Научная статья
УДК 004.056.5
DOI: 10.26583/bit.2025.3.03

# ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ КАК ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

**Григорий П. Гавдан[1], Артём А. Голубев[2], Артур Г. Голубев[3], Игорь Ю. Жуков[4], Элина П. Рыбалко[5]**
*[1,3,4,5]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия*
*[2]Российский технологический университет МИРЭА, пр-т Вернадского 78, Москва, 119454, Россия*
*[1]GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076*
*[2]artemgolubev-2003@yandex.ru, https://orcid.org/0009-0007-9509-6824*
*[3]arthur59@yandex.ru, https://orcid.org/0009-0003-4665-7032*
*[4]i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799*
*[5]rybalko.elina@mail.ru, https://orcid.org/0000-0001-6292-2535*

***Аннотация.*** Целью статьи является систематизация требований защиты государственных информационных систем как объектов критической информационной инфраструктуры (КИИ) и мер по повышению их устойчивости к киберугрозам. В конкурентной борьбе в настоящее время смогут выстоять только те государства, которые действительно способны обеспечить должную защиту своих государственных информационных систем (ГИС). Для ГИС России, насчитывающих в своем составе тысячи объектов КИИ, могут возникнуть в результате различных воздействий «значимые» последствия, так как выполнение требований федерального законодательства Российской Федерации является непростой задачей. С развитием информационных технологий и возрастающими объёмами информационных ресурсов в мире увеличивается, как количество угроз, так и количество (целенаправленных) атак на ГИС. Атаки и сбои в работе ГИС могут привести к достаточно серьёзным последствиям, таким, как утечка конфиденциальной информации, нарушение общественной безопасности, возникновению угроз национальной безопасности РФ. Объектом исследования являются ГИС, функционирующие в составе КИИ. Предметом исследования выступают нормативные правовые основы защиты ГИС; математические модели оценки устойчивости; угрозы и уязвимости ГИС в условиях противоборства Рассмотрены основные определения, приведены проблемы, приводятся результаты анализ нормативных правовых документов и математических моделей оценки устойчивости, и источники, подтверждающие важность проведённого исследования. В результате исследования показана возрастающая значимость и необходимость разрешения существующих проблем. Результаты исследования могут быть использованы при дальнейшем усовершенствовании безопасности ГИС в области КИИ.

***Ключевые слова:*** *анализ нормативно-правовой базы, архивный фонд, государственная информационная система, информационная безопасность, кибервоздействие, критическая информационная инфраструктура, математические модели, угрозы, уязвимость.*

***Для цитирования:*** *Гавдан, Григорий П. и др. Обеспечение безопасности государственных информационных систем как объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 32, № 3, с. 26–43, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1822. DOI: http://dx.doi.org/10.26583/bit.2025.3.03.*

Scientific article

# MANAGING THE SECURITY OF GOVERNMENT INFORMATION SYSTEMS AS CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

**Grigory P. Gavdan[1], Artyom A. Golubev[2], Artur G. Golubev[3], Igor Y. Zhukov[4], Alina P. Rybalko[5]**
*[1,3,4,5]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia*
*[2]Russian Technological University MIREA, 78 Vernadsky Ave., Moscow, 119454, Russia*
*[1]GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076*
*[2]artemgolubev-2003@yandex.ru, https://orcid.org/0009-0007-9509-6824*
*[3]arthur59@yandex.ru, https://orcid.org/0009-0003-4665-7032*
*[4]i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799*
*[5]rybalko.elina@mail.ru, https://orcid.org/0000-0001-6292-2535*

***Abstract.*** The article aims to systematize the protection requirements for state information systems (SIS) as critical information infrastructure (CII) objects and measures of improving their resilience to cyber threats. Only states capable of managing adequate protection of their SIS will be able to withstand current competitive struggles. For the Russian GIS, which includes thousands of critical information infrastructure objects, “significant” consequences may arise as a result of various impacts, since compliance with the requirements of the federal legislation of the Russian Federation is a difficult task. With the development of information technologies and increasing global information resources, both the number of threats and the volume of (targeted) attacks on SIS are growing. Attacks and failures in SIS operation can lead to serious consequences, such as confidential information leaks, public safety disruptions, and threats to Russia's national security. The research object is SIS functioning within CII. The research subject is the regulatory legal framework for SIS protection; mathematical models for resilience assessment; threats and vulnerabilities of SIS in adversarial conditions. Key definitions, problems, and results of the analysis of regulatory legal documents and mathematical models for resilience assessment are presented, along with sources confirming the importance of the conducted research. The research demonstrates the increasing significance and necessity of resolving existing problems. The research results can be used for further improvement of SIS security in the CII domain.

***Keywords:*** *analysis of the regulatory framework, archival fund, state information system, information security, cyber interference, conflict between legislative acts, critical information infrastructure, mathematical models, object of critical information structure, threats, vulnerability.*

***For citation:*** *GAVDAN, Grigory P. et al. Managing the security of government information systems as critical information infrastructure objects. IT Security (Russia), [S.l.], v. 32, no. 3, p. 26–43, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1822. DOI: http://dx.doi.org/10.26583/bit.2025.3.03.*

## Введение

Государственные информационные системы (ГИС) содержат важную информацию, касающуюся национальной безопасности страны, экономики, обороны, правопорядка и др. аспектов жизни современного общества. С развитием информационных технологий (ИТ) увеличивается количество угроз и атак для информационные системы (ИС) [1]. Отказы и сбои в работе ГИС могут привести к достаточно серьёзным последствиям.

Рассмотрим некоторые примеры осуществлённых атак на ГИС России:

– в 2023 г. была совершена хакерская атака в отношении Федеральной таможенной службы (ФТС) России, вследствие чего было нарушено функционирование Единой автоматизированной информационной системы (ЕАИС) таможенных органов[1];

[1]Хакеры обрушили электронную систему ФТС. Газета – ведомости. Статья. А. Литова, К. Потаева. URL: https://www.vedomosti.ru/business/articles/2023/04/11/970397-hakeri-obrushili-elektronnuyu-sistemu-fts (дата обращения: 29.12.2024).

– в 2024 г. в период проведения выборов была зафиксирована огромная серия атак на государственную автоматизированную системы (ГАС) «Выборы»[2];

– в апреле 2025 г. в Центре мониторинга и управления сети связи общего пользования (ЦМУ ССОП) «Главного радиочастотного центра» (ГРЧЦ, входит в структуру Роскомнадзора) специалисты отразили 941 DDoS-атаку[3];

По итогам доклада вице-премьера Дмитрия Чернышенко в ходе брифинга, посвящённого итогам внедрения национальной программы «Цифровая экономика» за 2022 г., свыше 50% ГИС России были подвержены серьёзным угрозам отказа. Также отмечается, что в России функционирует примерно 4000 ГИС, включающих зарубежное программное обеспечение (ПО) и оборудование[4], что для государства является особенно критичным. По данным исследования угроз компании BI.ZONE в 2024 г. наибольшее количество атак (15%) пришлось на государственные организации[5] (рис. 1).

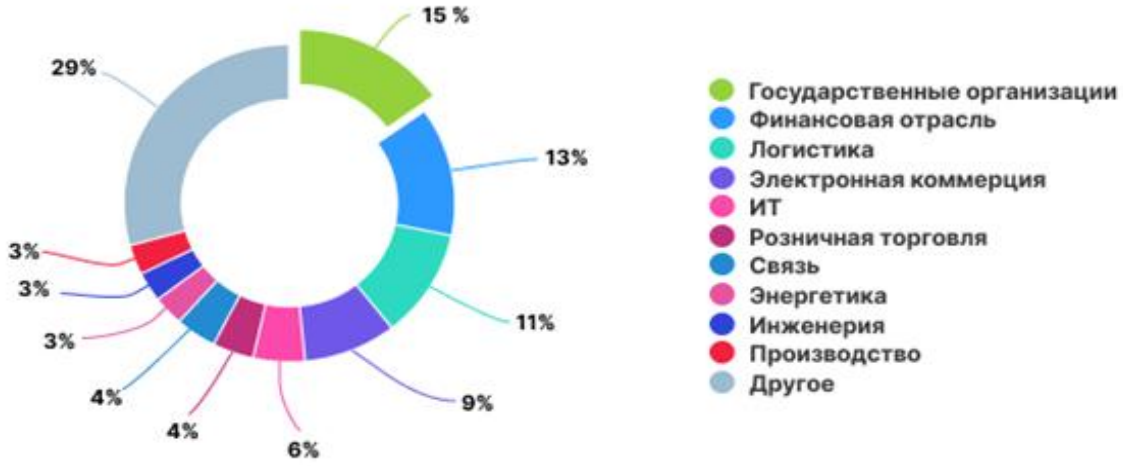


*Рис. 1. Ландшафт атакуемых отраслей за 2024 г.*[5]

В [2] отмечено, что «Эпоха интернета и больших данных несет с собой поток информации, которую можно использовать для принятия решений. В этой ситуации проблемой для своевременного и точного принятия решений является уже не отсутствие информации, а риск невозможности понимания и управления».

В настоящее время Россию продолжают обвинять в проведении информационных атак против т.н. «свободного мира» [3]: «Россия (по всему миру) использует информационные операции как часть (наступательные) киберусилий по влиянию на общественное мнение. Её кампании влияния сочетают тайные разведывательные операции и ложные онлайн-персонажи с государственными СМИ, посредниками и др.» [4]. Наряду с сушей, морем, воздухом и космосом, киберпространство, признается организацией североатлантического альянса (НАТО) как оперативная область [5]. Эксперты НАТО одобряют развитие, как оборонительного, так и оперативно кибернетического

[2]ЦИК: избирательная система попала под 12 млн DDoS-атак. URL: https://www.kommersant.ru/doc/6579031 (дата обращения: 01.12.2024).
[3]Официальный сайт Хабр. Сообщество IT-специалистов. URL: https://habr.com/ru/news/907548/ (дата обращения: 28.03.2025).
[4]Чернышенко заявил об уязвимости более половины цифровых госсистем. Газета – ведомости. Статья. Е. Киняева, А. Курашева. URL: https://www.vedomosti.ru/technology/articles/2023/01/20/959763-chernishenko-zayavil-ob-uyazvimosti-tsifrovih-gossistem (дата обращения: 02.12.2024).
[5]Threat Zone 2025. Большое ежегодное исследование ландшафта киберугроз в России и СНГ. URL: https://bi.zone/expertise/research/threat-zone-2025/ (дата обращения: 28.03.2025).

потенциала [6] государства. Так, США существенно раньше всех озаботились защитой информации (ЗИ), как в ГИС, так и критической информационной инфраструктуре (Federal Information and Information Systems и Critical Infrastructure). В США и странах запада (на основе финансирования научно-исследовательских проектов различного вида и рода направлений) продолжается заметное развитие и стремительный подъем информационных технологий. В США сосредоточены основные и ведущие научно-технические кластеры мира.

В настоящее время в России принято решение создать в министерствах и ведомствах России, а также в субъектах Федерации сеть ситуационных центров, работающих по единому регламенту. К сожалению, трудно надеяться на успех этой программы, поскольку и талантливых людей, которые способны построить эффективный и полезный центр и к тому же пользуются доверием руководства, и руководителей, готовых принять эту технологию принятия решений, в стране остро не хватает [7]. Также, не многие заказчики и операторы ГИС понимают важность комплексной защиты информации в ГИС.

Использование полученной злоумышленником информации может нанести достаточно серьезный ущерб. Именно поэтому необходимо осознанно подходить к выбору средств защиты информации в ГИС [8].

Приведённые примеры подтверждают актуальность выбранной темы исследования.

Проблема – это отсутствие комплексных методик защиты ГИС, учитывающих правовые, математические и др. аспекты.

Объектом исследования является ГИС, функционирующие в составе критической информационной инфраструктуры (КИИ).

Предметом исследования являются нормативные правовые основы защиты ГИС; математические модели оценки; угрозы и уязвимости ГИС в условиях противоборства.

В работе рассмотрены основные определения, приводятся результаты анализа нормативных правовых документов и математических моделей устойчивости, и источники, подтверждающие важность проведённого исследования.

## 1. Анализ нормативно-правовой базы

КИИ определяется как комплекс взаимосвязанных объектов, описанных выше, и каналов связи, необходимых для их функционирования. Таким образом, ГИС являются важной составной частью российской КИИ [9]. К основным нормативным правовым актам (НПА) в РФ касательно ГИС относят 187-ФЗ, 149-ФЗ, ГОСТ Р 59546-2021 и ГОСТ Р 57580.1-2017, представленные в табл. 1.

В свою очередь схема безопасности ГИС как объекта КИИ представляет собой циклический процесс, включающий несколько ключевых этапов: Анализ рисков → Аттестация объектов КИИ → Внедрение мер → Мониторинг → Актуализация.

На этапе анализа рисков определяются потенциальные угрозы безопасности информации (УБИ) и уязвимости системы. Этот этап позволяет выявить наиболее значимые риски, которые требуют принятия необходимых мер защиты.

Далее проводится аттестация объектов КИИ, целью которой является подтверждение соответствия системы защиты информации (СЗИ) ГИС требованиям безопасности информации (ТБИ). В ходе аттестации проводятся испытания и проверки, оценивается эффективность реализованных мер защиты и выявляются их недостатки.

На следующем этапе осуществляется внедрение необходимых мер ЗИ, направленных на снижение рисков, выявленных в ходе выполненного анализа. Эти меры могут быть как организационными, так и техническими.

*Таблица 1. Основные нормативные акты касательно ГИС*

| Документ | Извлечение | Применимость к ГИС как объекту КИИ |
|---|---|---|
| 187-ФЗ «О безопасности КИИ»[6] | Определяет критерии отнесения объектов к КИИ (ст. 4), требования к их защите (ст. 9-11) | Прямое регулирование безопасности ГИС как объекта КИИ. Включает требования по:<br>– классификации угроз<br>– созданию систем мониторинга инцидентов<br>– проведению аудита защищённости |
| 149-ФЗ «Об информации»[7] | Регламентирует работу с ГИС (ст. 18) | Формирует базовые требования к созданию и эксплуатации ГИС |
| Приказ ФСТЭК России №17 от 11.02.2013 [8] | Устанавливает требования к защите информации (ЗИ), не составляющей государственную тайну, в ГИС, определяя меры по обеспечению конфиденциальности, целостности и доступности информации. | Применяется ко всем ГИС, обрабатывающим информацию, не составляющую государственную тайну, устанавливая общие требования к ЗИ, в том числе к мерам технической защиты информации (ТЗИ) и организационным мероприятиям. |
| 152-ФЗ «О персональных данных»[9] | Регулирует отношения, связанные с обработкой персональных данных (ПДн), устанавливает требования к операторам, обрабатывающим ПДн. | Применяется в случаях, когда ГИС обрабатывает ПДн, устанавливая строгие требования к их защите и обработке в соответствии с законом. |
| Приказ ФСТЭК России от 25.12.2017 № 239[10] | Устанавливает требования по обеспечению безопасности значимых объектов КИИ (БЗОКИИ), включая ГИС, определяя меры по ЗИ от несанкционированного доступа (НСД), утечки, искажения и уничтожения. | Обязателен для исполнения всеми субъектами КИИ, чьи ГИС отнесены к значимым объектам, устанавливая конкретные требования к мерам ЗИ в соответствии с категорией значимости объекта КИИ. |
| ПП РФ от 06.07.2015 № 676[11] | Устанавливает требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации ГИС, а также к хранению содержащейся в их базах данных информации. | Определяет жизненный цикл ГИС как объекта КИИ, устанавливая требования к каждому этапу, включая планирование, разработку, внедрение и поддержку, а также к ЗИ на всех этапах. |
| Доктрина ИБ РФ (утв. Указом Президента РФ от 05.12.2016 № 646)[12] | Определяет основные направления государственной политики в области обеспечения информационной безопасности Российской Федерации. | Задаёт стратегические цели и задачи в области обеспечения информационной безопасности, ориентируя деятельность государственных органов и организаций, в том числе в сфере защиты ГИС как объектов КИИ. |
| Приказ ФСТЭК России от 21.12.2017 № 227 [13] | Регулирует порядок проведения аттестации объектов информатизации, включая ГИС, на соответствие требованиям о защите информации. | Устанавливает процедуру аттестации, которую должны проходить ГИС как объекты КИИ для подтверждения соответствия требованиям безопасности и возможности обработки защищаемой информации. Что подтверждает адекватность мер защиты. |

[6]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[7]Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2024) «Об информации, информационных технологиях и о защите информации».
[8]Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
[9]Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
[10]Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
[11]Постановление Правительства Российской Федерации от 06.07.2015 № 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».
[12]Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646).
[13]Приказ ФСТЭК России от 21.12.2017 № 227 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации».

После внедрения всех мер защиты организуется мониторинг безопасности, который позволяет непрерывно контролировать состояние безопасности ГИС, выявлять инциденты безопасности и своевременно на них реагировать.

Завершающим этапом является актуализация, в ходе которого СЗИ поддерживаются в рабочем состоянии, и адаптируются к изменяющимся угрозам и требованиям безопасности информации. Данный этап включает пересмотр политики безопасности, установку обновлений программного обеспечения (ПО), повторный анализ рисков и аттестацию. Механизм реализации требований для ГИС с примерами представлен в табл. 2.

*Таблица 2. Механизмы реализации требований*

| Этап | Регуляторные требования | Примеры для ГИС |
|---|---|---|
| Аттестация | Раздел VI 187-ФЗ[1] | Тестирование на устойчивость к DDoS-атакам. Проверка системы разграничения доступов. |
| Мониторинг | Статья 15.3 149-ФЗ[2] | Ежечасный сбор данных о состоянии сетевого трафика. Ведение журнала административных действий. |

Таким образом, схема представляет собой непрерывный цикл, обеспечивающий поддержание необходимого уровня безопасности ГИС как объекта КИИ.

Несоответствие терминологии:

конфликт возникает из-за разной трактовки понятий «ГИС» (149-ФЗ) и «объект КИИ» (187-ФЗ), примеры некоторых противоречий представлены в табл. 3.

*Таблица 3. Примеры противоречий*

| Термин / Закон | Определение | Проблематика |
|---|---|---|
| ГИС (ст. 14 149-ФЗ)[2] | Системы для реализации полномочий госорганов и межведомственного обмена данными | Не все ГИС автоматически становятся объектами КИИ –формально они могут не попадать под ст. 4 187-ФЗ[1] |
| Объект КИИ (ст. 4 187-ФЗ)[1] | Системы, обеспечивающие управление критически важными объектами (энергетика, транспорт, оборона и т.д.) | ГИС в «неприоритетных» сферах (например, архивы, наука) остаются без правового контроля КИИ, несмотря на их критичность |

Так, например, ГИС для управления архивными документами может быть критична для исторических исследований, но, если архив не включен в перечень ст. 4[6], её защита регулируется «слабее». В [10] подчеркивается, что создавая риски утраты данных более 40% ГИС Росархива не подпадают под критерии КИИ. 58% ГИС Росреестра не соответствуют критериям КИИ, но при этом хранят данные о границах РФ, критичные для национальной безопасности. Отсутствие детализации требований:

1) Устойчивость к продвинутым угрозам Advanced Persistent Threats-атакам (APT): требует «обеспечения устойчивости» (ст. 10), но не содержит критериев оценки и методов противодействия целенаправленным атакам. Например, атака на SolarWinds (2020 г.) показала уязвимость управления обновлениями ПО[14].

Для ГИС РФ отсутствуют нормативы по их проверке: сертификатов цифровой подписи в обновлениях; логирования изменений в конфигурациях и др. Так, например в

[14]Как происходила атака на SolarWinds. URL: https://www.securitylab.ru/blog/company/AngaraTech/350173.php (дата обращения: 02.04.2025).

2023 г. хакерская группа APT29 атаковала ГИС Минэкономразвития через уязвимости в CMS, не упомянутые ранее в стандартах ФСТЭК России[15].

2) Социальная инженерия.

Стандарты ФСТЭК России, например, акцентируют защиту ПО[16], но при этом не учитывается обучение персонала. В [11] отмечается, что 85% инцидентов в ГИС связаны с действиями сотрудников (например, пересылка учетных данных через фишинговые письма), а 73% инцидентов в ГИС связаны с утечкой учетных данных через поддельные формы авторизации.

Рассмотрим конфликт на реальном примере:

ГИС «Национальная система медицинских данных» (обрабатывает персональные данные пациентов):

– по 152-ФЗ: хранилище должно быть физически изолировано;

– по 187-ФЗ: необходимо подключение к ГосСОПКА для мониторинга кибератак, что подразумевает передачу метаданных во внешние системы.

Возникает правовая коллизия: ФСТЭК России требует «одновременного выполнения» требований, но технически это невозможно. Так, только 12% ГИС здравоохранения смогли реализовать эти два требования через полную виртуализацию трафика – остальные нарушают либо 152-ФЗ, либо 187-ФЗ.

Порядок сертификации СЗИ:

ГОСТ[17] требует использования сертифицированного СУБД.

Однако в 2023 г. 63% модулей систем управления ГИС используют open-source (открытые ПО) решения, например, такие как PostgreSQL, Kubernetes, не имеющие сертификатов ФСТЭК России. Сроки реагирования на инциденты: приказ[10] требует устранения уязвимостей категории «критические» за 24 часа.

На практике же среднее время обновлений ПО в ГИС органов власти – 14 дней [11].

Предложения по устранению коллизий:

1) Унификация терминологии: введение критерия «функциональной критичности» для ГИС (независимо от сферы) в поправках к 187-ФЗ;

2) Детализация ГОСТов: разработка профилей защиты для ГИС с учетом APT (аналогично NIST SP 800-53);

3) Межведомственные соглашения: создание исключений для передачи метаданных при интеграции с ГосСОПКА (аналогично GDPR, ст. 49).

Требование «локализации» (152-ФЗ «О персональных данных»):

Суть требования: при обработке персональных данных необходимо обеспечивать их хранение на территории РФ.

Обоснование: защита прав субъектов персональных данных, обеспечение контроля за обработкой данных со стороны российских органов власти.

Практическая реализация: размещение серверов и хранилищ данных, содержащих персональные данные, на территории РФ.

[15]Актуальные киберугрозы: II квартал 2023 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (дата обращения: 03.04.2025).

[16]Приказ ФСТЭК России от 14.03.2014 № 31-ФЗ (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» сайт ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (дата обращения 19.03.2024).

[17]ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

Последствия для ГИС: ГИС, обрабатывающие персональные данные граждан РФ, обязаны обеспечивать хранение этих данных на территории РФ.

Требование интеграции мониторинга (187-ФЗ «О безопасности КИИ»):

Суть требования: в соответствии с 187-ФЗ, объекты КИИ (включая ГИС) обязаны взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Обоснование: обеспечение централизованного мониторинга и реагирования на кибератаки на объекты КИИ.

Практическая реализация: подключение ГИС к ГосСОПКА, передача информации о событиях безопасности в ГосСОПКА.

Последствия для ГИС: ГИС должны передавать информацию о событиях безопасности (например, структурированные записи, текстовые файлы, журналы и др.) в ГосСОПКА для анализа и выявления кибератак. Соответственно, возникает конфликт требований.

Противоречие: требование «локализации» (152-ФЗ) подразумевает физическую изоляцию ГИС и хранение данных только на территории РФ, в то время как требование интеграции с государственной системой мониторинга (187-ФЗ) предполагает передачу части данных за пределы сети ГИС, а значит существует возможность хранения данных не только на территории РФ. Конфликт 152-ФЗ и 187-ФЗ представлен на рис. 2.

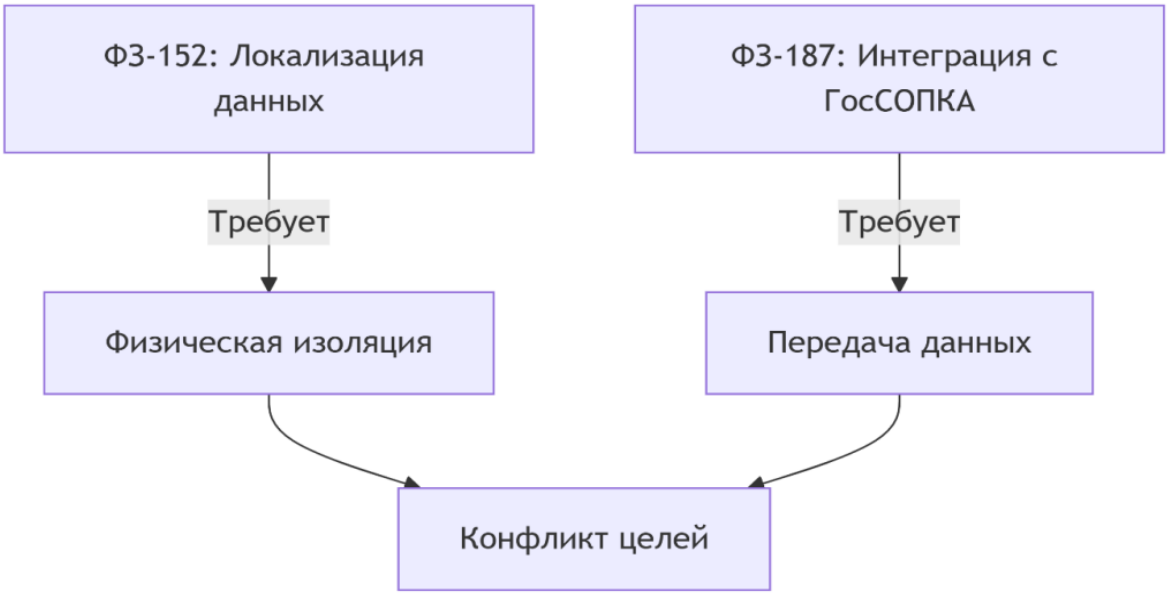


*Рис. 2. Конфликт 152-ФЗ и 187-ФЗ*

Причины конфликта:

– 152-ФЗ и 187-ФЗ преследуют разные цели (защита персональных данных и обеспечение безопасности КИИ);

– 152-ФЗ не учитывает особенности функционирования объектов КИИ.

Последствия конфликта:

– невозможность одновременного выполнения требований 152-ФЗ и 187-ФЗ;

– риск нарушения одного из законов;

– сложность обеспечения безопасности ГИС.

Возможные решения:

– разработка нормативных актов, устанавливающих исключения из требования «локализации» для ГИС, взаимодействующих с государственными системами мониторинга;

– использование необходимых технологий защиты информации, обеспечивающих конфиденциальность передаваемых данных (например, шифрование, анонимизация);

– разработка технических решений, позволяющих обеспечить интеграцию с государственными системами мониторинга без нарушения требования «локализации».

Пример демонстрирует, как коллизия между законодательными актами может создавать проблемы для операторов ГИС и требовать разработки специальных решений.

Рассмотрим некоторые примеры международного опыта решения выявленных проблем обеспечения безопасности КИИ.

1) Унификация терминологии и критериев.

США (PPD-21 / CISA):

– чёткое определение Critical Infrastructure (CI) через 16 секторов (энергетика, транспорт, здравоохранение и т.д.);

– введено понятие «Systems and Assets», что исключает спорные трактовки в NIST SP 800-53;

– результат: только 4% судебных споров связаны с классификацией объектов (DoD, 2023).

ЕС (Директива NIS2): разработана единая матрица значимости услуг, где критичность определяется через масштаб воздействия на население и зависимость других секторов.

2) Регуляторные конфликты, конфликты регуляторных требований из-за различий в законодательстве и правилах.

Решённая проблема: несовместимость требований к хранению данных и мониторингу. США (CLOUD Act):

– разрешает трансграничную передачу метаданных для мониторинга кибератак при наличии межправительственных соглашений;

– кейс: Microsoft передает данные о подозрительной активности в DHS даже для данных, хранящихся в ЕС US-EU Data Framework;.

– ЕС (GDPR, ст. 49): исключения для передачи персональных данных за пределы ЕС при защите общественных интересов (например, предотвращение кибератак) и наличии Binding Corporate Rules (BCR) для корпоративных систем.

3) Практические сложности внедрения.

Решённые проблемы:

– использование open-source без сертификации;

– неопределенность требований к защите от APT.

Германия (BSI Act): сертификация по схеме «Security by Design»:

– open-source решения (например, Kubernetes) проходят аудит на соответствие BSI-Grundschutz;

– пример: 62% государственных облаков ФРГ используют OpenStack с сертификатом BSI.

США (MITRE ATT&CK): стандартизация методов оценки устойчивости к APT через:

– матрицы тактик/техник атак (например, TTPs для атак на цепочки поставок);

– кейс: после атаки на SolarWinds CISA обязала внедрить MITRE тестирование для систем управления обновлениями.

4) Рекомендации для РФ на основе международного опыта:

а) принятие кластерного подхода (как в ЕС): разделение КИИ на кластеры (медиа, энергетика, транспорт и т.д.) с уникальными профилями защиты;

б) внедрение гибридных схем сертификации (опыт Германии): сертификация открытого ПО через независимые лаборатории (аналог BSI);

в) создание межведомственных киберполигонов: тестирование устойчивости ГИС к APT-атакам в контролируемой среде.

Примеры решений представлены в сводной таблице проблем (табл. 4).

*Таблица 4. Сводная таблица проблем*

| **Проблема** | **Страна** | **Решение** | **Результат** |
|---|---|---|---|
| Термино-логические противоречия | Канада | Закон С-26 (2022):<br>– введён критерий «прямого влияния на нацбезопасность» | Сокращение споров о классификации на 40% |
| Регуляторные конфликты | Франция | Руководства ANSSI:<br>– механизм «виртуальной – локализации» через шифрование данных | 89% медицинских систем соответствуют GDPR и NIS2 |
| Социальная инженерия | Сингапур | Программа CSA Cybersecurity Awareness Framework:<br>– ежегодные симуляции фишинга для госслужащих | Снижение успешных атак на 65% (2021–2023) |

Реализованные кейсы:

– США (DHS CDM): программа мониторинга федеральных систем, охватывающая 75% госсектора;

– Израиль (INCD Framework): обязательное использование аппаратных модулей безопасности (HSM) для ключей шифрования в ГИС.

## 2. Оценка устойчивости ГИС

Для оценки и обеспечения устойчивости ГИС как объекта КИИ к внешним воздействиям, могут применяться разнообразные математические аппараты и модели, которые позволяют анализировать уязвимости, прогнозировать последствия атак и оптимизировать стратегии защиты и др.

Оценки устойчивости, используемая в контексте анализа безопасности ИС, является инструментом для количественной и качественной оценки рисков и устойчивости системы к угрозам, что позволяет прогнозировать поведение системы в условиях внешних воздействий, оценивать эффективность мер ЗИ и принимать обоснованные решения по управлению рисками. В [12] рассматривается полумарковская модель кибератак. Модель является расширением классической марковской модели, которая описывает систему как последовательность состояний, где переход из одного состояния в другое происходит с определенной вероятностью. В отличие от марковских моделей, где время пребывания в каждом состоянии подчиняется экспоненциальному распределению, полумарковские позволяют использовать произвольные распределения времени пребывания в состояниях. Полумарковская модель представляет собой набор состояний, вероятностей перехода между этими состояниями и функций распределения времени пребывания в каждом состоянии. Состояния могут соответствовать различным этапам работы системы, уровням безопасности или фазам атак. Эти модели используются для анализа надежности и безопасности сложных систем, где время выполнения операций или время между событиями играет достаточно важную роль.

В контексте безопасности ГИС, полумарковские модели могут применяться для оценки времени, необходимого злоумышленнику для проведения атаки, или для анализа времени восстановления системы после сбоя.

Рассмотрим базовые уравнения:

Модель описывает систему с дискретными состояниями ($S_1$, $S_2$, $S_3$):

– $S_1$ — этап разведки (Reconnaissance),
– $S_2$ — внедрение эксплойта (Exploitation),
– $S_3$ — расширение привилегий (Privilege Escalation).

Переходная вероятность между состояниями:

$$P_{\text{ij}}(t) = Q_{\text{ij}}(t) \cdot \exp\left(-\lambda_j t\right),$$

где $Q_{\text{ij}}(t)$— вероятность выбора перехода из $i$ в $j$ за время $t$ (зависит от уязвимостей системы); $\lambda_j$ — интенсивность завершения этапа $j$ (например, скорость подбора пароля: $\lambda = \frac{\text{число попыток}}{\text{секунда}}$).

Пример:

При $\lambda_1 = 0.01$ сек$^{-1}$время пребывания в $S_1$ будет: $\text{E[T1]} = \frac{1}{\lambda 1} = 100$ секунд.

Матрица интенсивностей переходов:

$$\Lambda = \begin{pmatrix} -\lambda_1 & \lambda 1 Q12 & \lambda 1 Q13 \\ 0 & -\lambda_2 & \lambda 2 Q23 \\ \lambda 3 Q31 & 0 & -\lambda_3 \end{pmatrix}.$$

Применение: расчёт вероятности успешной атаки за время T = 1 час:

$$P_{\text{attack}} = 1 - \exp(-\Lambda \cdot \text{T}).$$

Рассматриваемый [13] метод Монте-Карло представляет собой статистическое моделирование, основанное на генерации случайных чисел для имитации различных сценариев и оценки вероятностей различных событий.

Метод Монте-Карло включает в себя многократное моделирование случайных событий и вычисление статистических характеристик результатов. Для каждого сценария генерируются случайные значения параметров, и на основе этих значений рассчитывается результат. Метод Монте-Карло может использоваться для оценки рисков безопасности ГИС путем моделирования различных сценариев атак и оценки вероятности успешной реализации каждой атаки. Например, можно моделировать различные варианты действий злоумышленника, учитывая различные уязвимости системы и меры защиты.

Для алгоритма симуляции используются параметры моделирования:

– $N_{\text{nodes}} = 100$ (узлов в кластере);
– $p_{\text{fail}} = 0.05$ (вероятность отказа узла/час);
– $R_{\text{threshold}} = 80\%$ (минимальная работоспособность).

Метод Монте-Карло используется для оценки устойчивости системы (например, кластера серверов) путем многократного моделирования её работы в случайных условиях. Это позволяет понять, как часто система выходит из строя при заданных параметрах надежности её компонентов. Запуск цикла симуляций ($N$ раз): для каждой симуляции определяется, какие узлы «выходят из строя» случайно. Для каждого узла генерируется случайное число от 0 до 1. Если это число меньше, чем $p_{\text{fail}}$, узел считается отказавшим.

Далее подсчитывается количество активных узлов (тех, которые не отказали) и вычисляется доля активных узлов ($\frac{\text{active}_{\text{nodes}}}{N_{\text{nodes}}}$). Если доля активных узлов меньше, чем $R_{\text{threshold}}$, то считается, что в этой симуляции система «отказала».

Для оценки устойчивости подсчитывается количество симуляций, в которых система «отказала» ($N_{\text{fail}}$).

Вычисляется вероятность отказа системы: $\frac{N_{\text{fail}}}{N_{\text{total}}}$.

Вычисляется устойчивость системы: $R = 1 - \left(\frac{N_{\text{fail}}}{N_{\text{total}}}\right)$. Это вероятность того, что система останется работоспособной.

В результате работы алгоритма получается оценка устойчивости системы ($R$), которая показывает, с какой вероятностью система будет оставаться работоспособной при заданных параметрах надежности её компонентов.

Для оптимизации метода Монте-Карло под требования ФСТЭК России необходимо учитывать следующие аспекты:

1) Учёт нормативных требований.

Банк данных (БД) угроз безопасности информации (УБИ) ФСТЭК России: позволяет использовать информацию из БД УБИ ФСТЭК России для определения вероятностей реализации различных угроз ($p_{\text{fail}}$) и для различных компонентов системы.

Требования к мерам защиты информации (ЗИ): учитывать требования ФСТЭК России к мерам ЗИ при моделировании отказов и восстановлений системы. Например, если система должна соответствовать определенному уровню защиты, то необходимо учитывать время, необходимое для восстановления системы после атаки или сбоя.

2) Адаптация параметров моделирования.

Детализация модели: учитывать особенности конкретной ГИС и ее компонентов при определении параметров моделирования. Например, для критически важных компонентов системы можно использовать более низкие значения $p_{\text{fail}}$ и более высокие значения $R_{\text{threshold}}$.

3) Валидация результатов.

Сравнение с реальными данными: сравнивать результаты моделирования с реальными данными об отказах и сбоях системы. Это позволит оценить точность модели и при необходимости внести корректировки.

Экспертная оценка: привлекать экспертов по информационной безопасности (ИБ) для оценки адекватности модели и интерпретации результатов.

4) Документирование.

Следует подробно документировать все этапы моделирования, включая описание параметров модели, алгоритма симуляции и результатов. Это позволит воспроизвести результаты моделирования и использовать их для принятия решений по управлению рисками. Обосновывать выбор параметров моделирования на основе нормативных требований, данных об отказах и сбоях системы и экспертных оценок.

Требуемая вероятность отказа $P_{\max} = \frac{10^{-3}}{\text{год}}$:

$$N_{\text{total}} > \frac{1}{P_{\max}} \Rightarrow 10^5 \text{ итераций достаточно.}$$

В целом, оптимизация метода Монте-Карло под требования ФСТЭК России требует учёта нормативных требований, адаптации параметров моделирования к особенностям конкретной ГИС, валидации результатов и подробного документирования процесса моделирования.

Теория нечётких множеств, которая позволяет описывать неопределенные и нечеткие понятия, такие как «высокий уровень угрозы» или «низкая вероятность реализации». При этом угрозы, признанные нереализуемыми, остаются в создаваемой БДУ с присвоением числового показателя, оповещающего о их нереализуемости. На каждом этапе создания должна проводиться переоценка показателей реализуемости угроз. Так, например, снижение неопределенности на этапе формирования требований, разработки концепции и создания технического задания (ТЗ) на создание АС, выполняется:

– формированием БД угроз;

– экспертной оценкой каждой УБИ с присвоением признака реализуемости, где снижение неопределённости [14] выполняется с использованием для формирования экспертного мнения группы экспертов с принятием согласованного решения по каждой УБИ.

Модель нечёткой логики состоит из набора нечётких правил, которые связывают входные с выходными параметрами. Входные и выходные параметры описываются с помощью нечётких множеств, которые позволяют учитывать неопределённость и неточность информации.

Модель нечёткой логики – это способ работы с информацией, которая не является чёткой или определённой. Для каждой лингвистической переменной определяется, насколько конкретное значение соответствует каждому словесному описанию (например, насколько число 7 соответствует «высокому» уровню угрозы).

Далее задаются правила, которые связывают разные лингвистические переменные (например, «ЕСЛИ уровень угрозы высокий И резервы низкие, ТО устойчивость низкая»).

Когда получаем конкретные значения входных параметров (например, уровень угрозы = 7, резервы = 30%), модель использует правила и функции принадлежности, чтобы определить значение выходного параметра (например, устойчивость системы).

Затем происходит дефаззификация (метод центра тяжести) – это преобразование нечёткого результата в конкретное число:

$$\text{Устойчивость} = \frac{\sum_{i=1}^{n} w_i}{\sum_{i=1}^{n} w_i \cdot c_i}.$$

Пример расчёта:

Предположим, уровень угрозы равен 7 (что соответствует высокой угрозе на 80% и средней угрозе на 20%), а резервы равны 30% (что соответствует низким резервам на 60% и оптимальным резервам на 40%):

$$\text{Устойчивость} = \frac{(0.8 \cdot 0.6) \cdot 0.2 + (0.2 \cdot 0.4) \cdot 0.7}{0.8 \cdot 0.6 + 0.2 \cdot 0.4} \approx 0.32.$$

Так, например, графы могут рассматриваться для представления и анализа различных аспектов системы, таких как сетевая топология, потоки данных, зависимости между компонентами и т.д.

Модель теории графов позволяет выявлять скрытые связи, критические узлы и потенциальные уязвимости в системе.

Компоненты системы (серверы, базы данных, пользователи, приложения) представляются в виде вершин графа, а связи между ними (сетевые соединения, потоки данных) – в виде рёбер. Используются различные алгоритмы теории графов для анализа структуры графа, выявления критических узлов, поиска кратчайших путей, обнаружения сообществ и т.д. Оцениваются риски, связанные с выявленными уязвимостями, и разрабатываются меры защиты для их устранения.

В [15] рассматривается модель массового обслуживания (МО) – это математический подход к анализу систем, в которых заявки (например, запросы к серверу, обращения пользователей в техподдержку) поступают в систему, ожидают обслуживания в очереди (если необходимо), и затем обслуживаются (обрабатываются).

Цель моделирования МО – оптимизировать работу системы, для минимизации времени ожидания в очереди, максимизировать пропускную способность и эффективно использовать ресурсы. Модель МО использует математические формулы и методы (часто основанные на теории вероятностей) для анализа характеристик системы

## 3. Угрозы и уязвимости государственных информационных систем

Обычно термин «уязвимость» ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором [16], например, правил или ошибкой в обеспечивающей безопасность конкретного компьютера программе. Более конкретно значение термина «уязвимость» в [16] определено исследовательской группой MITRE (США), занимающейся анализом критических проблем с безопасностью.

Уязвимость – это состояние вычислительной системы, которое позволяет [16]:

- использовать команды от имени др. пользователя;
- получать доступ к информации, закрытой от доступа для данного пользователя;
- показывать себя как иного пользователя или иной ресурс;
- производить атаку типа «отказ в обслуживании».

Так, в MITRE считают, что атака, производимая вследствие слабой или неверно настроенной политики безопасности, лучше описывается термином «открытость» (exposure) [17]. Созданная логическая цепочка трансформации информации подробно представлена в [17, с. 173]. Существует более 100 позиций и разновидностей УИБ ИС. По этому пользователю важно проанализировать все риски с использованием различных методик диагностики [17].

Анализ архитектуры ГИС критически важен для понимания её структуры, функциональности, и определения потенциальных векторов атак. Анализ архитектуры ГИС проводится с использованием технической документации и схем развёртывания. Итоговая архитектура ГИС включает в себя следующие ключевые компоненты:

– серверы приложений ($S1$–$S10$): предназначены для обработки запросов пользователей и выполнения бизнес-логики системы;

– шлюзы ($G1$–$G2$): обеспечивают связь между внутренними компонентами ГИС и внешними сетями, контролируют доступ к системе;

– базы данных ($DB1$–$DB3$): хранят данные, необходимые для функционирования ГИС;

– рабочие станции пользователей: используются для доступа к ГИС и работы с данными;

– сетевое оборудование: обеспечивает связь между всеми компонентами системы.

На основании анализа ГИС были составлены схемы соединений между компонентами, описывающие потоки данных и взаимодействия между ними. Каждый компонент был подробно описан с точки зрения его функций, уровней доступа и применяемых политик безопасности. Для систематического выявления потенциальных угроз[18] и уязвимостей была применена методология STRIDE, предложенная Microsoft [Shostack, 2014].

[18]Официальный сайт компании «СёрчИнформ» – ведущий российский разработчик средств ИБ. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/ (дата обращения: 27.04.2025)

В результате моделирования угроз были выявлены следующие потенциальные угрозы:

– подмена (Spoofing): злоумышленник выдаёт себя за другого пользователя или компонент системы;

– несанкционированное изменение данных (Tampering): злоумышленник изменяет данные в системе без разрешения;

– отказ от авторства (Repudiation): пользователь отрицает совершение действия в системе;

– раскрытие информации (Information Disclosure): злоумышленник получает доступ к конфиденциальным данным;

– отказ в обслуживании (Denial of Service): злоумышленник делает систему недоступной для законных пользователей;

– повышение привилегий (Elevation of Privilege): злоумышленник получает более высокие привилегии в системе, чем ему положено.

Для каждой угрозы были определены потенциальные цели злоумышленников, уязвимые компоненты системы и возможные последствия реализации угрозы.

В работе для примера рассматривается ГИС архивного фонда (ГИС АФ) предназначенная для обеспечения единого информационного пространства в сфере архивного дела. Её основная цель – обеспечить доступность информации об архивных фондах и документах для пользователей, улучшить управление архивными фондами, обеспечить сохранность архивных документов и повысить эффективность работы архивных учреждений. Были рассмотрены примерные исходные данные для моделирования такой ГИС АФ, которые помогут провести её анализ структуры и сформировать модель угроз.

Внешний веб-портал (Frontend) – это веб-сайт, с которым взаимодействуют пользователи. Этот компонент отвечает за визуальное представление данных и обработку действий пользователя.

Сервер приложений (Application Server) отвечает за обработку запросов от веб-портала, выполнение бизнес-логики и взаимосвязь с БД. Внутренняя коммуникация может использовать различные протоколы. Развернут на серверах Apache Tomcat, используется Spring Boot (Java) для обработки бизнес-логики и взаимодействия с БД.

База данных (Database) хранит информацию о пользователях, услугах и других данных. Используется система управления базой данных (СУБД) PostgreSQL (использует свой собственный протокол) с реляционной схемой для хранения данных о документах, фондах, и пользователях.

Сервер аутентификации (Authentication Server) проверяет подлинность пользователей, обычно с использованием протоколов OAuth 2.0, OpenID Connect, или SAML.

Сервер авторизации (Authorization Server) проверяет, имеет ли пользователь доступ к запрашиваемым ресурсам. Keycloak с интеграцией с LDAP для управления пользователями и ролями.

Система управления цифровыми архивами Open Content Management Interoperability Services (OpenCMIS) используется для управления электронными копиями документов (предназначена для работы с цифровыми архивами).

Сервер хранения документов Amazon S3 хранит большие объёмы данных и документов.

Система сканирования и оцифровки – решение на основе ABBYY FineReader или аналогичного ПО.

API шлюз (API Gateway) контролирует доступ к внутренним программным интерфейсам (API).

Система мониторинга (Monitoring System) отслеживает производительность и безопасность системы. Elasticsearch, Logstash, Kibana (ELK стек) для сбора и последующего анализа логов.

Протоколы SNMP/syslog/ специфичные используются для мониторинга и логирования (SNMP часто используется для мониторинга сетевых устройств, syslog – для сбора логов, а «специфичные» обозначают, что могут использоваться и др. протоколы).

Различные компоненты ГИС (Веб-портал, Сервер приложений, База данных и т.д.) отправляют данные мониторинга и логи в систему мониторинга и логирования. Это не прямая передача данных в функциональном смысле, а скорее отправка диагностической информации.

## Заключение

Существующая отечественная нормативная база создаёт системные противоречия между требованиями интеграции ГИС в КИИ и необходимостью их автономной работы. Рекомендации (на основе международного опыта), которые могут быть предложены для решения возникающих проблем, это:

а) принятие кластерного подхода;
б) внедрение гибридных схем сертификации;
в) создание межведомственных киберполигонов.

Проведенное исследование математических моделей для оценки устойчивости ИС к внешним воздействиям показывает, что: для оперативного реагирования (до 1 сек) будет эффективно использование модели нечёткой логики (используется в Real-Time SOC); для долгосрочного планирования предпочтительны полумарковские модели; метод Монте-Карло применим для аудита и проверки соответствия регуляторным требованиям; модель Теории графов применима для выявления критических точек системы; модель массового обслуживания подойдёт для оценки производительности при обработке запросов.

Исследование структуры ГИС архивного фонда на основе идентифицированных угроз, формирования нарушителя, оценки уязвимостей и построения матрицы рисков, анализа негативных последствий, сценариев и способов реализации угроз позволяет составить хорошую модель угроз ГИС АФ.

СПИСОК ЛИТЕРАТУРЫ:

1. Прогнозы Kaspersky на 2024 год: целевые атаки, ИИ-фишинг, эксплойты, BYOVD. URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-predstavila-prognoz-po-landshaftu-slozhnyh-ugroz-na-2024-god (дата обращения: 15.12.2024).
2. Audun Jøsang, Jin-Hee Cho, Feng Chen. Uncertainty Characteristics of Subjective Opinions. Conference: 2018 International Conference on Information Fusion (FUSION). URL: https://www.duo.uio.no/bitstream/handle/10852/72014/JCC2018-FUSION.pdf?sequence=1 (дата обращения 12.09.2024).
3. Рябова В. Китай признал существование кибервойск. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (дата обращения: 09.08.2024).
4. National security strategy of the United States of America DECEMBER 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 04.09.2024).
5. Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1-912764-11-2; ISSN: 2048-9870). URL: https://ccdcoe.org/uploads/2020/02/M_Pihelgas_-_Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf (дата обращения: 02.09.2024).

6. 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (дата обращения: 02.09.2024).
7. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности. Стратегические приоритеты. 2017, № 2(14), с. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (дата обращения: 15.12.2024).
8. Жумаева А.П. и др. О выборе средств защиты информации для государственных информационных систем. Известия Тульского государственного университета. Технические науки. 2018, № 10, с. 52–58. URL: https://www.elibrary.ru/item.asp?id=36617998/ (дата обращения: 02.09.2024) – EDN: YRBHCH.
9. Мещеряков В.А., Железняк В.П., Остапенко О.А. Об отнесении информационной системы к категории "государственных информационных систем". Информация и безопасность. 2014, т. 17, № 3, с. 500–502. – EDN: SZGPUZ.
10. Наталичев, Роман В. и др. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. т. 28, № 3, с. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01. – EDN JIMDXU.
11. Пенерджи, Рустем В.; Гавдан, Григорий П. Информационная безопасность государственных информационных систем. Безопасность информационных технологий, [S.l.], т. 27, № 3, с. 26–42, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.3.03. – EDN: PEHWST.
12. Муртазина, Я.Р., Жарнов Д.А. Анализ нормативно-правовой базы критической информационной инфраструктуры. Актуальные проблемы науки в студенческих исследованиях: Сборник материалов VIII Всероссийской студенческой научно-практической конференции, Альметьевск, 21–22 ноября 2018 года. Альметьевск: Издательство «Перо». 2018, с. 289–291. – EDN: GNCZPX.
13. Касенов, А.А. Полумарковская модель кибератак, воздействующих на информационную систему. Прикладная математика и фундаментальная информатика. 2021, т. 8, № 4, с. 19–25. DOI: 10.25206/2311-4908-2021-8-4-19-25. – EDN: MJPPVK.
14. Ильченко А.Н. Математическая модель и методика оценки угроз безопасности информации в информационной системе в условиях неопределенности, с. 60–65. Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (ИНФОБЕЗОПАСНОСТЬ – 2019) – EDN: CLBOVT.
15. Воеводин, В.А. Метод Монте-Карло для оценки устойчивости функционирования объекта информатизации в условиях массированных компьютерных атак. Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022, № 2, с. 66–75. DOI: 10.24143/2072-9502-2022-2-66-75. – EDN: DMUHSJ.
16. Рындюк, В.А. Использование методов нечеткой логики в решении задач защиты информации. Обработка, передача и защита информации в компьютерных системах 22: Сборник докладов Второй Международной научной конференции, Санкт-Петербург, 11–15 апреля 2022 года. Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения. 2022, с. 294–297. DOI: 10.31799/978-5-8088-1701-2-2022-2-294-297. – EDN: YLQZEN.
17. Белоус А.И., Солодуха В.А. Стандарты, концепции, методы и средства обеспечения. М: ТЕХНОСФЕРА, 2023. – 482 с. – ISBN 978-5-94836-612-8.

REFERENCES:

[1] Prognozy Kaspersky na 2024 god: celevye ataki, II-fishing, eksplojty, BYOVD. URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-predstavila-prognoz-po-landshaftu-slozhnyh-ugroz-na-2024-god (accessed: 15.12.2024) (in Russian).
[2] Audun Jøsang, Jin-Hee Cho, Feng Chen. Uncertainty Characteristics of Subjective Opinions. Conference: 2018 International Conference on Information Fusion (FUSION). URL: https://www.duo.uio.no/bitstream/handle/10852/72014/JCC2018-FUSION.pdf?sequence=1 (accessed: 12.09.2024).
[3] Ryabova V. Kitay priznal sushchestvovaniye kibervoysk. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (accessed: 09.08.2024) (in Russian).
[4] National security strategy of the United States of America DECEMBER 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed: 04.09.2024).
[5] Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1-912764-11-2; ISSN:

2048-9870). URL: https://ccdcoe.org/uploads/2020/02/M_Pihelgas_-_Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf (accessed: 02.09.2024).

[6] 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (accessed: 02.09.2024).

[7] Akhromeeva T.S., Malinetskiy G.G., Posashkov S.A. Strategies and risks of digital reality. Strategic priorities. 2017, no. 2(14), p. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (accessed: 15.12.2024) (in Russian).

[8] Zhumaeva A.P., et al. On the selection of information protection means for government informa tion systems. 2018, no. 10, p. 52–58. URL: https://www.elibrary.ru/item.asp?id=36617998 (accessed: 02.09.2024). – EDN: YRBHCH (in Russian).

[9] Meshcheryakov V.A., Zheleznyak V.P., Ostapenko O.A. Ob otnesenii informacionnoj sistemy k kategorii "gosudarstvennyh informacionnyh sistem"Informaciya i bezopasnost'. 2014, t. 17, no. 3, s. 500–502. – EDN: SZGPUZ (in Russian).

[10] Natalichev, Roman V. et al. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. IT Security (Russia), [S.l.], v. 28, n. 3, p. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01. – EDN JIMDXU (in Russian).

[11] Penerdji, Rustem V.; Gavdan, Grigory P. Information security of state information systems. IT Security (Russia), [S.l.], v. 27, no. 3, p. 26–42, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.3.03. – EDN: PEHWST (in Russian).

[12] Murtazina, Ya.R., Zharnov D.A. Analiz normativno-pravovoj bazy kriticheskoj informacionnoj infrastruktury. Aktual'nye problemy nauki v studencheskih issledovaniyah: Sbornik materialov VIII Vserossijskoj studencheskoj nauchno-prakticheskoj konferencii, Al'met'evsk, 21–22 noyabrya 2018 goda. Al'met'evsk: Izdatel'stvo «Pero». 2018, s. 289–291. – EDN: GNCZPX (in Russian).

[13] Kasenov, A.A. Semi-markov model of cyber attacks affecting the information system. Prikladnaya matematika i fundamental'naya informatika. 2021, t. 8, no. 4, s. 19–25. DOI: 10.25206/2311-4908-2021-8-4-19-25. – EDN: MJPPVK (in Russian).

[14] Ilchenko A.N. Matematicheskaya model i metodika otsenki ugroz bezopasnosti informatsii v informatsionnoy sisteme v usloviyakh neopredelennosti, s. 60-65. Sbornik dokladov XXIII plenuma FUMO VO IB i Vserossiyskoy nauchnoy konferentsii "Fundamentalnyye problemy informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii" (INFOBEZOPASNOST – 2019) – EDN: CLBOVT (in Russian).

[15] Voevodin, V.A. Monte carlo method for estimating informatization object stable functioning in conditions of massive computer attacks. Vestnik Astrahanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika. 2022, no 2, s. 66–75. DOI: 10.24143/2072-9502-2022-2-66-75. – EDN: DMUHSJ (in Russian).

[16] Ryndyuk, V.A. The use of fuzzy logic methods in solving information security problems. Obrabotka, peredacha i zashchita informacii v komp'yuternyh sistemah 22: Sbornik dokladov Vtoroj Mezhdunarodnoj nauchnoj konferencii, Sankt-Peterburg, 11–15 aprelya 2022 goda. Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet aerokosmicheskogo priborostroeniya. 2022, s. 294–297. DOI: 10.31799/978-5-8088-1701-2-2022-2-294-297. – EDN: YLQZEN (in Russian).

[17] Belous A.I., Soloduha V.A. Standarty, koncepcii, metody i sredstva obespecheniya. M.: TEHNOSFERA, 2023. – 482 s. – ISBN 978-5-94836-612-8 (in Russian).

*Статья поступила в редакцию 20.05.2025; одобрена после рецензирования 06.07.2025;*
*принята к публикации 20.07.2025*
*The article was submitted 20.05.2025; approved after reviewing 06.07.2025.*
*accepted for publication 20.07.2025*