действия СОИБ;

– пересмотр моделей угроз и нарушителей;

– изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

После пересмотра и корректировки СУИБ целесообразно заново провести внешний аудит, который покажет результаты работы организации над СУИБ. Тем самым организация снова войдет на этап планирования цикла Деминга.

Заключение

Наиболее эффективной СУИБ станет при следовании циклу У.Э. Деминга (PDCA), который заключается в следующем: «Plan-Do-Check-Act» или «планируй-реализуй-проверяй-действуй». Следуя циклу Деминга, на всех этапах жизненного цикла СЗИ целесообразно проводить различные аудиты, которые в свою очередь покажут большую часть уязвимостей, которые организация сможет устранить. Безопасность как ЗО КИИ, так и объектов КИИ напрямую зависит от правильного построение СУИБ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Закон Российской Федерации "«О безопасности критической информационной инфраструктуры Российской Федерации». Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак." от 26.07.2017 N 187-ФЗ.

2. Постановление Правительства РФ "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения" от 08.02.2017 № 127.

3. Постановление Правительства РФ "Об утверждении Правил поставки газа в Российской Федерации" от 05.02.1998 N 162.

4. Приказ ФСТЭК России «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» от 06.12.2017 N 227.

5. Приказ ФСТЭК России "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования" от 21.12.2017 N 235.

6. Приказ ФСТЭК России "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" от 25.12.2017 N 239.

7. Приказ ФСБ России "О Национальном координационном центре по компьютерным инцидентам" от 24.07.2018 N 366.

8. Приказ ФСБ России "Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения" от 24.07.2018 N 368.

9. Приказ ФСБ России "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты" от 06.05.2019 N 196.

10. Приказ ФСБ России "Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации" от 19.06.2019 N 281.

11. Приказ ФСБ России "Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации" от 19.06.2019 N 282.

12. Табакаева В. А., Карманов И. Н., Ан В. Р. Особенности интеллектуальных систем управления информационной безопасностью объектов критической информационной инфраструктуры [электронный ресурс] / Интерэкспо Гео-Сибирь. 2020. №2. URL: https://cyberleninka.ru/article/n/osobennosti-intellektualnyh-sistem-upravleniya-informatsionnoy-bezopasnostyu-obektov-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 11.04.2023).

13. ГОСТ Р ИСО 19011-2021 "Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента" от 11.05.2021.

14. Милославская Н.Г., Толстой А.И. Проверка деятельности по управлению информационной безопасностью: учеб. пособие для вузов, 220966 изд. Горячая линия - Телеком, 2022.

15. Кузнецов Д. Защита КИИ: от слов к делу [Электронный ресурс] // «Information Security/ Информационная безопасность: электрон. журн. 2019. N 3. URL: http://cs.groteck.ru/IB_3_2019/4/index.html (дата обращения: 31.03.2023).

16. Стандарт Банка России СТО БР ИББС-1.0-2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения" (принят и введен в действие распоряжением Банка России от 17 мая 2014 г. N Р-399).

17. Кидяева С. М., Шабурова А. В., Селифанов В. В. Вопросы организации менеджмента рисков значимых объектов критической информационной инфраструктуры [Электронный ресурс]// Интерэкспо Гео-Сибирь. 2022. №. URL: https://cyberleninka.ru/article/n/voprosy-organizatsii-menedzhmenta-riskov-znachimyh-obektov-kriticheskoy-informatsionnoy-infrastruktury (дата обращения: 15.04.2023).

18. Ан В. Р. Табакаева В. А., Селифанов В. В. разработка критериев оценки соответствия требованиям безопасности на объекте информатизации // Интерэкспо Гео-Сибирь. 2021. №. URL: https://cyberleninka.ru/article/n/razrabotka-kriteriev-otsenki-sootvetstviya-trebovaniyam-bezopasnosti-na-obekte-informatizatsii (дата обращения: 21.04.2023).

19. Ан В.Р., Табакаева В.А., Селифанов В.В. разработка методики аудита кибербезопасности государственных информационных систем, относящихся к значимым объектам критической информационной инфраструктуры, функционирующих на базе центров обработки данных // Интерэкспо Гео-Сибирь. 2020. №1. URL: https://cyberleninka.ru/article/n/razrabotka-metodiki-audita-kiberbezopasnosti-gosudarstvennyh-informatsionnyh-sistem-otnosyaschihsya-k-znachimym-obektam (дата обращения: 11.04.2023).

УДК 62:935.2
DOI 10.33764/2618-981X-2023-6-232-237

П. П. Солощенко[1], Г. В.Симонова[1]*

Реверс-инжиниринг как ключевой инструмент импортозамещения при работе сервисной службы ООО «ЦСМ»

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: ppp131144@mail.ru

Аннотация. После введения экономических санкций и отказа западных компаний поставлять запчасти и материалы в Россию значительное число отечественных предприятий оказались в тяжёлой ситуации, а иногда и на гране остановки производства. Ежедневно возникает объективная необходимость воссоздать пришедшую в негодность деталь или целый узел импортного оборудования. Подобные проблемы возникают и в случае, если деталь отечественного производства, но уже больше не выпускается. Трудности подобного рода могут быть решены применением аддитивных технологий совместно с методами обратного проектирования, или, реверсивным инжинирингом. В статье рассмотрен метод внедрения реверс-инжиниринга в сервисную службу ООО «Центра стандартизации и метрологии», проведен анализ наиболее востребованных запасных частей и составлен их каталог, также выявлен ряд перспективных организаций субподрядчиков.

Ключевые слова: оборудование, отказ, реверс инжиниринг, сервисная служба., импортозамещение, экономическая целесообразность

P.P. Soloshchenko[1], G.V. Simonova[1]*

Reverse Engineering as a Key Tool For Import Substitution in the Work of the Service Department of CSM LLC

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: ppp131144@mail.ru

Abstract. After the introduction of economic sanctions and the refusal of Western companies to supply spare parts and materials to Russia, a significant number of domestic enterprises found themselves in a difficult situation, and sometimes even on the verge of stopping production. Every day there is an objective need to recreate a part that has become unusable or a whole assembly of imported equipment**.** Similar problems also arise, if the part domestically produced, but is no longer produced. Difficulties of this kind can solved by using additive technologies in conjunction with reverse engineering methods, or reverse engineering. The article considers the method of implementing reverse engineering in the service department of "Center Standardization and Metrology" LLC, analyzes the most popular spare parts and compiles their catalog, and also identifies a number of promising subcontractor organizations.

Keywords: equipment, failure, reverse engineering, customer service, import substitution, economic feasibility

Введение

Реверс-инжиниринг, или обратный инжиниринг представляет собой процесс воссоздания существующего продукта или компонента путем изучения его конструкции и конструктивных особенностей. Реверс-инжиниринг имеет огромную практическую ценность в промышленном секторе [1].

Существует несколько причин, по которым обратный инжиниринг является важным инструментом для современного бизнеса. Наличие необходимых комплектующих для производства помогает оставаться конкурентоспособной организацией, понимание и использование эффективных разработок своих конкурентов или других компаний позволяет реализовать оперативное воссоздание отсутствующих на рынке материалов или изделий. Таким образом, реверс-инжиниринг дает возможность быстро и эффективно выпускать аналогичные продукты или улучшать существующие, что приводит к увеличению прибыли [2, 3].

Задачи, которые решает реверс-инжиниринг:

– производство запасных частей по моделям цифрового склада;

– производство не выпускаемых запасных частей и запрещённых для поставки в РФ;

– оптимизация сложных сборок с целью их агрегации в единое изделие.

В настоящее время сервисная служба ООО «Центр стандартизации и метрологии» (ЦСМ) испытывает сложности при ремонте средств измерений иностранных производителей по причине антироссийских санкций и действующих запретов на импорт техники и компонентов. Сейчас работоспособность сервисной службы большей частью зависит от замещения деталями российского производства. Произвести узлы средств измерений, на которые отсутствует конструкторская и технологичная документация, позволяет реверс-инжиниринг [8, 9].

Процесс обратного проектирования обычно включает сканирование или измерение существующего продукта с использованием 3D-сканеров или другого подходящего оборудования. С помощью этих отсканированных данных можно создать 3D-модель, чтобы точно определить особенности, которые делают продукт уникальным или особенным. После создания модели воссоздается исходный продукт, при необходимости внося в него определенные изменения [6].

Кроме того, обратный инжиниринг можно использовать для оптимизации продукта путем улучшения методов производства, исправления ошибок или недостатков в конструкции. Этот процесс помогает увеличить жизненный цикл продукта и обеспечивает экономичный метод обслуживания.

Методы и материалы

Для реверс-инжиниринга можно использовать несколько устройств. 3D-сканеры – это наиболее часто используемое оборудование, которое фиксирует физические атрибуты объекта в цифровом виде. Технология 3D-сканирования необходима для захвата даже самой сложной геометрии, органических форм, а реверс-инженеры могут получить ценные данные о материалах и составе. Другие устройства включают координатно-измерительные машины (КИМ) и альтернативы КИМ.

КИМ, (рис. 1) – это приборы для точных контактных измерений объектов. Устройства работают при помощи специальных датчиков (зондов), определяющих положение точек на поверхности объектов [7].

Перемещением измерительной головки может управлять компьютер или оператор. КИМ определяет положение датчика по изменению его положения в

сравнении с исходной позицией по осям XYZ. Для работы в труднодоступных участках КИМ изменяет угол наклона датчика при движении.

Рис. 1. Координатно-измерительная машина

3D-сканер (рис. 2) работает путем захвата данных с поверхности физического объекта для описания его формы в точном цифровом трехмерном формате. В отличие от данных измерений на КИМ, высококачественные данные 3D-сканирования используются не только для контроля и анализа размеров [4, 5]. Полученные бесконтактным измерением данные позволяют быстрее и доступнее проводить цифровой анализ и инспекцию с помощью визуального, углубленного метода исследования.

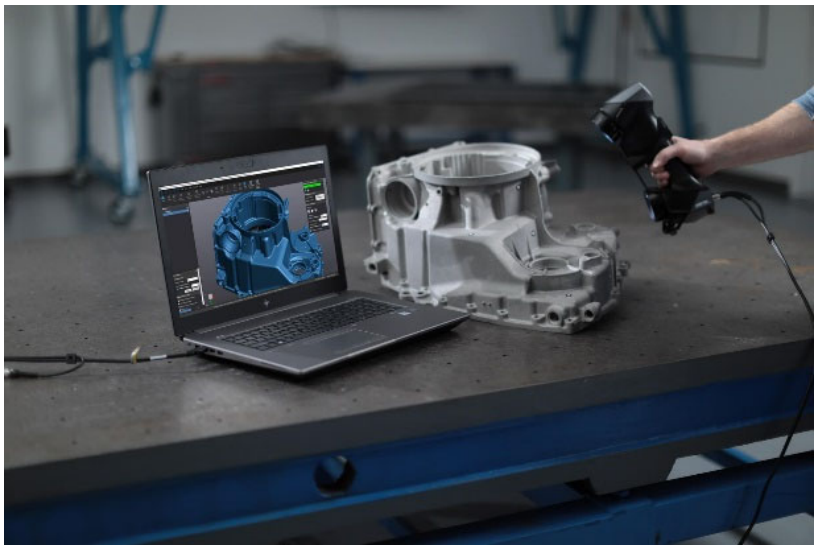


Рис. 2. 3D-сканер

Ключевое преимущество реверс-инжиниринга заключается в том, что он позволяет производителям воссоздавать существующий продукт или систему с большей точностью и детализацией.

Рентабельность: процесс обратного проектирования часто дешевле, чем импорт оригинальных запасных частей. Затраты на реверс-инжиниринг связаны с исследованиями и разработками, которые будут сведены к минимуму по мере увеличения количества деталей, с использованием этого метода. Кроме этого, обратный инжиниринг гарантирует, что воспроизводимые запасные части имеют характеристики и качество, аналогичные оригинальным деталям [10, 11].

Для реализации предложенной программы по производству запасных частей для бесперебойной работы сервисной службы ООО «ЦСМ» необходимо решить следующие задачи:

– выявить компании, основным направлением которых является реверс - инжиниринг;

– создать цифровой каталог запасных частей, необходимых для работы сервисной службы;

– разработать технические задания по каталогу выбранных запасных частей;

– наладить сотрудничество с производствами, которые способны воспроизвести запасные части по техническому заданию;

– рассчитать экономику каждого изделия [2, 12].

Результаты

Одной из основных статей расходов, связанных с обратным проектированием, являются затраты на исследования и разработки. На старте проекта целесообразней отдавать заказы в компанию направлением которой является реверс-инжиниринг. В данной работе был проведен сравнительный анализ по трем организациям соответствующей направленности. Сравнение проводилось по стоимости работ и срокам выполнения заказа. На основании выполненного сравнения был сделан выбор компании «PLM УРАЛ». Компания уже 30 лет успешно работает в этом направлении и имеет большой опыт в реверс-инжиниринге. «PLM УРАЛ» предлагает КИМ типа "рука" Hexagon Absolute Arm двух типоразмеров: 8325-7 и 8540-7, а так же лазерный сканер RS6. Готовая модель экспортируется в форматах. iges, .stp, .x_t, .model, .catpart, .ftp. Организация «PLM УРАЛ» выполняет работы как на территории заказчика, так и в собственном сервисном центре (табл. 1).

В сервисный центр ООО «ЦСМ» поступает пятнадцать типов различных турбинных и роторных счетчиков газа иностранных производителей. Специалистами сервисной службы на базе анализа был создан каталог изделий, необходимых для бесперебойной работы сервисного центра по ремонту газовых счетчиков газа производителя "Actaris Gaszahlerbau GmbH", Германия.

Таблица 1

Наименование	Внешний вид	Материал	Цена у производителя, руб.
Магнитная муфта в сборе		ШХ15, [15] РС термопластик	2800
Основание ротора		В95 [15]	17800
Колеса синхронизации		20ХМ	9300

Заключение

В данной статье рассматривается роль обратного инжиниринга в импортозамещении в сервисной службе ООО «ЦСМ». Внедрение реверс-инжиниринга в сервисном отделе является ответственным процессом, так как позволяет заменить любые импортные запчасти, необходимые клиентам. Этот процесс будет выгоден, поскольку он снижает затраты без ущерба для качества и повышает удовлетворенность клиентов.

На основании анализа были выделены организации готовые к сотрудничеству и удовлетворяющие потребность в проектировании запасных частей для сервисного центра, был составлен каталог необходимых запасных частей. Эта

работа оценивает преимущества использования обратного инжиниринга, возможные затраты и связанные с этим риски, а также шаги, необходимые для реализации этой стратегии. С помощью результатов этой работы можно создать эффективную и прибыльную систему импортозамещения запасных частей, которая расширит возможности сервисного центра.

В рамках данной работы планируется дальнейшее исследования по внедрению реверс-инжиниринга в сервисный центр ООО «ЦСМ», а также расширение каталога запасных частей и налаживание сотрудничества с новыми организациями по проектированию и производству запасных частей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Водин Д.В. Применение технологии обратного инжиниринга в машиностроении // Технические науки: проблемы и перспективы: материалы IV Междунар. науч. конф. (г. Санкт-Петербург, июль 2016 г.). СП6.: Свое издательство, 2016. – С. 67–69.

2. Моисеева Н.К. Стратегический менеджмент: учебник. / Н.К. Моисеева, Г.Д. Костина. – М.: МИЭТ, 2016. – 220 с.

3.РМГ 128-2013 «ГСИ. Требования к созданию лабораторий, осуществляющих испытания и измерения» введен 01.05.2015 – Москва: Стандартинформ, 2015 – 16 с.

4.Гуськова, В. П. Хроматографические методы разделения и анализа : учебное пособие / В. П. Гуськова, Л. С. Сизова. – 2-е изд., испр. и доп. – Кемерово : КемГУ, 2015. – 148 с. – ISBN 978-5-89289-888-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/72028 (дата обращения: 24.03.2023). – Режим доступа: для авториз. пользователей

5. Баранов В.В. Система разработки прикладного программного обеспечения с использованием языка высокого уровня. / В.В. Баранов, А.А. Звонарев, К. Чжао // Вестник Вологодского государственного университета. Серия: Технические науки, № 2 (4), 2019 – с. 27 – 30.

6. Тарнавский Ю. Основы реверс-инжиниринга .Net-приложений. [Электронный ресурс]. Режим доступа: https://s3r.ru/2012/10/bez-rubriki/basics_dot_net_reversing/.

7. Алехина Т.А., Захаркина Н.В. Импортозамещение как основной инструмент развития экономики России // Вестник Дагестанского государственного технического университета. Технические науки. 2018. № 45 (1) – С. 223–235.

8. Жакевич А.Г. Импортозамещение: проблемы и перспективы // Вестник Международного института экономика и права. 2015. № 1 (18) – С. 36–39.

9. Алексеев Н.Е. Импортозамещение как институт укрепления национального суверенитета // Мировая политика. 2019. № 2 – С. 43–50.

10. Елецкий Н.Д., Столбовская А.Г. Импортозамещение в России: не проблема, а задача // Молодой ученый. 2015. № 6 (86) – С. 406–408.

11. Березинская О., Ведев А. Зависимость российской экономики от импорта // Экономическое развитие России. 2017. Т. 24, № 4 – С. 19–25.

12. Управление промышленными предприятиями: стратегии, механизмы, системы: моногр. / О.В. Логиновский, А.А. Максимов, В.Н. Бурков и др.; под ред. О.В. Логиновского, А.А. Максимова. М.: ИНФРА-М, 2018 – 410 с.

13. ГОСТ Р 57306- 2016 ИНЖИНИРИНГ Терминология и основные понятия в области инжиниринга введен 30.11.2016 – Москва: Стандартинформ, 2016 – 4 с.

14. ГОСТ 18322-2016 Межгосударственный стандарт система технического обслуживания и ремонта техники Введен 01.09.2017- Москва: Стандартинформ, 2017 – 17 с.

15. ГОСТ 4784-2019 Алюминий и сплавы алюминиевые деформируемые Введен 01.09.2019- Москва: Стандартинформ, 2019 – 35 с.

УДК 539.1.076
DOI 10.33764/2618-981X-2023-6-238-242

А. В. Топчиенко[1], Д.М. Никулин[1]*

Методы контроля параметров пучка заряженных частиц

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: A.V.Topchienko@inp.nsk.su

Аннотация. Контроль параметров пучка заряженных частиц является актуальной задачей при разработке и эксплуатировании ускорителей заряженных частиц. Качество пучков в современных ускорителях имеет непосредственное отношение к эффективности их работы. В первую очередь осуществляется контроль геометрических характеристик пучка заряженных частиц. В статье рассматриваются известные методы контроля параметров пучка заряженных частиц, основанные на контактных, оптических и электромагнитных датчиках. Приводятся физические принципы, на которых работают контактные, оптические и электромагнитные датчики. Целью данной работы: изучить и проанализировать известные методы контроля параметров пучка заряженных частиц, выявить недостатки и преимущество одних методов относительно других.

Ключевые слова: пучок заряженных частиц, синхротронное излучение, ускоритель заряженных частиц

A. V. Topchienko[1], D. M. Nikulin[1]*

Methods for Monitoring Parameters of a Charged Particle Beam

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: Topchienko-AV2021@sgugit.ru

Abstract. Charged particle accelerator Monitoring the parameters of a charged particle beam is an urgent task in the development and operation of charged particle accelerators. The quality of beams in modern accelerators is directly related to the efficiency of their operation. First of all, the geometric characteristics of the charged particle beam are controlled. The article discusses well-known methods for monitoring the parameters of a charged particle beam based on contact, optical and electromagnetic sensors. The physical principles on which contact, optical and electromagnetic sensors work are given. The purpose of this work is to study and analyze known methods for controlling the parameters of a charged particle beam, to identify the disadvantages and advantages of some methods relative to others.

Keywords: a beam of charged particles, synchrotron radiation, charged particles accelerator

Введение

Пучки заряженных частиц являются необходимым инструментом при разработке перспективных технологий в области проведения исследований физических, химических и механических свойств материалов [1]. В мире работают и ежегодно запускаются ускорители заряженных частиц – один из основных инструментов физиков и научных работников об изучении фундаментальных свойств материи [2, 3]. Ускорители заряженных частиц применяются в медицин-

ских целях: получение и использование радиоактивных изотопов в медицине, позитронно-эмиссионная томография, радионуклидная терапия, производство ядерных мембран и т.д. [4-7].

Так как одной из главных задач является транспортировка заряженных частиц из одного места в другое, контролируются в основном геометрические характеристики пучка: группировка, фокусировка, поперечные и продольные размеры. Данные характеристики управляются при помощи согласованной работы многих устройств, в первую очередь прецизионных электромагнитных устройств, с помощью которых пучок заряженных частиц фокусируют, отклоняют, поворачивают и ускоряют.

Сложность измерения параметров пучка движущихся в ускорителях заряженных частиц связана, в первую очередь, с энергиями и скоростями, близкими к скорости света.

Известные методы контроля параметров пучка заряженных частиц

Все разнообразие методов контроля параметров пучка заряженных частиц можно разделить на три типа по физическим принципам, лежащим в основе работы датчика:

– контактные датчики, непосредственно взаимодействующие с частицами пучка;

– оптические датчики, регистрирующие излучение пучка в видимом, ультрафиолетовом или рентгеновском диапазонах;

– электромагнитные датчики, сигналы которых формируются электромагнитными полями, индуцированными пучком [8].

I. Контактные датчики

Так как контактные датчики взаимодействуют с пучком заряженных частиц, плотность мощности которых может достигать до 10^{15} Вт/см^2, то они используются для однопролетной диагностики. Главным недостатком контактных датчиков является вызываемое им разрушающее воздействие на пучок заряженных частиц при физическом взаимодействии с ним. Самыми распространенными контактными датчиками являются:

1. Цилиндр Фарадея. По сути, является металлическим электродом, располагающемся на пути пролета пучка заряженных частиц. Возникающий в электроде ток, при поглощении материалом электрода пучка заряженных частиц является мерой тока пучка в вакууме.

2. Люминофорный экран. Помещается на пути пучка заряженных частиц, под действием которых люминофор начинает светится и позволяет визуализировать пучок на люминофоре (рис. 1).

3. Микроканальный датчик. Представляет собой микроканальную пластину, предназначенную для усиления тока вторично-эмиссионных электронов, с помощью которых формируется изображение пучка заряженных частиц.

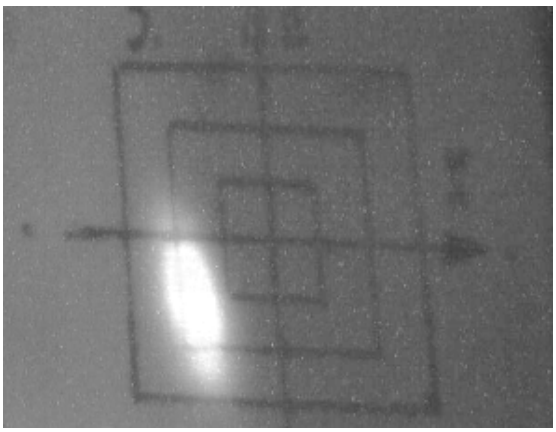


Рис. 1. Изображение пучка заряженных частиц на люминофоре

4. Ионизационный датчик. Изображение пучка заряженных частиц формируется электронами при ионизации им остаточного газа.

5. Пучковый датчик. Принцип работы заключается в сканировании электронным (пробным) пучком исследуемого пучка заряженных частиц (рис. 2).

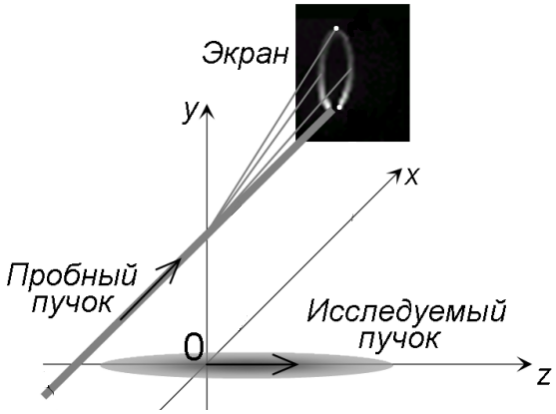


Рис. 2. Расположение пробного и исследуемого пучков

6. Лазерные измерители профиля пучка. Основаны на эффекте Комптона – рассеянии фотонов на пучке заряженных частиц [9].

II. Оптические датчики

Оптические датчики используются для визуального наблюдения синхротронного излучения (магнитотормозное излучение), генерируемого релятивистским пучком в поле поворотных магнитов. Оптическими датчиками могут быть:

1. Фотоэлектронный умножитель (ФЭУ) – чувствительный прибор, работающий в видимом, инфракрасном и ультрафиолетовом диапазонах (рис. 3) [10]. Способен усиливать световой поток до 10^8 раз, что позволяет регистрировать до одного фотона.

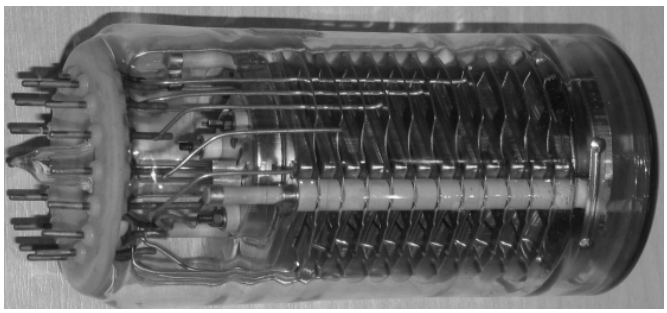


Рис. 3. Фотоэлектронный умножитель

2. Диссектор – представляет из себя электронно-оптический преобразователь [11] (рис. 4), в котором, вместо люминесцентного экрана устанавливается диафрагма с малым отверстием.

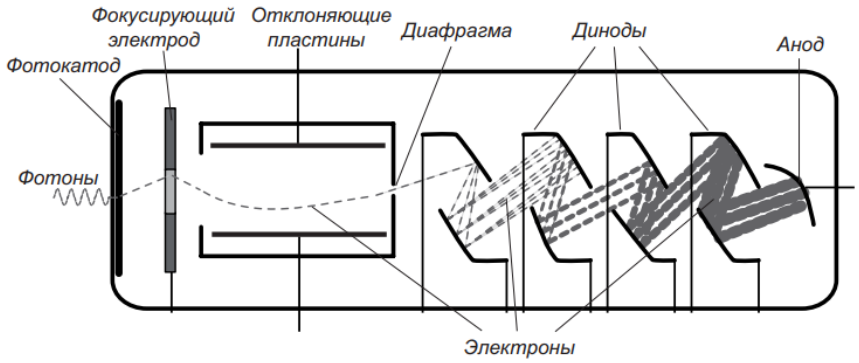


Рис. 4. Устройство диссектора

3. Стрик-камера – электронно-оптическая камера со скоростной разверткой, позволяющая диагностировать пучок заряженных частиц с пикосекундным временным разрешением, высокой частотой сканирования и высокой чувствительностью [12].

4. ПЗС-матрица – оптико-электронный преобразователь, формирующий двумерное изображение поперечного распределения плотности пучка заряженных частиц.

III. Электромагнитные датчики

Электромагнитные датчики основаны на эффекте возбуждения в них электромагнитного поля пролетающим пучком заряженных частиц. Физические характеристики поля несут информацию о параметрах пучка заряженных частиц. Перечисленные ниже датчики, нашли распространение практически на всех ускорителях заряженных частиц:

1. Резонаторный датчик – представляет собой замкнутый объем (напр. цилиндрический резонатор) с проводящими стенками, в которых возникают стоячие электромагнитные волны, возбуждаемые пучком заряженных частиц. По вза-

имодействию электромагнитной волны с пробным зарядом можно судить о параметрах пучка заряженных частиц.

2. Электростатический датчик – представляет собой систему из двух проводников, один из которых заземлен, а другой является сигнальным. Движущиеся заряды пучка индуцируют ток в цепи сигнального проводника, содержащей сопротивление нагрузки, на котором возникает напряжение, являющееся выходным сигналом датчика [8].

3. Магнитоиндукционный датчик. В магнитоиндукционном датчике проводник образует виток, в котором возникает электродвижущая сила, благодаря изменению потока магнитного поля, создаваемого движущимися зарядами пучка. В виток включено сопротивление нагрузки, с которого снимается сигнал датчика. Достоинством магнитоиндукционного датчика является нечувствительность к частицам пучка, попадающим в датчик, а также к вторичным электронам, выбиваемым частицами пучка из вакуумной камеры и тоже попадающим в датчик [8].

Заключение

Разнообразие методов контроля параметров заряженных частиц позволяет исследователям и разработчикам использовать тот, который наиболее подходит в конкретных случаях. Учитываются сложность, доступность, стоимость. Самым простым, с точки зрения используемой аппаратуры, смотрятся оптические методы контроля пучка заряженных частиц, т.к. оптические датчики взаимодействуют не с самим пучком, а с его синхротронным излучением.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. F. Watt, A.A. Bettiol, J.A. van Kan et al. // Int. Journal of Nanoscience, vol.4, No.3 (2005), pp. 269-286
2. Дмитриев С.Н., Реутов В.Ф. Ядерная физика и нанотехнология. Дубна: Изд. ОИЯИ, 2008. 73с
3. Пенионжкевич Ю.Э., Вахтель В.М. Современные ускорители заряженных частиц и их приложение. Воронеж, Изд. дом ВГУ, 2018
4. Флеров Г.Н. Вестник АН СССР. 1984; 4: 35.
5. Черняев А.П. Ускорители в современном мире. М.: МГУ, 2012. 368с.
6. Penionzhkevich Yu.E. Phys. At. Nucl. 2008; 71: 1127.
7. Ю. Э. Пенионжкевич. Современные ускорители заряженных частиц и их приложение. Вестник международной академии наук (Русская секция). Т.1. 2021. С.77-83.
8. Смалюк, В.В. Диагностика пучков заряженных частиц / Под ред. чл.-корр. РАН Н.С. Диканского. Новосибирск: Параллель, 2009. 294 с.
9. Гинзбург И.Ф., Коткин Г.Л., Сербо В.Г., Тельнов В.И. // Ядерная физика. 1983. Т. 38. С. 372–377.
10. Flyckt S.O., Marmonier C. Photomultiplier Tubes: Principles and Applications. Brive: Photonis, 2002.
11. Зинин Э.И. Стробоскопический метод электронно-оптической хронографии с пикосекундным разрешением на основе диссектора с электростатической фокусировкой и отклонением: Препр. ИЯФ СО АН СССР 81-84. Новосибирск, 1981.
12. Scheidt K. Review of Streak Cameras for Accelerators : Features, Applications and Results // Proc. of EPAC 2000. Vienna, Austria, 2000.

УДК 539.1.076
DOI 10.33764/2618-981X-2023-6-243-248

А. В. Топчиенко[1], Д.М. Никулин[1], В.В. Балакин[2,3]*

Проектирование оптической системы для диагностики параметров пучка заряженных частиц

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Институт ядерной физики им. Г. И. Будкера СО РАН, г. Новосибирск, Российская Федерация
[3] Новосибирский государственный технический университет, г. Новосибирск, Российская Федерация
*e-mail: A.V.Topchienko@inp.nsk.su

Аннотация. В связи со спецификой работы Инжекционного Комплекса ВЭПП-5 (Встречные Электрон-Позитронные Пучки) в Институте ядерной физики Сибирского отделения Российской академии наук (ИЯФ СО РАН) диагностика параметров пучков заряженных частиц является актуальной задачей. В настоящее время существует множество способов диагностики пучков заряженных частиц, которые делятся на три группы: контактные, электромагнитные и оптические. Выбран метод оптической диагностики по синхротронному излучению пучка заряженных частиц, так как данный метод является не деструктивным и не влияет на параметры пучка заряженных частиц. Целью статьи является проектирование оптической системы для диагностики пучка заряженных частиц на инжекционном комплексе ВЭПП-5. В статье рассматривается проектирование оптической системы в программе «Zemax». Определены обязательные технические требования и необходимые параметры для проектирования оптической системы.

Ключевые слова: инжекционный комплекс, контроль параметров пучка, оптическая система

A. V. Topchienko[1], D. M. Nikulin[1], V.V. Balakin[2,3]*

Optical System Design for Charge Particle Beam Parameters Diagnostic

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Budker Institute of Nuclear Physics of Siberian Branch Russian Academy of Sciences, Novosibirsk, Russian Federation
[3] Novosibirsk State Technical University, Novosibirsk, Russian Federation
* e-mail: A.V.Topchienko@inp.nsk.su

Abstract. Due to the specifics of the operation of the oncoming electron-positron beams-5 injection complex (VEPP-5) at the Institute of Nuclear Physics of the Siberian Branch of the Russian Academy of Sciences, diagnostics of parameters of charged particle beams is an urgent task. Currently, there are many ways to diagnose charged particle beams, which are divided into three groups: contact, electromagnetic and optical. The method of optical diagnostics based on synchrotron radiation of a charged particle beam is chosen, since this method is not destructive and does not affect the parameters of a charged particle beam. The purpose of this article is to design an optical system for diagnostics of a charged particle beam at the VEPP-5 injection complex. The article discusses the design of an optical system in the Zemax program. The mandatory technical requirements and necessary parameters for the design of the optical system are defined.

Keywords: injection complex, beam parameter control, optical system

Введение

Инжекционный комплекс ВЭПП-5 [1] является источником электронных и позитронных пучков для двух коллайдеров ИЯФ СО РАН – ВЭПП-4 [2] и ВЭПП-2000 [3].

Инжекционный комплекс состоит из электронной пушки, двух линейных ускорителей, конверсионной системы, накопителя-охладителя и транспортных каналов. Место установки оптической скамьи, на которой располагается оптическая система, показано красной линией (рис. 1).

Рис.1. Схема инжекционного комплекса ВЭПП-5

Производительность комплекса и эффективность работы зависит от параметров пучков заряженных частиц. К качеству пучков в современных ускорителях предъявляются высокие требования, поэтому эксплуатация ускорительных установок без точных и надежных систем диагностики пучка, обеспечивающих возможность регулярной настройки параметров ускорителя по результатам измерений, затруднительна.

Среди многообразия оптических методов [4] был выбран способ измерений поперечных размеров пучка заряженных частиц с помощью прибора с зарядовой связью (ПЗС-матрицы).

ПЗС-матрица представляет собой электронный прибор в виде двухмерной решетки из фоточувствительных элементов (пикселей), каждый из которых может регистрировать количество света, попавшего на его поверхность. При попадании света на пиксель его энергия переводится в электрический заряд, который затем с помощью электрических полей считывается и преобразуется в изображение [5].

Проектирование оптической системы

Для того, чтобы зарегистрировать пучок заряженных частиц, пролетающий в ускорителе необходимо разработать принципиальную оптическую систему установки с ПЗС-матрицей. К оптической системе для контроля пучка заряженных частиц предъявлялись следующие технические требования, которые должны быть соблюдены при ее проектировании [6]. Для измерения параметров поперечного пучка заряженный частиц используется ПЗС-матрица размером

6,784×5,427 мм. Из-за особенностей расположения магнитных элементов накопителя-охладителя присутствуют фиксированные расстояния от точки излучения синхротронного излучения до первого зеркала 500 мм и от первого зеркала до расположения второго зеркала 550 мм [7-9].

Расчет оптической схемы проводился по следующим формулам:

$$f'_{\text{экв.}} = \frac{f'_1 \cdot f'_2}{f'_1 + f'_2 - d'}, \quad (1)$$

где f'_1 – фокусное расстояние первого компонента; f'_2 – фокусное расстояние второго компонента; d – расстояние между компонентами.

$$d = 2f'\text{об}_{\text{экв}} \cdot tg\omega, \quad (2)$$

где $f'\text{об}_{\text{экв}}$ – эквивалентное фокусное расстояние объектива; $tg\omega$ – расходимость синхротронного излучения, излучаемого пучком заряженных частиц.

В ходе расчета получилось значение эквивалентного фокусного расстояния, равное 1500 мм.

В программе «Zemax» рассчитывались оптические параметры такие как фокусное расстояние, аберрации, отражение, преломление и многие другие. «Zemax» позволяет моделировать световые пучки, распространяющиеся через линзы и другие элементы оптических систем [10]. Редактор проектирования оптической системы представлен на рис. 2.

Тип	поверхности	Комментарий	Радиус		Толщина		Стекло		Полудиаметр	
OBJ	Стандартная		бесконечность		бесконечность				бесконечность	
1	Стандартная		бесконечность		500.000				1.966	
2	Разрыв ко..				0.000		-		0.000	
3*	Стандартная		бесконечность		0.000		MIRROR		30.000	U
4	Разрыв ко..				-550.000		-		0.000	
5	Разрыв ко..				0.000		-		0.000	
6*	Стандартная		бесконечность		0.000		MIRROR		30.000	U
7	Разрыв ко..				0.000		-		0.000	
8*	Стандартная		бесконечность		500.000				3.799	
9	Стандартная		бесконечность		0.000				4.671	
10*	Стандартная		97.050		4.000		LZ_K8		15.000	U
11*	Стандартная		-99.310		2.000		LZ_TF1		15.000	U
12*	Стандартная		-648.600		196.000				15.000	U
13	Разрыв ко..				0.000		-		0.000	
14*	Стандартная		бесконечность		0.000		MIRROR		20.000	U
15	Разрыв ко..				0.000		-		0.000	
16	Стандартная		бесконечность		-25.850	V			0.358	
STO	Стандартная		бесконечность		0.000				0.200	U
18*	Стандартная		-32.060		-7.000		LZ_TK2	S	7.811	U
19*	Стандартная		15.596		-3.000		LZ_TF1	S	7.811	U
20*	Стандартная		23.390		-218.684	M			7.811	U
IMA	Стандартная		бесконечность		-				2.650	

Рис. 2. Редактор оптической системы

С помощью программы «Zemax» изначально спроектировали параксиальную модель для проверки расчета. Впоследствии, вместо параксиальных компонентов, были вставлены реальные линзы. Представленная оптическая система с реальными компонентами приведена на рис. 3.

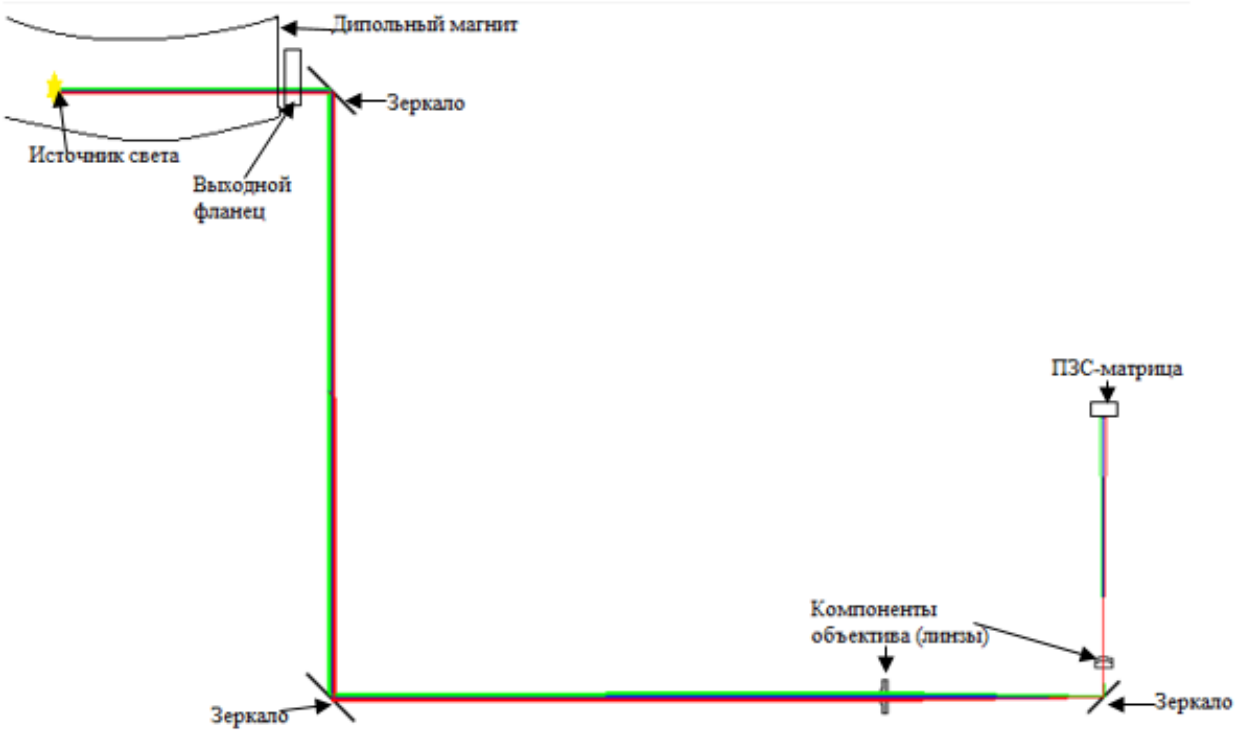


Рис. 3. Оптическая система для диагностики

На рис. 3 показана оптическая схема для диагностики пучка заряженных частиц. В дипольном магните синхротронное излучение, испущенное заряженными частицами, распространяется по касательной к траектории движения пучка заряженных частиц и через систему зеркал по средствам объектива фокусируется на ПЗС-матрице. Объектив состоит из двух компонентов для возможности изменения фокусного расстояния. Расчет показал размер изображения пучка заряженных частиц, равный 5,3 мм, что меньше минимального размера ПЗС-матрицы, что полностью соответствует поставленным требованиям.

Результаты и обсуждение

Был проведен анализ изображения пучка заряженных частиц (рис. 4).

Анализируя данную диаграмму, можно сделать вывод о том, что оптическая система дифракционно-ограниченная, среднеквадратичное значение радиуса много меньше радиуса кружка Эйри.

Спроектированная оптическая система была установлена на оптической скамье на накопителе-охладителе инжекционного комплекса ВЭПП-5 и получено изображение пучка позитронов на ПЗС-матрице (рис. 5).

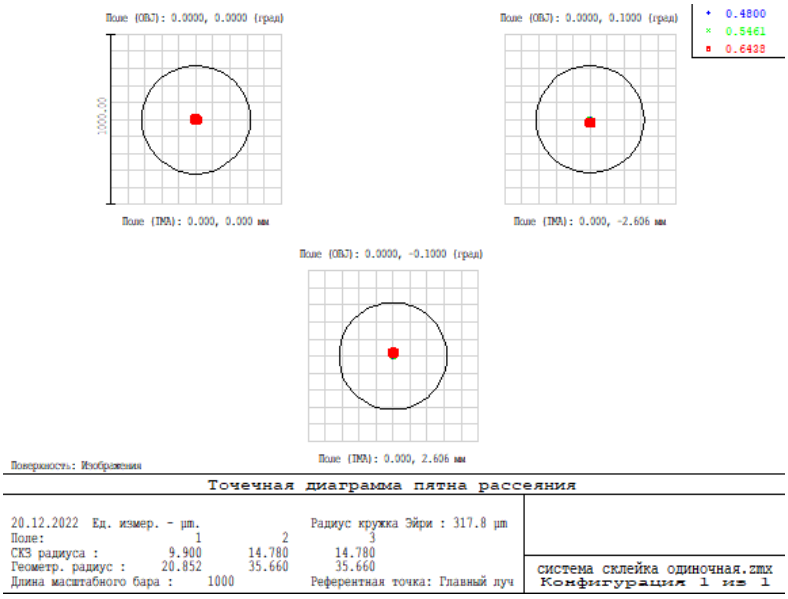


Рис. 4. Диаграмма пятна рассеяния

Рис.5. Зарегистрированное ПЗС-матрицей синхротронное излучение от пучка позитронов

Заключение

По заданным техническим требованиям была спроектирована оптическая система на накопителе-охладителе для диагностики пучков заряженных частиц. Оптическая система рассчитана в программе «Zemax», определены ее характерные параметры. Спроектированная оптическая система была установлена на оптической скамье инжекционного комплекса ВЭПП-5, получены первые результаты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Беркаев Д.Е. «VEPP-5 Injection Complex: two colliders operation experience», «Proc. IPAC'17. Paper WEP1K026. – Т №12 2017 г. – С. 2982-2984.

2. Левичев Е.Б. «Status and upgrade of the VEPP-4 storage-ring facility».Phys. Part. Nucl. Lett. 13. – Т №7 2016 г. С. 876-883.

3. Землянский И.М. «Commissioning of e+/e- transfer Line from BINP Injection Complex to VEPP-2000 Facility». «Proc. RuPAC'16. Paper TUPSA001» . – Т №6 2016 – С. 213-215.

4. Смалюк, В.В. Диагностика пучков заряженных частиц: под ред. чл.-корр. РАН Н.С. Диканского; Параллель, 2009. – 294 с.

5. Дубовик, А.С. Прикладная оптика : учебное пособие для вузов: издательство «Недра», 1989. – 612 с.

6. Мешков, О. Н. Методы оптической диагностики электрон-позитронных пучков и взаимодействия плазмы с сильноточным электронным пучком. Физика элементарных частиц и атомного ядра, Новосибирск – 2019 г. – Т. 43. – С. 451 – 499.

7. Михайлин В. В. Синхротронное излучение в спектроскопии : учебное пособие: московский государственный университет. — Москва : МГУ, 2011. – 164 с.

8. Свешникова, И.С. Расчет и проектирование оптических систем : учебник для вузов. – издательский центр «Логос» – Москва, 2000 – 189 с.

9. Старостенко, А.А. Статус и перспективы инжекционного комплекса ИЯФ: письма в ЭЧАЯ. – 2016. – Т. 13. – № 7. – С. 1493–1499.

10. Хацевич, Т.Н. Компьютерные методы проектирования оптических систем : учебник. – Новосибирск: СГУГиТ, 2022. – 156 с.

УДК 004.056
DOI 10.33764/2618-981X-2023-6-249-256

Е. П. Усольцева[1], А. В. Шабурова[1]*

Проблема экономической оценки эффективности затрат на защиту персональных данных

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: usoliz@yandex.ru

Аннотация. Защита персональных данных (далее – ПДн) является важнейшей частью защиты информации. С ростом числа кибератак и утечек данных стало крайне важно защищать ПДн от любого несанкционированного доступа или использования. Однако дать оценку экономической эффективности защиты ПДн не так просто. При подготовке к написанию данной статьи не было найдено единой общепринятой методики такой оценки. Для достижения цели исследования в ходе анализа литературы были рассмотрены различные методы экономической оценки эффективности затрат на защиту ПДн: сравнительный анализ, на основе количественной оценки риска информационной безопасности; показатели статистической меры на основе вероятностной модели исходов; метод анализа иерархий; экономико-математическая модель выбора оптимального набора технических средств защиты. В итоге был сделан вывод, что необходимо разработать такой метод экономической оценки эффективности затрат на защиту ПДн, чтобы лучше показать значимость выделяемых средств на защиту ПДн.

Ключевые слова: персональные данные, экономическая эффективность, информационная безопасность

E. P. Usoltseva[1], A. V. Shaburova[1]*

The Problem of Economic Evaluation of the Cost Effectiveness of Personal Data Protection

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: usoliz@yandex.ru

Abstract. Personal data protection (hereinafter referred to as PD) is an essential part of information security. With the increasing number of cyberattacks and data leaks, it has become extremely important to protect PD from any unauthorized access or use. However, it is not so easy to assess the economic effectiveness of PD protection. In preparation for writing this article, no single generally accepted methodology for such an assessment was found. To achieve the purpose of the study, during the analysis of the literature, various methods of economic evaluation of the cost effectiveness of PD protection were considered: comparative analysis, using a quantitative assessment of information security risk (hereinafter referred to as InfoSec); indicators of statistical measures based on a probabilistic outcome model; hierarchy analysis method; economic and mathematical model for choosing the optimal set of technical means of protection. As a result, it was concluded that it is necessary to develop such a method of economic assessment of the cost effectiveness of PD protection in order to show better the significance of the funds allocated for PD protection.

Keywords: personal data, economic efficiency, information security

Введение

В настоящее время ежедневно создается и обновляется огромное количество персональных данных (далее – ПДн). В связи с растущей тенденцией кибератак [1-3] и нарушений конфиденциальности [4] защита ПДн стала достаточно важной темой для субъектов ПДн, правительств и организаций по всему миру.

По данным исследований [5-7], утечки ПДн являются частой проблемой, которая может привести к краже личных средств с банковских счетов, взлому личных электронных почт и т.д. Например, в сфере здравоохранения отмечен рост количества утекших записей (за период январь-сентябрь 2021 г. – январь-сентябрь 2022 г.) (рис. 1).

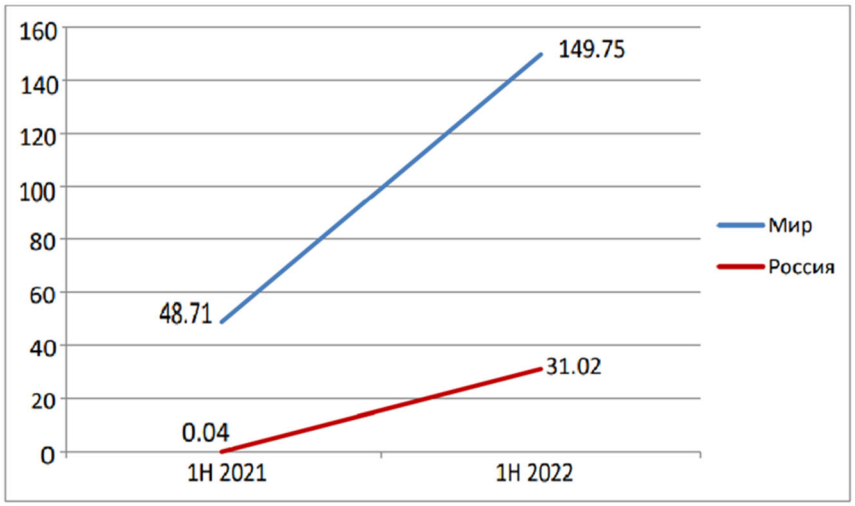


Рис. 1. Количество утекших записей в здравоохранении, млн [7]

Защита ПДн представляется важным фактором в обеспечении доверия граждан и сотрудников по отношению к организации. Как заявил президент компании Salesforce М. Бениофф [8]: «Доверие должно быть наивысшей ценностью в вашей компании, и если это не так, значит, случится что-то плохое». Защита ПДн является необходимым условием для поддержания доверия и сохранения репутации организации.

Примером того, как важно доверие к обеспечению конфиденциальности персональных данных, является ситуация с Агентством национальной безопасности США (АНБ) в 2016 [9], когда стала известно, что АНБ без согласия граждан массово собирали их данные, и эти действия были подвергнуты критике и затем была подана жалоба в суд [10].

В России же, можно привести пример утечек ПДн Яндекс.Еды и Delivery Club [11]. Реакция общественности на штраф в 60 тысяч рублей для такой крупной утечки вызвала резонанс в правительстве [12] и Минцифры совместно с государственными органами и бизнес-сообществом разрабатывают новую систему штрафов за утечку ПДн по словам заместителя директора Департамента обеспечения кибербезопасности Минцифры России Бадягиной А.М. [13].

Так же, оценка эффективности мер обеспечения безопасности ПДн, как правило, производится качественная, а не количественная, но такая оценка не показывает величину возможного материального ущерба, что было бы более наглядно для людей, не имеющих образования по информационной безопасности (далее – ИБ).

Цель статьи: показать, какие методы оценки эффективности затрат на защиту ПДн существуют и показать значимость защиты ПДн.

Методы и материалы

В результате проведенного анализа для описания проблемы авторами было обосновано использование следующих методов:

– метод сравнительного анализа, на основе количественной оценки риска ИБ, который показывает количественную, но не экономическую оценку эффективности;

– метод показателей статистической меры на основе вероятностной модели исходов, который позволяет учитывать разные состояния системы;

– метод анализа иерархий, который учитывает множество критериев и экспертное мнение;

– методический подход к экономической оценке внедрения технических средств защиты информации, который предлагает включение оценки срока окупаемости.

Материалами послужили научные статьи, статистические данные, аналитические исследования организаций, занимающихся ИБ.

Результаты

Согласно пп. 4 п. 2 ст. 19 152-ФЗ часть безопасности ПДн достигается, путем оценки эффективности мер, принятых для обеспечения безопасности ПДн до ввода информационной системы ПДн в эксплуатацию [14]. Не уточняется, что данная оценка должна быть количественная.

Оценка эффективности мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн, проводится не реже одного раза в три года в соответствии с приказом ФСТЭК России от 18.02.2013 №21 [15]. Так же не указывается, что нужно проводить количественную оценку.

Оценку эффективности систем защиты производили в научных публикациях [16-19].

В статье [16] предлагается оценивать эффективность мер с помощью сравнительного анализа эффективности системы защиты до и после реализации предложенных мер, с помощью количественной оценки риска ИБ. Для этого, авторы [16] выделяют четыре этапа (рис. 2).

Таким образом, реализация этапов позволит провести оценку эффективности предложенных мер защиты ПДн по критерию сравнительной оценки величины риска ИБ для ИСПДн [16]. Здесь же необходимо отметить, что экономиче-

скую оценку эффективности защиты ПДн авторы не предлагают, но метод важен с точки зрения учета оценки рисков в ИСПДн.

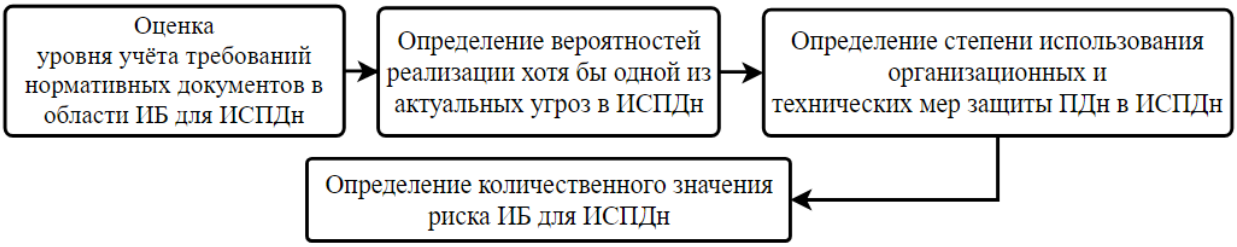


Рис. 2. Этапы оценки риска ИБ для ИСПДн [16]

В публикации [17] было предложено описывать показатели эффективности защиты информации статистической мерой, которая вычисляется с помощью использования вероятностной модели исходов. Так же, было предложено рассматривать разные состояния объектов информационных технологий (далее – ОИТ). Перечень этапов представлен на рис. 3 [17].

Рис. 3. Этапы метода на основе показателей статистической меры, включающей вероятностную модель исходов

С точки зрения обеспечения минимума среднего риска для организаций матрица потерь имеет значение при выборе того, как обеспечить защиту информации. Выбор и построение матрицы потерь – задача, зависящая от заданной цели. В зависимости от выбранных показателя эффективности и пороговой эффектив-

ности элементы матрицы потерь будут иметь различный физический смысл. Так авторы [17] приходят к выводу, что их метод позволяет развить комплексную систему защиты информации.

Авторы следующей статьи [18] предложили метод анализа иерархий. Суть метода состоит в декомпозиции задачи на более простые составные части и дальнейшей обработке последовательных суждений аналитика по парным сравнениям. Для этого, они разделяют метод на этапы (рис. 4).

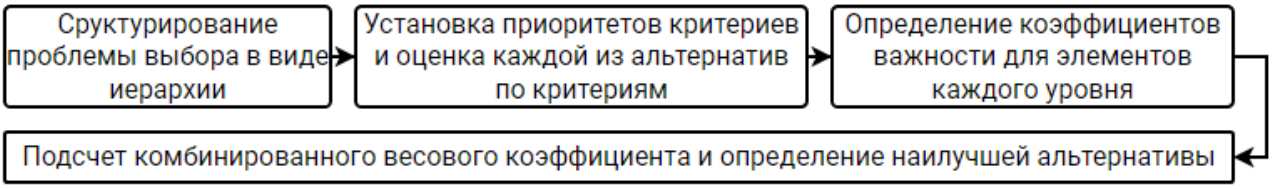


Рис. 4. Алгоритм применения метода анализа иерархий [18]

По мнению авторов [18], использование метода анализа иерархий имеет немало преимуществ. Они заключаются в четкой математической основе метода, легкости вычислительных алгоритмов, возможности изменения системы защиты ПДн, а также учёта множества критериев выбора. Кроме того, метод может быть реализован в программе для работы с электронными таблицами, что также является его достоинством.

В итоге авторы [18] приходят к выводу, что применение метода позволяет наглядно представить общую оценку с учётом выбранных альтернатив. Однако метод основан на экспертном мнении о важности предложенных в методе экономических коэффициентов, что не совсем верно, учитывая, что субъективный фактор может повлиять на точность оценки. Но экспертное мнение может быть важным при обсуждении достоверности полученных результатов.

В публикации [19] была построена экономико-математическая модель выбора оптимального набора технических средств защиты. Для этого метода авторы [19] предлагают следующие этапы (рис. 5).

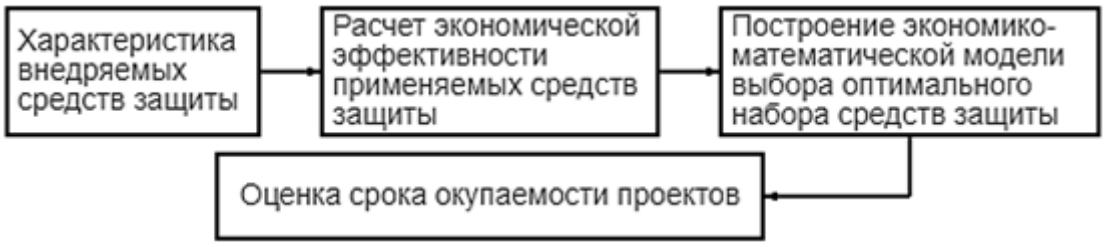


Рис. 5. Этапы методического подхода к экономической оценке внедрения технических средств защиты информации [19]

Расчет экономической эффективности внедряемых мер рассчитали на основе вероятности реализации угроз, путем умножения вероятности реализации

угроз на вероятность уязвимости актива и стоимость ценного актива. Вероятностные значения угроз и ущерба были получены экспертным путем и с использованием статистических данных.

На основе этого в статье [19] сопоставляют стоимость информации и величину возможного ущерба. Далее, была построена экономико-математическая модель выбора оптимального набора технических средств защиты. Затем была произведена оценка срока окупаемости приведенных средств защиты информации.

Метод авторов [19] может применяться для оценки целесообразности инвестиций в проекты с учетом ограничений бюджета, фиксированных затрат и возможной будущей прибыли организаций.

Обсуждение

При написании статьи были проанализированы подходы к оценке экономической эффективности защиты ПДн. Для сравнения были разработаны критерии, которые отображены в табл. 1. Таблица позволяет увидеть, что каждый метод не учитывает все из аспектов.

Таблица 1

Сравнительная таблица методов

Метод	Критерий сравнения					
	Учет требований законодательства	Оценка вероятности рисков ИБ	Стоимость ПДн	Экспертное мнение	Учет состояний ОИТ при воздействии угроз	Оценка срока окупаемости
Сравнительный анализ, с помощью количественной оценки риска ИБ	+	+	-	+	-	-
Показатели статистической меры на основе вероятностной модели исходов	-	+	-	-	+	-
Метод анализа иерархий	-	-	-	+	-	-
Методический подход к экономической оценке внедрения технических средств защиты информации	-	+	+	+	-	+

Учет требований законодательства требуется для учета несения возможной административной и уголовной ответственности за его несоблюдение [12, 14].

Оценка вероятности рисков нужна для оценки возмещения возможного ущерба при реализации таких рисков.

Стоимость ПДн важно учитывать, так как необходимо сопоставить адекватность затраченных средств на защиту ПДн со стоимостью ПДн [20].

Экспертное мнение требуется как при оценке рисков, так и при подведении итогов расчетов.

Учет состояний ОИТ при воздействии угроз так же важен, если, например, в организации или на предприятии имеется несколько баз ПДн и для них используются разные средства защиты.

Оценка срока окупаемости важна, если, к примеру, в данный момент затрачено много средств на защиту ПДн, например, для покупки бессрочной лицензии средства защиты, но далее амортизация такого средства приблизится к нулю.

Таким образом, можно сделать вывод, что нужно разработать такой метод, который учитывает все из выше приведенных аспектов, а именно:

– оценивает риски возникновения угроз на основании законодательства по ПДн;
– учитывает разные состояния ОИТ при воздействии угроз;
– учитывает стоимость (себестоимость) ПДн;
– оценивает сроки окупаемости купленных средств защиты информации.

Заключение

В данной статье авторами были рассмотрены методы оценки экономической эффективности защиты ПДн и сделан сравнительный анализ этих методов. Получен вывод, что необходимо создание метода, который бы включал в себе разные аспекты, указанные в обсуждении.

Важно помнить, что вложения в защиту персональных данных являются инвестицией, которая должна обеспечить надежность используемых средств защиты информации и доверие субъектов ПДн, а также защитить организации от штрафных санкций и прочей ответственности. Однако, даже при наличии надежной системы защиты ПДн необходимо постоянно ее совершенствовать и обновлять, учитывая новые угрозы и требования законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Актуальные киберугрозы: IV квартал 2022 года // Positive Technologies : [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/ (дата обращения: 13.04.2023).

2. Эксперты предсказали рост кибератак на российские компании в 2023 году. Число инцидентов увеличится минимум на 50% // РБК : [сайт]. – URL: https://www.rbc.ru/technology_and_media/13/10/2022/6346cdcc9a7947891c7fd5fc (дата обращения: 13.04.2023).

3. Число кибератак в России и в мире // TAdviser : [сайт]. – URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире (дата обращения: 13.04.2023).

4. Как крупные компании расплачиваются за нарушение конфиденциальности данных: 15 кейсов // RB.RU : [сайт]. – URL: https://rb.ru/story/15-privacy-violations/ (дата обращения: 13.04.2023).

5. РКН: 230 млн записей с личными данными россиян утекли в сеть с начала 2022 года // Коммерсантъ RU : [сайт]. – URL: https://www.kommersant.ru/doc/5559664 (дата обращения: 13.04.2023).

6. Group-IB: объём попавших в сеть персональных данных россиян в 2022 году вырос в 40 раз // Хабр : [сайт]. – URL: https://habr.com/ru/news/t/712488/ (дата обращения: 13.04.2023).

7. Утечки конфиденциальной информации в сфере здравоохранения, отчет за 9 месяцев 2022 г. // Экспертно-аналитический центр InfoWatch : [сайт]. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-konfidentsialnoy-informatsii-v-sfere-zdravookhraneniya.pdf (дата обращения: 13.04.2023).

8. IN SALESFORCE WE TRUST: HOW CULTURE FEEDS THE BOTTOM LINE / B. Smith / UpperEdge, 2019. URL: https://upperedge.com/salesforce/in-salesforce-we-trust-how-culture-feeds-the-bottom-line/ (дата обращения: 13.04.2023).

9. COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF / ACLU, 2006. URL: https://www.aclu.org/sites/default/files/images/nsaspying/asset_upload_file137_23491.pdf (дата обращения: 13.04.2023).

10. ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law // ACLU : [сайт]. – URL: https://www.aclu.org/press-releases/aclu-sues-stop-illegal-spying-americans-saying-president-not-above-law?redirect=cpredirect/23486 (дата обращения: 13.04.2023).

11. Утечка персональных данных Delivery Club, Яндекс.Еда. Минцифры предлагают штрафовать процентами от оборота за утечку ПДн // MaskSafe : [сайт]. – URL: https://masksafe.ru/news/all/utechka-personalnykh-dannykh-delivery-club-yandeks-eda-mintsifry-predlagayut-shtrafovat-protsentami (дата обращения: 13.04.2023).

12. Предложено наказывать оборотными штрафами компании, допускающие утечку персональных данных // Гарант : [сайт]. – URL: https://www.garant.ru/news/1603061/ (дата обращения: 13.04.2022).

13. Вебинар «Защита персональных данных» [видеозапись] // ВКонтакте : [сайт]. – URL: https://vk.com/rkn?z=video-76229642_456239441%2Fpl_-76229642_-2 (дата обращения: 13.04.2023).

14. Закон Российской Федерации «О персональных данных» от 27.07.2006 № 152 // Собрание законодательства Российской Федерации. – 2006 г. – № 31. – Ст. 3451 с изм. и допол. в ред. от 14.07.2022.

15. Приказ ФСТЭК РФ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21 // Банк данных «Приказы и распоряжения Министерства юстиции Российской Федерации». – 2013 г. – № 28375. – с изм. и допол. в ред. от 14.05.2020. – URL: https://minjust.consultant.ru/ (дата обращения: 13.04.2023).

16. Курачинова, М.Р. К вопросу об оценке эффективности принимаемых мер защиты персональных данных в информационных системах персональных данных / М.Р. Курачинова, А.А. Шхануков, Д.Е. Юдин // Студенческая наука для развития информационного общества. – 2018. – С.115-118.

17. Кулешов, Ю.Е. Методический подход к оценке эффективности защиты информации / Ю.Е. Кулешов, В.А. Сергиенко, С.И. Паскробка // Проблемы инфокоммуникаций. – 2018. – №1. – С.45-53.

18. Клиндух, О.В. Оценка эффективности защитных мер персональных данных в учебном заведении на основе метода анализа иерархий / О.В. Клиндух, А.А. Рычкова // Новые импульсы развития: вопросы научных исследований. – 2021. – №4. – С. 58-65.

19. Козьминых, С.И. Методический подход к экономической оценке внедрения технических средств защиты информации в кредитно-финансовой организации / С.И. Козьминых // Вопросы кибербезопасности. – 2020. – №3 (37). – С. 87-96.

20. Усольцева, Е.П. Проблема оценки стоимости персональных данных / Е.П. Усольцева, А.В. Шабурова // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 268-274.

УДК 004:378
DOI 10.33764/2618-981X-2023-6-257-262

Г. К. Фаршатов[1], П. Ю. Бугаков[1]*

Анализ применения экспертных систем при подготовке специалистов в области информационных технологий на базе СГУГиТ

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: farshatov-gk2022@sgugit.ru

Аннотация. Автоматизация различных сфер жизнедеятельности человека с использованием программно-аппаратных систем является важной задачей современного общества. Одним из распространенных типов систем, автоматизирующих умственную деятельность, являются экспертные системы. Данный тип систем позволяет аккумулировать знания в определенной отрасли и передавать их менее квалифицированным пользователям. Применение экспертных систем в образовании позволяет частично автоматизировать обучение. В связи с этим цель работы заключается в анализе применения экспертных систем при подготовке специалистов в области информационных технологий на базе СГУГиТ. Рассмотрены различные аспекты применения экспертных систем в образовании. Выделены основные требования, которым должна соответствовать экспертная система, применяемая в образовании. Проведен анализ возможности использования существующих программных решений. Сделан вывод об эффективности применения экспертных систем и необходимости разработки собственного решения в соответствии со сформированными требованиями.

Ключевые слова: экспертная система, обучающие программы, информация, оболочки, знания

G. K. Farshatov[1], P. Yu. Bugakov[1]*

Analysis of the use of expert systems in the training of specialists in the field of information technology on the basis of the SSUGT

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: farshatov-gk2022@sgugit.ru

Abstract. Automation of various spheres of human activity using software and hardware systems is an important task of current society. Expert systems are one of the widespread types of systems for automatization mental activity. This type of system allows to accumulate knowledge in a particular industry and transfer it to less qualified users. The use of expert systems in education makes it possible to partially automate training. In this regard, the purpose of the work is to analyze the use of expert systems in the training of specialists of information technology in SSUGT. Various aspects of the use of expert systems in education were considered. The main requirements that the expert system used in education should meet are highlighted. The analysis of the possibility of using existing software solutions is carried out. It is concluded that the use of expert systems is efficiently and it is necessary to develop own solutions in accordance with the formed requirements.

Keywords: expert system, tutorials programs, information, shells, knowledge

Введение

Одним из распространенных типов систем, автоматизирующих умственную деятельность, являются экспертные системы. Данный тип систем позволяет аккумулировать знания в определенной отрасли и передавать их менее квалифицированным пользователям. Применение данного типа систем позволяет существенно сократить расходы при обучении новых специалистов.

Образование является одной из крупных отраслей с ярко выраженной структурой, состоящей из небольшого количества экспертов (преподавателей) и значительно большего количества людей, формирующих свой квалификационный уровень в процессе обучения (студентов). Применение экспертных систем в образовании может частично автоматизировать процесс обучения, что, в свою очередь, будет способствовать уменьшению нагрузки на преподавателей и сохранению качества обучения в целом. Однако на текущий момент использование экспертных систем в образовании является достаточно редким.

В связи с этим, целью работы является анализ применения экспертных систем при подготовке специалистов в области информационных технологий на базе СГУГиТ.

Методы и материалы

Помимо экспертных систем существует множество различных электронных обучающих программ. В процессе их использования был выявлен ряд проблем. Рассмотрим более подробно основные из них:

1. Многие обучающие программы линейного или разветвленного типа рассчитаны на подачу в виде курса, когда теоретический материал сопровождается практическими заданиями для проверки понимания материала. Любой курс рассчитан на определенный начальный уровень знаний обучающегося. При этом могут возникать ситуации, в которых обучающийся не знает определенного материала, на который ссылается курс. В связи с этим возникают проблемы с освоением курса или необходимость использовать дополнительные источники. В экспертных системах важной характеристикой является наличие подсистемы выводов, которая отображает на основе каких знаний был получен ответ.

2. В привычных обучающих программах информация, хранимая в программе, строго формализирована и не позволяет формировать индивидуальные ответы на возникший у обучающегося вопрос. Более того, существуют ситуации, когда обучающийся в силу отсутствия опыта не совсем понимает как правильно сформулировать вопрос, где именно необходимо искать ответ, особенно если проблема касается сразу нескольких разделов учебного материала. Экспертная система способна формировать выводы на основе множества знаний и в некоторой степени воспринимать вопросы в более свободной форме. За счет данной особенности обучающемуся легче искать информацию в системе, а в силу развитых механизмов формирования результата полученный вывод получается более подробным и точным.

3. Большинство обучающих программ может содержать «лишнюю» информации, в зависимости от имеющегося уровня подготовки обучаемого. Данная проблема возникает, с одной стороны, из-за имеющихся у обучающегося знаний

в той или иной предметной области, а с другой – из-за излишне детализированного пояснения учебного материала, содержащегося в учебной программе. Экспертная система позволяет подготавливать материал таким образом, чтобы в нем было минимизировано количество лишней информации, а при необходимости дополнительная информация может быть получена из подсистемы пояснений.

4. Классические обучающие программы зачастую основаны на едином суждении, а следовательно, и способе передачи знаний. Отсутствие множества мнений влечет за собой одностороннее освещение учебного материала. Кроме того, для некоторых обучающихся информация, предоставляемая программой, может быть понятна и очевидна, но для других стиль изложения или форма представления учебного материала могут показаться излишне сложными. Экспертные системы позволяют аккумулировать множество формулировок одного и того же материала, что способствует повышению качества его восприятия и развитию критического мышления обучающегося.

Результаты

Учитывая все особенности применения обучающих экспертных систем, можно сформировать следующие требования для их использования в СГУГиТ.

1. Поскольку форма преставления учебного материала может сильно варьироваться, то необходимо обеспечить гибкость в отношении интерфейса пользователя и видов хранимой информации. Экспертная система должна иметь функционал для хранения информации различных типов таких как: тексты, изображения, видеофайлы, а также различные файлы пользовательских форматов. Помимо хранения данных необходимо обеспечить их корректное отображение на уровне интерфейса. Данные могут иметь различные сложные связи и ссылки между собой. В связи с этим экспертная система должна иметь высокую вариативность в разрезе формата вывода информации.

2. Пользователями экспертной системы являются студенты. Многие проблемы, возникающие при обучении, могут коррелировать друг с другом. Из-за этого большое количество знаний, хранимых в системе, могут подходить под одинаковую формулировку изучаемого вопроса. В таких ситуациях экспертная система должна не только предоставить возможность ознакомиться со всеми подходящими знаниями, но и уметь со временем адаптироваться под запросы обучающихся.

3. Экспертами для данной системы выступают преподаватели. Они не всегда могут обладать четким пониманием как должны быть представлены их знания в системе. Вследствие этого необходимо, чтобы экспертная система обладала инструментами для взаимодействия экспертов-преподавателей с административным персоналом, способным помочь решить проблемы с добавлением тех или иных знаний.

4. Поиск информации в экспертной системе должен осуществляться в достаточно простой форме. Удобным с точки зрения студента форматом поиска знаний в системе является «строка поиска», подобная поисковым сервисам Google или Яндекс [1, 2]. При этом необходимо учесть, что пользователь зача-

стую может не совсем корректно понимать в чем именно заключается проблема. Поэтому поиск должен обладать элементами обучения, позволяющими адаптировать систему под обучающегося и формулировать более информационно емкие релевантные результаты.

Готовых решений в области обучающих экспертных систем практически нет. Существуют различные локальные решения, применяемые в конкретных университетах. К примеру, Chopin в АлтГТУ и Formula Tutor в СПбГУ [3, 4]. Данные решения являются проприетарным продуктом для конкретных университетов и не представлены к публичному ознакомлению. В целом, говоря о готовых решениях в области обучающих экспертных систем, можно сделать вывод об их практическом отсутствии на рынке [5–7].

Кроме готовых решений существуют оболочки экспертных систем, позволяющие частично настроить экспертную систему в соответствии с необходимыми требованиями и наполнить базу знаниями в определенной предметной области. Наиболее распространенными из них являются Crystal, «Малая Экспертная Система 2.0», CLIPS, ARITY Expert Development Package, AION, ECLIPSE.

Crystal работает на персональных компьютерах и снабжена интеллектуальным интерфейсом. Имеется возможность создания гибридных экспертных систем. В состав оболочки включена обширная библиотека встроенных функций. Интерфейс разработчика: меню, редактор баз знаний, графические средства, средства подготовки текстовых файлов и экранов, средства трассировки и отладки. В базу знаний может входить не более 300 правил [8].

Программа «Малая Экспертная Система 2.0» представляет из себя простую оболочку экспертной системы, на основе байесовской системы логического вывода. Оболочка предназначена для проведения консультации с пользователем в какой-либо прикладной области с целью определения вероятностей возможных исходов и использует для этих целей оценку правдоподобности некоторых предпосылок, которые система получает от пользователя [9].

CLIPS – интегрированная производственная С-подобная языковая система, разработанная в Космическом центре NASA с 1985 по 1996 год. Она представляет собой язык программирования на основе правил, предназначенный для создания экспертных систем и других программ, ориентированных на эвристическое решение задачи [10].

ARITY Expert Development Package – это экспертная система, которая интегрирует продукционное и фреймовое представления знаний с различного рода коэффициентами уверенности [8].

AION – система разработки программ, адаптированная для работы на различных программно-аппаратных платформах. Она включает в себя объектно-ориентированное представление знаний, прямой, обратный, двунаправленный поиск решения, а также правила сопоставления с образцом, графику, запросы на/из других языков, а также графический интерфейс пользователя [8].

ECLIPSE система для персональных компьютеров. Синтаксис языка, используемого в пакете, совместим с языком системы CLIPS, разработанной для

NASA. Отличия заключаются в управлении данными путем сопоставления с образцом, использовании прямого и обратного вывода, в поддержке множества целей, объектно-ориентированном представлении знаний и интегрировании с dBase.

В целом все рассмотренные оболочки обладают рядом недостатков, не позволяющих применить их на базе СГУГиТ. К наиболее важным недостаткам стоит отнести:

– отсутствие развитых современных средств для создания дружественного интерфейса взаимодействия с пользователем;
– невозможность прикреплять к выводам дополнительные медиафайлы;
– множество ограничений, касающихся формирования базы знаний;
– строго формализированные формы для ввода вопроса пользователя;
– отсутствие обучения на основе взаимодействия системы с пользователем.

Заключение

В результате выполнения анализа применения экспертных систем для подготовки специалистов в области информационных технологий можно сделать вывод о достаточно высокой эффективности рассматриваемого технологического решения для данной отрасли. При этом на текущий момент существуют только проприетарные продукты с ограниченным функционалом, разработанные для использования в определенной организации / университете. Также отсутствуют программные продукты (оболочки экспертных систем), с помощью которых можно осуществить разработку экспертной системы, соответствующей поставленным требованиям.

В настоящее время в СГУГиТ направление подготовки обучающихся 09.03.02 Информационные системы и технологии является одним из наиболее востребованных среди абитуриентов. В связи с этим можно сделать вывод о том, что разработка обучающей экспертной системы для поддержки процесса подготовки студентов в области информационных технологий с учетом всех поставленных требований может рассматриваться как технически осуществимая и востребованная.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Google [Электронный ресурс] // Google. – Режим доступа: https://www.google.ru/ (дата обращения 15.04.2023).

2. Яндекс [Электронный ресурс] // Яндекс. – Режим доступа: https://ya.ru/ (дата обращения 15.04.2023).

3. Экспертная система для обучения [Электронный ресурс] // Д.В. Смолин. – Режим доступа: http://sdv56.narod.ru/DOCS/DOC/vipes.htm (дата обращения 15.04.2023).

4. Столяров А.И. Генерация тестовых заданий в экспертно-обучающих системах : научная статья // Вестник российского университета дружбы народов. Серия: информатизация образования. -Москва : Российский университет дружбы народов, 2012 - 47-60 с. -ISSN: 2312-864X.

5. Молчанов А.А Использование экспертных систем в системе открытого образования : научная статья // Психолого-педагогический журнал гаудеамус -Тамбов : Тамбовский государственный университет имени Г.Р. Державина, 2014. - 57-68 с. -ISSN: 1810-231X.

6. Каримова П.М. Применение экспертной системы в образовании // Вестник таджикского национального университета -Москва : Московский институт стали и сплавов, 2020 - 191-195 с. -ISSN: 2074-1847.

7. Шкурская Н М. Обучающие и экспертные системы : учебное пособие / Шкурская Н М. - Минск : Белорусский государственный университет, 2016. - 51 с.

8. Экспертные системы. [Электронный ресурс] – Режим доступа: http://bourabai.ru/alg/expert22.htm (дата обращения 15.04.2023).

9. CLIPS: A Tool for Building Expert Systems [Электронный ресурс] // Secret Society Software, LLC. – Режим доступа: https://clipsrules.net/ (дата обращения 15.04.2023).

10. Столяров А.И. Опыт применения оболочки «Малая экспертная система 2.0» для создания системы медицинской диагностики [Электронный ресурс] // Магнитогорский государственный технический университет имени Г.И. Носова. – Режим доступа: https://technology.snauka.ru/2016/12/11465 (дата обращения 15.04.2023).

УДК 528.71
DOI 10.33764/2618-981X-2023-6-263-267

Д. Л. Фишев[1], С. Н. Новиков[1,2]*

Анализ и оценка ситуации на рынке информационной безопасности в условиях санкционного давления на Российскую Федерацию

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: dvs2954@mail.ru

Аннотация. Данная статья рассматривает текущую ситуацию на рынке информационной безопасности в России в условиях санкционного давления на страну. Анализируются основные вызовы, стоящие перед российскими компаниями в области информационной безопасности, и делается вывод о необходимости разработки эффективных мер по защите информации. Одним из основных трендов является увеличение спроса на услуги по защите данных и информации, но вызовы связаны с отсутствием квалифицированных специалистов в этой области и недостаточным развитием рынка информационной безопасности. В статье предлагается ряд рекомендации по улучшению ситуации с отсутствием квалифицированных специалистов и по исправлению ситуации недостаточного развития российского рынка информационной безопасности. В целом, статья является актуальной и полезной для понимания текущей ситуации на рынке информационной безопасности в России.

Ключевые слова: информационная безопасность, анализ статистических данных, SWOT-анализ

D. L. Fishev[1], S. N. Novikov[1]*

Analysis and Assessment of the Situation on the Information Security Market in the Context of Sanctions Pressure on the Russian Federation

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: dvs2954@mail.ru

Abstract. This article examines the current situation in the information security market in Russia under sanctions pressure on the country. The main challenges facing Russian companies in the field of information security are analyzed, and a conclusion is made about the need to develop effective measures to protect information. One of the main trends is an increase in demand for data and information protection services, but the challenges are related to the lack of qualified specialists in this field and insufficient development of the information security market. The article offers a number of recommendations to improve the situation with lack of qualified specialists and to remedy the situation with insufficient development of Russian information security market. In general, the article is relevant and useful for understanding the current situation on the information security market in Russia.

Keywords: information security, statistical data analysis, swot-analysis

Введение

В результате беспрецедентного санкционного давления на Российскую Федерацию вопросы информационной безопасности (далее – ИБ) становятся еще более актуальными. Шквал кибератак и утечки данных могут нанести значительный ущерб как государству, так и отечественным компаниям в целом. Поэтому для разработки эффективных мер по защите информации необходимо проанализировать и оценить рынок ИБ. В данной статье мы проанализируем текущее состояние рынка ИБ на фоне влияния санкций на Российскую Федерацию и рассмотрим основные вызовы, которые стоят перед российскими компаниями в области ИБ.

Методы и материалы

Для анализа и оценки состояния рынка ИБ под давлением санкции против Российской Федерации были использованы следующие научные методы:

1) анализ статистических данных. Были обобщены и проанализированы данные о количестве кибератак и обнаружений уязвимостей программного обеспечения на российскую информационную инфраструктуру (рис. 1);

2) SWOT-анализ. Для определения сильных и слабых сторон российского рынка ИБ, а также возможностей и угроз был проведен SWOT-анализ (табл. 1). Исследования основываются на анализе статей крупных информационно-аналитических компаний, специализирующихся на вопросах ИБ [1 – 3].

Результаты

Анализ статистических данных показал, что с момента начала специальной военной операции в 2022 году количество инцидентов увеличилось на 80 %. Порядка 98 % веб-приложений подвержены кибератакам, утечки данных выявлены в 90 % приложений [1, 4]. Кибератаки направлены на информационную инфраструктуру как в частном, так и в государственном секторах. Так, каждая четвертая компания потеряла от них от 1 млн. до 500 млн. рублей. При мониторинге инцидентов кибератак в России показатели с каждым кварталом увеличиваются [5].

В нынешней ситуации санкции, наложенные англосаксонским миром на Российскую Федерацию, привели к серьезным проблемам ИБ для российских компаний. В частности, многие западные компании, работавшие в России, перестали оказывать услуги отечественным компаниям, что привело к определенному дефициту [6]. В этой связи отечественные компании были вынуждены обратиться к российским разработчикам решений и поставщикам услуг ИБ. Отметим, что российские компании не всегда готовы предоставить потребителям высококачественные услуги сферы ИБ. Это объясняется тем, что наш, отечественный рынок решений в сфере ИБ все еще не развит достаточно хорошо, что отчасти объясняется отсутствием квалифицированных специалистов в данной области [7].

Как указано выше, одной из основных проблем российского рынка ИБ является нехватка квалифицированных специалистов в этой области. В результате многие компании-потребители услуг ИБ не могут должным образом защитить

свою информацию. Также огромной проблемой для российского рынка ИБ является недостаточное развитие инфраструктуры. Это факт приводит к тому, что многие отечественные компании вынуждены посредством серого импорта обращаться к западным поставщикам услуг сферы ИБ, что является проблемой в нынешних условиях.

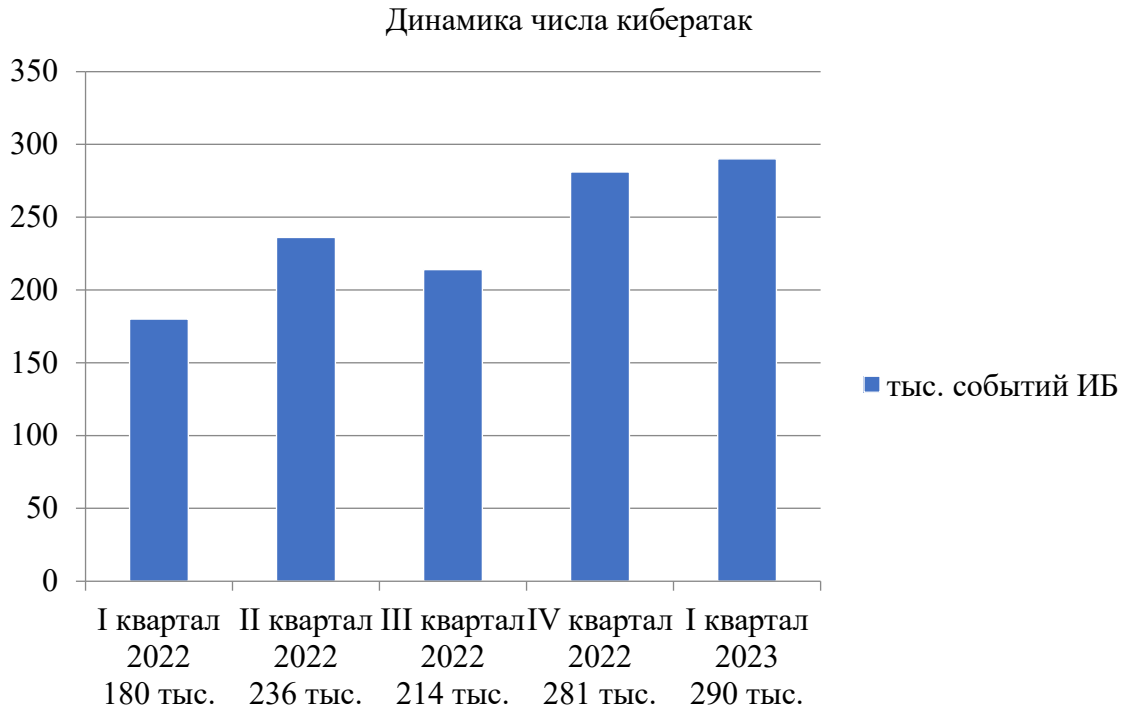


Рис. 1. Сводная статистика по событиям кибертатак

Таблица 1

SWOT-анализ для выявления сильных и слабых сторон российского рынка ИБ

Сильные стороны:	Слабые стороны:
– высокий уровень технической экспертизы и компетенции в области кибербезопасности; – наличие крупных компаний, специализирующихся на ИБ; – наличие сильных технических университетов и научных центров, занимающихся проблемами ИБ.	– нехватка квалифицированных специалистов по ИБ; – не достаточно хорошо развита инфраструктура для обеспечения ИБ; – недостаточная государственная поддержка отрасли; – отсутствие финансирования и инвестиций в отрасль.
Возможности:	Угрозы:
– рост спроса на услуги по обеспечению ИБ в связи с увеличением количествакибератак и угроз; – развитие новых технологий в области кибербезопасности.	– санкции и ограничения на международное сотрудничество; – усиление кибератак и угроз из-за рубежа и киберпреступников; – недостаточная осведомленность пользователей о необходимости обеспечения ИБ.

Для решения проблемы дефицита квалифицированных специалистов на рынке ИБ первым шагом следует провести унификацию образования в России, то есть выход из Болонской системы высшего образования. Тем самым будущее за нашей собственной уникальной системой образования, в основе которой будет лежать интересы национальной экономики и безопасности. Вторым шагом следует рассмотреть вопрос увеличения бюджетных ассигнований федерального бюджета, тем самым разработать и нарастить количество профильных образовательных программ, чтобы готовить различных экспертов, а не одинаковых кадров. Также можно увеличить возможность получения образования на коммерческой основе за счет средств предприятий и организаций. Третьим шагом следует рассмотреть вопрос, чтобы у новых специалистов появилась заинтересованность в сфере ИБ. Для этого привлекать экспертов ведущих компаний по ИБ читать лекции и рассказывать о деятельности компаний, выдавать гранты на обучение с возможностью стажировки и предоставлением рабочих мест после окончания университетов. Четвертым шагом в этом вопросе стоит рассмотреть возможность улучшения условии труда путем увеличения заработной платы.

Также оценивая рынок ИБ России в настоящее время, для его развития следует продумать вопросы поддержки отечественных компаний, чтобы у них была возможность развивать свои новые технологии, тем самым сделать их конкурентоспособными на мировом рынке [8]. С уходом зарубежных компаний освободились ниши, которые теперь могут занять российские компании [9]. Важно также укреплять законодательство в сфере ИБ, чтобы защитить права и интересы пользователей и компаний. При этом необходимо создавать специальные законы.

Цель данных мер заключается в том, чтобы достичь большого прогресса в защите информации и в борьбе с киберугрозами на территории Российской Федерации.

Заключение

Таким образом, можно сделать следующие выводы, что основной тенденцией российского рынка ИБ является рост спроса на услуги по защите информации. Однако проблемами являются дефицит квалифицированных специалистов и неразвитость российского рынка ИБ.

В целом, для развития российского рынка ИБ необходимо принять ряд мер, которые будут направлены на создание благоприятной среды для развития компаний, повышение квалификации специалистов, расширение научно-исследовательской базы, поддержку государства и укрепление законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Актуальные киберугрозы: итоги 2022 года. – Текст: электронный //Российская компания, специализирующаяся на разработке решений в сфере информационной безопасности: [ptsecurity.com] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 05.05.2023).

2. Информационная безопасность (рынок России). – Текст: электронный // Портал выбора технологий и поставщиков: [www.tadviser.ru]. – URL:https://www.tadviser.ru/in-

dex.php/Статья:Информационная_безопасность_(рынок_России)?ysclid=lhk98voole825367744 (дата обращения: 05.05.2023).

3. Анализ российского рынка информационной безопасности. – Текст: электронный // Независимый российский информационно-аналитический центр: [anti-malware.ru.] - URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-InfoSec-Market/ (дата обращения: 05.05.2023).

4. ТАСС: информационное агентство России: [www.tass.ru]. – Москва, 1999 –URL: https://tass.ru/ekonomika/15562907?ysclid=lhk8w4dtk3645727213 (дата обращения: 05.05.2023). – текст: электронный.

5. Кибератаки на российские компании 1 квартал 2023 года. – Текст: электронный//Комплекссервисов для защиты каналов связи, защиты от угроз кибербезопасности: [rt-solar.ru] - URL:https://rt-solar.ru/upload/iblock/ad3/3j9s24qws3lcnjmoilaowut9afff7jco/Otchet-Kiberataki-na-rossiyskie-kompanii-v-I-kvartale-2023-goda.pdf?ysclid=lhk3th3pbq873211372 (дата обращения: 05.05.2023).

6. Едакин А. Какие интернет-компании ушли из России? Последствия и альтернативы. - Тест: электронный // Тендерная площадка: [Workspace.ru] – URL: https://workspace.ru/blog/exodus-of-companies/ (дата обращения: 06.05.2023).

7. Гиацинтова С.Т. Актуальные аспекты управления персоналом в IT-компаниях // Управление человеческим потенциалом. – 2009. – № 2. – с. 146-149.

8. Постановление Правительства РФ от 06.04.2022 №598 «О внесении изменений в Правила предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий». Правительство РФ. – текст: электронный.

9. Аллуш Мухамед Фехд. Влияние санкций на рынок ИТ // Материалы IX Международной студенческой научной конференции. Студенческий научный форум. - (дата обращения: 10.05.2023). – текст: электронный.

УДК 006:331.1
DOI 10.33764/2618-981X-2023-6-268-276

А. С. Фролов[1], Е. А. Усанькова[1]*

Управление развитием персонала метрологической службы на основе мотивации

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: a.frolov99950@gmail.com

Аннотация. Развитие персонала – важнейшая часть управления организацией. Управление развитием персонала является необходимым элементом эффективного управления бизнесом и является ключевым фактором обеспечения успеха на современном рынке. Для развития личностных качеств работников в метрологической лаборатории подходит хорошо подобранная система мотивации сотрудников. Чтобы сотрудники были мотивированы принести качественные и своевременные результаты, им нужно давать возможность раскрыть свой потенциал в полной мере. Правильно выбранная стратегия мотивации сотрудников может преподнести отличные результаты и спланировать развитие организации на далекое будущее. В организациях вроде метрологической лаборатории ООО «ЦСМ» с небольшим количеством сотрудников возникают проблемы с подбором персонала, способного развиваться, учиться и показывать необходимые для руководства результаты. Для того чтобы решать эти проблемы руководство компании внедряет и использует различные формы мотивации. Важной частью мотивационной составляющей любой компании является текучесть персонала. Результаты исследования текучести персонала метрологической лаборатории показывают хорошо подобранную руководителями ООО «ЦСМ» систему мотивации, благодаря которой сотрудники могут показывать отличные результаты в своей работе. Эффективное развитие и управление персоналом возможно благодаря правильно выбранному стилю руководства, исходя из особенностей коллектива и правильно подобранной форме мотивации труда. Управление развитием персонала в центре сертификации и метрологии на основе мотивации включает в себя комплекс мер, направленных на создание условий для профессионального роста и развития каждого сотрудника. Важным аспектом является индивидуальный подход и учет потребностей и интересов каждого сотрудника, а также создание команды, способной достичь высоких результатов в работе лаборатории.

Ключевые слова: мотивация, управление, персонал

A. S. Frolov[1], E. A. Usankova[1]*

Management of Metrological Service Personnel Development Based on Motivation

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: a.frolov99950@gmail.com

Abstract. Personnel development is an essential part of the organization's management. Personnel development management is a necessary element of effective business management and is a key factor in ensuring success in the modern market. A well-chosen employee motivation system is suitable for the development of personal qualities of employees in a metrological laboratory. In order for employees to be motivated to bring high quality and timely results, they need to be given the opportunity to reach their full potential. A well-chosen employee motivation strategy can bring excellent

results and plan the development of the organization for the distant future. In an organization like the metrological laboratory of CSM LLC with a small number of employees, problems arise in the selection of personnel who are able to develop, learn and show the results necessary for management. In order to solve these problems, the company's management implements and uses various forms of work motivation. An important part of the motivational component of any company is staff turnover. The results of the study of the staff turnover of the metrological laboratory show a well-chosen motivation system by the managers of CSM LLC, thanks to which employees can show excellent results in their work. Effective development and personnel management is possible thanks to a properly chosen leadership style based on the characteristics of the team and a properly selected form of labor motivation. Motivation-based personnel development management at the certification and metrology center includes a set of measures aimed at creating conditions for professional growth and development of each employee. An important aspect is an individual approach and consideration of the needs and interests of each employee, as well as the creation of a team capable of achieving high results in the laboratory.

Keywords: motivation, management, personnel

Введение

Руководители современных компаний постоянно задумываются над эффективностью развития персонала, причем именно это направление играет значительную роль в развитии бизнеса [1]. Опыт многих компаний показывает, что инвестиции в новое оборудование не всегда приносят повышение производительности труда и прибыли, если наряду с этим не учитывать «человеческий фактор». Вклад в человеческий фактор, предполагает крупные вложения в развитие персонала - это обучение и развития сотрудников организации, направленных на повышение их профессионального уровня, улучшение качества работы и достижение более высоких результатов [2]. Этот процесс может включать в себя обучение новым навыкам, повышение квалификации, тренинги для развития мягких навыков, таких как коммуникативные и лидерские, а также многое другое. Целью развития персонала является обеспечение эффективной работы организации и поддержание конкурентоспособности на рынке [3].

Тема управления развитием персонала является актуальной для метрологических организаций, которые борются за конкурентное преимущество друг с другом. Одно из главных конкурентных преимуществ - это наличие квалифицированного персонала, способного быстро адаптироваться к новым условиям рынка и динамично развиваться.

Управление развитием персонала позволяет метрологическим организациям обеспечивать своих сотрудников всем необходимым для успешной работы, таким как знания, навыки, опыт и мотивацию. Кроме того, управление развитием персонала позволяет предсказать потребности компании в персонале на будущее и составить план развития и обучения сотрудников соответствующим образом [4].

В целом, управление развитием персонала является необходимым элементом эффективного управления бизнесом и является ключевым фактором обеспечения успеха на современном рынке [5].

Некоторые компании считают, что обучение и развитие сотрудников – это ненужная траты времени и денег. Это мнение основывается на проблемах, с ко-

торыми сталкиваются компании при постановке вопроса о грамотном и правильном управлении развитием персонала:

– неподготовленность руководства. Часто руководители не имеют достаточных знаний и навыков для эффективного управления персоналом. Отсутствие квалифицированных кадров, способных проводить обучение и развитие сотрудников, также может стать проблемой;

– отсутствие планирования. Многие компании не имеют четкого плана развития персонала на долгосрочную перспективу. Это может привести к тому, что сотрудники не получают необходимых навыков и знаний для достижения более высоких результатов;

– ограниченный бюджет на развитие персонала. Некоторые компании могут ограничивать бюджет на обучение и развитие сотрудников, что может стать препятствием на пути развития персонала;

– неверная оценка потребностей персонала в обучении и развитии. Некоторые компании могут не оценивать достаточно точно потребности своих сотрудников в обучении и развитии. Это может привести к ненужным тратам времени и ресурсов на обучение, которое не приносит реальной пользы сотрудникам;

– несвоевременная реакция на изменения в компании и рынке. Развитие персонала должно быть гибким и адаптивным к изменениям в компании и на рынке. Если компания не реагирует своевременно на эти изменения, то сотрудники могут терять актуальные знания и навыки и становится менее конкурентоспособными [6].

Без разрешения данных проблем и без развития персонала компания не сможет достичь высоких результатов на рынке.

Концепция управления развитием персонала является относительно новой и широко обсуждается в последние годы. В связи с быстро меняющейся экономической и технологической средой компании осознают необходимость управления развитием своего персонала для того, чтобы быть конкурентоспособными.

Новизной в этой теме является переход от традиционного обучения и развития персонала к системному подходу, который включает в себя оценку потребностей в развитии персонала, планирование развития, разработку программ обучения, оценку результатов и корректирование действий.

Новой тенденцией является обращение большего внимания не только на развитие профессиональных навыков, но и личностному развитию персонала, включая развитие социальных и мягких навыков, таких как коммуникативные умения, руководство и управление конфликтами.

Таким образом, управление развитием персонала становится все более комплексным и включает в себя множество подходов и методик, направленных на достижение более высокой эффективности в управлении персоналом и повышении уровня конкурентоспособности компаний [7].

Методы и материалы

Для развития личностных качеств работников в метрологической организации ООО «ЦСМ» (Центр Сертификации и Метрологии) подходит хорошо подобранная система мотивации сотрудников.

Управление развитием персонала в метрологической организации на основе мотивации подразумевает использование эффективных механизмов и методов (внутренних и внешних), которые помогут мотивировать сотрудников к достижению высоких результатов (рис. 1).

Рис. 1. Внутренние и внешние механизмы и методы мотивации труда

В метрологических лабораториях важно уделять внимание мотивации персонала. Чтобы сотрудники были мотивированы принести качественные и своевременные результаты, им нужно давать возможность раскрыть свой потенциал в полной мере [8]. Как показывают исследования, работающие с мотивацией люди более склонны к творчеству, высокой активности, улучшению качества своей работы и состоянию духа.

Этот процесс в ООО «ЦСМ» начинается с того, что руководители метрологических лабораторий начинают заинтересовываться уровнем мотивации своих сотрудников. Руководители должны знать, что мотивирует их сотрудников и какие способы создания мотивации необходимо использовать [9].

Для этого руководство ООО «ЦСМ» старается поддерживать открытый диалог с сотрудниками по вопросам их мотивации, чтобы лучше понимать, что необ-

ходимо, чтобы поддерживать их мотивацию на высоком уровне. Это позволяет не только повысить качество работы, но и укрепить командный дух сотрудников, а также уменьшить текучесть кадров.

Важной составляющей управления персоналом в ООО «ЦСМ» является создание условий, которые сделают работу в лаборатории комфортной и интересной для сотрудников. Одним из эффективных методов мотивации является возможность повышения квалификации и профессионального роста. Для этого обеспечивается доступ к обучающим курсам, семинарам, тренингам и другим специализированным мероприятиям от заводов изготовителей по работе с поверяемыми средствами измерений, а также доступ к обучающим курсам по определенным видам измерений для повышения квалификации поверителей [10].

Также важно и создание системы поощрения достижений и успехов сотрудников. В качестве мотивации используются бонусы, премии (каждый месяц по результатам работы организации), повышение зарплаты (согласно знаниям и умениям поверителей) и ее индексирование, создание условий для развития карьеры (от стажера до инженера-метролога), поддержка при профессиональном росте (программа наставничества для стажеров) и т.д.

Для управления развитием персонала руководство также использует и индивидуальный подход. Учитываются потребности и интересы каждого сотрудника, чтобы мотивировать его к росту и развитию. Для этого проводятся анкетирования, внутренний аудит, личные разговоры, направленные на выявление целей и мотивов сотрудников [11].

Каждый работник может иметь свои индивидуальные мотивы, поэтому руководители ООО «ЦСМ» принимают во внимание все эти факторы, чтобы создать мотивационную систему, которая будет работать наиболее эффективно для каждого сотрудника [12].

Кроме того, в ООО «ЦСМ» важен командный дух и его развитие в виде сотрудничества между работниками лаборатории. Для этого проводятся корпоративные мероприятия (игры в баскетбол, веселые старты и т.д.), тренинги по командной работе, возможность спокойного общения и выполнения совместной работы между специалистами [13].

Важной частью в поиске молодых кадров, способных к дальнейшему обучению и развитию для ООО «ЦСМ» являются студенты последних курсов университета, но не каждый способный студент после выпуска хочет связать свою жизнь с метрологией, и для того, чтобы замотивировать студентов работать в метрологической лаборатории, необходимо привести следующие основные аргументы:

1. Карьерные возможности: работа в метрологии предоставляет много возможностей для карьерного роста и развития. На работу в качестве стажеров принимаются студенты 3-4 курсов высших учебных заведений на должность техника-метролога, в последствии после получения дипломов они, имея год-два опыта, могут аттестоваться на должность инженера-метролога и иметь право самостоятельно производить поверку средств измерений [14].

2. Работа в новых технологиях: вовлечение студентов в работу в метрологии путем использования новых приборов и эталонов, что позволяет студентам расширять свои знания и умения.

3. Значимость задач: работа в метрологической лаборатории является важной для контроля и оценки точности и надежности производимых изделий и услуг. Студенты могут чувствовать удовлетворение от того, что важный для общества процесс осуществляется благодаря их работе. Понимание того, что поверяемые ими приборы применяются в различных областях (от обычных коммунальных сетей до огромных нефтеперерабатывающих заводов) положительно сказывается на мотивационную составляющую их работы.

4. Команда профессионалов: работа в метрологической лаборатории предполагает работу с профессионалами, которые являются экспертами в своей области. За каждым студентом закреплен наставник, который его обучает, рассказывает, объясняет и отвечает на все его вопросы. Это позволяет студентам учиться у опытных коллег и повышать свои профессиональные навыки [15].

В ООО «ЦСМ» проводятся как лекционные занятия в течение учебного года, так и приглашают студентов на прохождение учебной и практической практики после учебного года. Во время практики студентам рассказывают и показывают особенности работы метролога, а также вовлекают их в процесс работы, что позволяет студентам приобрести понимание работы и увидеть ее привлекательность [16].

Важной частью мотивационной составляющей любой компании является текучесть кадров. Текучесть персонала объясняется целым рядом причин [17]. Условно их можно разделить на объективные (внешние) причины и субъективные (внутренние). Под текучестью персонала в теории управления понимается движение рабочей силы, обусловленное неудовлетворенностью работника рабочим местом или неудовлетворенностью организацией (рис. 2). Для ликвидации текучести кадров в ООО «ЦСМ» предпринимается действия, описанные в статье выше.

Рис. 2. Факторы, влияющие на движение и текучесть кадров

Показатели текучести кадров могут стать показателем эффективности работ по управлению развитием персонала и мотивации. Если организация имеет высокую текучесть кадров, это может быть связано с отсутствием мероприятий по

развитию персонала и неэффективной системой мотивации [18]. В рамках данного исследования произведем расчет коэффициента текучести персонала ООО «ЦСМ» для определения уровня удовлетворенности коллектива и дадим оценку руководству касательно их методов мотивационной составляющей за последний год работы (апрель 2022 года – март 2023 года):

$$Кт = \frac{Ру}{Чср} * 100\%, \quad (1)$$

где $Кт$ – коэффициент текучести кадров; $Ру$ – количество уволенных сотрудников за анализируемый период, чел; $Чср$ – среднесписочная численность сотрудников за анализируемый период, чел.

Среднесписочная численность сотрудников за анализируемый период рассчитывается по формуле:

$$Чср = \frac{Ч_1 + Ч_2 + ... + Ч_{11} + Ч_{12}}{12}, \quad (2)$$

где $Ч_1, Ч_2, ... Ч_{11}, Ч_{12}$ – численность работников по месяцам, чел. [19].

Результаты

Сначала определим среднесписочную численность сотрудников ООО «ЦСМ» за период апрель 2022 года – март 2023 года:

$Ч_1 - Ч_5$ (апрель –август 2022) – 19 чел.;

$Ч_6 - Ч_{10}$ (сентябрь 2022 – январь 2023) – 20 чел.;

$Ч_{11}$ (февраль 2023) – 18 чел.;

$Ч_{12}$ (март 2023) – 19 чел.

$$Чср = \frac{19*5 + 20*5 + 18 + 19}{12} = 19,3 чел;$$

$$Кт = \frac{2}{19,3} * 100 = 10,4\%.$$

Обсуждение

По результатам расчета коэффициент текучести в ООО «ЦСМ» за период апрель 2022 года – март 2023 года составляет 10,4 %, что является нормой для метрологических лабораторий. Естественный уровень текучести персонала способствует обновлению производственных коллективов. Этот процесс происходит непрерывно и не требует каких-либо чрезвычайных мер со стороны кадровых служб и руководства [20].

Заключение

Подводя итог, можно констатировать то, что эффективное развитие и управление персоналом возможно благодаря правильно выбранному стилю руководства, исходя из особенностей коллектива и правильно подобранной форме мотивации труда.

Таким образом, управление развитием персонала в центре сертификации и метрологии на основе мотивации включает в себя комплекс мер, направленных на создание условий для профессионального роста и развития каждого сотрудника. Важным аспектом является индивидуальный подход и учет потребностей и интересов каждого сотрудника, а также создание команды, способной достичь высоких результатов в работе лаборатории.

В целом, управление развитием персонала на основе мотивации является важным инструментом для достижения успеха метрологической лаборатории. При правильном подходе к управлению можно создать условия, которые позволят сотрудникам в полной мере использовать свой профессиональный и карьерный потенциал, что положительно скажется на результативности и конкурентоспособности лаборатории.

Благодарности

Выражаю благодарность за поддержку и помощь в исследовании способов мотивации и применения их на практике метрологической лаборатории ООО «ЦСМ» и группе компаний «Центр экспертиз и оценки соответствия».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кокуева Ж. М. Управление персоналом наукоемких предприятий: Учебное пособие по курсам "Управление персоналом" и "Менеджмент" / Ж. М. Кокуева, В. В. Яценко. Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2007. С. 4-22.

2. Шекшня С. В. Управление персоналом современной организации: Учеб. - практ. пособие / С. В. Шекшня; С. В. Шекшня. Москва: РГБ, 2007. С. 24-37.

3. Филатова В. В. Современные требования к персоналу организации / В. В. Филатова, С. А. Чунакова, С. В. Плеханов // Управление качеством на этапах жизненного цикла технических и технологических систем: Сборник научных статей 4-й Всероссийской научно-технической конференции, Курск, 27 мая 2022 года / Редколлегия: Е.В. Павлов (отв. редактор). Курск: Юго-Западный государственный университет, 2022. С. 234-237.

4. Храмова Т. М. Управление персоналом организации. Технологии управления развитием персонала: Учебник / Т. М. Храмова, О. П. Ходенкова, О. К. Минева и др. Москва: Общество с ограниченной ответственностью «Научно-издательский центр ИНФРА-М», 2016. С. 121-142.

5. Дейнека А. В. Управление персоналом. Учебник / А. В. Дейнека. Москва: Дашков и К, 2010. С. 23-78.

6. Попазова О. А. Управление персоналом организации: Учебник / О. А. Попазова, Э. Б. Молодькова. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2019. С. 128-143.

7. Геранюшкина Г. П. Психология управления: учебное пособие / Г. П. Геранюшкина, В. Н. Мунгалов. Иркутск: Байкальский государственный университет, 2016. С. 61-83.

8. Старцев В. А. Управление профессиональным развитием персонала как фактор эффективного функционирования промышленной организации.: / Старцев Вячеслав Александрович. Москва, 2009. С. 11-26.

9. Олейник О. С. Формированне, развитие и эффективность использования персонала предприятия / О. С. Олейник // Науковий огляд. 2016. № 5(26). С. 25-41.

10. Горгорова В. В. Мотивация персонала, стратегия мотивации, материальное стимулирование, нематериальное стимулирование, эффективность мотивации персонала / В. В. Горгорова, Л. А. Кобина // Инженерный вестник Дона. 2013. № 4(27) С. 54-80.

11. Павлова М. А. Мотивация персонала как средство повышения эффективности труда в профессиональной деятельности / М. А. Павлова // Транспортные системы: безопасность, новые технологии, экология: Международная научно-практическая конференция, Якутск, 16 апреля 2021 года. Якутск: Якутский институт водного транспорта (филиал) ФГБОУ ВО СГУВТ, 2021. С. 369-373.

12. Чернобровина Ю. Э. Мотивация трудовой деятельности персонала как фактор эффективности российских компаний / Ю. Э. Чернобровина // Евразийский союз ученых. 2016. С. 89-91.

13. Ефремова С. В. Формирование и развитие мотивационной системы управления персоналом на предприятии / Ефремова Светлана Васильевна. Москва, 2004. С. 9-25.

14. Стоянов Л. А. Мотивация как важнейшая часть организации труда в современных условиях / Л. А. Стоянов, Э. М. Абдулахаирова // Современный менеджмент и управление: тенденции и перспективы развития: Сборник научных трудов, Симферополь, 20 ноября 2019 года / Под общей редакцией М.Н. Стефаненко. Симферополь: Общество с ограниченной ответственностью "Аэтерна", 2019С. 362-369.

15. Полякова О. С. К вопросу о развитии персонала на основе эффективного управления мотивацией / О. С. Полякова // Устойчивость экосистем в условиях цифровой нестабильности: сборник трудов международной научно-практической конференции, Симферополь, 30 мая 2022 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 514-516.

16. Обраскова Т. С. Формирование системы управления мотивацией персонала в производственной организации / Т. С. Обраскова // Новая наука: Теоретический и практический взгляд. 2015. № 5-3. С. 95-101.

17. Тимохина О. А. Формирование системы адаптации персонала как фактор снижения текучести персонала в организации / О. А. Тимохина, Т. А. Власова // Донецкие чтения 2021: образование, наука, инновации, культура и вызовы современности: Материалы VI Международной научной конференции, Донецк, 26–27 октября 2021 года. Том 5. Донецк: Донецкий национальный университет, 2021. С. 102-104.

18. Кравченко М. В. Формирование процесса управления текучестью персонала в организации / М. В. Кравченко //. 2018. Т. 8, № 11(27). С. 556-560.

19. Бойкова М. А. Система обучения персонала как инструмент снижения текучести кадров / М. А. Бойкова // Современные исследования проблем управления кадровыми ресурсами: сборник научных статей II Международной научно-практической конференции, Москва, 25–26 апреля 2017 года. Том 1. Москва: Московский технологический университет (МИРЭА), 2017. С. 67-73.

20. Шатович Д. А. Текучесть персонала как одна из проблем в управлении организацией / Д. А. Шатович // Современные технологии управления персоналом: Сборник трудов V Международной научно-практической конференции, Симферополь, 27–28 сентября 2018 года / Под научной редакцией О.С. Резниковой. – Симферополь: Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2018. С. 535-539.

УДК 004.352.246
DOI 10.33764/2618-981X-2023-6-277-283

Д. В. Хан[1], А. Н. Поликанин[1]*

Система идентификации сотрудников и студентов с помощью QR-кода и использования оптической камеры

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: han_denis_2000@mail.ru

Аннотация. Предмет исследования**.** В статье представлена технология идентификации сотрудников и студентов в помещениях с использованием оптических средств и QR-кода. В работе описываются этапы разработки системы идентификации, включая выбор необходимых инструментов и методов, разработку соответствующего программного обеспечения и тестирование системы контроля управления доступом с использованием QR-кода на практике. Результаты исследования показывают, что данная система идентификации может решить проблемы несанкционированного доступа в помещения и отслеживания посещаемости студентов на занятиях. Цель исследования. Внедрение системы идентификации сотрудников и студентов с помощью QR-кода и использованием оптической камеры для создания эффективного инструмента контроля доступа в здания и помещения учебных заведений, повышения безопасности и контроля посещаемости. Методология исследования. Процесс проведения анализа требований, проектирование системы, разработка программного обеспечения и тестирование. Результат исследования. Сравнительный анализ систем контроля доступа разного уровня, также были выявлены преимущества и недостатки разрабатываемого продукта. В процессе создания по выбранным техническим критериям были учтены нормативно-правовые акты и государственные стандарты для сертификации системы. Для реализации разработки продукта был выбран подходящий язык программирования и перечень технических средств для оптимальной работы разработки. По результатам была выявлена и эффективность создаваемого продукта. Уникальность заключается в разработке собственного кода и компиляции QR-кода, смартфона, микроконтроллера и электромеханического замка в одной системе, что не имеет аналогов на рынке. Выводы. Создание технологии идентификации сотрудников и студентов в помещениях с использованием оптических средств и QR-кода является эффективным решением для университетов и других организаций, которые хотят обеспечить безопасность и контроль доступа в своих помещениях. Кроме того, технология отметки посещаемости на занятиях поможет улучшить качество образования, позволяя преподавателям отслеживать и анализировать данные о посещаемости студентов.

Ключевые слова: система контроля доступом, QR-код, оптические средства идентификации, разработка программного обеспечения, электромеханический замок

D. V. Khan[1], A. N. Polikanin[1]*

System of Employee and Student Identification Using QR Code and Optical Camera

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: han_denis_2000@mail.ru

Abstract. Subject of the research. The article presents a technology for identifying employees and students in premises using optical devices and QR codes. The paper describes the stages of system

development, including the selection of necessary tools and methods, the development of relevant software, and the practical testing of the access control system using QR codes. The research results demonstrate that this identification system can address unauthorized access issues in premises and track student attendance in classes. Research objective. The implementation of an identification system for employees and students using QR codes and optical cameras to create an effective access control tool in educational buildings and premises, enhancing security and attendance monitoring. Research methodology. The process involved requirements analysis, system design, software development, and testing. Research outcome. A comparative analysis of access control systems at different levels was conducted, and the advantages and disadvantages of the developed product were identified. Normative acts and state standards were taken into account for system certification during the development process based on selected technical criteria. Appropriate programming languages and technical resources were chosen to optimize the development process. The effectiveness of the created product was determined. The uniqueness lies in the development of proprietary code and the integration of QR codes, smartphones, microcontrollers, and electromechanical locks into one system, which has no analogs on the market. Conclusions. Creating a technology for identifying employees and students in premises using optical devices and QR codes is an effective solution for universities and other organizations aiming to ensure security and access control in their premises. Additionally, the attendance tracking technology can improve the quality of education by enabling teachers to monitor and analyze student attendance data.

Keywords: access control system, QR code, optical identification devices, software development, electromechanical lock

Введение

В современном мире информационные технологии занимают все более важное место, необходимо создавать инновационные решения, которые позволят улучшить качество подготовки специалистов и работы учебных заведений. В связи с этим, разработка технологии идентификации сотрудников и студентов в помещениях с помощью оптических средств и QR-кода является актуальной задачей. Одной из проблем, с которой сталкиваются университеты, является пропуск студентов и сотрудников в здания без необходимого разрешения. Это может привести к серьезным последствиям, таким как кража, утечка конфиденциальной информации и т. д. Для решения этой проблемы в настоящей статье предлагается использование технологии идентификации на основе QR-кода и оптических средств [1].

Каждый сотрудник и студент будет иметь индивидуальный токен, который будет определять его в системе. На каждом кабинете будет установлен QR-код, который определит доступ входящего в помещение. Также планируется создание системы отметок посещения на занятиях, с помощью считывания QR-кода, которая будет закреплена за определенной аудиторией [2].

Так как продукт будет создаваться в Российской Федерации, то для получения сертификации на соответствие требованиям ФСТЭК, необходимо соблюдать следующие требования:

– соблюдение правил криптографической защиты информации, установленных законодательством РФ;

– соблюдение требований безопасности, установленных в соответствии с законодательством РФ;

– обеспечение соответствия технических средств и программного обеспечения требованиям безопасности, установленным законодательством РФ;

– обеспечение защиты персональных данных пользователей;

– прохождение испытаний на соответствие требованиям ФСТЭК;

– подготовка полного пакета документации, включающей технические условия и технический паспорт, результаты испытаний, а также протоколы оценки соответствия требованиям ФСТЭК;

– получение разрешения на эксплуатацию от ФСБ России.

Главной целью исследования является внедрение системы идентификации сотрудников, студентов с помощью QR-кода и использованием оптической камеры для создания эффективного инструмента контроля доступа в здания и помещения учебных заведений, повышения безопасности и контроля посещаемости.

Методы и материалы

Для создания системы идентификации сотрудников и студентов в помещениях с помощью QR-кода и использованием оптической камеры использовались следующие методы и материалы [3]:

1. Оптические камеры: для сканирования QR-кодов, сбора изображений и их последующей обработки.

2. QR-коды: для генерации уникальных кодов, используемых для идентификации сотрудников и студентов. QR-коды могут быть созданы с помощью специальных программных инструментов.

3. Электромеханический замок: для управления доступом к помещениям на основе идентификации с помощью QR-кода. Электромеханический замок может быть установлен на дверь помещения и управляться с помощью программного обеспечения.

4. Микроконтроллеры: для обработки и анализа данных, полученных с оптических камер и других устройств, и управления электромеханическим замком.

5. Программное обеспечение: для разработки системы идентификации, обработки и анализа изображений, генерации QR-кодов и управления электромеханическим замком.

Используемые средства указаны в табл. 1.

Таблица 1

Название	Стоимость
Arduino UNO R3	1678 рублей
Замок электромеханический ES1096A	695 рублей
Контроллер на Wi-Fi модуле ESP8266 4Mb WeMos D1 Mini	385 рублей

В разработке системы идентификации сотрудников и студентов на микроконтроллере, использовался язык программирования C++, так как является машиноориентированным языком программирования и позволяет работать непо-

средственно с подобным оборудованием, а также широко используется для разработки встроенных систем. Кроме того, многие производители микроконтроллеров предоставляют библиотеки и инструменты для работы с их продукцией на языках C и C++, что также может облегчить процесс разработки [5].

В программе для Arduino используются библиотеки для работы с QR-кодами и оптической камерой, а также для управления электромеханическим замком.

Программа начинается с инициализации всех подключенных компонентов: оптической камеры, замка, LED-индикатора и т.д. Затем идет процесс сканирования QR-кода с помощью оптической камеры. После этого происходит проверка считанного кода на соответствие допустимому списку кодов.

Если QR-код действителен, то зажигается зеленый LED-индикатор и происходит открытие замка на некоторое время, чтобы пользователь мог открыть дверь. Если QR-код недействителен, то зажигается красный LED-индикатор и замок остается закрытым.

В коде также может быть предусмотрена возможность ввода новых QR-кодов в список допустимых кодов, например, через интерфейс взаимодействия с программой [4].

Для соединения всех заявленных элементов системы входа с QR-кодом и электромеханическим замком выполнены следующие шаги:

1. Подготовить аппаратное обеспечение:

– собрать и подключить к Arduino плате модуль камеры;

– подключить к плате Arduino электромеханический замок и убедиться в его работоспособности;

– подключить плату Ethernet Shield к Arduino для доступа к Интернету.

2. Настроить программное обеспечение:

– загрузить на Arduino код для работы с камерой и QR-кодами;

– настроить параметры камеры для корректной работы;

– настроить программу для отправки информации об идентифицированном пользователе на сервер;

– на серверной стороне необходимо разработать программное обеспечение для приема информации об идентификации и управления доступом.

3. Протестировать работу системы:

– убедиться в работоспособности всех элементов системы;

– протестировать идентификацию пользователей с помощью QR-кода и работу электромеханического замка [9].

После выполнения этих шагов система готова к использованию. При поднесении QR-кода к камере информация об идентифицированном пользователе будет отправляться на сервер, где будет приниматься решение о доступе пользователя к помещению. Если доступ разрешен, электромеханический замок откроется. Алгоритм работы иллюстрирован на рис. 1.

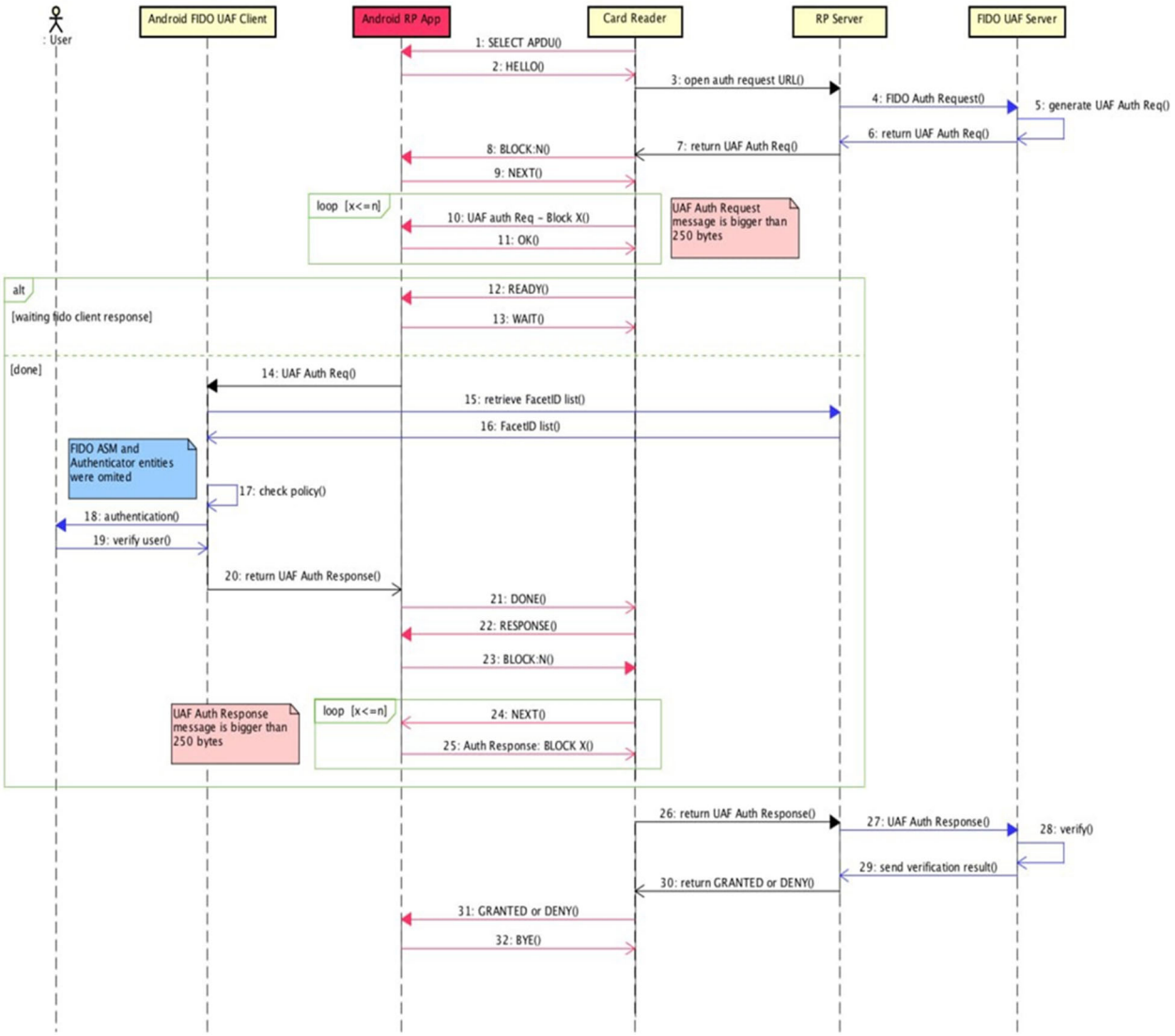


Рис. 1. Принцип работы системы

Результаты

Результаты исследования показали, что созданная система идентификации сотрудников и студентов на основе QR-кода и оптических средств является эффективным инструментом контроля доступа в здания и помещения учебных заведений.

В ходе исследования были разработаны и опробованы методы и материалы для создания системы, включая использование оптических средств, QR-кода, микроконтроллера, электромеханического замка и программного обеспечения. Был выбран язык программирования C++ для микроконтроллера, так как он обладает необходимыми функциями и библиотеками для эффективной работы системы.

Разработанная система имеет уникальность за счет сочетания QR-кода, смартфона, микроконтроллера и электромеханического замка в одной системе, что не имеет аналогов на рынке. Результаты исследования показали работоспособность и эффективность создаваемого продукта.

На рис. 2 изображен готовый прототип оборудования.

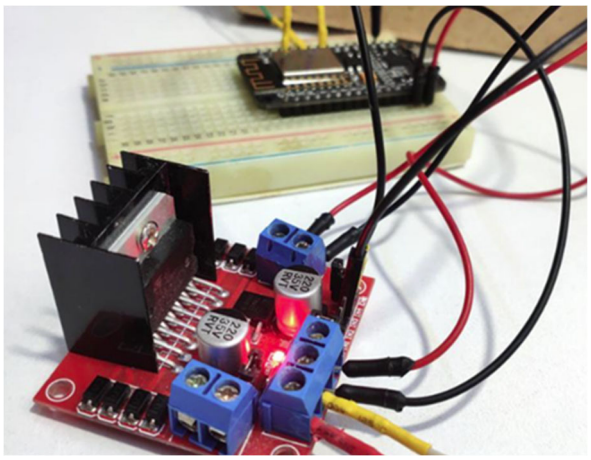


Рис. 2. Подключение Arduino Uno к вайфай модулю

Также на рис. 3 и рис. 4 описан программный код для используемого микроконтроллера.

```
// Определяем переменные wifi
String _ssid     = "Wi-Fi"; // Для хранения SS
String _password = "123456"; // Для хранения па
String _ssidAP = "ATGarland";   // SSID AP точ
String _passwordAP = "012345678"; // пароль то
```

Рис. 3. Определение переменных Wi-Fi

```
bool flag = false;          // флаг состояния замка
bool flag_bloc = false;     // флаг блокировки
byte n_bloc = 0;            // счетчик неверных попыток ввода пороля
boolean flag_limit = false;       // текущий статус конечника
static uint32_t tmr1, tmr2;
```

Рис. 4. Скетч работы электромеханического замка

Конечные результаты исследования системы идентификации сотрудников и студентов с использованием QR-кода и оптической камеры включают:

– разработанная система успешно прошла тестирование на точность идентификации. Система может точно определить личность сотрудника или студента, основываясь на сканировании QR-кода;

– была создана программа на Arduino, которая позволяет подключить оптическую камеру и электромеханический замок к системе идентификации. Эта программа может работать автономно без подключения к Интернету;

– была проведена оценка эффективности системы идентификации. В результате исследования было выявлено, что система позволяет ускорить процесс идентификации, снизить нагрузку на администрацию и повысить уровень безопасности;

– в целом, результаты исследования свидетельствуют о том, что система идентификации с использованием QR-кода и оптической камеры является эффективным и удобным решением для организаций, которые нуждаются в надежной системе идентификации сотрудников и студентов.

Заключение

В заключении можно отметить, что система идентификации сотрудников и студентов с помощью QR-кода и оптической камеры представляет собой удобное и быстрое решение для автоматизации процесса контроля доступа и учета рабочего времени в организациях и учебных заведениях. Она позволяет значительно сократить время на проверку идентификационных данных, уменьшить количество ошибок и снизить риски несанкционированного доступа. Также следует отметить, что система может быть легко интегрирована с другими программными и аппаратными средствами, что расширяет ее возможности и повышает эффективность использования. В целом, система идентификации сотрудников и студентов с помощью QR-кода и оптической камеры является важным инструментом для повышения безопасности и улучшения управления в организациях и учебных заведениях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Александров А.А., Иванов, И.И. Система идентификации сотрудников и студентов с помощью QR-кода и использованием оптической камеры // Технологии информационной безопасности. – 2021. – Т. 3, № 1. – С. 10-15.
2. Жданов Д.А., Скороход А.В. QR-код в маркетинге и рекламе // Маркетинг в России и за рубежом. – 2015. – Т. 4. – С. 11-18.
3. Карасик Л.А. Использование QR-кодов в образовательном процессе // Инновации в образовании. – 2015. – № 1(19). – С. 29-33.
4. Королев, А.Ю. Стандартизация системы маркировки товаров // Маркетинг и маркетинговые исследования. – 2016. – Т. 6. – С. 74-81.
5. Логинова М.С., Томин И.В., Кривенко М.С. Развитие технологии QR-кодов // Наука и техника в России. – 2018. – Т. 1. – С. 74-77.
6. Ломов Б.Ф. Программирование на языке Си: 6-е издание. – Москва: Вильямс, 2018. – 704 с.
7. Масленникова Ю.А. Использование QR-кодов в бизнесе // Бизнес-информатика. – 2019. – № 3. – С. 94-99.
8. Саркисян Г.С. Оптические камеры: устройство, принцип работы, применение // Радио и связь. – 2017. – 240 с.
9. Соколов А.И., Смирнова Е.В. Использование QR-кодов в системах безопасности // Безопасность сетевых и информационных технологий. – 2018. – Т. 6, № 1. – С. 34-39.
10. Яковлев А.И., Алешина И.А. QR-коды в цифровой маркетинговой коммуникации // Маркетинговые исследования. – 2017. – Т. 3. – С. 77-83.

УДК 004.056
DOI 10.33764/2618-981X-2023-6-284-290

А. В. Цыпкина[1], А. В. Шабурова[1]*

Применение вероятностного метода оценки опасности объектов КИИ при возникновении чрезвычайных ситуаций

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: arina.arina99@mail.ru

Аннотация. В современных условиях глобальной информатизации общества большинство объектов оборонной промышленности требуют комплексный подход к защите от различных угроз, включая терроризм, чрезвычайные ситуации, стихийные бедствия и преступную деятельность. В данной статье будет рассматриваться оборонное предприятие со стороны физической защиты от чрезвычайных ситуаций, возникающих от рук злоумышленников. Основной целью статьи является категорирование объектов критической информационной инфраструктуры для предотвращения возникновения чрезвычайных ситуаций с применением вероятностного метода, результатом которого будет являться вероятность безопасного состояния объекта критической информационной инфраструктуры, а также предложены меры по совершенствованию физической защиты рассматриваемой организации. Актуальность темы категорирования критической информационной инфраструктуры объясняется важностью оборонной промышленности в обеспечении национальной безопасности Российской Федерации.

Ключевые слова: категорирование, объект КИИ, чрезвычайная ситуация, физическая защита

A. V. Cypkina[1], A. V. Shaburova[1]*

Application of a Probabilistic Method for Assessing the Danger of CII Objects in the Event Of Emergencies

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: arina.arina99@mail.ru

Abstract. In modern conditions of global informatization of society most objects of the defense industry require an integrated approach to protection from various threats, including terrorism, emergencies, natural disasters and criminal activity. In this article, a defense enterprise will be considered from the side of physical protection against emergencies arising at the hands of intruders. The main purpose of the article is to categorize objects of critical information infrastructure to prevent the occurrence of emergency situations using a probabilistic method, the result of which will be the probability of a safe state of the object of critical information infrastructure, and also proposed measures to improve the physical protection of the organization in question. The relevance of the topic of categorizing critical information infrastructure is explained by the importance of the defense industry in ensuring the national security of the Russian Federation.

Keywords: categorization, CII object, emergency situation, physical protection

Введение

В настоящее время вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации уделяется большое внимание.

В отношении значимых объектов критической информационной инфраструктуры деструктивные воздействия нарушителей могут повлечь за собой негативные последствия для предприятия и даже возникновение чрезвычайных ситуаций (далее – ЧС). Основной целью статьи является определение вероятности безопасного состояния объекта критической информационной инфраструктуры (далее – КИИ) с помощью вероятностного метода при возникновении чрезвычайных ситуаций. Обеспечение безопасности информационных инфраструктур на оборонных предприятиях является одним из важнейших направлений деятельности организации [1].

Методы и материалы

Чрезвычайной ситуацией является обстановка на определенной территории или акватории, возникшая в результате опасного природного явления, аварии, катастрофы, стихийного бедствия или другого неблагоприятного события, которая может привести к человеческим жертвам, ущербу здоровью людей или окружающей среде, значительные материальным потерям и нарушению условий жизнедеятельности людей. Чрезвычайные ситуации различаются по характеру источника (природные, техногенные, биолого-социальные и военные) и по масштабам (трансграничные, федеральные, региональные, территориальные, местные, локальные) [2].

При оценке угроз безопасности информации необходимо определить потенциальные источники угроз безопасности информации, связанные с действиями людей или групп людей (антропогенные источники угроз), которые могут совершить несанкционированный доступ или воздействовать на информационные ресурсы и компоненты систем и сетей, – актуальные нарушители [3, 4].

Для оборонного предприятия основными нарушителями были определены:

а) внешние нарушители:
   1) специальные службы иностранных государств;
   2) отдельные физические лица (хакеры);

б) внутренние нарушители:
   1) авторизованные пользователи систем и сетей;
   2) системные администраторы и администраторы безопасности.

Используя классификацию ЧС природного и техногенного характера, принятую в постановлении Правительства Российской Федерации от 21 мая 2007 № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера», определим возможный характер масштаба ЧС, возникшей от рук злоумышленников [5].

По классификации ЧС, исходя из размера зоны ЧС, для внутреннего нарушителя масштаб ЧС будет иметь локальный характер, а для внешнего нарушителя – муниципальный и межмуниципальный характер. Классифицируя объект, присваиваем возможному масштабу ЧС межмуниципальный характер.

В пределах концепции защиты будут рассматриваться угрозы, связанные с физическим доступом на объект защиты [6].

Возможными угрозами нарушения функционирования объекта при возникновении нештатных ситуаций внешнего характера могут выступать стихийные

бедствия, физические воздействия от рук злоумышленников и инциденты, связанные с технологическими процессами.

Обусловленное влияние внешних физических условий и окружающей среды при эксплуатации защищаемого объекта оборонной промышленности несёт ряд ограничений на применение технических средств охраны и допуск на охраняемый объект, что объясняется особенностью технологического процесса предприятия.

Исходя из вышеизложенного, для построения физической защиты исследуемого объекта будем осуществлять категорирование КИИ по методу Костина В.Н [7, 8].

Результаты

С использованием информационно-вероятностного метода был оценен потенциальный масштаб чрезвычайных ситуаций. Для каждого из шести уровней масштаба потерь была определена доля энтропии. В табл. 1 представлены результаты, где нелинейно были распределены потенциалы опасности чрезвычайных ситуаций.

Таблица 1

Соотношение потенциалов опасности ЧС по шестибалльной и энтропийной шкале

Оценочные шкалы	Уровень масштаба потерь при ЧС различного характера					
	локальный	муниципальный	межмуниципальный	региональный	межрегиональный	федеральный
Шестибалльная	1	2	3	4	5	6
Энтропийная	0,0066	0,116	0,173	0,555	0,621	0,878

Проанализировав таблицу, можно сделать вывод, что объекту исследования по шестибальной шкале присваивается 2 и 3 баллы по муниципальному и межмуниципальному характерам.

Категорирование проводится с учетом наихудших сценариев действий нарушителя наиболее опасного типа. Определяются шесть категорий потерь, которые применяются для оценки опасности защищаемых объектов:

– политические (снижение уровней авторитета властей и политическая нестабильность);

– людские (утрата жизней людей, их здоровья);

– финансовые (потеря материальных ценностей);

– экономические (затраты на переселение людей из зоны ЧС и выплаты компенсаций);

– экологические (потери природных ресурсов, ухудшение экологии);

– культурно-информационные (утрата художественных ценностей и передовых технологий).

Был проведен анализ потенциальных рисков объекта в случае возникновения чрезвычайных ситуаций с использованием метода главных компонент, в рамках которого было изучено взаимодействие между параметрами частных видов потерь. С использованием информационно-вероятностного подхода была проведена оценка уровня риска для различных категорий объектов, и на основе полученных результатов был предложен соответствующий уровень вероятности нахождения объекта в состоянии, которое можно считать безопасным [10].

Табл. 2 содержит информацию об оценках опасности при авариях каждой категории объектов, оцененных по шестибалльной шкале в шести масштабах потерь.

Таблица 2

Параметры последствий ЧС объектов по шестибалльной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	*5 кат.*	6 кат.	7 кат.
Политические	5	4	3	3	*2*	2	1
Людские	5	4	4	3	*2*	2	1
Финансовые	5	5	4	3	*2*	2	1
Экономические	6	5	4	3	*3*	2	1
Экологические	6	5	4	3	*3*	2	2
Информационные	6	5	4	3	*3*	2	2

Проанализировав табл. 2 и сравнив полученные оценки частных видов потерь, получаем 5 категорию для оборонного предприятия.

Исследования были проведены в отношении каждой категории масштаба потерь, в результате чего были определены соответствующие энтропийные величины ущерба. Табл. 2 была преобразована в табл. 3, где шестибальная шкала опасности представлена энтропийной величиной масштаба потерь.

Таблица 3

Характеристики категорий объектов по энтропийной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	*5 кат.*	6 кат.	7 кат.
Политические	0,621	0,555	0,173	0,173	*0,116*	0,116	0,0066
Людские	0,621	0,555	0,555	0,173	*0,116*	0,116	0,0066
Финансовые	0,621	0,621	0,555	0,173	*0,116*	0,116	0,0066
Экономические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,0066
Экологические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116
Информационные	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116

С помощью входных данных из табл. 3 была проведена оценка энтропийного потенциала опасности для каждой категории объекта, и результаты данной оценки представлены в табл. 4.

Таблица 4

Потенциалы категорируемых объектов по энтропийной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	*5 кат.*	6 кат.	7 кат.
Политические	0,621	0,555	0.173	0,173	*0,116*	0,116	0,0066
Людские	0,621	0,555	0,555	0,173	*0,116*	0,116	0,0066
Финансовые	0,621	0,621	0,555	0,173	*0,116*	0,116	0,0066
Экономические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,0066
Экологические	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116
Информационные	0,878	0,621	0,555	0,173	*0,173*	0,116	0,116
Энтропийный потенциал опасности	1,371	1,182	1,011	0,522	*0,289*	0,206	0,102
P безопасного состояния объекта	0,999	0,95	0,90	0,77	*0,69*	0,65	0,60

Вероятность безопасного состояния объекта исследования является значение показателя защищенности объекта, значение которого может быть определено исходя из потенциалов опасности категорируемых объектов. Вероятность безопасного состояния нашего объекта равна 69 %.

Соответственно, при возникновении чрезвычайной ситуации потенциал опасности категорируемых объектов составляет 31 %, что так же является их интегральной характеристикой. Потенциал привлекательности защищаемого объекта определяется потенциалом опасности каждой категории объекта, который в свою очередь, зависит от параметров частных потерь [11, 12].

Заключение

Для минимизации потенциала опасности предприятия необходимо рассматривать комплексную защиту, включающую и обеспечение безопасности на физическом уровне, что в последствии становится первой преградой для злоумыш-

ленника. Инструментом для обеспечения безопасности выступает система физической защиты. Это совокупность действий и мер, связанных с физическим, инженерно-техническим проектированием и организационными мероприятиями для предотвращения несанкционированного доступа к объекту [13].

На рассматриваемом оборонном предприятии уже имеется действующая физическая защита, но для совершенствования защиты и повышения безопасного состояния объекта рекомендуется установить средство контроля и управлением доступа и устройства пространственного зашумления, сетевые помехоподавляющие фильтры [14].

В результате с помощью применения вероятностного метода был найден потенциал опасности объекта КИИ оборонного предприятия при возникновении ЧС и предложены рекомендации по физической защите для повышения эффективности информационной безопасности предприятия оборонно-промышленного комплекса [15].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 05.04.2023).
2. ГОСТ Р 22.2.06-2016. Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Оценка риска чрезвычайных ситуаций при разработке паспорта безопасности критически важного объекта и потенциально опасного объекта : нац. стандарт Рос. Федерации : изд. офиц. – Введ. 2017- 06-01. – Москва : Стандартинформ, 2016. – 8 с.
3. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. – Текст : электронный // ФСТЭК России : сайт – 2022. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 05.04.2023).
4. Костин В. Н. Оценка потенциала опасности нарушителей на основе информационного метода и метода главных компонент / В. Н. Костин // Информационные технологии и вычислительные системы, 2016, № 3. – С. 74–81.
5. Постановление Правительства РФ от 21.05.2007 № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера». – Текст: электронный // Справочная правовая система КонсультантПлюс. – Режим доступа: по подписке (дата обращения 05.04.2023).
6. Костин В. Н. Задачи концептуального проектирования систем физической защиты критически важных объектов / В. Н. Костин // Проблемы информационной безопасности. Компьютерные системы, 2020, № 1. – С. 58–67.
7. Костин В. Н. Информационно-вероятностный метод формирования категорий потенциально опасных объектов / В. Н. Костин, А. К. Пономарев // Вестник компьютерных и информационных технологий, 2015, № 6 (132). — С. 34–42.
8. Костин В. Н. Оценка значимости частных видов потерь критически важных объектов при возникновении чрезвычайной ситуации / В. Н. Костин, А. С. Боровский // Научно-технический вестник Поволжья, 2020, № 8. – С. 8 – 11.
9. Костин В. Н. Оценка величины значимости чрезвычайных ситуаций на основе информационно-вероятностного метода / В. Н. Костин // Проблемы информационной безопасности. Компьютерные системы, 2019, № 3. – С. 17–23.
10. Костин В. Н. Оценка потенциала опасности критически важных объектов при возникновении чрезвычайных ситуаций на основе информационно вероятностного метода и метода главных компонент / В. Н. Костин // Информационные технологии, 2020, Т. 26, № 5. – С. 297–301.

11. Костин В. Н. Обоснование требований к эффективности подсистем физической защиты объектов информатизации / В. Н. Костин, Н. А. Соловьев, Н. А. Тишина // Научно-технический вестник Поволжья, 2018, № 4. – С. 125–128.

12. Костин В. Н. Модернизация структуры физической защиты критически важных объектов информатизации на основе выбора эффективных решений // Вестник компьютерных технологий, 2019, № 12 (186). — С. 27–39.

13. Панин О. Категорирование объектов для создания эффективных систем физической защиты – Текст: непосредственный // Безопасность. Достоверность. Информация, 2007, № 70. – С. 20–24.

14. Мельников Ю.С. Актуальные вопросы физической защиты информации – Текст: непосредственный // Проблемы науки, Москва, 2020, № 7 (55). – С. 35–40.

15. Давыдов Д.М. Особенности обеспечения информационной безопасности инновационной деятельности предприятий оборонно-промышленного комплекса – Текст: непосредственный // Инновации и инвестиции, 2019, № 10. – С. 8–10.

УДК 528.88
DOI 10.33764/2618-981X-2023-6-291-296

*А. Ю. Чермошенцев[1], М. И. Кузнецов[1]**

Применение данных дистанционного зондирования при маркшейдерском обеспечении разработки месторождений углеводородного сырья

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: m4s71.98@gmail.com

Аннотация. При решении маркшейдерских задач на месторождениях углеводородного сырья необходимо обеспечить точность и безопасность выполнения работ. Благодаря техническому прогрессу существенно расширился набор инструментов, позволяющих повысить точность, производительность и безопасность работ. В статье рассматриваются способы маркшейдерского обеспечения разработки и эксплуатации месторождений углеводородного сырья с использованием дистанционного зондирования. Анализируются возможности использования данных, получаемых с различных носителей, для выполнения комплекса маркшейдерских работ.

Ключевые слова: дистанционное зондирование, маркшейдерские работы, месторождения

*A. Yu. Chermoshentsev[1], M. I. Kuznetsov[1]**

Application of Remote Sensing Data in Mine Surveying Support for the Development of Hydrocarbon Deposits

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: m4s71.98@gmail.com

Abstract. When solving mine surveying tasks at hydrocarbon deposits, it is necessary to ensure the accuracy and safety of work. Thanks to technical progress, the set of tools has significantly expanded to improve the accuracy, productivity and safety of work. The article discusses methods of mine surveying support for the development and operation of hydrocarbon deposits using remote sensing. The possibilities of using data obtained from various platforms to perform a complex of mine surveying work are analyzed.

Keywords: remote sensing, mine surveying, deposits

Введение

Маркшейдерское обеспечение разработки месторождений углеводородного сырья, такого как нефть, свободный газ и газовый конденсат, имеет важную роль для осуществления безопасного технологического цикла. Решению этой задачи посвящены исследования как методов выполнения маркшейдерских работ, так и создания специальных приборов и оборудования для их производства. Маркшейдерское обеспечение тесно связано с другими видами работ, например, буровыми, геологоразведочными, строительно-монтажными, эксплуатацией объектов обустройства и проектно-изыскательными. Современные методы сбора и об-

работки данных позволяют существенно повысить производительность работ и скорость обработки результатов измерений.

В последнее время большое внимание уделяется обновлению нормативной документации, определяющей технические требования к производству и проектированию работ. Многие из имеющихся документов утратили актуальность в связи с переходом на современное оборудование и методы обработки данных. К разработке нормативно-технической документации должны активно привлекаться не только органы государственной власти, но и предприятия, к сфере деятельности которых относится рассматриваемый вопрос. Примером подобного взаимодействия государственных и производственных структур является Предварительный национальный стандарт Российской Федерации «Нефтяная и газовая промышленность. Маркшейдерское обеспечение поиска, разведки, обустройства и разработки месторождений углеводородного сырья» [1], разработанный с участием таких крупных компаний, как «Газпром нефть», «Роснефть» и «Татнефть». Данный стандарт утвержден и введен в действие в 2022 году и учитывает все современные тенденции развития геопространственной отрасли. В частности, отмечается перспектива технологий дистанционного зондирования Земли (ДЗЗ), которые находят широкое применение при выполнении работ в различных сферах (инженерные изыскания, геология, мониторинг чрезвычайных ситуаций и др.). Цель статьи заключается в анализе возможностей применения данных дистанционного зондирования для маркшейдерского обеспечения разработки месторождений углеводородного сырья.

Методы и материалы

Маркшейдерское обеспечение включает в себя множество задач, производство которых регулируется различными нормативными документами [1-5]. К таким задачам относятся:

– выполнение установленных законодательством мероприятий по безопасному ведению работ, связанных с пользованием недрами и промышленной безопасности для обеспечения эксплуатации объектов обустройства;

– выполнение комплекса маркшейдерских, геодезических, картографических, топографических, гидрологических работ, обеспечивающих подготовку, ввод в разработку и промышленную разработку месторождения;

– ведение маркшейдерской документации на всех этапах освоения месторождения и ее сохранность;

– контроль пространственного положения объектов систем разработки, обустройства и соответствия проектному положению;

– разработка мер, направленных на своевременное и качественное освоение месторождений, обеспечение безопасного ведения работ, связанных с пользованием недрами, и промышленной безопасности;

– планирование и проектирование маркшейдерских работ;

– совершенствование организации и методов работ на основе широкого внедрения достижении науки и техники, передового опыта.

При разработке месторождений существует два вида контроля операционный и периодический.

Операционный включает в себя следующие виды контроля:

– ведение горных работ в границах лицензированного участков или горных отводов;

– инженерно-геодезические изыскания, инженерно-гидрографические работы, позиционирование морского нефтегазового сооружения, строительно-монтажные работы и их соответствие проектной документации;

– пространственное положение оси ствола скважины;

– работы, выполненные подрядными организациями.

Периодическому контролю подлежат:

– маркшейдерская документация;

– здания и сооружения, в том числе опасных производственных объектов, для обеспечения безопасной технической эксплуатации;

– сдвижение и деформация земной поверхности в пределах границ ведения горных работ.

В соответствии с [1], метод измерений и наблюдений (геодезический методы, метод спутниковых измерений или методы дистанционного зондирования) может выбираться исполнителем работ при условии, что он соответствует требованиям к точности измерений, климатическим условиям района и является наиболее выгодным по сравнению с другими. Под данными ДЗЗ как правило понимают лазерное сканирование, космическую съемка и аэрофотосъемку. Каждый из этих методов отличается, в первую очередь, территориальным охватом, а также детальностью получаемых материалов. В соответствии с этим требуется определить задачи, при решении которых методы ДЗЗ могут способствовать оптимизации и повышению безопасности маркшейдерского контроля.

Аэрофотосъемка с применением беспилотных авиационных систем различного типа, на борту которых установлена электронная система управления, барометр, магнитометр, ГНСС-приемник и другое оборудование [6, 7], позволяет получить данные, необходимые для моделирования, анализа, мониторинга, решения вопросов эксплуатации и т.д.

Материалы съемки, получаемые аппаратурой, установленной на борту космических аппаратов, отличается широким охватом [8]. Разрешающая способность снимков, доступных для выполнения производственных работ, пока уступает данным аэрофотосъемки, но высокая периодичность, достигаемая за счет большого числа аппаратов, введенных в эксплуатацию за последние годы, позволяет использовать их для целей мониторинга [9–11].

Активные методы дистанционного зондирования, к которым относятся радиолокационная и лазерно-локационная съемка, позволяют выполнять измерения независимо от погодных условий и времени суток [12, 13]. Кроме того, за счет определения дальности до снимаемого объекта и особенностей взаимодействия сигнала с отдельными частями объекта, появляется возможность создания цифровых моделей рельефа исследуемой территории, а также определения смещений поверхности, произошедших за период между съемками [14].

Результаты

На основании анализа возможностей решения задач маркшейдерского контроля с применением данных дистанционного зондирования Земли была составлена сравнительная таблица.

Таблица 1

Возможности применения данных ДЗЗ для маркшейдерского контроля

Виды маркшейдерского контроля	Предлагаемые методы ДЗЗ			
	Беспилотные авиационные системы	Лазерное сканирование	Космическая съемка (оптическая)	Радиолокационная съемка
Операционный контроль инженерно-геодезических изысканий	+	–	+	–
Операционный контроль ведения горных работ в границах лицензированного участков	+	–	+	–
Периодический контроль зданий и сооружений	–	+	–	+
Периодический контроль сдвижений и деформаций земной поверхности	+	+	–	+

Обсуждение

Данные, полученные методами дистанционного зондирования Земли, могут использоваться для разных целей. При выполнении горных работ происходят изменения на техногенном и антропогенном уровнях, что, несомненно, сказывается на окружающей среде, которые в последствии могут привести к катастрофам и т.д. Поэтому задача операционного и периодического контроля выполне-

ния работ должна решаться с применением технологии, обеспечивающей наиболее точную и оперативную информацию. Наибольшая оперативность на небольших территориях открытых разработок обеспечивается применением беспилотных авиационных систем, однако имеет ряд ограничений по погодным условиям. Этих недостатков лишены лазерные сканеры, обеспечивающие высокую точность измерений вне зависимости от внешних факторов.

Заключение

Методы ДЗЗ внедряются в горную отрасль и позволяют повысить экономическую эффективность и оперативность выполнения работ по операционному контролю состояния месторождений углеводородного сырья.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ПНСТ 657-2022. Нефтяная и газовая промышленность. Маркшейдерское обеспечение поиска, разведки, обустройства и разработки месторождений углеводородного сырья. М., 2022. (Федеральное агентство по техническому регулированию и метрологии).

2. ГОСТ Р 53713-2009. Месторождения нефтяные и газонефтяные. Правила разработки. М., 2009. (Федеральное агентство по техническому регулированию и метрологии).

3. ГОСТ Р 55415-2013. Месторождения газовые, газоконденсатные, нефтегазовые и нефтегазоконденсатные. Правила разработки. М., 2013. (Федеральное агентство по техническому регулированию и метрологии).

4. ГОСТ Р 58942-2020. Система обеспечения точности геометрических параметров в строительстве. Технологические допуски. М., 2020. (Федеральное агентство по техническому регулированию и метрологии).

5. СП 11-114-2004. Инженерные изыскания на континентальном шельфе для строительства морских нефтегазопромысловых сооружений. М., 2004. (Федеральное агентство по техническому регулированию и метрологии).

6. Шляхова М. М., Дедкова В. В. Контроль состояния защитных сооружений магистральных трубопроводов по материалам аэрофотосъемки с беспилотного воздушного судна ГЕОСКАН 401 // Региональные проблемы дистанционного зондирования Земли : материалы IX Международной научной конференции. 2022. С. 167–169.

7. Шляхова М. М., Дедкова В. В. Перспективы применения аэросъемок для контроля состояния защитных сооружений магистральных трубопроводов // Региональные проблемы дистанционного зондирования Земли : материалы VII Международной научной конференции,. 2020. С. 316–318.

8. Дедкова В. В., Шляхова М. М. Мониторинг технического состояния магистральных трубопроводов методами дистанционного зондирования // Региональные проблемы дистанционного зондирования Земли : материалы VII Международной научной конференции. 2020. С. 192–195.

9. Дедкова В. В., Комиссаров А. В. Анализ методов и средств контроля защитных сооружений магистральных трубопроводов // Вестник СГУГиТ. 2020. Т. 25, № 4. С. 77–84.

10. Гордиенко А. С., Ткач А. В. Исследование состояния окружающей среды в районе нефтеразработок по космическим снимкам // Вестник СГУГиТ (Сибирского государственного университета геосистем и технологий). 2022. Т. 27, № 6. С. 55-63.

11. Ткач А. В., Гордиенко А. С. Исследование состояния объектов гидрографии в районе нефтеразработок по данным дистанционного зондирования Земли // Интерэкспо Гео-Сибирь. 2022. Т. 4. С. 15-20.

12. Деменков И. О., Шляхова М. М., Ходаковская Е. О. Сравнительный анализ воздушных лазерных сканеров для мониторинга защитных сооружений магистральных Регулирова-

ние земельно-имущественных отношений в России: правовое и геопространственное обеспечение, оценка недвижимости, экология, технологические решения. – 2022. – № 1. – С. 222-225

13. Чермошенцев А. Ю., Чалкова Т.А. Современные направления ДЗ для мониторинга состояния объектов нефтедобывающей отрасли // Регулирование земельно-имущественных отношений в России: правовое и геопространственное обеспечение, оценка недвижимости, экология, технологические решения. 2021. № 3. С. 175-182.

14. Муродов С. Д., Чермошенцев А. Ю. Методика мониторинга смещений зданий и сооружений по данным космической радиолокационной съемки // Интерэкспо Гео-Сибирь. 2020. Т. 6, № 2. С. 36-40.

УДК 528.8
DOI 10.33764/2618-981X-2023-6-297-303

*А. Ю.Чермошенцев[1], В. К. Сухотин[1]**

Обзор методов сегментации точек лазерных отражений, полученных по данным лазерного сканирования

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: Suhotin-V2022@sgugit.ru

Аннотация. Обработка данных лазерного сканирования подразумевает преобразование сырых данных, полученных с помощью лазерного сканера, в массив данных, который может быть использован для создания трехмерных моделей объектов. Результаты могут быть использованы в различных областях, таких как архитектура, инженерное дело, медицина и т.д. Цель данной работы заключается в сравнении различных методов сегментации для выбора оптимальных методов при решении тех или иных задач. Рассмотрены методы сегментации на основе выделения краев, машинного обучения и иерархической структуры. Выделены преимущества и недостатки каждого метода.

Ключевые слова: сегментация, лазерное сканирование, классификация, дистанционное зондирование

*A. Yu. Chermoshentsev[1], V. K. Sukhotin[1]**

Overview of Methods for Segmentation of Point Cloud Data from Laser Scanning

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russia
*e-mail: Suhotin-V2022@sgugit.ru

Abstract. Processing of laser scanning data involves the transformation of raw data obtained using a laser scanner into a data array that can be used to create three-dimensional models of objects. The results can be used in various fields such as architecture, engineering, medicine, etc. The purpose of this work is to compare different segmentation methods to select the best ones for solving certain problems. Segmentation methods based on edge detection, machine learning and hierarchical structure are considered. The advantages and disadvantages of each method are highlighted.

Keywords: segmentation, laser scanning, classification, remote sensing

Введение

Сегментация и дальнейшая классификация облаков точек в настоящее время является одним из наиболее важных направлений развития методов обработки данных лазерного сканирования. Современные лазерные сканеры обеспечивают высокое разрешение за сравнительно небольшое время работы, что приводит к большим объемам данных. Ручная сегментация больших объемов данных отнимает много времени, поэтому процессы сегментации и классификации необходимо автоматизировать [1].

Массив точек лазерного сканирования – это цифровая модель объекта, состоящая из нескольких точек с пространственными координатами. Он содержит

геометрические характеристики отсканированного объекта, такие как форма, размер, положение и ориентация в пространстве [7]. Для успешной обработки и представления данных лазерного сканирования в процессе обработки выполняется сегментация с последующей классификацией.

Сегментация – это процесс разделения массива точек на группы в соответствии с заданными критериями (кривизна, форма, плотность и т.д.). Сегментация позволяет детальнее изучить структуру и свойства объектов. Этот процесс может выполняться вручную или автоматически без участия оператора [6].

Классификация является следующим шагом после сегментации, и каждой сегментированной группе присваивается класс (например, поверхность земли или растительность) в соответствии с ее особенностями и характеристиками для лучшей визуализации и дальнейшей обработки. Классификация таким образом может быть использована для определения того, какие объекты присутствуют в исходном облаке точек [2].

В данной статье описаны различные методы сегментации и классификации, чтобы выбрать наилучший метод для конкретной задачи. Были выделены преимущества и недостатки каждого метода.

Методы и материалы

Во время исследования различные виды сегментации были выделены три основные группы: сегментация на основе выделения краев, сегментация на основе машинного обучения, сегментация на основе иерархической структуры.

Сегментация массива точек на основе выделения краев является важным методом обработки данных в компьютерном зрении и геоинформатике. Этот метод использует алгоритмы выделения краев, такие как операторы Собеля, Лапласа и Кенни. Сегментация облака точек на основе выделения краев может использоваться для разделения облака точек на различные сегменты [9]. Структура сегментации на основе обнаружения краев показана на рисунке 1.

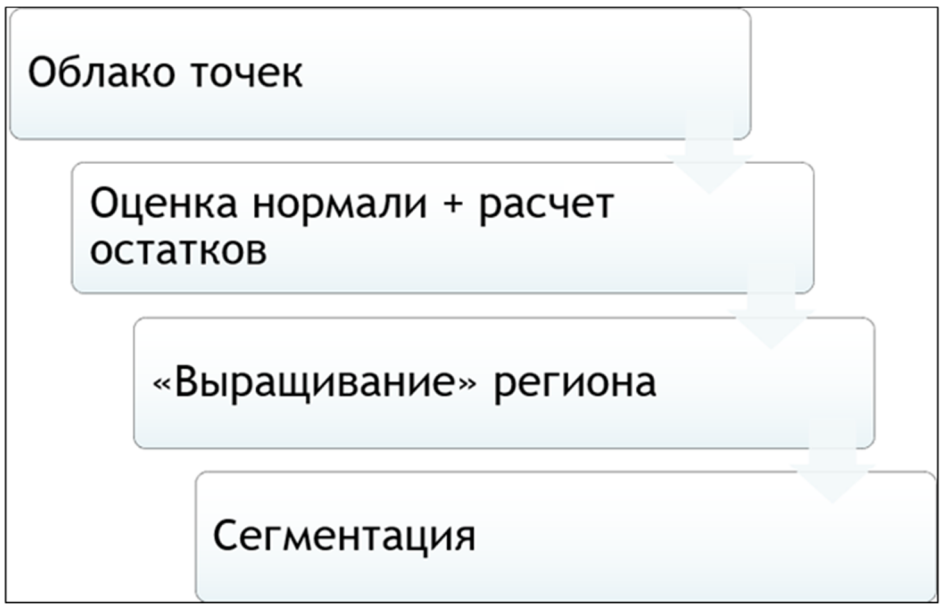


Рис. 1. Алгоритм сегментации на основе выделения краев

Основная цель алгоритма сегментации – разделить исходный массив точек на значимые подмножества и избежать как недостаточной, так и избыточной сегментации. Метод сегментации состоит нескольких этапов, показанных на рис. 2.

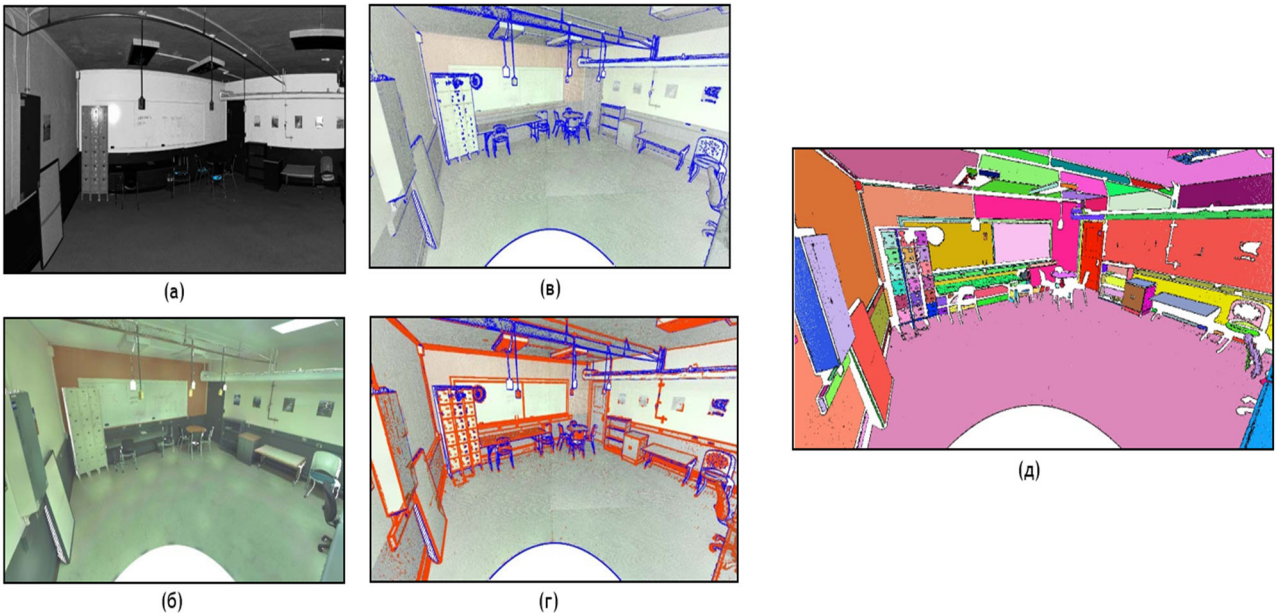


Рис. 2. Пример сегментации на основе выделения краев: а) выбор точек; б) уточнение соответствия в) оценка нормальности; г) сопоставление сегментов; д) «выращивание» области

Чтобы продемонстрировать эффективность предложенного метода, была исследована комната с 9 135 288 точками. Эта комната содержит различные объекты разного размера. Кроме того, этот набор данных содержит различные типы шума и нежелательных точек, таких как смешанные пиксели, точки с большими ошибками измерения (диапазон движения) из-за преломления на ярких или прозрачных объектах, маленькие объекты и точки, захваченные с геометрическими формами, которые не могут быть идентифицированы в данных [8]. Время обработки этого набора данных составило 10 секунд при использовании 8 потоков (без учета операций ввода-вывода данных).

В этом разделе представлены методы, использующие машинное обучение. Эти методы характеризуются использованием алгоритмов машинного обучения, которые обучаются на больших объемах помеченных данных.

PointNet - это унифицированный алгоритм (рис. 3). Он принимает облако точек в качестве прямого входа и выдает либо метки классов для всех входов или сегментов, либо метки сегментов для каждой входной точки. Базовая структура представленной сети удивительно проста, поскольку на первом этапе каждая точка рассматривается как идентичная и независимая. На первом этапе каждая точка представлена только тремя координатами (x, y, z).

Основное преимущество заключается в том, что обычные сверточные алгоритмы требуют очень регулярных форматов входных данных, таких как сетки изоб-

ражений или трехмерные воксели, для выполнения оптимизации ядра и других оптимизаций. Поскольку не существует стандартного формата для облаков точек и сеток, многие ученые часто преобразуют такие данные в регулярные 3D-воксели или коллекции изображений, прежде чем загрузить их в нейронную сеть для обработки. Однако такое преобразование представления данных может привести к очень большому объему данных и усложнить присущую инвариантность [9].

Основным элементом данного подхода является применение одной симметричной функции – функции максимального объединения. Фактически, сеть выбирает интересные или информативные точки в облаке точек и обучается набору оптимизационных функций или критериев, которые кодируют выбранные элементы.

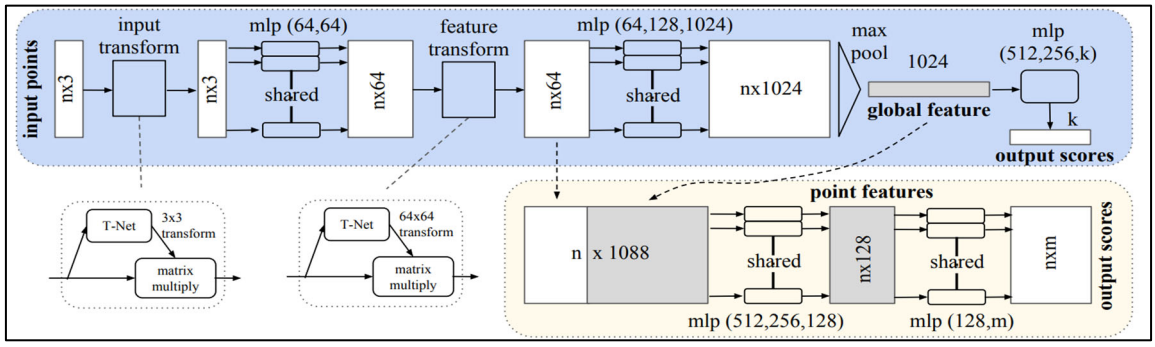


Рис. 3. Алгоритм PointNet

На (рис. 4). представлены примеры семантической сегментации и обнаружения объектов. Во время тестирования было отснято 271 комната с различными объектами. Все точки были классифицированы на 13 классов, и алгоритм показал точность проверки 78,62 % по сравнению с другими алгоритмами такого типа: первый ряд – входной набор точек со стенами и потолком, скрытыми для наглядности; второй и третий ряды - точки, принадлежащие к разным семантическим областям, обозначенные разными цветами, предсказания для точек, принадлежащих к одной семантической области, и сравнительная семантическая сегментация [10].

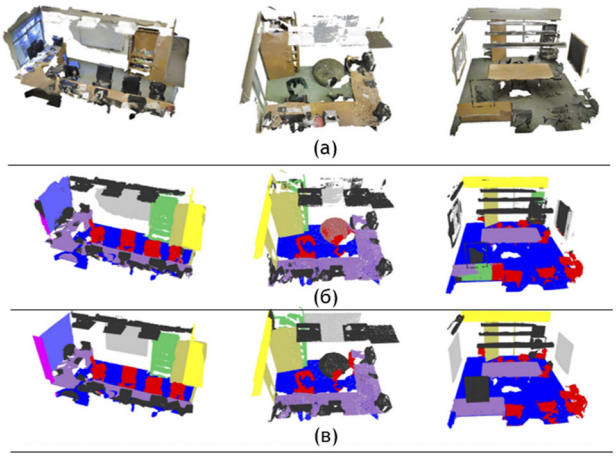


Рис. 4. Пример обработки облака точек PointNet

Сегментация на основе иерархической структуры использует иерархический подход для сегментации изображения. Этот подход основан на том, что объекты на изображении могут быть определены как набор более мелких объектов, которые, в свою очередь, могут быть определены как набор более мелких объектов. Таким образом, изображения могут быть сегментированы в иерархическую структуру объектов [4].

Алгоритмы сегментации на основе иерархической структуры начинают с разбиения изображения на простейшие сегменты. Затем эти сегменты объединяются в более крупные сегменты в соответствии с различными критериями, такими как цвет, текстура или форма. Этот процесс продолжается до тех пор, пока все сегменты не будут объединены в единую структуру [5].

Алгоритмы кластеризации, которые классифицируют объекты на основе сходства, также могут быть применены для сегментации 3D облаков точек. Широко используемый алгоритм K-Means, который может разделить точки данных на K (заранее заданный параметр, определяющий количество кластеров), был применен для классификации облаков точек на пять кластеров на основе кривизны. Недостатком алгоритма кластеризации K-Means является то, что количество кластеров должно быть определено заранее, что невозможно в большинстве случаев. Чтобы преодолеть этот недостаток, для сегментации облаков точек был использован алгоритм Mean Motion, популярный непараметрический метод кластеризации рассеянных данных [11].

Было проведено два теста по обработке облака воздушных точек. Первый тестируемый набор данных состоял из 3 433 000 точек и охватывал городскую территорию размером 5 км x 5 км. Этот набор данных включал здания, рельеф, дороги и растительность (рис. 5) показывает результаты обработки всего набора данных.

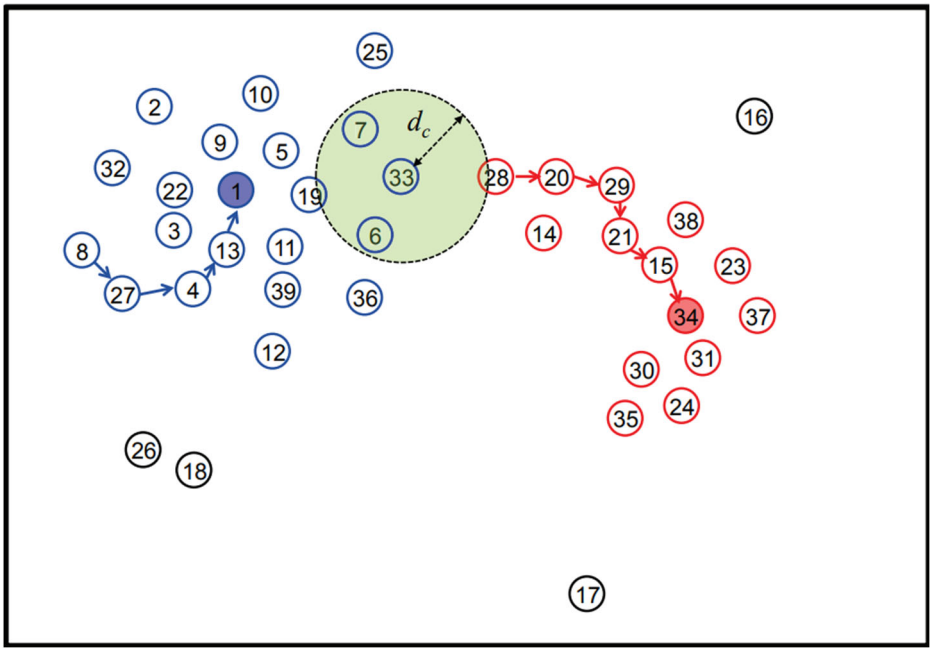


Рис. 5. Иллюстрация процедуры иерархической процедуры

Из него видно, что местность разделена дорогой (слева внизу, оранжевый) на два сегмента, фиолетовый и светло-желтый, соответственно, и что местность в фиолетовой части полностью разделена на один сегмент, хотя на поверхности есть разные объекты. Крыши зданий также в основном сегментированы, но небольшие структуры сохранились.

Второй набор данных был протестирован, как показано на (рис. 6). Он показывает, что такие объекты, как деревья и здания, почти полностью отделяются от земли в единый сегмент, а детали крыш хорошо сохраняются [8].

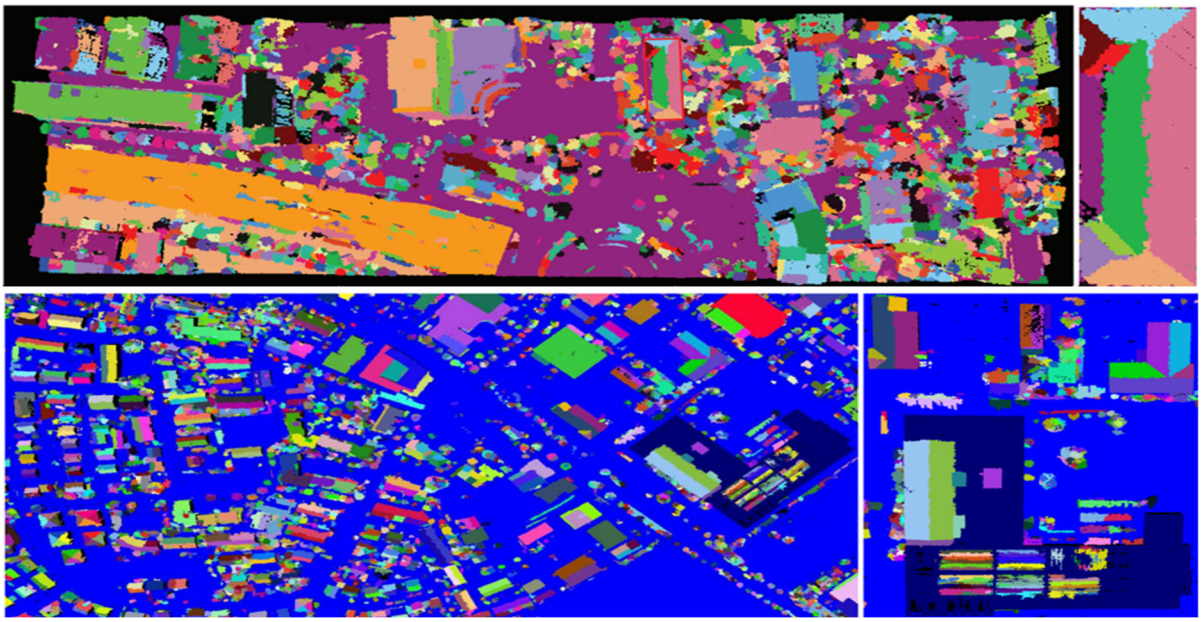


Рис. 6. Результат иерархической сегментации

Заключение

В работе были рассмотрены различные типы сегментации точек лазерного сканирования и сделаны следующие выводы.

Выбор метода сегментации зависит от конкретной задачи и характеристик данных, таких как плотность объектов и количество шума. Выбор метода сегментации зависит от конкретной задачи и характеристик данных, таких как плотность объектов и количество шума. Рекомендуется попробовать различные методы и выбрать тот, который дает наилучшие результаты для данной задачи.

Сегментация на основе выделения краев обеспечивает быструю и полностью автоматическую сегментацию. Неточные результаты получаются в случае шума или неравномерной плотности точек.

Сегментация на основе машинного обучения разделяет объекты с различными материалами, чувствительна к неоднородной плотности облака точек и сильно зависит от материалов различных частей объекта.

Сегментация на основе иерархии позволяет проводить кластеризацию на разных уровнях и анализировать данные на разных уровнях детализации. Новые точки данных могут быть добавлены к существующим кластерам. Некоторые

точки данных не могут быть отнесены ни к одному кластеру на любом уровне иерархии, что может привести к потере информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Велижев, А. В. Автоматическая сегментация облаков точек на основе элементов поверхности : статья / А. В. Велижев., Р. В. Шаповалов., Д. Потапов – Текст : непосредственный // Москва : МГУ. – 2020. – С. 2–3.
2. Джид, А. Д. Обзор методов сегментации и классификации облака точек архитектурных объектов : статья / А. Д. Джид – Текст : непосредственный // Москва : ГУЗ. – 2019. – С. 6–8.
3. Джид, А. Д. Разработка методик обработки результатов наземного лазерного сканирования для 3D-кадастра : диссертация / А. Д. Джид – Текст : непосредственный // Москва : ГУЗ – 2021. – С. 36-40.
4. Дьяченко, Р. А. Разработка методики классификации точек лазерного отражения на основе программного обеспечения Bentley Microstation : статья / Р. А. Дьяченко., Д. А. Гура., Д. А. Беспятчук. – Текст : непосредственный // Краснодар : КГТУ. – 2023. – С. 4-8.
5. Мсаллам, М. Повышение производительности классификации трехмерных облаков точек за счет увеличения данных : статья / М. Мсаллам., В. И. Сырямкин – Текст : непосредственный // Томск : ТГУ. – 2020. – С 70-72.
6. Ткачева, А. А. Классификация облака точек лазерного сканирования в задаче реконструкции естественных ландшафтных сцен : статья / А. А. Ткачева – Текст : непосредственный // Красноярск : СГАУ. – 2016. – С. 2.
7. Ткачева, А. А. Сегментация исходного облака точек лиственной массы lidar-данных на отдельные облака деревьев : статья / А. А. Ткачева – Текст : непосредственный // Красноярск : СГАУ. – 2015. – С. 2.
8. Fast edge detection and segmentation of terrestrial laser scans through normal variation analysis – Текст : электронный. – URL: https://www.researchgate.net/publication/319863884_FAST_EDGE_DETECTION_AND_SEGMENTATION_OF_TERRESTRIAL_LASER_SCANS_THROUGH_NORMAL_VARIATION_ANALYSIS (дата обращения 22.04.2023).
9. Pairwise linkage for point cloud segmentation – Текст : электронный. – URL: https://www.researchgate.net/publication/303801203_PAIRWISE_LINKAGE_FOR_POINT_CLOUD_SEGMENTATION (дата обращения 22.04.2023).
10. PointNet: Deep Learning on Point Sets for 3D Classification and Segmentation – Текст : электронный. – URL: https://arxiv.org/abs/1612.00593 (дата обращения 21.04.2023).
11. Segmentation of point clouds using smoothness constraint – Текст : электроный. – URL: https://www.researchgate.net/publication/228340970_Segmentation_of_point_clouds_using_smoothness_constraint (дата обращения 21.04.2023).

УДК 69.03:004.9
DOI 10.33764/2618-981X-2023-6-304-312

С. А. Чигридов[1], Е. Н. Кулик[1]*

Оценка пригодности территории для малоэтажного жилого строительства методами геоинформационного моделирования

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: serg.chigridov2017@yandex.ru

Аннотация. Исследование направлено на оценку пригодности территории административных районов Новосибирской области для малоэтажного жилого строительства (МЖС) с использованием геоинформационных систем (ГИС) и геоинформационного моделирования (ГИМ), учитывая различные критерии, такие как удаленность, доступность, экологичность. ГИС используется для создания картографических материалов. С помощью многокритериальной оценки (МКО) и ГИМ оцениваются и ранжируются различные районы на основе их пригодности для МЖС. В результате анализа выявлено, что на исследуемой территории имеется большое количество участков для МЖС, которые могут быть дополнительно обследованы. ГИМ также позволило определить несколько ограничений, которые необходимо учитывать при выборе участка для малоэтажного жилого строительства. Полученные данные показали, что ГИС, МКО и ГИМ являются эффективными инструментами оценки территории. В работе представлен комплексный подход, базирующийся на системном анализе к оценке пригодности районов для МЖС, который можно использовать в качестве основы для совершенствования методики и будущей реализации прикладных приложений. Методика может применяться к разным регионам и гибко адаптироваться под конкретные нужды, обеспечивая информационную поддержку устойчивого развития территорий, выделяемых для малоэтажного жилого строительства.

Ключевые слова: геоинформационное моделирование, малоэтажное жилое строительство, анализ пространственных данных, многокритериальная оценка

S. A. Chigridov[1], E. N. Kulik[1]*

Assessment of the Suitability of the Territory for Low-Rise Residential Construction by Methods of Geoinformation Modeling

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: serg.chigridov2017@yandex.ru

Annotation. The study is aimed at assessing the suitability of the territory of the administrative districts of the Novosibirsk region for low-rise residential construction (LRRC) using geoinformation systems (GIS) and geoinformation modeling (GIM), taking into account various criteria such as remoteness, accessibility, ecological compatibility. GIS is used to create cartographic materials. With the help of a multi-criteria assessment (MCA) and GIM, various districts are evaluated and ranked based on their suitability for the LRRC. As a result of the analysis, it was revealed that there are a large number of sites for LRRC in the study area, which can be additionally surveyed. GIM also made it possible to identify several constraints that must be taken into account when choosing a site for low-rise residential construction. The data obtained showed that GIS, MCA and GIM are effective tools for assessing the territory. The paper presents an integrated approach based on a system analysis to assess the suitability of areas for LRRC, which can be used as a basis for improving the methodology and future implementation of applied applications. The methodology can be applied to different

regions and flexibly adapted to specific needs, providing information support for the sustainable development of areas allocated for low-rise residential construction.

Keywords: geoinformation modeling, low-rise residential construction, spatial data analysis, multi-criteria assessment

Введение

Малоэтажное жилое строительство является важным компонентом расширения городской среды. Процесс определения оптимальных районов для строительства имеет решающее значение для обеспечения устойчивого территориального развития. ГИМ является ценным инструментом, который может быть использован при определении оптимальных районов для малоэтажного жилищного строительства. ГИМ использует анализ пространственных данных для создания подробных карт и моделей поверхности. Цель исследования – анализ технологии использования ГИМ при оценке пригодности территорий для малоэтажного жилого строительства.

Исходные данные и методология исследования

Исходными данными в исследовании являются векторные покрытия на территорию Новосибирской области (НСО), полученные с сервиса «OpenStreetMap» [15], а именно:

– дорожная сеть;
– железнодорожная сеть;
– земельные участки;
– линейная гидрография;
– площадная гидрография;
– населенные пункты НСО;
– административное деление НСО.

А также тематические покрытия, созданные в ходе исследования по поиску территорий, пригодных для размещения животноводческих производств [11]:

– защитные территории (заповедники, заказники);
– газо- и нефтепроводы;
– степень хозяйственной освоенности территории.

Дополнительно, для учета рельефа местности, была получена цифровая модель рельефа (ЦМР) на всю территорию НСО с сервиса SRTM [14].

Для определения минимальной площади застройки за эталон был выбран жилой микрорайон «Пригородный простор» в селе Толмачево, Новосибирского района (рис. 1), так как на территории данного микрорайона есть все базовые объекты, необходимые для проживания (жилые здания, парковочные места для личного автотранспорта, детские игровые площадки, детский сад, контейнерная площадка, территории для выгула собак). Площадь выбранного участка составила 330 120 кв. м. По средним подсчетам, на данной территории проживает порядка 2 000–2 500 человек.

Рис. 1. Территория микрорайона «Пригородный простор»

После сбора исходных данных и определения минимальной площади, был создан алгоритм обработки (рис. 2).

В первую очередь строится полигональный объект слоя «Область поиска», ограничивающий регион поиска, относительно границ г. Новосибирска по красной линии городской черты. Значение расстояния было выбрано равным 60 км. Данное значение определено эмпирически, на основе опроса, проведенного среди лиц, проживающих в п. Самарский, Тогучинского района, Новосибирской области, работающих на постоянной основе в г. Новосибирск.

Далее, основным принципом обработки является проведение межслойных оверлейных операций (удаление буферов, построенных по значениям минимальных расстояний из слоя, ограничивающего площадь поиска). Минимально допустимые расстояния определяются на основе государственных законодательно установленных ограничений (водный кодекс, СП градостроительство) [1, 2, 4–9]. В табл. 1 представлены значения минимальных расстояний от используемых в исследовании объектов (уже используемых в проекте и планируемых (*) к использованию).

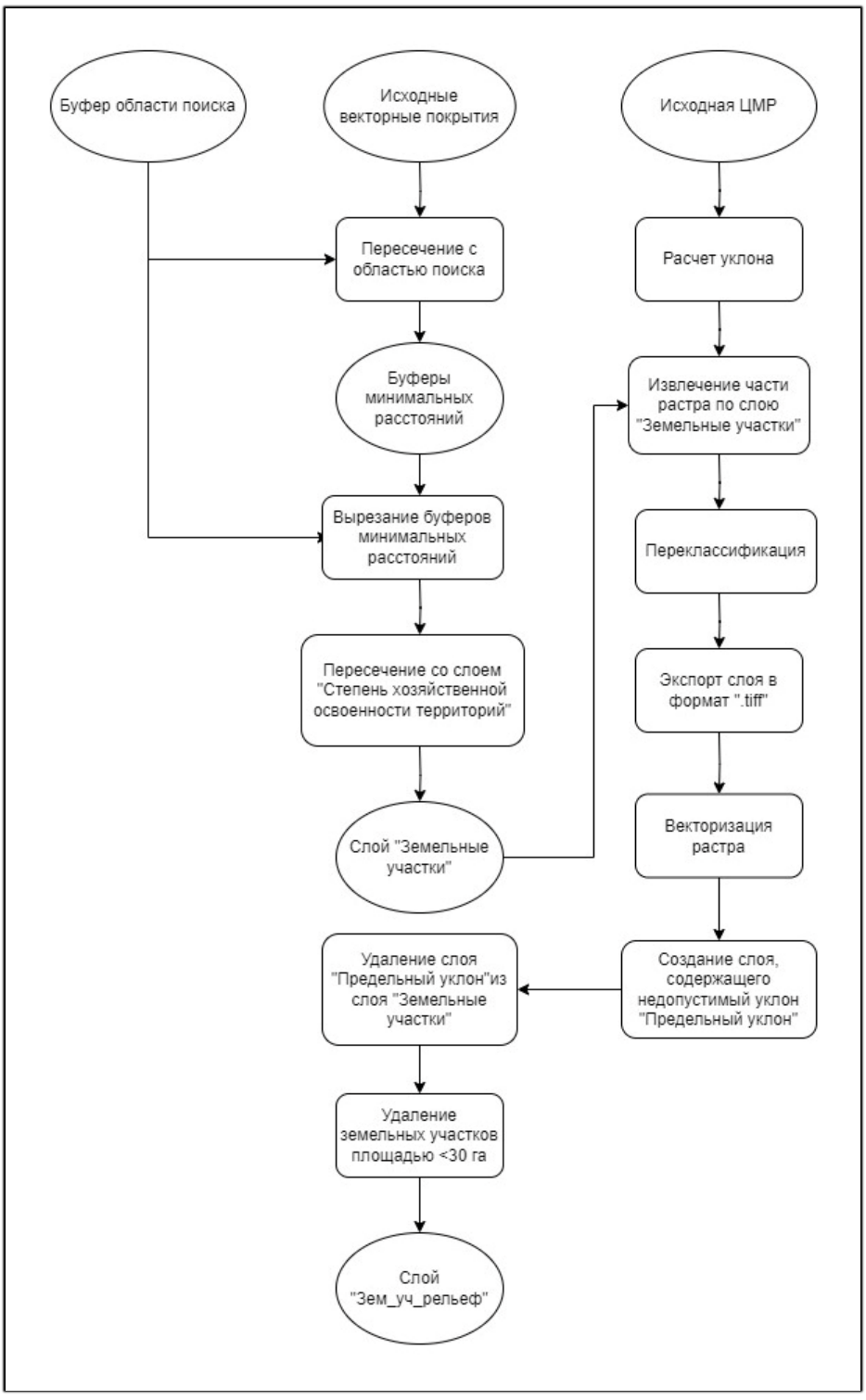


Рис. 2. Принципиальная схема ГИМ

Для оптимизации работы модели, охват слоев, буферы из которых в дальнейшем будут использоваться, был предварительно ограничен по экстенту слоя «Область поиска». Площади, расположенные внутри построенных буферов, были удалены из полигонального слоя «Область поиска». Также, из слоя «Область поиска» были исключены объекты слоя «Земельные участки», так как объекты данного слоя относятся к занятым участкам. После данной операции, вы-

полняется генерализация обследуемого региона путем построения сетки, и разбиения области интереса на элементарные участки с размером сторон ячеек 1 км на 1 км (100 га). Генерализация позволит уменьшить время обработки, выявить перспективные сегменты, для которых в дальнейшем можно провести более детальный анализ. Слой сетки был пересечен со слоем «Область поиска», для разбиения области интереса на ячейки.

Таблица 1

Исходные векторные данные

Название объектов	Минимальное расстояние, км
Дорожная сеть	0,3
Железнодорожная сеть	0,3
Линейная гидрография	0,2
Площадная гидрография	0,2
Газо-нефтепровод	0,5
ООПТ	1
Лесной фонд	*
Земли сельскохозяйственного назначения	*
Предприятия топливно-энергетического комплекса	*
Потенциальные зоны ЧС	*
Градиент грунтовых вод	*

Далее операции наложения и пересечения слоев обеспечили выбор только тех участков, которые находятся в пределах зон «освоенные» и «средне освоенные» из базового слоя «Степень хозяйственного развития территории». В результате выборки из слоя с областью интереса были исключены территории, расположенные в большей степени, в Колыванском, а также частично в Мошковском и Коченевском районах.

Следующим шагом было исключение земельных участков, для которых проведенный анализ рельефа местности показал, что их уклон превышает допустимую норму. Максимальным значением изменения превышений, при котором развитие территорий под строительство не является сложным процессом, а также не требует больших работ по механизированному выравниванию участков, является 15 % [3, 10, 12].

Результаты

В результате работы модели геоинформационной обработки был получен слой, содержащий земельные участки, потенциально удовлетворяющие требованиям для жилой застройки (рис. 3).

Общая площадь составила 282 324 Га. Из них 650 элементарных участков сохранили исходную площадь. В завершении анализа были исключены участки, площадь которых менее порога в 30 Га, установленного ранее. Что повлекло уменьшение общей площади на 214,7 Га. Административными районами, имею-

щими наибольшую площадь, подходящую для малоэтажного жилого строительства, стали:

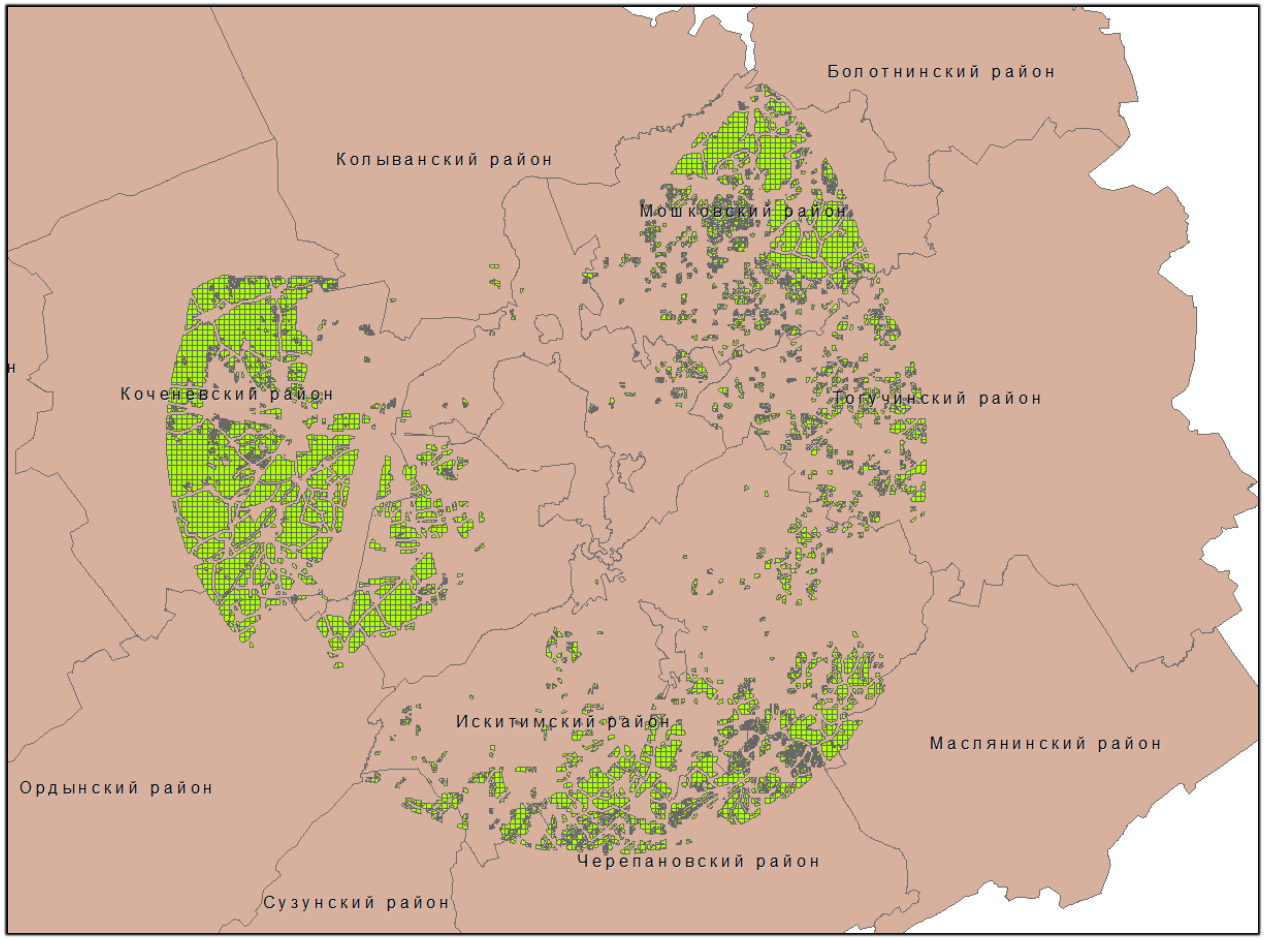


Рис. 3. Удовлетворяющие условиям земельные участки

- Коченевский – 107 763 Га;
- Мошковский – 55 176 Га;
- Искитимский – 43 694 Га;
- Новосибирский – 23 697 Га;
- Черепановский – 22 797 Га.

Доступность данных

Одними из основных проблем применения ГИС для прикладных исследований являются доступность и качество (полнота, пространственная и атрибутивная детальность) данных. В некоторых случаях необходимые данные могут быть недоступны или их детальность может быть низкой, что может повлиять на точность итогового результата. Кроме того, анализ может оказаться времязатратным и потребовать специальных сведений, доступность которых может быть ограничена.

Несмотря на обширные инструментальные возможности геоинформационного моделирования, без наличия необходимых детальных и надежных данных,

получить абсолютно совершенный результат не представляется возможным. Во главе любого качественного ГИС анализа всегда находятся пространственные данные. Необходимы цифровые материалы достаточной полноты, крупного приведенного масштаба с подробной статистической информацией в атрибутивных базах данных. По факту, нельзя утверждать, что таких данных не существует, однако не секрет, что некоторые аналитические данные являются собственностью частных компаний, доступ к которым имеют только корпоративные сотрудники. Перспектива сотрудничества с данными компаниями позволит усовершенствовать модель, повысив качество оценки территорий.

Для модели анализа текущей прикладной направленности необходимы результаты геологических изысканий, предоставляющие сведения о наличии и градиенте распределения грунтовых вод, так как при освоении пригородных территорий не всегда представляется возможность подключения коммуникаций к центральным водопроводным/канализационным сетям, что в свою очередь остро ставит вопрос о необходимости установки скважин и очистных сооружений. Данная задача влияет на общий объем инвестиций развития территорий, что скажется на рентабельности проектов. Также, необходимы данные о расположении линий электропередач (ЛЭП), инженерных коммуникаций (водоснабжение, водоотведение, газ), лесном фонде, особо охраняемых территориях и т.д.

Заключение

В данной работе представлен комплексный и системный подход к оценке пригодности районов для МЖС, который можно использовать в качестве ориентира для будущих разработок сервиса, по оценке территорий. Для расширения рассматриваемых факторов оценки территории будет информативно полезным проведение расчета показателей геоэкологического потенциала территории для выяснения зон с потенциально слабыми параметрами экологической устойчивости (геодинамические, ландшафтные и социально-экономические показатели). В дальнейшем, планируется при совершенствовании модели геоинформационной обработки пространственных данных использовать данные дистанционного зондирования Земли (спутниковые изображения) для учета распределения лесного фонда, с целью исключения негативного воздействия, нарушения экологической обстановки, что позволит параллельно выполнять оценку затрат на вырубку, при наличии на нее соответствующих разрешений. Дополнительно будет интегрирована модель расчета «распространения примесей в атмосфере», для исключения земельных участков, попадающих под воздействие загрязняющего эффекта промышленных производств и топливно-энергетических генерирующих компаний.

Не умоляя количества сложностей с получением необходимых исходных сведений и нетривиальность методологических процедур, позиция геоинформационного моделирования убедительно подтверждает важность своего инструментария для сферы таких прикладных пространственных задач, как оценка пригодности территории для малоэтажного жилищного строительства. Поскольку спрос на комфортное, качественное и экологичное жилье продолжает расти, возникает потребность в более точных и совершенных методах определения терри-

торий, пригодных для застройки. Используя геоинформационное моделирование, планировщики, инвесторы и девелоперы смогут принимать более обоснованные решения о том, где строить, что сможет спровоцировать создание более устойчивых и пригодных для комфортной жизни районов. Подход к решению данной задачи может применяться к разным природно-климатическим зонам и адаптироваться под конкретные условия и нужды, обеспечивая безопасное и успешное развитие территорий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Водный кодекс Российской Федерации. [принят Государственной Думой 12 апреля 2006 года; одобрен Советом Федерации 26 мая 2006 года] – 2006. – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/901982862
2. Водоснабжение. Наружные сети и сооружения : свод правил 31.13330.2021. [Утвержден приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 27 декабря 2021 г. N 1016/пр и введен в действие с 28 января 2022 г.] – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/728474306#7D20K3
3. Градостроительная оценка рельефа при архитектурном проектировании. – Россия, 2019. – Текст : электронный. – URL: https://vuzdoc.org/231949/agro/gradostroitelnaya_otsenka_relefa_arhitekturnom_proektirovanii
4. Градостроительство. Планировка и застройка городских и сельских поселений. [Утвержден приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 30 декабря 2016 г. N 1034/пр и введен в действие с 1 июля 2017 г.] – 2006. – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/456054209
5. Здания жилые многоквартирные : свод правил 54.13330.2016. [УТВЕРЖДЕН приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 3 декабря 2016 г. N 883/пр и введен в действие с 4 июня 2017 г.] – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/456054198#7D20K3
6. Инженерные изыскания для строительства : свод правил 47.13330.2016. [Утвержден и введен в действие Приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 30 декабря 2016 г. N 1033/пр и введен в действие с 1 июля 2017 г.] – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/456045544#7D20K3
7. Канализация. Наружные сети и сооружения : свод правил 32.13330.2012. [утвержден приказом Министерства регионального развития Российской Федерации (Минрегион России) от 29 декабря 2011 года]. – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/1200094155#7D20K3
8. Особо охраняемые природные территории Новосибирской области. – Новосибирск, 2023. – Текст : электронный. – URL: https://mpr.nso.ru/page/2668
9. Стоянки автомобилей : свод правил 113.13330.2016. [УТВЕРЖДЕН приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 7 ноября 2016 г. N 776/пр и введен в действие с 8 мая 2017 г.] – Текст : электронный // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/456044290#7D20K3
10. Характеристика пригодности территории под застройку по условиям рельефа. – Россия, 2011. – Текст : электронный – URL: https://studopedia.ru/11_14407_harakteristika-prigodnosti-territorii-pod-zastroyku-po-usloviyam-relefa.html

11. Чигридов С. А. Методы геоинформационного анализа при решении задач организации сельскохозяйственных производств / С. А. Чигридов. – Текст : непосредственный // LXX Региональная студенческая научная конференция, Новосибирск, 4-9 апреля 2022 г. – Новосибирск : Сборник тезисов-докладов в 2 ч., Ч. 2. – Новосибирск : СГУГиТ, 2022. – 152-153с.

12. Яковенко Н.Е., Тулянов А.С. Учет особенностей рельефа участка при проектировании зданий – Текст : электронный // Строительство и техногенная безопасность. 2022. №25 (77). URL: https://cyberleninka.ru/article/n/uchet-osobennostey-reliefa-uchastka-pri-proektirovanii-zdaniy.

13. Chougale, Santosh & Krishnaiah, Chikkamadaiah & Deshbhandari, Praveen. (2018). Site suitability analysis for urban development using GIS based multicriteria evaluation technique: a case study in Chikodi Taluk, Belagavi District, Karnataka, India. IOP Conference Series: Earth and Environmental Science. 169. 012017. 10.1088/1755-1315/169/1/012017. – Индия. – Текст : электронный. – URL: https://www.researchgate.net/publication/326725659_Site_suitability_analysis_for_urban_development_using_GIS_based_multicriteria_evaluation_technique_a_case_study_in_Chikodi_Taluk_Belagavi_District_Karnataka_India/citation/download

14. SRTM. – [США, 2012]. – [сайт]. – URL: https://www.dwtkns.com/srtm/

15. OpenStreetMap. – [Нидерланды, 2004] – [сайт]. – URL: https://www.open Ullah, Kazi & Mansourian, Ali. (2014). Evaluation of Land Suitability for Urban Land-Use Planning: Case Study Dhaka City. Transactions in GIS. 20. 10.1111/tgis.12137. – Бангладеш. – Текст : электронный. – URL: https://www.researchgate.net/publication/269984329_Evaluation_of_Land_Suitability_for_Urban_LandUse_Planning_Case_Study_Dhaka_City.

16. Weldemariam Gezahegn Weldu, Iguala Anteneh Deribew. Identification of Potential Sites for Housing Development Using GIS Based Multi-Criteria Evaluation in Dire Dawa City, Ethiopia. – Эфиопия. – ISBN 2307-4531. – Текст : электронный. – URL: https://core.ac.uk/download/pdf/249335129.pdf.

УДК 528.71
DOI 10.33764/2618-981X-2023-6-313-317

В. Л. Шмелев[1]*, *Е. Ю. Воронкин*[1]

Разработка программного обеспечения для метрологической службы

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: shmelevvl@mail.ru

Аннотация. В статье рассматривается процесс разработки программного обеспечения для метрологической службы, основные проблемы, с которыми столкнулась организация при работе без автоматизированной системы, а также описание используемых методов и методик для решения этих проблем. Основной упор делается на использование языка программирования JavaScript, платформы Node.js и noSQL базы данных MongoDB, фреймворка Express.js, ORM Mongoose для работы с базой данных, HTML, CSS и Bootstrap и Git. Разработанные модули упрощают работу и делают ее более эффективной. Разработанное программное обеспечение включает в себя модули для внесения данных о поверках в Федеральный информационный фонд Аршин и передачи сведений о деятельности аккредитованных лиц в Федеральную службу по аккредитации. Также были разработаны модули для автоматической генерации отчетов и статистических данных.

Ключевые слова: разработка ПО, метрология, JavaScript, Node.js, Express.js

V. L. Shmelev[1]*, *E. Y. Voronkin*[1]

Software Development for Metrological Service

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: shmelevvl@mail.ru

Abstract. The article discusses the process of software development for metrological service, main problems faced by the organization when working without an automated system, as well as description of the methods and techniques used to solve these problems. The main emphasis is on the use of the JavaScript programming language, the Node js and NoSQL databases of MongoDB, the Express.js, ORM Mongoose for working with database, HTML, CSS and Bootstrap and Git. The developed modules already simplify the work and make it more efficient. The developed software includes modules for entering verification data into the Federal Information Fund "Arshin" and transmitting information about the activities of accredited persons to the Federal Accreditation Service. Modules for automatic generation of reports and statistical data were also developed.

Keywords: software development, metrology, JavaScript, Node.js, Express.js

Введение

Метрологическая служба – это организация, которая занимается поверкой, калибровкой и аттестацией измерительных приборов и систем. Она выполняет регулярный контроль точности измерений и гарантирует соответствие измерительных приборов стандартам. В современном мире, когда точность измерений имеет большое значение, метрологическая служба является незаменимым подразделением любой организации, занимающейся производством, контролем качества и научной деятельностью [1, 2].

Как показывает практика, многие организации сталкиваются с проблемами при работе метрологической службы. Разработка программного обеспечения позволит решить проблемы с коммуникацией между отделами и улучшить эффективность работы. В данной статье мы рассмотрим основные проблемы, с которыми столкнулась организация при работе без автоматизированной системы, а также опишем технологии использованные в процессе разработки программного обеспечения для решения этих проблем.

Методы и материалы

Актуальные организации сталкиваются с необходимостью автоматизировать свои процессы для оптимизации работы и повышения эффективности. Метрологическая служба не исключение из этого правила. В данном случае, мы имеем дело с подразделением, которое занимается поверкой приборов и контролирует соответствие измерительных приборов требованиям точности и качества [3]. Для этого требуется вести учет и контроль документов, обеспечить своевременный доступ к информации и рационально использовать ресурсы. Однако, до сих пор все работы велись в разных программах, и коммуникация между подразделениями происходила в WhatsApp, Trello и Outlook. Данные хранились в Google таблицах, которые были не стабильны и работали медленно. Кроме того, много времени приходилось тратить на ручное формирование протоколов поверки, договоров, актов дефектовки, актов технического обслуживания и других документов.

Таким образом, до начала разработки программного обеспечения организация столкнулась с рядом проблем [4, 5]. Основные проблемы были связаны с отсутствием единой системы хранения данных, ручным формированием отчетов и документов, а также неэффективной коммуникацией между отделами. Для решения этих проблем было принято решение разработать собственное программное обеспечение, призванное повысить эффективность работы, объединив все функциональные задачи, и решить проблемы с коммуникацией между отделами.

При разработке программного обеспечения для метрологической службы были использованы следующие программные продукты и языки разработки.

– Язык программирования JavaScript и платформы Node.js для разработки серверной части приложения.

– Фреймворк Express для упрощения работы с HTTP-запросами и маршрутизации.

– Базы данных MongoDB для хранения и обработки больших объемов данных.

– HTML, CSS и фреймворк Bootstrap для разработки пользовательского интерфейса.

– Git система контроля версий для управления версиями кода и совместной работы над проектом.

Разработка программного обеспечения началась с анализа потребностей метрологической службы. Был проведен аудит документооборота, изучены потребности пользователей и выявлены основные проблемы. На основе полученной информации была составлена концепция будущего ПО [6].

Одним из основных инструментов для разработки программного обеспечения, является язык программирования JavaScript. Это язык высокого уровня, позволяющий создавать интерактивные веб-приложения, управлять поведением элементов страницы и обрабатывать пользовательский ввод. Для работы с языком программирования JavaScript была выбрана платформа Node.js [7–9]. Node.js – это платформа для создания серверных приложений, которая работает на языке программирования JavaScript. В качестве базы данных была выбрана база данных MongoDB, так как она предоставляет более гибкий подход к хранению данных, позволяя изменять схему данных и легко масштабировать систему. Для корректной работы запросов и их администрирования при работе с базой данных был использован ORM Mongoose, который предоставляет собой удобный API для выполнения запросов к базе данных. Минималистичный и гибкий фреймворк Express.js использовался для разработки веб-приложений на Node.js, поскольку он позволяет быстро создавать серверные приложения и обрабатывать HTTP-запросы.

Для разработки пользовательского интерфейса были использованы HTML, CSS и Bootstrap. HTML используется для разметки содержимого веб-страницы, CSS – для стилизации элементов страницы, а Bootstrap позволяет создавать красивые и адаптивные интерфейсы с минимальными усилиями, а также предоставляет множество готовых компонентов и стилей, которые можно использовать в проекте [11, 12].

Для контроля версий была использована система Git, которая позволяет отслеживать изменения в коде, сохранять их и возвращаться к предыдущим версиям при необходимости. Это облегчает совместную работу нескольких разработчиков над проектом и позволяет избежать ошибок при работе с кодом.

В работе были использованы принципы agile-разработки, такие как итеративный подход к разработке, регулярные совещания команды и участие заказчика в процессе разработки [14–16]. Это позволило команде быстро реагировать на изменения требований заказчика и создавать продукт, отвечающий его потребностям.

Результаты

Разработка программного обеспечения проходила поэтапно. На первом этапе был проведен анализ требований организации к программному обеспечению. Были выявлены основные задачи, которые должно решать ПО: автоматизация формирования документов (отчетов, протоколов поверки, договоров, актов дефектовки, актов технического обслуживания и других), улучшение коммуникации между отделами, хранение данных в одном месте для удобного доступа.

На втором этапе была проведена разработка архитектуры программного обеспечения. Было решено создать несколько модулей: модуль для передачи сведений о поверках в Федеральный информационный фонд «Аршин» и модуль для автоматизации передачи сведений о деятельности аккредитованных лиц в федеральную службу по аккредитации.

1. Разработанный модуль автоматизирует процесс передачи информации о поверке из внутренней системы в Федеральный информационный фонд «Ар-

шин». Данные о поверке формируются в удобном для пользователя виде в системе и автоматически передаются в Федеральный информационный фонд «Аршин».

2. Второй модуль автоматизирует процесс передачи сведений об аккредитованных лицах в Федеральную службу по аккредитации. Данные о деятельности аккредитованных лиц формируются в системе и автоматически передаются в систему федеральной службы по аккредитации, что позволяет сократить время на оформление документации и избежать ошибок при ручном заполнении форм.

На третьем этапе было написано кодовое ядро программного обеспечения с использованием выбранных инструментов и технологий. Каждый модуль был разработан в соответствии с требованиями организации, а также были учтены рекомендации экспертов в области метрологии.

На четвертом этапе было проведено тестирование программного обеспечения в условиях, максимально приближенных к реальным, чтобы выявить возможные ошибки и недочеты.

Заключение

Разработка программного обеспечения для метрологической службы организации - это весьма сложный и ответственный процесс, требующий знания специфики работы метрологической службы и умения выбирать правильные инструменты и технологии. Однако, благодаря правильному подходу к разработке и использованию современных технологий, можно значительно повысить эффективность работы метрологической службы, сократить временные затраты и уменьшить вероятность ошибок.

Конечно, разработка программного обеспечения не является конечной целью и требует постоянного совершенствования и улучшения, чтобы соответствовать новым требованиям организации и изменяющемуся законодательству. Однако, правильно разработанное программное обеспечение – это инструмент, который может значительно помочь в повышении эффективности работы метрологической службы и обеспечении точности измерений в организации.

Разработка программного обеспечения для метрологической службы является необходимой задачей, которая позволяет улучшить эффективность работы организации, сократить временные и материальные затраты, а также повысить качество предоставляемых услуг. При разработке программного обеспечения для метрологической службы необходимо учитывать особенности ее деятельности, а также выбирать технологии и методы разработки, которые позволяют достичь наилучших результатов. В данной статье были рассмотрены методы и методики разработки программного обеспечения для метрологической службы, а также два модуля, которые позволяют сократить время на ручное формирование отчетов и документов. Новое программное обеспечение позволяет оптимизировать работу метрологической службы, что улучшает качество ее услуг и повышает удовлетворенность клиентов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шаров, А. В. Организация метрологической службы предприятия: учебное пособие / А. В. Шаров. – М.: Инфра-М, 2019.

2. Кузнецов, В. А. Метрология, стандартизация и сертификация: учебник для вузов / В. А. Кузнецов, Н. В. Кузнецова. – М.: Издательский дом "Дело", 2018.

3. ГОСТ 8.563-96. Общие требования к метрологической службе организации.

4. ГОСТ Р ИСО/МЭК 17025-2019. Общие требования к компетентности испытательных и калибровочных лабораторий.

5. Федеральный закон от 26 июня 2008 года № 102-ФЗ "Об обеспечении единства измерений".

6. Федеральный закон от 28 июля 2012 года № 133-ФЗ "Об аккредитации в национальной системе аккредитации".

7. Федеральный закон от 27 декабря 2002 года № 184-ФЗ "О техническом регулировании".

8. Приказ Минэкономразвития России от 13 августа 2014 года № 508 "Об утверждении Правил проведения поверки средств измерений".

9. Приказ Федеральной службы по аккредитации от 29 декабря 2017 года № 190 "Об утверждении Правил аккредитации организаций, осуществляющих поверку средств измерений".

10. Приказ Федеральной службы по аккредитации от 29 декабря 2017 года № 191 "Об утверждении Правил аккредитации испытательных лабораторий".

11. Приказ Федеральной службы по аккредитации от 29 декабря 2017 года № 192 "Об утверждении Правил аккредитации калибровочных лабораторий".

12. Леонтьев, В. А. Автоматизация процессов поверки средств измерений на базе программного обеспечения / В. А. Леонтьев, Е. В. Леонтьева // Информационные технологии и вычислительные системы. – 2018. – № 2. – С. 35-39.

13. Григорьев, А. А. Разработка программного обеспечения для автоматизации процесса поверки средств измерений / А. А. Григорьев, Н. А. Григорьева // Вестник Волгоградского государственного технического университета. – 2019. – № 9. – С. 52-56.

14. Булычев, А. В. Программное обеспечение для автоматизации процесса поверки средств измерений / А. В. Булычев, А. И. Гребенщиков // Вестник Казанского технологического университета. – 2017. – Т. 20, № 5. – С. 234-238.

15. Короткова, Е. А. Разработка программного обеспечения для метрологической службы предприятия / Е. А. Короткова, А. В. Коротков // Метрология, стандартизация, сертификация. – 2018. – № 3. – С. 25-30.

16. Калугин, А. В. Программное обеспечение для автоматизации процесса поверки средств измерений на базе языка программирования Python / А. В. Калугин, Р. Р. Шамшин // Метрология, стандартизация, сертификация. – 2019. – № 2. – С. 35-39.

УДК 681.7
DOI 10.33764/2618-981X-2023-6-318-325

Е. А. Шмурыгин[1], И. О. Михайлов[1]*

Принципиальная схема устройства для селективного подбора оптических компонентов бинокулярных телескопических систем

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: podosinovik00@mail.ru

Аннотация. Бинокулярные телескопические системы играют ключевую роль в различных областях, в которых точность наблюдения и высокая качественная передача изображения имеют важное значение. В настоящее время самой экономически выгодной технологией сборки сложных устройств является селективная сборка. Решение технических и технологических проблем в области селективной сборки весьма интересная и актуальная задача, которой посвящена эта статья. В статье обусловлена суть и область применения селективной сборки. Рассмотрены основные требования к оптическим характеристикам бинокулярных приборов, предъявляемых к ним при изготовлении и приёмке. Приведена принципиальная схема устройства для селективного подбора оптических компонентов бинокулярных телескопических систем, основанная на определении фокусных расстояний бесконтактным автоматизированным способом. Представлен предварительный анализ принципиальной схемы устройства на точность. Результаты исследования, представленные в статье, демонстрируют эффективность предлагаемой принципиальной схемы устройства для селективного подбора оптических компонентов в бинокулярных телескопических системах. Предлагаемая схема позволяет повысить качество изображения, точность и оптимизировать производство бинокулярных приборов в различных сферах применения.

Ключевые слова: селективная сборка, бинокулярная телескопическая система, объектив, определение фокусного расстояния, принципиальная схема, измерительное устройство

E. A. Shmurygin[1], I. O. Mikhailov[1]*

Schematic Diagram of a Device for Selective Selection of Optical Components of Binocular Telescopic Systems

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: podosinovik00@mail.ru

Abstract. Binocular telescopic systems play a key role in various fields where the accuracy of observation and high-quality image transmission are important. Currently, the most cost-effective technology for assembling complex devices is selective assembly. Solving technical and technological problems in the field of selective assembly is a very interesting and urgent task, which this article is devoted to. The article determines the essence and scope of selective assembly. The basic requirements for the optical characteristics of binocular devices imposed on them during manufacture and acceptance are considered. A schematic diagram of a device for the selective selection of optical components of binocular telescopic systems based on the determination of focal lengths by contactless automated method is presented. A preliminary analysis of the schematic diagram of the device for accuracy is presented. The results of the research presented in the article demonstrate the effectiveness of the proposed schematic diagram of a device for selective selection of optical components in binocular telescopic systems. The proposed scheme makes it possible to improve image quality, accuracy and optimize the production of binocular devices in various fields of application.

Keywords: selective assembly, binocular telescopic system, lens, focal length determination, schematic diagram, measuring device

Введение

Бинокулярные телескопические приборы нашли применение в астрономии, спортивных мероприятиях, милитаризме, а также в научных и инженерных исследованиях. Однако, чтобы обеспечить оптимальное функционирование и достичь высокой оптической производительности в бинокулярных системах, необходимо уделить особое внимание селективному подбору оптических компонентов.

Ключевой проблемой в области оптического приборостроения является обеспечение требуемой точности изготовляемой детали или сборки.

Точность изготовления деталей – один из основных факторов, характеризующих качество прибора. Не менее важным является точность последующей сборки.

В настоящее время распространение получили следующие методы, обеспечивающие требуемую точность изделий в процессе сборки:

– метод полной взаимозаменяемости;

– меод неполной взаимозаменяемости (вероятностные методы);

– метод групповой взамозаменяемости (селективная сборка);

– метод регулировки (сборка с использованием конструктивных компенсаторов).

В рамках сборочного процесса ни один из вышеперечисленных методов не обеспечивает оптимального сочетания производительности, экономичности и качества производимых изделий.

Целью данной работы является представление принципиальной схемы устройства для селективного подбора оптических компонентов в бинокулярных телескопических системах. Основной задачей исследования является разработка нового подхода, который позволит эффективно собирать бинокулярные приборы, учитывая особенности каждой линзы.

Теоретическая значимость заключается в представлении новой принципиальной схемы устройства, основанной на передовых методах оптического моделирования и анализа. Это позволяет значительно повысить качество изображения и оптимизировать производительность бинокулярных систем. Практическая значимость заключается в разработке методологии для выбора оптимальных оптических компонентов, что способствует созданию более точных и функциональных бинокулярных телескопических систем.

Селективная сборка

Под селективной сборкой понимается широкий выбор методов, так или иначе использующих подбор необходимых комплектующих элементов изделия по их разным сопрягаемым параметрам. Зная параметры элементов, возможно рассчитывать на более высокое качество изделия, чем при использовании стандартных компонентов, не учитывающих специфические требования [3].

Область применения селективных методов – сборка прецизионных изделий механики, электроники, радиотехники, оптики и т.п. Необходимость в применении селективных методов сборки актуальна всегда, когда требуются высокие точностная характеристика или стабильность характеристик технического ихделия.

При современном развитии технологий в некоторых случаях требуемая точность комплектующих вообще не может быть гарантирована. Требуемую точность сопряжения в данном случае можно осуществить специальным подбором деталей. Такой подбор требует соблюдения значимых параметров комплектующих. Элементы, из которых формируется сборка, представляют собой отдельные детали, ранее собранные узлы, их части или даже материалы [5,11].

Важной задачей в селективной сборке является формирование сборочных комплектов, т.е. наборов деталей, направляемых на сборку.

Данный метод сборки напрямую зависит от контроля ключевых параметров всех собираемых элементов и рационального комплектования их в изделии. Методы селективной сборки относятся к классу современных новейших технологий. Именно новейших, несмотря на почтенный возраст всех основных идей. Дело в том, что с развитием современной вычислительной техники, средств измерения, контроля и автоматизации позволило в полной мере реализовать заложенные в них возможности [4].

Осуществление селективных методов сборки требует использования (а в некоторых случаях и разработки) прецизионных измерительных и контрольных средств, вычислительной техники и программного обеспечения. Высокая стоимость и сложность подобных систем предъявляют особые требования к обоснованию целесообразности их использования, что может быть получено лишь в рамках специальных математических методов, позволяющих прогнозировать эффективность селективной сборки и комплексно охарактеризовать ее. Комплексная оценка эффективности позволяет получить информацию о различных аспектах производственного процесса, таких как уровень готовности производства, объемы незавершенного производства, количество изделий, вышедших с дефектами, функциональные характеристики и т.д. Подобный анализ позволяет уже на ранних стадиях проектирования спрогнозировать возможные качества изделия и принять аргументированные решения о целесообразности или же нецелесообразности подобных действий [9,12].

Основные требвания к бинокулярным приборам

Особенность оптических свойств бинокулярных устройств определяют специфику требований, предъявляемых к ним при изготовлении и приёмке. Такие требования описаны в оптических свойствах бинокулярных приборов [7] и дополняются частными техническими условиями для каждого прибора.

Важнейшими характеристиками всех групп бинокулярных телескопических приборов с параллельными оптическими осями является параллельность оптических осей обеих труб [2].

Согласно [1], абсолютная разница увеличений оптических каналов бинокулярного устройства не должна превышать для дневных приборов 2 % при 2ω′ меньше 50°; 1,5 % при 2ω′ больше 50° (2ω′ - угловое поле в пространстве изображений) и 3 % для приборов ночного видения.

Принципиальная схема устройства

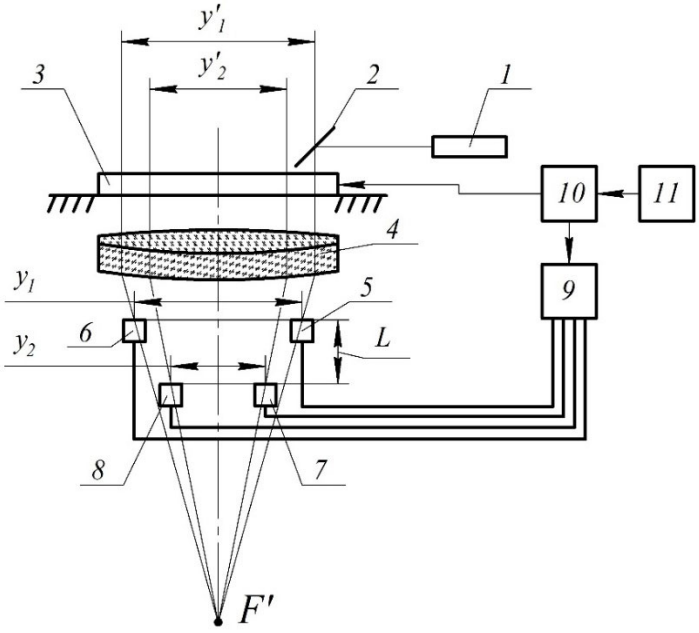
Названное требование на разность увеличений оптических каналов бинокулярных приборов могут быть обеспечены одним из двух способов:

– повышением точности изготовления линз прибора, что для массового производства является весьма затратным и экономически не выгодным решением;

– применить селективную сборку оптических узлов прибора. Этот способ весьма распространен в производстве и позволяет без ужесточения требований к точности изготовления линз комплектовать оптические функциональные узлы бинокулярных приборов. Комплектование выполняется ручным способом при измерении оптических характеристик каждого из компонентов. При этом очевидна низкая производительность и снижение количества выпускаемой продукции.

Предлагается автоматизация процесса селективного подбора оптических компонентов по их фокусному расстоянию, измеряемому при помощи опто-электронных модулей [8,13].

Ниже, на рис. 1 представленна принципиальная схема, основанная на измерении увеличения при двух положениях объекта относительно контролируемой системы.



1 – источник излучения; *2* – зеркало; *3* – каретка; *4*– проверяемый компонент; *5,6,7,8* – фотоприемники; *9* – блок обработки информации; *10* – датчик линейных перемещений; *11*– электродвигатель

Рис. 1. Принципиальная схема измерительного устройства

Данная схема работает следующим образом. Свет от лазерного источника излученя 1 отклоняемый зеркалом 2 падает на проверяемый компонент 4. При перемещении зеркала 2, установленного на каретке перпендикулярно оптической оси контролируемой детали пучок лучей за контролируемой деталью будет приломляться и затем его энергетический центр будет совмещаться с линиями раздела фотоприемных устройств (ФПУ) 5 – 8. Каретка с закрепленным зеркалом приводится в движение за сет электродвигателя 11. При совмещении пучка лучей с линией раздела фотоприемника в блоке обработки информации 9 запоминается отсчет с датчика линейного перемещения 10. При известном расстояния между плоскостями установки фотоприёмников определяется фокусное расстояния контролируемой детали.

Расстояние между плоскостями установки фотоприемников жестко фиксировано и равно L. Расстояние между фотоприемниками 5 и 6 равно y_1, а между фотоприемниками 7 и 8 – y_2. Датчик линейного перемещения подключен к входу блока обработки информации 9.

При движении каретки, узкий пучок лучей сканирует контролируемый компонент, и в тот момент, когда энергетический центр узкого пучка лучей, преломленного контролируемым компонентом, совмещается с линией раздела любого фотоприемника, в блоке управления информации запоминается отсчет с датчика линейных перемещений. Поскольку имеется четыре фотоприемника, то в блоке управления информации будет четыре фиксированных отсчета положения каретки. Попарная разность этих отсчетов дает значения изображений отрезков y'_1 и y'_2. Соответственно отрезкам y_1 и y_2.

По формуле 1 можно рассчитать фокусное расстояние оптической системы:

$$f' = \frac{L}{\frac{y_1}{y'_1} - \frac{y_2}{y'_2}} = \frac{L}{\frac{1}{\beta_1} - \frac{1}{\beta_2}} = \frac{L\beta_1\beta_2}{\beta_2 - \beta_1}, \qquad (1)$$

где L – расстояние между плоскостями установки фотоприемников; y_1 – расстояние между фотоприемниками 5 и 6; y_2 – расстояние между фотоприемниками 7 и 8; β_1 – увеличение в плоскости y_1; β_2 – увеличение в плоскости y_2.

В данном выражении величина L, y_1 и y_2 являются параметрами устройства и могут быть определены заранее с достаточной точностью. Необходимо измерить отрезки y_1 и y_2. По этим пяти параметрам в блоке управления определяется значение фокусного расстояния.

На основании формулы (1) выполняется предварительный анализ на точность, которая будет определяться среднеквадратическим отклонением (СКО) измеряемой величины [10].

$$\text{СКО}_{f'_{об}} = \sqrt{\left(\Delta f'_{y_1}\right)^2 + \left(\Delta f'_{y_2}\right)^2 + \left(\Delta f'_{y'_1}\right)^2 + \left(\Delta f'_{y'_2}\right)^2 + \left(\Delta f'_L\right)^2}, \qquad (2)$$

где $\Delta f'_{y1}$, $\Delta f'_{y2}$, $\Delta f'_{y'1}$, $\Delta f'_{y'1}$ – погрешности, связанные с погрешностями измерения соответствующих расстояний, мм; $\Delta f'_L$ – погрешность аттестации размера L, мм.

Предполагается, что контроль и подбор в пары будет выполняться для телескопической системы с видимым увеличением Г, равным 30^{x}, в которой фокусные расстояния окуляра $f'_{ок}$ и объектива $f'_{об}$ соответственно равны 10 и 300 мм.

На основании формулы (2) вычисляется СКО искомого значения [6,14]:

$$\begin{aligned} \text{СКО}_{f'_{об}} &= \sqrt{\left(\Delta f'_{y_1}\right)^2 + \left(\Delta f'_{y_2}\right)^2 + \left(\Delta f'_{y'_1}\right)^2 + \left(\Delta f'_{y'_2}\right)^2 + \left(\Delta f'_{L}\right)^2} = \\ &= \sqrt{-0,75^2 + -1,2^2 + 0,375^2 + 0,96^2 + 0,06^2} = \pm\, 1,494 \text{ мм}. \end{aligned} \tag{3}$$

Относительная погрешность измерений составляет

$$\frac{\text{СКО}_{f'_{об}}}{f'_{об}} = \frac{1,494}{300}100 = \pm\, 0,498\ \%. \tag{4}$$

Погрешность увеличения, связанная с погрешностью измерения фокусного расстояния по формуле (5)

$$\Delta\Gamma_{f'_{об}} = \frac{1}{f'_{ок}}\text{СКО}_{f'_{об}} = \frac{1}{10}1,494 = \pm\, 0,15^{\times}. \tag{5}$$

Погрешности изготовления объектива и окуляра приводят к погрешности их фокусных расстояний и, как следствие к погрешности увеличения оптической системы. Погрешность можно оценить величиной среднеквадратического отклонения $\text{СКО}_{\Sigma\Gamma}$

$$\text{СКО}_{\Gamma} = \sqrt{\left(\Delta\Gamma_{f'_{об}}\right)^2 + \left(\Delta\Gamma_{f_{ок}}\right)^2} = \sqrt{0,15^2 + 0,15^2} = \pm\, 0,21^{\times}. \tag{6}$$

Итоговая погрешность $\text{СКО}_{\Sigma\Gamma}$ в паре объективов оптических каналов

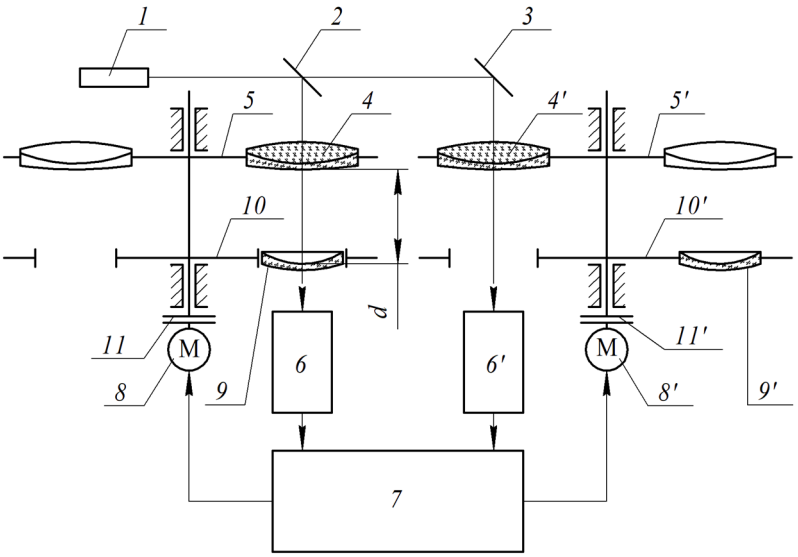
$$\text{СКО}_{\Sigma\Gamma} = \sqrt{2 \cdot \text{СКО}_{\Gamma}{}^2} = \sqrt{2 \cdot 0,21^2} = \pm\, 0,3^{\times}, \tag{7}$$

что в относительном выражении составит:

$$\frac{\text{СКО}_{\Sigma\Gamma}}{\Gamma} = \frac{0,3}{30}100 = \pm\, 1\ \%. \tag{8}$$

Принципиальная схема устройства приведена на рис. 2. Устройство работает следующим образом. От лазерного источника излучения 1 свет падает на светоделительный элемент 2, а вслед и на поверхность зеркала 3. Таким образом два сформированных пучка лучей, отклоненных на 90°, проходят через первую пару линз объектива 4, 4’, установленных на поворотном столике 5, 5’, а затем и через вторую пару линз 9, 9’, установленных на поворотном столике 10, 10’. При-

ломленный пучек лучей попадает на измерительный оптико-электронынй модуль 6, 6’, полученный результат попадает в блок обработки сигнала 7, где происходит его анализ. При подборе пар оптических систем объективов, столы на которых расположены оптические компоненты первого объектива после измерения фокусного расстояния останавливают движение, а столы, отвечающие за второй объектив, осуществляют движение до тех пор, пока не будет подобрана пара к первой оптической системе объектива. Вращение верхней пары столов осуществляется с помощью шаговых электродвигателей 8, 8’, а для нижней пары применяется муфта независимого управления столами 11, 11’.



1 – источник излучения; *2* – светоделительный элемент; *3* – зеркало; *4, 4′* – первый компонент объектива бинокулярного прибора; *5, 5′* – поворотный стол с первым оптическим компонентом; *6, 6′* – измерительный оптико-электронный модуль; *7* – блок обработки сигнала; *8, 8′* – шаговый электродвигатель; *9, 9′* – второй компонент объектива бинокулярного прибора; *10, 10′* – поворотный стол со вторым оптическим компонентом; *11, 11′* – муфта независимого управления столами

Рис. 2. Принципиальная схема устройства

Заключение

Разработка метода и устройства для селективного подбора пар объективов бинокулярных приборов является актуальной задачей для современной оптической промышленности. Предлагается принцип работы и предварительная схема устройства автоматического поэлементного подбора линз объективов бинокулярных приборов.В предложенной схеме возможно вносить необходимые правки систематических погрешностей устройства через электронный блок управления.

Предварительный анализ принципиальной схемы на точность, показал, что погрешность подбора объективов по критерию увеличения двух оптических каналов соответствует основному требованию на качество бинокулярных приборов и не превышает 1,5 %.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 50909-96. Приборы визуальные наблюдательные. Требования безопасности и методы испытаний. – Введ. 1996 – 04 – 01. – М.: Изд-во стандартов, 1997. – 12 с.- Текст: электронный. – Библиотека нормативной докумментации. – URL: https://files.stroyinf.ru/Data/94/9443.pdf (дата обращения: 10.04.2023).

2. ГОСТ 13095-82. Объективы. Методы измерения фокусного расстояния. – Введ. 1984 – 03 – 01. – М.: Изд-во стандартов, 1988. – 10 с. – Текст: электронный. – Библиотека нормативной докумментации. – URL: https://files.stroyinf.ru/Data2/1/4294838/4294838049.pdf (дата обращения: 10.04.2023).

3. Еськова, Л.М. Оптические измерения: учеб. пособие для вузов / Л. М. Еськова. – М.: Наука, 2003. – 129 с.

4. Капустина Н.М. Автоматизация проектирования технологических процессов в машиностроении: учебник для вузов. – М.: Машиностроение, 1995. – 415 с.

5. Кузнецов А. К., Исаев А. Н., Шайко И. И. Метрология: учебник для вузов. – М.: Наука, 2006. – 345с.

6. Креопалова Г. В. Оптические измерения: учебник для вузов. – М.: Машиностроение, 1987. – 264 с.

7. МРТУ 3-525-67. Особенность оптических свойств бинокулярных приборов. [Текст]. – Введ. 1994 – 11 – 14. – М.: Изд-во стандартов, 1995. – 12 с.

8. Пизюта Б. А., Михайлов И.О. Новые оптико-электронные приборы для оптических измерений: учеб. пособие для вузов. – Новосибирск: СГГА, 1996. – 77 с.

9. Погарев Г.В. Юстировка оптических приборов. – М.: Машиностроение, 1978. – Текст: непосредственный.

10. Разработка и исследование аппаратуры для измерения основных характеристик оптических систем и приборов.: сайт. – URL: http://mi-kron.narod.ru/special/stati/dis_av_ref/index.htm (дата обращения: 04.15.2023). Режим доступа: открытый. – Текст: электронный.

11. Демин В.В., Симонова Г.В. Оптические измерения: учебник для вузов. – М.: Академия, 2014. – 176 с.

12. Ершов А.Г. Автоколлимационный способ измерения фокусного расстояния объектива // Известия высших учебных заведений. Приборостроение. – 2016 № 7 С. 537 – 542.

13. Измерительная установка и способ для определения положения фокальной плоскости и эффективного фокусного расстояния оптической системы. Современная оптика [Электронный ресурс] – Режим доступа: https://goo.su/CafQf– Загл. с экрана. – Текст: электронный.

14. Карпов А. И. Оптические измерения. – М.: Академия, 2016. – 151 с.

СОДЕРЖАНИЕ

CONTENTS

Научное издание

ИНТЕРЭКСПО ГЕО-СИБИРЬ

XIX Международный научный конгресс

Сборник материалов в 8 т.

Т. 6

Магистерская научная сессия

«ПЕРВЫЕ ШАГИ В НАУКЕ»

Материалы публикуются в авторской редакции

Компьютерная верстка *О. И. Голиков*

Изд. лиц. ЛР № 020461 от 04.03.1997.
Подписано в печать 07.07.2023. Формат 60 × 84 1/16.
Усл. печ. л. 19,43. Тираж 34 экз. Заказ 96.
Гигиеническое заключение
№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плахотного, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плахотного, 8.