ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056:658.5

ИНТЕГРАЦИЯ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫ В КОМПЛЕКСНУЮ СИСТЕМУ БЕЗОПАСНОСТИ ОБЪЕКТОВ КИИ РЕГИОНАЛЬНОГО УРОВНЯ

Пензовская Елена Сергеевна,
студент, кафедра защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Россия, г. Санкт-Петербург
e-mail: l.pes.0502@mail.ru

Аннотация

В статье рассматривается проблема интеграции специальных технических средств физической защиты в комплексную систему безопасности объектов критической информационной инфраструктуры регионального уровня. Актуальность исследования обусловлена ростом комбинированных физико-кибернетических угроз и необходимостью обеспечения единой картины событий безопасности. Цель работы заключается в разработке методики интеграции СТС физической защиты в комплексную систему безопасности объектов КИИ регионального уровня. Предлагаемая методика включает классификацию интеграционных признаков технических средств, архитектурную модель взаимодействия подсистем и алгоритм корреляции событий. Результаты демонстрируют сокращение времени обнаружения инцидентов на 40–55% (с 8–12 мин до 4–5 мин), повышение полноты регистрации событий до 95–97% и снижение уровня ложных тревог до 60%. Практическая значимость заключается в возможности применения предложенной методики на региональных объектах КИИ с ограниченными ресурсами и распределённой инфраструктурой.

Ключевые слова: критическая информационная инфраструктура, физическая защита, специальные технические средства, интеграция систем безопасности, региональный уровень, корреляция событий, SIEM, PSIM

INTEGRATION OF SPECIAL TECHNICAL MEANS OF PHYSICAL PROTECTION INTO A COMPREHENSIVE SECURITY SYSTEM OF REGIONAL-LEVEL CII FACILITIES

Penzovskaya Elena Sergeevna,
student, Department of Secure Communication Systems, Prof. M. A. Bonch-Bruyevich Saint Petersburg State University of Telecommunications, Russia, Saint Petersburg
e-mail: smirnov.av@stud.penza.ru
e-mail: l.pes.0502@mail.ru

ABSTRACT

The article examines the problem of integrating special technical means of physical protection into a comprehensive security system of regional-level critical information infrastructure facilities. The relevance of the study is driven by the growth of combined physical-cyber threats and the need to ensure a unified security event view. The purpose of the work is to develop a methodology for integrating special technical means of physical protection into a comprehensive security system of regional-level CII facilities. The proposed methodology includes a classification of integration features of technical means, an architectural model of subsystem interaction, and an event correlation algorithm. The results demonstrate a 40–55% reduction in incident detection time (from 8–12 minutes to 4–5 minutes), an increase in event registration completeness to 95–97%, and a reduction in false alarms by up to 60%. The practical significance lies in the possibility of applying the proposed methodology to regional CII facilities with limited resources and distributed infrastructure.

Keywords: critical information infrastructure, physical protection, special technical means, security systems integration, regional level, event correlation, SIEM, PSIM

Введение

Обеспечение безопасности объектов критической информационной инфраструктуры (КИИ) регионального уровня представляет собой комплексную задачу, требующую согласованного функционирования множества подсистем защиты. В условиях роста комбинированных угроз, сочетающих физическое проникновение и кибератаки, традиционный подход к раздельному функционированию систем физической и информационной безопасности демонстрирует недостаточную эффективность [6, с. 22; 12].

Актуальность исследования определяется несколькими факторами. Во-первых, региональные объекты КИИ характеризуются распределённостью площадок, ограниченным бюджетом на безопасность и необходимостью поддержания работоспособности при нестабильном канале связи с центром мониторинга [3, с. 234; 4, с. 56]. Во-вторых, нормативные требования к защите КИИ, установленные Федеральным законом № 187-ФЗ и подзаконными актами ФСТЭК России, предполагают комплексный подход к оценке защищённости, включающий как технические, так и организационные меры [1; 2]. В-третьих, значительная часть инцидентов начинается с событий физического уровня или сопровождается ими, что требует корреляции событий физической и информационной подсистем [7, с. 42; 12].

Проблема исследования заключается в отсутствии структурированной методики интеграции специальных технических средств физической защиты — систем контроля и управления доступом, видеонаблюдения, охранной сигнализации и периметральных датчиков — с системами мониторинга информационной безопасности. Существующие решения либо ориентированы на крупные федеральные объекты с существенными ресурсами, либо представляют собой разрозненные подсистемы без единого центра анализа событий [6, с. 22; 14].

Цель исследования заключается в разработке такой методики. Гипотеза состоит в том, что поэтапная интеграция СТС физической защиты, основанная на их классификации по интеграционным признакам, построении единой архитектуры и корреляции событий в контуре SIEM/SOC, позволит сократить время обнаружения инцидентов, повысить полноту регистрации событий и снизить уровень ложных срабатываний. Для достижения поставленной цели в работе решаются следующие задачи: проанализировать специфику региональных объектов КИИ и требования к их защите; разработать классификацию СТС по интеграционным признакам; предложить архитектурную модель интеграции;

сформировать алгоритм корреляции событий; провести апробацию и оценить результативность предложенной методики.

Обзор исследований и место работы в научном контексте

Вопросы обеспечения безопасности КИИ активно исследуются в российской научной среде. Киселев Н. Н. в серии работ рассмотрел законодательные и организационные меры защиты объектов критической инфраструктуры [3, с. 234], техническую защиту информации как составляющую комплексной безопасности [9, с. 10], а также метод автоматизации процедуры аттестации объектов КИИ в удалённых регионах [4, с. 56]. Существенное значение имеет исследование декомпозиции требований оценки защищённости объекта КИИ по функциональному назначению, где подчёркивается необходимость учёта физической защиты как неотъемлемого элемента комплексной системы [10, с. 479].

Майоров А. В. совместно с коллегами разработал программное обеспечение сбора данных о сетевом трафике корпоративных информационных систем, что создаёт техническую основу для интеграции телеметрии различных подсистем безопасности [5, с. 69]. Вместе с тем в указанных работах вопрос интеграции СТС физической защиты с системами мониторинга ИБ рассмотрен фрагментарно, без формирования единой последовательности проектных и эксплуатационных действий для регионального уровня [7, с. 42; 14].

Зарубежные исследования фокусируются преимущественно на концепции Physical Security Information Management (PSIM), предполагающей централизованное управление событиями физической безопасности [14]. Однако применение таких систем в условиях российских региональных объектов КИИ ограничено требованиями импортозамещения и спецификой нормативного регулирования [15].

Таким образом, в научной литературе недостаточно представлены комплексные исследования, в которых классификация СТС, архитектурная модель взаимодействия подсистем и алгоритм корреляции событий объединены в единую методику интеграции для объектов КИИ регионального уровня [12; 14].

Научная новизна данной работы заключается в следующем:

Предложена архитектурная модель интеграции СТС физической защиты в комплексную систему безопасности, адаптированная для объектов КИИ регионального уровня с учётом ограничений по ресурсам и каналам связи.

Разработана матрица классификации СТС по интеграционным признакам, позволяющая стандартизировать подключение разнородных технических средств и использовать её как один из этапов предлагаемой методики.

Архитектурная модель, матрица классификации СТС и алгоритм многофакторной корреляции событий представлены как взаимосвязанные элементы единой методики интеграции, ориентированной на применение на объектах КИИ регионального уровня.

Материалы и методы

В настоящей работе под методикой интеграции СТС физической защиты в комплексную систему безопасности объектов КИИ регионального уровня понимается последовательность организационно-технических этапов, обеспечивающих включение разнородных средств физической защиты в единый контур мониторинга, анализа и реагирования. Методика основана на принципах модульности, масштабируемости и отказоустойчивости [14; 15].

Этап 1. Анализ объекта защиты. На данном этапе определяются состав объекта КИИ, критические зоны, перечень действующих СТС физической защиты, используемых средств ИБ, параметры каналов связи, а также нормативные и эксплуатационные ограничения [1; 2; 3, с. 234].

Этап 2. Классификация СТС по интеграционным признакам. Для каждого средства определяются канал передачи событий, частота генерации сообщений, критичность, тип журналирования и требования к доступности. Результатом этапа является матрица интеграции, представленная в таблице 1.

Этап 3. Построение архитектуры интеграции. На основе результатов классификации формируется четырёхуровневая архитектурная модель, включающая уровень СТС, уровень централизации событий, уровень мониторинга ИБ и уровень реагирования.

Этап 4. Нормализация и передача событий. Выполняются унификация форматов данных, настройка журналирования, буферизации и маршрутизации событий между подсистемами.

Этап 5. Настройка правил корреляции. Разрабатываются правила многофакторной корреляции с учётом временных, пространственных и логических связей между событиями физической и информационной подсистем [7, с. 42; 8, с. 16].

Этап 6. Оценка эффективности интеграции. Методика оценивается по критериям времени обнаружения инцидента, полноты регистрации событий, уровня ложных срабатываний, устойчивости к отказам каналов связи и времени реагирования на инцидент [11, с. 164; 15].

Архитектурно предлагаемый подход реализуется в виде четырёх уровней взаимодействия, каждый из которых обеспечивает отдельную функцию в общей методике интеграции.

Уровень 1 — СТС физической защиты. Он включает системы контроля и управления доступом, видеонаблюдение с аналитикой, охранную сигнализацию, периметральные средства и системы контроля транспорта.

Уровень 2 — подсистема централизации событий (PSIM-модуль). Она осуществляет сбор, нормализацию и первичную фильтрацию событий от всех СТС, включая унификацию форматов данных, дедупликацию сообщений, присвоение уровней критичности и локальное буферирование [13; 14].

Уровень 3 — система мониторинга информационной безопасности (SIEM/SOC). На данном уровне выполняются корреляция событий физической и информационной подсистем, формирование инцидентов, эскалация уведомлений и ведение журналов аудита [7, с. 42; 8, с. 16].

Уровень 4 — подсистема реагирования. Она включает автоматические сценарии противодействия инцидентам и регламентированные действия дежурной смены [15].

Для практической реализации интеграции используются совместимые форматы и протоколы обмена, в том числе Syslog/CEF, JSON/REST API, OPC UA и ONVIF, что обеспечивает совместимость физических и информационных подсистем [13; 14].

В качестве критериев оценки эффективности используются время обнаружения инцидента, полнота регистрации событий, уровень ложных срабатываний, устойчивость к отказам каналов связи и время реагирования на инцидент [11, с. 164; 15].

Тем самым классификация СТС, архитектурная модель и алгоритм корреляции образуют не разрозненные решения, а последовательные этапы единой методики интеграции.

Таблица 1 представляет классификацию СТС физической защиты по интеграционным признакам, которая используется на втором этапе предлагаемой методики и позволяет стандартизировать подключение разнородных технических средств к единой платформе мониторинга.

Таблица 1 — Классификация СТС физической защиты по интеграционным признакам

Тип СТС	Канал передачи событий	Частота генерации	Критичность	Тип журналирования	Требования к доступности
СКУД	TCP/IP, RS-485	Средняя (10–100 соб./мин)	Высокая	Синхронное	99,5%
Видеонаблюдение	RTSP, ONVIF	Высокая (постоянный поток)	Средняя	Асинхронное с буфером	95%
Охранная сигнализация	Контактные линии, IP	Низкая (событийно)	Критическая	Синхронное с подтверждением	99,9%
Периметральные датчики	Проводные, радиоканал	Низкая (событийно)	Высокая	Синхронное	99,5%
Контроль транспорта	TCP/IP, RFID	Средняя	Средняя	Асинхронное	95%

Методика предполагает использование отечественного программного обеспечения для всех компонентов системы в соответствии с требованиями импортозамещения [2; 15]. В качестве рекомендуемых решений рассматриваются SIEM-системы «MaxPatrol SIEM» и «СёрчИнформ SIEM» для корреляции событий ИБ, платформы «Орион» и «ParsecNET» в роли PSIM-модуля, а также «ViPNet Coordinator» для защиты каналов связи. Для сбора телеметрии сетевых устройств может применяться решение, аналогичное разработанному Майоровым А. В. [5, с. 69], что обеспечивает совместимость форматов данных между подсистемами.

Результаты

Результаты исследования соотносятся с поставленными задачами. В рамках решения третьей задачи разработана структурная схема комплексной системы безопасности объекта КИИ регионального уровня (рисунок 1).

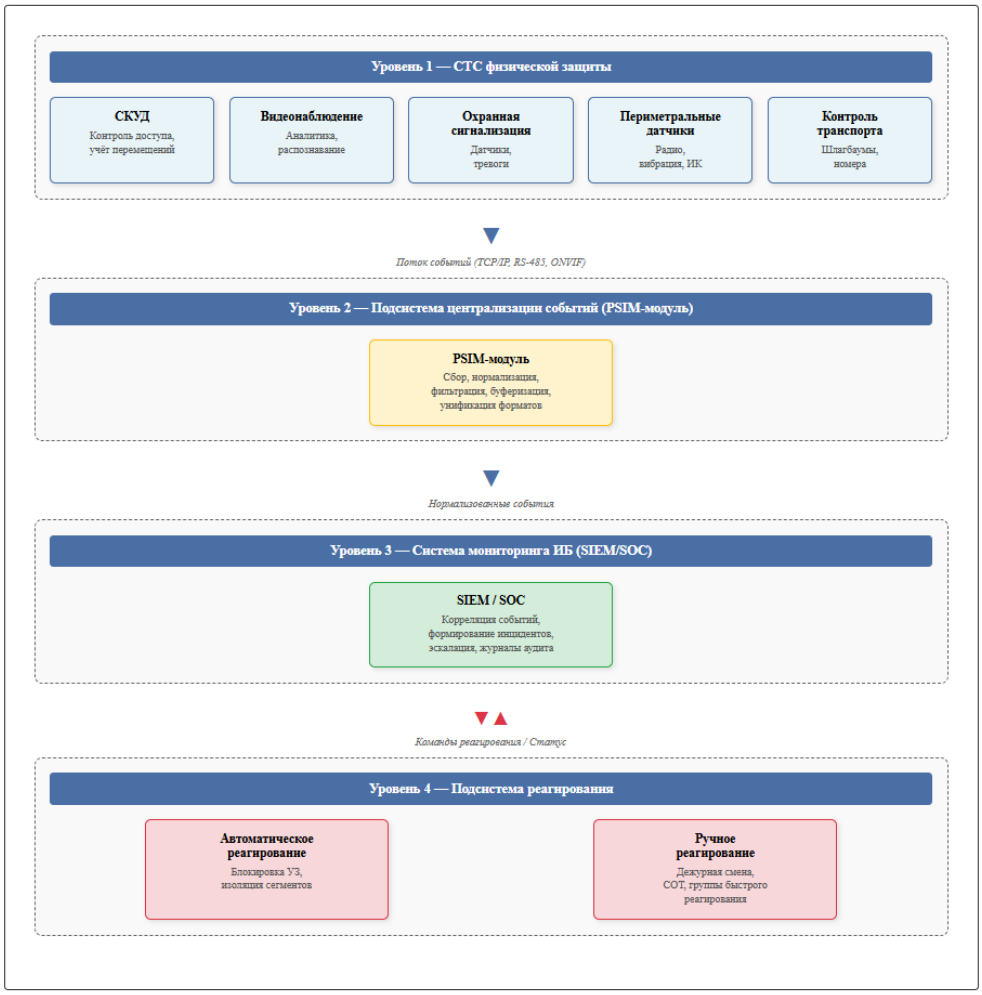

Рисунок 1 – Структурная схема комплексной системы безопасности объекта КИИ

Источник: Составлено автором

В рамках решения четвёртой задачи разработан алгоритм многофакторной корреляции событий, основанный на трёх принципах: временно́го окна (30–300 сек в зависимости от типа события), пространственной привязки (совпадение физической зоны и сетевого сегмента) и порогового накопления (число однотипных событий за период) [8, с. 16]. Событие физической подсистемы рассматривается как инцидент при наличии коррелирующего события информационной подсистемы; одиночные неподтверждённые события понижаются до Low без эскалации [7, с. 42].

Правило 1. Единичное срабатывание периметрального датчика без сопутствующих событий в течение 60 сек -> приоритет Low, регистрация без эскалации (фильтрация ложного срабатывания) [8, с. 16].

Правило 2. Срабатывание датчика движения в зоне без соответствующего события СКУД в течение 30 сек -> пометка «требует проверки», уведомление оператора без автоблокировки [7, с. 42].

Правило 3. Срабатывание периметрального датчика + подключение неизвестного сетевого устройства в той же зоне в течение 300 сек -> инцидент «Возможное несанкционированное подключение», приоритет High [8, с. 16].

Правило 4. Движение в серверной комнате в нерабочее время (видеоаналитика) + обращение к базе данных из IP-адреса той же подсети -> инцидент «Комбинированная атака», приоритет High [7, с. 42; 8, с. 16].

Правило 5. Несколько последовательных неудачных попыток аутентификации + срабатывание охранного датчика в той же зоне в течение 120 сек -> инцидент «Попытка

несанкционированного доступа с обходом СКУД», приоритет Critical; автоматическая блокировка учётной записи и изоляция сетевого сегмента [8, с. 16; 15].

Применение данных правил в ходе апробации обеспечило фильтрацию до 60% ложных тревог и сокращение времени обнаружения комбинированных инцидентов до 4-5 минут [8, с. 16].

В рамках решения пятой задачи апробация методики проведена на модели регионального объекта КИИ (условный центр обработки данных второй категории значимости). В ходе тестирования зафиксированы следующие показатели:

Снижение времени обнаружения инцидентов. При раздельной работе подсистем среднее время от физического проникновения до детекции в системе мониторинга составляло 8-12 минут. После интеграции с корреляцией событий время сократилось до 4-5 минут (улучшение на 40-55%) [8, с. 16].

Повышение полноты регистрации событий. До интеграции до 15% событий физической защиты не фиксировались в журналах ИБ из-за различий форматов. После внедрения PSIM-модуля полнота регистрации достигла 95-97% [14].

Снижение уровня ложных срабатываний. Корреляция событий (например, срабатывание датчика движения + попытка доступа к серверу из той же зоны) позволила отфильтровать до 60% ложных тревог, вызванных техническими сбоями или действиями персонала [8, с. 16].

Устойчивость при потере связи. PSIM-модуль обеспечивает автономную работу до 72 часов с локальным буферированием событий. После восстановления канала данные синхронизируются с центром мониторинга без потерь [14].

Упрощение процедур аттестации. Единая система журналов событий упрощает подготовку документации для ФСТЭК России, сокращая время аттестации на 20-25% [4, с. 56].

Сравнение с подходами, описанными в литературе, показывает, что предложенная модель превосходит традиционные решения по критерию «стоимость/эффективность» для объектов регионального уровня [13; 14]. В отличие от комплексных PSIM-платформ федерального класса, требующих значительных инвестиций в инфраструктуру, данная методика допускает поэтапное внедрение с использованием существующих СТС.

Обсуждение

Полученные результаты показывают, что предложенная методика интеграции СТС физической защиты в единую систему мониторинга безопасности обеспечивает повышение оперативности обнаружения комбинированных инцидентов и снижение числа ложных тревог по сравнению с раздельным функционированием подсистем [7, с. 42; 12]. Тем самым полученные данные соотносятся с выдвинутой гипотезой и подтверждают практическую целесообразность интеграции.

Однако внедрение методики сопряжено с рядом рисков и ограничений:

Необходимость модернизации устаревших СТС, не поддерживающих сетевые протоколы передачи событий [13];

Требования к квалификации персонала дежурной смены (понимание как физической, так и информационной безопасности) [15];

Зависимость от стабильности каналов связи между распределёнными площадками объекта [4, с. 56];

Потенциальные уязвимости самого PSIM-модуля, который становится единой точкой отказа при неправильной архитектуре [14].

Для минимизации рисков рекомендуется:

Резервирование каналов связи (проводные + беспроводные) [15];

Регулярное тестирование сценариев отказа компонентов [4, с. 56];

Разграничение прав доступа к PSIM-модулю по принципу наименьших привилегий [11, с. 164];

Включение проверок целостности PSIM в процедуры аттестации КИИ [11, с. 164].

Требования к эксплуатации системы включают ежедневный мониторинг журналов событий, еженедельную проверку работоспособности каналов интеграции, ежеквартальное тестирование сценариев реагирования. Документирование всех изменений конфигурации обязательно для прохождения периодических оценок защищённости [2; 11, с. 164].

Заключение

В ходе исследования решена задача разработки методики интеграции специальных технических средств физической защиты в комплексную систему безопасности объектов КИИ регионального уровня. Для достижения поставленной цели были последовательно решены основные задачи исследования: проанализированы особенности региональных объектов КИИ и требования к их защите, разработана классификация СТС по интеграционным признакам, предложена четырёхуровневая архитектурная модель взаимодействия подсистем, сформирован алгоритм многофакторной корреляции событий физической и информационной безопасности, а также проведена апробация предложенного подхода. По результатам работы установлено, что предложенная методика обеспечивает объединение разнородных СТС физической защиты и средств мониторинга ИБ в единый контур обработки событий. Практическая апробация показала сокращение времени обнаружения инцидентов с 8–12 до 4–5 минут, повышение полноты регистрации событий до 95–97%, снижение уровня ложных срабатываний до 60%, а также возможность автономной работы PSIM-модуля при потере связи с центром мониторинга в течение до 72 часов [4, с. 56; 8, с. 16; 14]. Таким образом, поставленная цель достигнута, основные задачи решены, а выдвинутая гипотеза подтверждена. Практическая значимость исследования состоит в возможности применения разработанной методики при модернизации и проектировании систем безопасности объектов КИИ регионального уровня, в том числе в условиях ограниченных ресурсов, распределённой инфраструктуры и необходимости соблюдения требований импортозамещения. Перспективы дальнейшего развития работы связаны с расширением набора корреляционных правил, использованием методов интеллектуального анализа событий и интеграцией предложенной методики с инструментами предиктивной аналитики угроз.

Список литературы:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
3. Киселев Н. Н. Законодательство и организационные меры как основа информационной безопасности критически важной информационной инфраструктуры регионального уровня управления в медицинском учреждении / Н. Н. Киселев // Вектор научной мысли. – 2025. – № 3(20). – С. 229–239. – EDN QUSTNG.
4. Киселев Н. Н. Метод автоматизации процедуры аттестации объектов критической информационной инфраструктуры в удаленных регионах России / Н. Н. Киселев // Вопросы защиты информации. – 2025. – № 1(148). – С. 53–58. – DOI 10.52190/2073-2600_2025_1_53. – EDN JVLLXU.

5. Майоров А. В. Программное обеспечение сбора данных о сетевом трафике корпоративных информационных систем / А. В. Майоров, Н. Н. Киселев, Д. Г. Зыбин // Информационные технологии в УИС. – 2025. – № 4. – С. 63–74. – EDN PQGDTQ.
6. Гвоздев Е. В. Обоснование и разработка понятийного аппарата для развития комплексной безопасности промышленных предприятий // Системные технологии. — 2023. — № 2 (47). — С. 73–78. — DOI: 10.55287/22275398_2023_3_73. — URL: https://cyberleninka.ru/article/n/obosnovanie-i-razrabotka-ponyatiynogo-apparata-dlya-razvitiya-kompleksnoy-bezopasnosti-promyshlennyh-predpriyatiy (дата обращения: 19.03.2026)
7. Соколова А. И., Бутин А. А. Особенности интеграции SIEM-системы с другими средствами защиты информации // Информационные технологии и математическое моделирование в управлении сложными системами: электрон. науч. журн. — 2024. — № 2. — С. 38–46. — URL: https://ismm.irgups.ru/sites/default/files/articles_pdf_files/osobennosti_integracii_siem-sistemy_s_drugimi_sredstvami_zashchity_informacii_0.pdf (дата обращения: 03.03.2026).
8. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. — 2016. — Вып. 4(47). — С. 5–27. — DOI: 10.15622/sp.47.1. — URL: https://ia.spcras.ru/index.php/sp/article/view/3366 (дата обращения: 03.03.2026).
9. Киселев Н. Н. Техническая защита информации как составляющая информационной безопасности критически важной инфраструктуры / Н. Н. Киселев // Идеи, гипотезы, поиск... : XXVI региональная научная конференция аспирантов и молодых исследователей, Магадан, 22 апреля 2021 года. Том Выпуск 26. – Москва: Издательство «Знание-М», 2021. – С. 5–15. – DOI 10.38006/00187-081-4.2021.5.15. – EDN JHRWLO.
10. Киселев Н. Н. Декомпозиция требований оценки защищенности объекта КИИ по функциональному назначению // Материалы конференции XIV Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (ИБРР-2025). – 29–31.10.2025. – С. 478–480.
11. Киселев Н. Н., Красов А. В. Требования защищённости объекта КИИ с учетом развития требований регуляторов // Сборник трудов «Региональная информатика и информационная безопасность» Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» и Санкт-Петербургской международной конференции «Региональная информатика». – 2025. – Выпуск 15. – С. 162–165.
12. Гибадуллин Д. Актуальность интеграции с информационной и физической безопасностью [Электронный ресурс] // Хабр. — 2025. — 2 мая. — URL: https://habr.com/ru/companies/innostage/articles/906416/ (дата обращения: 03.03.2026).
13. Каранкевич М. Принципы и приемы интеграции систем контроля и учета доступа с другими информационными системами предприятия [Электронный ресурс] // Secuteck.ru. — 2022. — 7 октября. — URL: https://www.secuteck.ru/articles/principy-i-

priemy-integracii-sistem-kontrolya-i-ucheta-dostupa-s-drugimi-informacionnymi-sistemami-predpriyatiya (дата обращения: 03.03.2026).
14. Скворцов А., Чечков Г., Христофоров А., Чичварин М., Висленев С. PSIM-системы в России: признаки, эффекты, перспективы [Электронный ресурс] // Secuteck.ru. — 2020. — 13 ноября. — URL: https://www.secuteck.ru/articles/psim-sistemy-v-rossii-priznaki-ehffekty-perspektivy (дата обращения: 03.03.2026).
15. Хмыров А. Проектирование систем защиты объектов КИИ: что важно знать и учитывать? [Электронный ресурс] // Anti-Malware.ru. — 2022. — 16 декабря. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/CII-systems-protection (дата обращения: 03.03.2026).

References:

1. Federal Law of 26 July 2017 No. 187-FZ “On the Security of the Critical Information Infrastructure of the Russian Federation”.
2. Order of the Federal Service for Technical and Export Control of Russia (FSTEC of Russia) of 25 December 2017 No. 239 “On Approval of the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation”.
3. Kiselev, N. N. Legislation and organizational measures as the basis of information security for region-level critical information infrastructure management in a medical institution / N. N. Kiselev // Vektor nauchnoy mysli (Vector of Scientific Thought). — 2025. — No. 3(20). — pp. 229–239. — EDN QUSTNG.
4. Kiselev, N. N. A method for automating the certification procedure of critical information infrastructure objects in remote regions of Russia / N. N. Kiselev // Voprosy zashchity informatsii (Information Protection Issues). — 2025. — No. 1(148). — pp. 53–58. — DOI 10.52190/2073-2600_2025_1_53. — EDN JVLLXU.
5. Mayorov, A. V. Software for collecting corporate information system network traffic data / A. V. Mayorov, N. N. Kiselev, D. G. Zybin // Informatsionnye tekhnologii v UIS (Information Technologies in the Penal System). — 2025. — No. 4. — pp. 63–74. — EDN PQGDTQ.
6. Gvozdev, E. V. Substantiation and development of the conceptual framework for advancing the comprehensive security of industrial enterprises // System Technologies. — 2023. — No. 2 (47). — pp. 73–78. — DOI: 10.55287/22275398_2023_3_73. — URL: https://cyberleninka.ru/article/n/obosnovanie-i-razrabotka-ponyatiynogo-apparata-dlya-razvitiya-kompleksnoy-bezopasnosti-promyshlennyh-predpriyatiy (accessed: 19.03.2026).
7. Sokolova, A. I.; Butin, A. A. Features of integrating a SIEM system with other information security tools // Informatsionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami (Information Technologies and Mathematical Modeling in the Management of Complex Systems): electronic scientific journal. — 2024. — No. 2. — pp. 38–46. — URL: https://ismm.irgups.ru/sites/default/files/articles_pdf_files/osobennosti_integracii_siem-sistemy_s_drugimi_sredstvami_zashchity_informacii_0.pdf (accessed: 03 Mar 2026).

8. Fedorchenko, A. V.; Levshun, D. S.; Chechulin, A. A.; Kotenko, I. V. Analysis of security event correlation methods in SIEM systems. Part 1 // Trudy SPIIRAN (Proceedings of SPIIRAS). — 2016. — Issue 4(47). — pp. 5–27. — DOI: 10.15622/sp.47.1. — URL: https://ia.spcras.ru/index.php/sp/article/view/3366 (accessed: 03 Mar 2026).
9. Kiselev, N. N. Technical information protection as a component of information security for critical infrastructure / N. N. Kiselev // Ideas, hypotheses, search...: XXVI Regional Scientific Conference of Postgraduate Students and Young Researchers, Magadan, 22 April 2021. Vol. Issue 26. — Moscow: Znanie-M Publishing House, 2021. — pp. 5–15. — DOI 10.38006/00187-081-4.2021.5.15. — EDN JHRWLO.
10. Kiselev, N. N. Decomposition of requirements for assessing the security of a CII object by functional purpose // Proceedings of the XIV St. Petersburg Interregional Conference "Information Security of Russia's Regions" (IBRR-2025). — 29–31 Oct 2025. — pp. 478–480.
11. Kiselev, N. N.; Krasov, A. V. Security requirements for a CII object considering the evolution of regulator requirements // Proceedings volume "Regional Informatics and Information Security" of the St. Petersburg Interregional Conference "Information Security of Russia's Regions" and the St. Petersburg International Conference "Regional Informatics". — 2025. — Issue 15. — pp. 162–165.
12. Gibadullin, D. Relevance of integration with information and physical security [Electronic resource] // Habr. — 2025. — 2 May. — URL: https://habr.com/ru/companies/innostage/articles/906416/ (accessed: 03 Mar 2026).
13. Karankevich, M. Principles and techniques for integrating access control and accounting systems with other enterprise information systems [Electronic resource] // Secuteck.ru. — 2022. — 7 Oct. — URL: https://www.secuteck.ru/articles/principy-i-priemy-integracii-sistem-kontrolya-i-ucheta-dostupa-s-drugimi-informacionnymi-sistemami-predpriyatiya (accessed: 03 Mar 2026).
14. Skvortsov, A.; Chechkov, G.; Khristoforov, A.; Chichvarin, M.; Vislenev, S. PSIM systems in Russia: features, effects, prospects [Electronic resource] // Secuteck.ru. — 2020. — 13 Nov. — URL: https://www.secuteck.ru/articles/psim-sistemy-v-rossii-priznaki-ehffekty-perspektivy (accessed: 03 Mar 2026).
15. Khmyrov, A. Designing security systems for CII facilities: what is important to know and consider? [Electronic resource] // Anti-Malware.ru. — 2022. — 16 Dec. — URL: https://www.anti-malware.ru/analytics/Technology_Analysis/CII-systems-protection (accessed: 03 Mar 2026).