БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 9–36

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 338.2:005.922.1:004 DOI: 10.17212/2782-2230-2026-2-9-36

ФАКТОРЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ СТРОИТЕЛЬНОГО ДЕВЕЛОПМЕНТА*

И.А. ПЛОТНИКОВ[1], В.Д. КОЛЫЧЕВ[2]

[1] *РФ, 115409, г. Москва, Каширское шоссе, 31, Национальный исследовательский ядерный университет «МИФИ», студент 2-го курса магистратуры кафедры управления бизнес-проектами (№ 72) факультета бизнес-информатики и управления комплексными системами. E-mail: megavanek18@list.ru*

[2] *РФ, 115409, г. Москва, Каширское шоссе, 31, Национальный исследовательский ядерный университет «МИФИ», кандидат технических наук, доцент кафедры финансового мониторинга (№ 75) Института финансовых технологий и экономической безопасности. E-mail: kolychev@mephi.ru*

Исследование посвящено проблемам информационной безопасности в сфере строительного девелопмента в условиях цифровизации отрасли. Цель работы – систематизировать факторы информационной безопасности для строительного девелопмента, выявить основные угрозы и разработать рекомендации по защите информационных активов. Методология включает анализ нормативно-правовой базы (ФЗ-152 «О защите персональных данных», ГОСТ Р 58439.1-2019, ГОСТ Р 71452-2024), оценку актуальных киберугроз, изучение специфики информационных систем девелоперских компаний (в том числе с применением BIM-технологий), а также разработку системы ключевых показателей эффективности (KPI) и алгоритма их мониторинга. Выявлены основные угрозы: инсайдерские атаки, компрометация цепочки поставок, уязвимости облачной инфраструктуры, фишинг. Разработана методология обеспечения информационной безопасности, адаптированная к отраслевым особенностям (долгосрочность проектов, множественность участников, объемные BIM-модели). Сформирована система KPI, охватывающая технические (время обнаружения инцидентов, процент защищенных систем), организационные (обучение персонала, выполнение плана мероприятий) и нормативные показатели (соответствие ФЗ и ГОСТ). Предложен интегральный показатель результативности информационной безопасности и концепция панели мониторинга (дашборда) для визуализации данных. Результаты могут использоваться девелоперскими компаниями для построения и оценки систем защиты информации, принятия управленческих решений, прогнозирования рисков и минимизации ущерба от кибератак. Комплексный подход, сочетающий технические меры (DLP, IDS, шифрование), организационные мероприятия (обучение, аудит партнеров) и непрерывный мониторинг KPI,

* Статья получена 14 апреля 2026 г.

позволяет обеспечить устойчивую защиту информационных активов и превратить безопасность в конкурентное преимущество.

Ключевые слова: панель индикаторов безопасности, строительный девелопмент, киберугрозы, управление доступом, защита данных, информационные системы, ключевые показатели эффективности

ВВЕДЕНИЕ

Сфера строительного девелопмента, являющаяся важной экономической отраслью, активно изменяется в условиях повсеместного внедрения цифровых технологий в бизнес-процессы. Компании-девелоперы в настоящее время применяют интегрированные программные решения (экосистемы) для контроля реализации инвестиционно-строительных проектов и оперируют обширными массивами данных, включающими конфиденциальные материалы по объектам, финансовую отчетность, а также персональные данные заказчиков и контрагентов.

Как показывают статистические данные, в 2024 году в России было зарегистрировано 765,4 тыс. киберпреступлений, что на 13,1 % больше, чем годом ранее [1]. На долю организаций из стран СНГ в период с июля 2024 года по сентябрь 2025 года пришлось от 14 до 18 % всех результативных кибератак в мире, при этом процент успешных вторжений, завершившихся утечкой данных, возрос с 41 до 54 % [1]. Для девелоперской отрасли эти цифры особенно значимы, поскольку компании аккумулируют стратегически важные активы: архитектурные чертежи, сметную документацию, договоры, информацию о клиентах и инвестиционных планах.

Настоящая статья ставит своей целью обобщение сведений о значимых для строительного девелопмента факторах информационной безопасности, определение ключевых направлений угроз и формулировку предложений по созданию эффективной системы защиты информационных ресурсов.

Практическая значимость настоящей работы заключается в выработке предложений по разработке отраслевой методологии анализа проблем и направлений совершенствования деятельности в области информационной безопасности для компаний в сфере строительного девелопмента. Предлагаемая методология учитывает специфику сектора (применение BIM-технологий, продолжительный цикл реализации проектов, разветвленную сеть поставщиков) и современный ландшафт киберугроз.

В основе исследования лежит изучение действующей российской нормативно-правовой базы, международных стандартов и актуальных тенденций в области кибербезопасности.

1. ОСОБЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ СТРОИТЕЛЬНОГО ДЕВЕЛОПМЕНТА

1.1. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРОИТЕЛЬНОЙ ОТРАСЛИ

Российские правовые нормативно-технические акты в сфере информационной защиты направлены на создание многоуровневой системы требований к безопасности и хранению коммерческих данных, а также к сохранению ценной информации в момент их создания и к последующему практическому использованию для организаций в сфере строительного девелопмента.

- Федеральный закон № 152-ФЗ «О персональных данных». Этот закон вводит обязательные нормы по обработке и защите персональной информации, которую компании-девелоперы получают от своих клиентов. От организаций требуется внедрение комплекса технических и административных мер, таких как системы разграничения доступа, использование шифрования и непрерывное отслеживание инцидентов. Несоблюдение этих предписаний влечет за собой применение финансовых взысканий и может серьезно повлиять на деловую репутацию.
- ГОСТ Р 58439.1–2019. Указанный государственный стандарт регламентирует основные термины и принципы построения информационной среды при строительстве с применением BIM-технологий. Документ определяет порядок управления данными на всех этапах существования объекта – от проектирования до эксплуатации, уделяя особое внимание вопросам минимизации рисков и обеспечения защиты информации. Требования стандарта:

– формирование и фиксация в документах политики обращения с информацией;

– установление критериев информационной безопасности для каждой фазы реализации проекта;

– внедрение процедур, регулирующих доступ к данным;

– проведение регулярных проверок документированной оценки рисков, связанных с передачей информации.

- ГОСТ Р 71452–2024. Этот стандарт, действующий с 1 июля 2025 года, закрепляет принципы совмещения функциональной безопасности и киберзащиты на протяжении полного жизненного цикла систем промышленной автоматики (IACS). Несмотря на первостепенную направленность на промышленный сектор, его положения могут быть распространены и на системы управления зданиями и сооружениями. Стандарт обязывает использовать механизмы

контроля привилегий, защищенные криптографией каналы обмена данными, средства для управления уязвимостями и платформы для наблюдения за событиями безопасности.

1.2. УГРОЗЫ, ВЛИЯЮЩИЕ НА ЦИФРОВУЮ ТРАНСФОРМАЦИЮ СТРОИТЕЛЬНОЙ СФЕРЫ

Цифровизация строительной отрасли затрагивает все уровни – от проектирования до эксплуатации. Информационные технологии обеспечивают целостность данных, увеличивают производительность труда, выстраивают новые командные формы и упрощают взаимодействие участников сложных отраслевых строительных инвестиционных проектов, повышая гибкость и управляемость процессов на основе массивов данных, формируемых в режиме реального времени.

Современные IT-инструменты позволяют создавать строительные объекты быстрее и безопаснее, поскольку в цифровых процессах появляются механизмы автоматического контроля, прогнозирования и документирования. На уровне компаний образуется эффект, заключающийся в снижении издержек, ускорении выполнения работ, возрастании доли заимствований до 80 % за счет формирования документации в электронном виде; появляются возможности масштабирования проектов без увеличения числа ошибок за счет сокращения продолжительности жизненного цикла.

Информационные системы девелоперских компаний характеризуются специфическим набором функций и особенностями архитектуры. Современные корпоративные системы управления проектами (Project Management Information Systems), особенно в инвестиционно-строительной сфере, включают модули планирования, финансирования, контроля качества, управления человеческими ресурсами и логистики [14]. Кроме того, широкое внедрение технологии информационного моделирования (BIM – Building Information Modeling) создает сложные распределенные информационные среды, посредством которых множество участников цепочек поставок взаимодействуют через общие платформы хранения данных [2, 12].

Ниже перечислены специфические характеристики ИС в сфере девелопмента.

1. Множественность участников. В реализации проекта участвуют заказчики, проектировщики, подрядчики, субподрядчики, поставщики материалов, органы государственного контроля. Каждый участник требует дифференцированного доступа к информации, что существенно усложняет систему управления доступом.

2. Объемные графические данные. BIM-модели содержат большие объемы трехмерных чертежей, спецификаций и расчетов, требующих защиты от несанкционированного копирования.

3. Долгосрочность проектов. Жизненный цикл строительного проекта может составлять от нескольких лет до десятилетий, что подразумевает длительное хранение и управление конфиденциальной информацией [1].

4. Интеграция с облачными сервисами. Внедрение облачных решений для совместной работы команд в формате BaaS (Backend as a Service) создает новые векторы атак через ошибки в конфигурации облачной инфраструктуры [1].

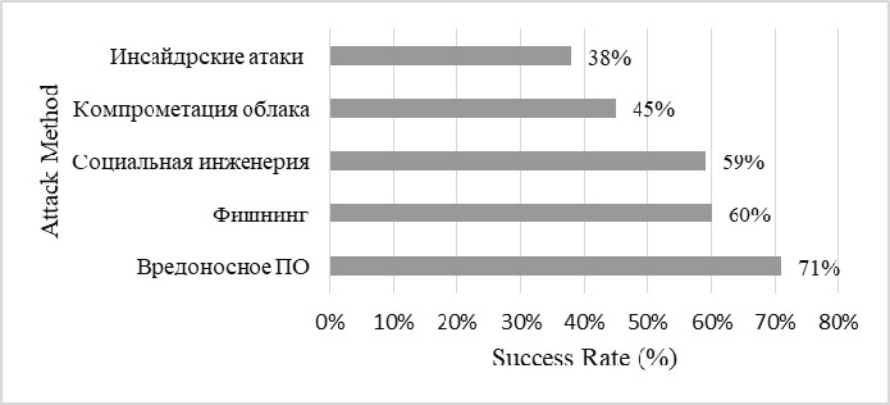

Рис. 1. Основные методы кибератак и процент успешных атак на организации СНГ в 2024–2025 годах

Fig. 1. Main methods of cyberattacks and the percentage of successful attacks on CIS organizations in 2024–2025

Ключевыми факторами, формирующими картину киберугроз в период 2025–2026 гг., остаются скорость цифровой трансформации и состояние международных отношений. Злоумышленники нацелены на нарушение функционирования стратегических цифровых активов предприятий, кражу и уничтожение информационных ресурсов, а также на подрыв деловой репутации организации.

Защита экономических интересов компании в строительной отрасли характеризуется сочетанием универсальных и отраслевых особенностей. Сравнительный анализ специфики обеспечения процессов экономической безопасности строительного сектора и практик, распространенных в смежных областях экономики, представлен в табл. 1.

Таблица 1

Table 1

Особенности обеспечения процессов экономической безопасности для строительных организаций [2, 8]

Features of ensuring economic security of construction organizations [2, 8]

Универсальные практики (сходства)	Отраслевые практики (различия)
1. Финансовый контроль и мониторинг вложений, расходов и доходов, сокращение финансовых рисков и оптимизация издержек	1. Особенности реализации инвестиционно-строительного проекта, имеющего ряд специфических характеристик: выбор площадки и месторасположение, рельеф местности, специальные требования к материалам или технологиям строительных работ
2. Управление, идентификация, анализ и моделирование рисков компании	2. Длительный инвестиционно-экономический цикл. Вопросы экономической безопасности при реализации длительного проекта становятся наиболее актуальными, поскольку наблюдается увеличение продолжительности жизненного цикла строительного проекта
3. Анализ законодательных норм и стандартов, включая налоговое законодательство, правила безопасности и трудовое право	3. Лицензирование и сертификации для реализации условий проведения высотных работ в замкнутых пространствах, включая необходимость получения лицензий для работы со специальным техническим оборудованием
4. Кадровая безопасность. Необходимость привлечения новых трудовых ресурсов и обеспечения их безопасности	4. Промышленная безопасность производства. Наличие высокого риска травматизма обусловливает необходимость обеспечения требований охраны труда одним из наиболее важных аспектов экономической безопасности

В сфере строительного бизнеса существуют универсальные проблемы, связанные с защитой финансовых интересов, но отраслевая специфика требует повышенного внимания к следующим аспектам: к организации инвестиционно-строительных процессов, минимизации рисков в рамках долгосрочных капитальных вложений и неукоснительному следованию жестким нормативам безопасности [3].

При оценке степени воздействия различных угроз на экономическую стабильность, безопасность и устойчивость строительной компании оказывается

важным распределить их по источнику возникновения: внешние или внутренние. Такая классификация позволяет четко определить, на каких группах рисков следует сконцентрировать дополнительные усилия, чтобы сократить возможность негативного воздействия на операционную, финансовую и инвестиционную деятельность, а также спрогнозировать потенциальный масштаб ущерба.

Визуализация угроз экономической безопасности в инвестиционно-строительной сфере представлена на рис. 2.

Рис. 2. Угрозы экономической безопасности строительных организаций

Fig. 2. Threats to the economic security of construction organizations

Очевидно, что уровень экономического ущерба, связанный с различными факторами и угрозами экономической безопасности в строительной сфере, может разниться и зависеть от горизонта планирования и оценки показателей

эффективности деятельности строительной компании, рыночной конъюнктуры, технологической развитости и уровня цифровизации.

Однако в последнее время наиболее очевидным является соотнесение угроз экономической безопасности, связанных с нарушением целостности объектов цифровой инфраструктуры строительной компании, с критическим или катастрофическим уровнем, поскольку проявление перечисленных угроз в практической деятельности компании приводит к частичной или полной приостановке процессов функционирования.

1.3. ОСОБЕННОСТИ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ СОЗДАНИЯ ЦИФРОВЫХ ДВОЙНИКОВ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ

Внедрение автоматизированных систем создания цифровых двойников объектов в сфере строительного девелопмента инициирует разработку многоуровневой модели с регулярным изменением и возможной перестройкой необходимых для повышения информационной безопасности процессов.

1. В рамках анализа процессов информационной безопасности при внедрении цифровой системы класса BIM на предприятии необходимо предусмотреть следующее:

– дифференцированное предоставление прав доступа на основе функциональных ролей;

– двухфакторную аутентификацию для доступа к критичным данным и подсистемам цифровых двойников строительных объектов;

– логирование всех операций по работе с конфиденциальной информацией и данными, содержащими сведения контрактации или коммерческого характера;

– автоматизацию выявления и отзыва избыточных прав доступа [5].

2. Управление рисками инсайдерских атак требует разработки комплексной программы внутренней безопасности, включающей следующие действия:

– проведение регулярного обучения персонала основам информационной безопасности и социальной инженерии;

– проверку биографических данных при найме, особенно для должностей с доступом к критичной информации;

– мониторинг подозрительной активности пользователей в корпоративной сети;

– четкое определение классификации информации и правил работы с ней [7].

3. Технологии аудита и управление безопасностью логистических цепочек поставок в рамках внедрения BIM-системы подразумевают уменьшение

рисков компрометации посредством сети партнерств или контрагентов, при этом необходимо:

– проведение регулярных аудитов безопасности подрядчиков и субподрядчиков;

– включение требований информационной безопасности в контрактную документацию;

– использование контроля целостности кода и цифровых подписей для проверки обновлений программного обеспечения;

– разграничение доступа партнеров только к необходимому объему информации [2].

4. Для защиты облачной инфраструктуры в современных условиях работы цифровых сервисов и автоматизированной системы создания цифровых двойников необходимы следующие шаги:

– регулярный аудит конфигураций облачных сервисов для выявления некорректных настроек;

– внедрение систем управления конфигурациями (Configuration Management);

– непрерывный мониторинг облачной инфраструктуры и событий доступа;

– использование шифрования для защиты данных в облачном сервисе [2].

5. Применение современных технологий защиты данных в условиях создания цифровых моделей сложных строительных объектов подразумевает необходимость внедрения:

– систем контроля доступа к файловым хранилищам (Data Loss Prevention);

– антивирусной защиты и систем обнаружения вторжений;

– инструментов для управления уязвимостями и анализа безопасности;

– систем резервного копирования и аварийного восстановления [2].

6. Для непрерывного мониторинга и реагирования на инциденты в сфере информационной безопасности в современных условиях необходимы дополнительные усилия:

– организация центров управления безопасностью (Security Operations Center) или привлечение услуг управляемых поставщиков безопасности (Managed Security Service Provider);

– разработка регламентов и процедур реагирования на инциденты;

– проведение регулярных модельных сценарных экспериментов кибератак;

– постоянный анализ событий безопасности и уязвимостей [2].

На основе перечисленных выше направлений совершенствования процессов управления информационной безопасностью при внедрении автоматизи-

рованных систем создания цифровых двойников сложных объектов необходима разработка продуманной системы ключевых показателей эффективности для взвешенной и обоснованной оценки угроз и анализа рисков деятельности предприятий сферы строительного девелопмента.

2. СИСТЕМА КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРОИТЕЛЬНОМ ДЕВЕЛОПМЕНТЕ

2.1. РАЗРАБОТКА НАБОРА ПОКАЗАТЕЛЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Эффективность системы информационной безопасности строительного предприятия представляет собой сложный комплексный показатель. Его формирование зависит от нескольких ключевых направлений деятельности компании: во-первых, от способности технических средств противостоять кибератакам и утечкам данных, во-вторых, от качества внутренних регламентов и действий сотрудников, направленных на защиту информации, и, в-третьих, от полноты соблюдения отраслевых стандартов и законодательства в данной сфере.

Для объективной оценки и дальнейшего развития системы безопасности необходима тщательно разработанная система ключевых показателей эффективности (KPI). Такой набор KPI должен быть сбалансированным, охватывать как операционные, так и стратегические цели и отражать специфику строительной отрасли.

Ключевые показатели эффективности для оценки информационной безопасности строительных компаний можно разделить на несколько основных групп. Технические KPI, такие как количество успешно отраженных атак, время обнаружения инцидентов, процент защищенных систем, являются основой для оценки технической защищенности. Организационные KPI, в свою очередь, фокусируются на эффективности процессов управления безопасностью: соблюдение сроков проведения аудитов, выполнение плана мероприятий по безопасности и процент сотрудников, прошедших обучение по ИБ [6].

Также значимыми являются и показатели, связанные с необходимостью выполнения нормативных требований и управлением рисками. Сюда относятся такие метрики, как количество нарушений законодательства, процент выполненных требований стандартов, уровень покрытия рисков мерами защиты,

а также показатели эффективности системы управления инцидентами. Кроме того, современные строительные компании всё чаще включают в свои системы оценки KPI, связанные с безопасностью цепочки поставок и защитой BIM-данных (например, уровень безопасности партнеров, степень защиты BIM-моделей, контроль доступа к проектной документации).

Таблица 2

Table 2

Технические показатели информационной безопасности

Technical indicators of information security

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Количество успешно отраженных атак	Абсолютное число за период	Системы обнаружения вторжений, журналы безопасности	Ежемесячно	100 % критичных атак
Среднее время обнаружения инцидента	∑ (время обнаружения) / количество инцидентов	SIEM-системы, системы мониторинга	Ежемесячно	< 1 часа
Процент защищенных систем	Защищенные системы / все системы × 100 %	Инвентаризация ИТ-активов, системы защиты	Ежеквартально	≥ 95 %
Количество выявленных уязвимостей	Абсолютное число за период	Сканеры уязвимостей, системы управления уязвимостями	Ежемесячно	Ежегодное снижение
Процент устраненных уязвимостей	Устраненные уязвимости / выявленные уязвимости × 100 %	Системы управления уязвимостями, отчеты	Ежемесячно	≥ 90 % критичных

Набор представленных показателей может быть использован для повышения уровня безопасности цифровых систем класса BIM, в которых сохраняется актуальная информация о цифровых двойниках строительных объектов. Организационные показатели, представленные в табл. 3, применяются с целью улучшения организации процессов информационного аудита и повышения устойчивости цифровой инфраструктуры.

Таблица 3

Table 3

Организационные показатели информационной безопасности

Organizational indicators of information security

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Процент сотрудников, прошедших обучение	Обученные сотрудники / все сотрудники × 100 %	Системы обучения, журналы инструктажей	Ежеквартально	100 %
Соблюдение сроков аудитов безопасности	Аудиты в срок / все аудиты × 100 %	План аудитов, отчеты	Ежеквартально	≥ 95 %
Выполнение плана мероприятий	Выполненные мероприятия / все мероприятия × 100 %	План мероприятий, отчеты	Ежемесячно	≥ 90 %
Количество инсайдерских инцидентов	Абсолютное число за период	Системы мониторинга, отчеты	Ежемесячно	0
Эффективность управления доступом	Нарушения доступа / все операции доступа × 100 %	Системы управления доступом, журналы	Ежемесячно	≤ 0,1 %

Набор показателей управления рисками и инцидентами, а также методики расчета достигнутых значений показателей эффективности процессов информационной безопасности для предприятия в сфере строительного девелопмента представлены в табл. 4.

Показатели эффективности процессов безопасности цепочки поставок и хранения данных, накапливаемых в цифровых системах, представлены в табл. 5.

Таблица 4

Table 4

Показатели соответствия и управления рисками

Compliance and Risk Management Indicators

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Соответствие требованиям ФЗ-152	Выполненные требования / все требования × 100 %	Аудит соответствия, отчеты	Ежеквартально	100 %
Соответствие ГОСТ Р 58439.1–2019	Выполненные требования / все требования × 100 %	Аудит соответствия, отчеты	Ежеквартально	≥ 95 %
Уровень покрытия рисков	Риски с мерами / все риски × 100 %	Реестр рисков, план мероприятий	Ежеквартально	≥ 90 %
Среднее время реагирования на инцидент	∑ (время реагирования) / количество инцидентов	Системы управления инцидентами	Ежемесячно	Менее 4 часов
Эффективность восстановления	Успешные восстановления / все восстановления × 100 %	Системы резервного копирования, тесты	Ежеквартально	100 %

Таблица 5

Table 5

Показатели безопасности цепочки поставок и BIM-данных

Supply chain and BIM data security indicators

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Уровень безопасности партнеров	Партнеры с аудитом / все партнеры × 100 %	База партнеров, отчеты аудитов	Ежеквартально	100 % ключевых партнеров
Защита BIM-моделей	Защищенные модели / все модели × 100 %	Системы управления BIM, системы защиты	Ежемесячно	100 %

Окончание табл. 5

End of the tab. 5

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Контроль доступа к проектной документации	Нарушения доступа / все операции × 100 %	Системы управления документами, журналы	Ежемесячно	≤ 0,05 %
Безопасность облачной инфраструктуры	Аудит конфигураций / все конфигурации × 100 %	Системы управления облаком, отчеты	Ежемесячно	100 % критичных
Защита персональных данных	Нарушения защиты персональных данных / все операции × 100 %	Системы защиты персональных данных, отчеты	Ежемесячно	

Анализ предложенного набора показателей оценки эффективности процессов информационной безопасности предприятия в сфере строительного девелопмента позволяет обоснованно подойти к задаче формирования информационной панели индикаторов.

2.2. ФОРМИРОВАНИЕ ПАНЕЛИ МОНИТОРИНГА ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Создание эффективной панели мониторинга (дашборда) для оценки информационной безопасности строительной компании является стратегически важным шагом, направленным на повышение управляемости, прозрачности и, как следствие, защищенности информационных активов. В основе этой инициативы лежит четкое понимание основных целей, визуализацию которых выполняет дашборд, обеспечивающий мониторинг и оперативный контроль достижения установленных на этапах предварительного планирования ключевых показателей эффективности [8, 10] в сфере информационной безопасности в режиме реального времени. Это означает, что руководители и специалисты по ИБ должны иметь возможность в любой момент времени видеть актуальное состояние индикаторов по всем критически важным аспектам защиты информации.

Вторая ключевая цель – визуальные модели принятия управленческих решений в сфере информационной безопасности. Сложные массивы инфор-

мации, собранные из различных источников, зачастую трудно воспринимаются в виде таблиц или сырых данных. Дашборд трансформирует эти данные в наглядные графические модели [9], диаграммы и индикаторы, оперативно выявляя закономерности, сравнивая показатели и, самое главное, принимая обоснованные и своевременные управленческие решения, основанные на фактических достижениях измеряемых показателей эффективности деятельности [6, 9].

Не менее важной задачей является выявление проблемных зон и трендов в области информационной безопасности. Панель мониторинга должна отображать текущие значения, демонстрируя динамику изменения показателей эффективности, указывая на негативные тренды, отклонения от плановых значений показателей, отображая потенциальные риски [4]. Предлагаемый подход позволяет менеджменту компании оперативно реагировать на возникающие проблемы, прежде чем они преобразуются в угрозы различных уровней (см. рис. 2).

Система дашбордов [9] способствует повышению прозрачности процессов информационной безопасности, делая информацию о состоянии защиты доступной для всех заинтересованных сторон [15] на соответствующих уровнях управления [5].

Для достижения перечисленных выше целей система мониторинга должна решать немало задач, включая автоматизацию сбора данных из разнородных источников. В деятельности строительного предприятия используется широкий спектр инструментов обеспечения информационной безопасности, включая персонифицированные средства защиты данных, системы мониторинга событий (SIEM), решения для анализа уязвимостей, механизмы контроля доступа и регистрационные журналы. Объединение перечисленных компонентов в единую инфраструктуру для централизованной обработки данных – первостепенная задача, решение которой позволит сформировать и представить унифицированные отчеты из разных источников в едином стандартизированном формате [14], обеспечивая при этом настройку системы оповещений о критических отклонениях, уведомляя ответственных лиц о выходе показателей безопасности за допустимые пределы и гарантируя, что ни одна выявленная угроза не останется незамеченной.

При этом критически важной задачей остаётся и формирование обоснованной системы разграничения доступа для разных уровней управления. Дашборд должен быть адаптирован [9, 10] под потребности различных категорий пользователей – от топ-менеджеров, которым нужны обобщенные стратегические показатели, до специалистов по ИБ, которым необходима детальная техническая информация [13, 14].

2.3. АЛГОРИТМ ФОРМИРОВАНИЯ СИСТЕМЫ ИЗМЕРИТЕЛЕЙ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Создаваемый алгоритм формирования системы показателей результативности информационной безопасности [8] включает четыре укрупненных этапа.

Первый этап заключается в составлении перечня показателей, которые отражают различные стороны процессов управления информационной безопасностью предприятия и являются значимыми для оценки.

Второй этап направлен на формирование обоснованной структуры системы показателей эффективности. На этом этапе устанавливаются цели процессов защиты информации, выявляются препятствия (ограничения), мешающие их достижению, проводится анализ этих препятствий и оценивается их степень влияния. Для количественного измерения предлагается использовать средневзвешенную оценку по формуле

$$P_i = \left(\sum R_{ij} V_{ij}\right) \Big/ n_i \ , \qquad (1)$$

где P_i – итоговая значимость *i*-го препятствия (в баллах), принимающая значения от 0 до 25; R_{ij} – оценка вероятности возникновения *i*-го препятствия, данная *j*-м экспертом (от 0 до 5 баллов). Оценка выставляется по шкале, где 0 баллов соответствует 0 % вероятности, а 5 баллов – 100 % вероятности; V_{ij} – оценка серьезности последствий *i*-го препятствия, данная *j*-м экспертом (от 0 до 5 баллов). Шкала серьезности построена следующим образом: 0 – последствия отсутствуют; 1 – незначительные последствия; 2 – последствия слабой значимости, способные повлиять на вспомогательные процессы; 3 – существенные последствия, затрагивающие основные процессы, снижающие конкурентоспособность и незначительно ухудшающие экономические показатели; 4 – серьезные последствия, ведущие к заметному ухудшению рыночных позиций и экономических результатов; 5 – критические последствия, способные привести к ликвидации организации; n_i – общее количество экспертных оценок, полученных для *i*-го препятствия.

Для отбора наиболее значимых препятствий применяется правило Парето: из всего множества выявленных проблем для дальнейшего анализа оставляют 20 % проблем, получивших наивысшие значения P_i. Второй этап завершается соответствием отобранных препятствий показателям из перечня, сформированного на первом этапе.

Третий этап включает непосредственно расчет показателей. На этом этапе определяют периодичность их измерения, фиксируют текущие значения, устанавливают целевые ориентиры и пороговые границы, а также вычисляют интегральный показатель результативности и разрабатывают план мероприятий, необходимых для достижения намеченных целей.

Четвертый этап предполагает разработку документа, регламентирующего функционирование системы, ввод ее в действие, проведение аудита и последующую эксплуатацию в установленном порядке.

Графическая модель предложенной последовательности действий представлена на рис. 3.

2.4. ИНТЕГРАЛЬНЫЙ ПОКАЗАТЕЛЬ РЕЗУЛЬТАТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для расчета интегрального показателя результативности информационной безопасности предложена следующая формула:

$$R = \frac{\sum_{i=1}^{n} P_i B_i f(\mathrm{KPI}_i)}{n}, \qquad (2)$$

где R – интегральный показатель результативности информационной безопасности; P_i – значимость (вес) i-го показателя панели индикаторов в баллах; B_i – балл в выбранной шкале, соответствующий достигнутому значению i-го показателя в одной из трех выделенных зон (измеренное достигнутое значение показателя ниже критического уровня соответствует зоне «1», или «красной зоне»; если значение выше критического, но ниже установленного целевого (нормативного) уровня – соответствие зоне «2», или «желтой зоне»; если достигнутое значение превосходит целевой уровень – соответствие зоне «3», или «зеленой зоне»); n – число показателей в сформированной информационной панели мониторинга.

С целью оценки достигнутых значений показателей будем использовать $f(\mathrm{KPI}_i)$ – функцию корректировки по конкретному значению KPI, при этом для маркировки сведений о наличии критических отклонений в значениях показателей введем следующую шкалу:

$$f(\mathrm{KPI}_i) = \begin{cases} 0{,}5, & \text{если в «красной зоне» (рискованно),} \\ 1{,}0, & \text{если в «желтой зоне» (умеренный риск),} \\ 1{,}5, & \text{если в «зеленой зоне» (идеально).} \end{cases} \qquad (3)$$

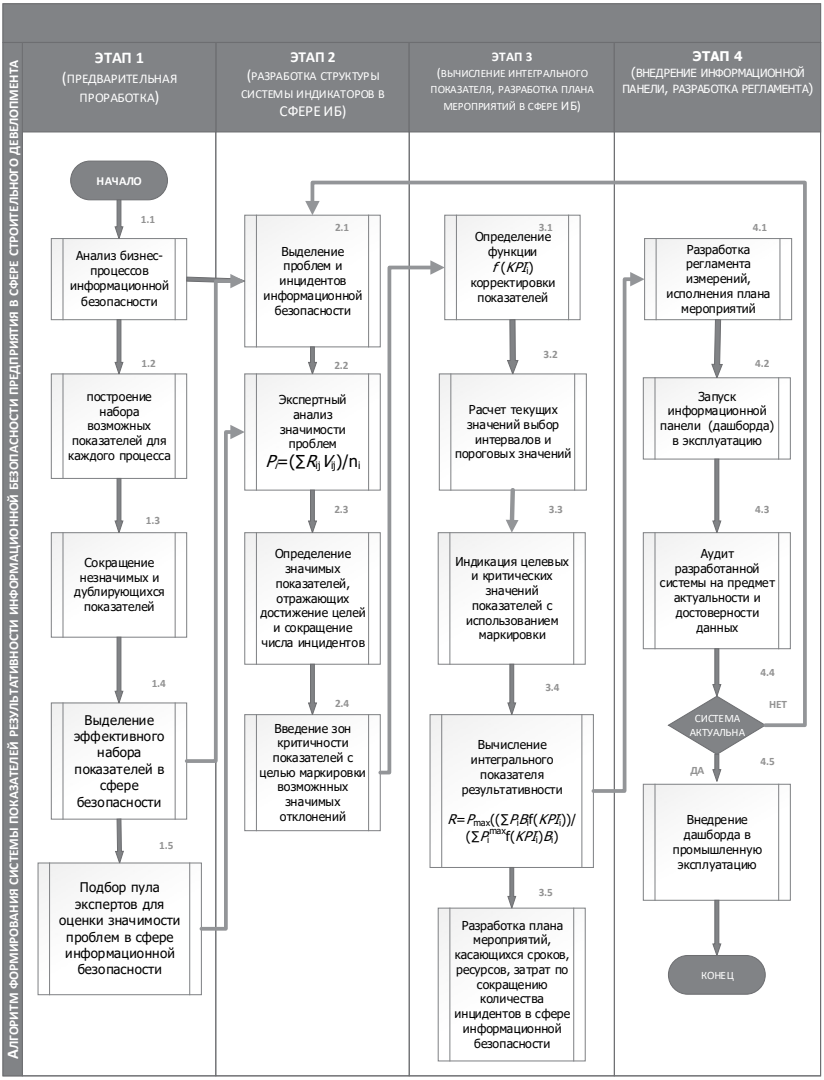

Рис. 3. Алгоритм формирования системы показателей результативности информационной безопасности предприятия в сфере строительного девелопмента

Fig. 3. Algorithm for forming a system of performance indicators for information security of an enterprise in the field of construction development

Модифицированная формула для определения интегрального показателя результативности приобретает следующий вид:

$$R = P_{\max}\left(\frac{\sum_{i=1}^{n} P_i B_i f(\mathrm{KPI}_i)}{\sum_{i=1}^{n} P_i^{\max} \max f(\mathrm{KPI}_i) \max B_i}\right), \quad (4)$$

где $P_i^{\max}$ – максимальный вес *i*-го показателя, $\max B_i$ – максимальный балл зоны (B_i), $f(\mathrm{KPI}_i)$ – коэффициент достижения значения показателя эффективности, при этом множитель $P_{\max}$ выступает в качестве нормировочного в установленном диапазоне значения показателя эффективности.

На рис. 4 представлена цветовая визуальная панель [9] для анализа ключевых показателей результативности процессов информационной безопасности предприятия [8] в сфере строительного девелопмента.

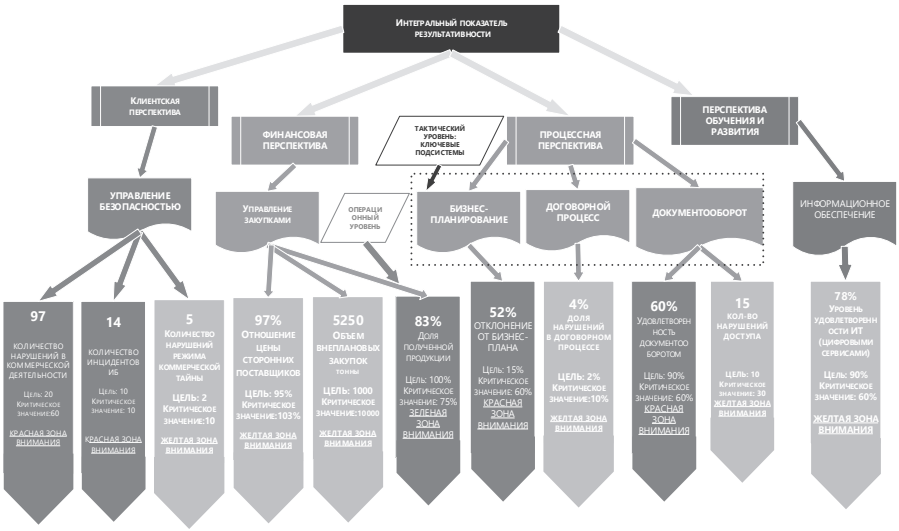

Рис. 4. Цветовая панель [9] отслеживания ключевых показателей результативности строительного предприятия

Fig. 4. Color panel [9] for tracking key performance indicators of a construction company

В соответствии с предлагаемым подходом каждый показатель в системе оценки результативности по итогам проведенных измерений может находиться в одном из трех состояний. Первое состояние фиксируется, когда фактическое значение оказывается ниже установленного критического порога (эта область обозначается как зона 1 либо «красная зона»). Второе состояние соответствует значениям, превышающим критический уровень, но еще не достигшим запланированного целевого ориентира (зона 2 или «желтая зона»). Третье состояние наступает при превышении целевого значения (зона 3, или «зеленая зона»). Для обеспечения возможности последующих вычислений каждому из указанных состояний может быть поставлен в соответствие числовой коэффициент. С целью индикации «красной зоны», как было отмечено ранее, предусматривается значение «–1», для индикации «желтой зоны» – «0», для индикации зеленой зоны – «+1».

Внедрение системы ключевых показателей эффективности для оценки информационной безопасности в строительном девелопменте [11] позволяет не только контролировать текущее состояние защиты информационных активов, но и создавать основу для их непрерывного совершенствования. Предложенная система KPI охватывает все ключевые аспекты информационной безопасности: техническую защищенность, организационные меры, соответствие нормативным требованиям, управление рисками, безопасность цепочки поставок и защиту BIM-данных [12].

Панели индикаторов (*dashboards*) представляют собой мощный инструмент управления информационной безопасностью, который демонстрирует свою высокую эффективность в условиях турбулентной экономической среды и растущих киберугроз [9]. Они способны оперативно удовлетворять трансформирующиеся потребности менеджмента [14], предоставляя наглядную и структурированную информацию о ключевых аспектах защиты информационных активов [13].

Эффективность внедрения системы KPI в сфере информационной безопасности в значительной степени обусловлена процессом выбора набора показателей. Качество и релевантность выбранных индикаторов обеспечивает информационную наполненность, содержательность и полезность систем мониторинга. В системе должны присутствовать показатели, отражающие различные перспективы информационной безопасности, что обеспечивает комплексное видение ситуации.

На рис. 5 представлена модель отображения отобранных значений показателей результативности в формате диаграммы, которая может быть использована в качестве панели мониторинга (дашборда) для повышения эффективности принимаемых решений [8, 9] в сфере информационной безопасности.

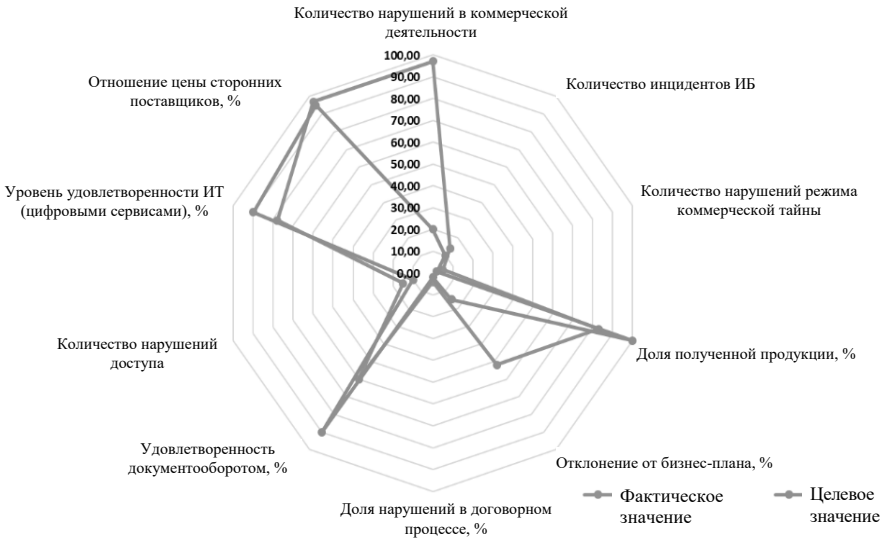

Рис. 5. Модель визуализации показателей эффективности информационной безопасности предприятия в сфере строительного девелопмента

Fig. 5. Model for visualizing the performance indicators of information security of an enterprise in the field of construction development

Таким образом, оказывается возможным формировать и анализировать новые формы и методы развития технологий информационной безопасности, защиты данных и связанной с ними процессной деятельности на предприятии [11], прикладывая дополнительные усилия по поддержанию устойчивого уровня роста, развитию организации на основе полученных значений показателей эффективности, сопоставляя их с установленными на этапах предварительного планирования целевыми значениями [13].

По мнению авторов, предложенная методика позволяет строительным компаниям [10, 11] не только оценивать текущее состояние информационной безопасности, но и прогнозировать будущие риски, принимать обоснованные управленческие решения и обеспечивать устойчивое развитие системы защиты информационных активов в условиях цифровой трансформации строительной отрасли [13, 15].

ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования систематизированы и проанализированы ключевые факторы информационной безопасности, актуальные при внедрении и использовании автоматизированных систем в сфере строительного девелопмента в условиях активной цифровизации отрасли.

Специфика информационных систем в строительном девелопменте предопределяет специфический набор требований для организации процессов информационной безопасности. Множественность участников инвестиционно-строительных проектов, работа с объемными BIM-моделями и цифровыми двойниками строительных объектов, долгосрочность жизненного цикла объектов и интеграция с облачными сервисами создают сложную инфраструктуру и архитектуру информационных активов, требующую дифференцированного подхода, в частности, к правилам и регламентам управления доступом. Предложения по организации процессов информационной безопасности на предприятиях в сфере строительного девелопмента разработана с учетом анализа отраслевых особенностей и их влияния на формирование рисков и выполнения условий безопасной эксплуатации объектов на основе технологий цифровизации.

Как показал анализ нормативно-правовой базы, включая Федеральный закон № 152-ФЗ и стандарты серии ГОСТ Р (58439.1–2019, 71452–2024), устанавливаются обязательные условия защиты персональных данных и информации на протяжении всего жизненного цикла строительного объекта, что является не только юридической необходимостью, но и основой для выстраивания доверительных отношений с клиентами, партнерами и контрагентами и обеспечивает экономическую безопасность и снижение рисков возможной компрометации деятельности компании.

Проведенный анализ ландшафта угроз показывает, что строительные компании сталкиваются как с распространенными киберугрозами (фишинг, ransomware), так и со специфическими рисками, такими как компрометация цепочки поставок через субподрядчиков, инсайдерские атаки со стороны сотрудников и уязвимости в конфигурации облачной инфраструктуры. Набор мер по организации эффективной системы защиты должен быть комплексным и включать не только технические меры (DLP, IDS, шифрование), но и организационные – регулярное обучение персонала, аудит партнеров и разработку согласованных и непротиворечивых регламентов работы с конфиденциальной информацией.

Предложенная в статье методика построения системы показателей результативности на основе панелей мониторинга (dashboards) позволяет интегрировать показатели результативности управления процессами информаци-

онной безопасности в общую систему управления компанией [8]. В частности, включение таких индикаторов, как количество инцидентов информационной безопасности или степень соблюдения режима коммерческой тайны, в единую панель KPI делает безопасность измеримым и управляемым бизнес-процессом [9], а не обособленной технической функцией.

Реализация предложенных мер – от внедрения систем управления цифровыми двойниками сложных строительных объектов, разработки многоуровневой системы управления доступом и повышения информационной безопасности до создания центра мониторинга и реагирования на инциденты (SOC) – требует существенных инвестиционных вложений и проведения серии организационных изменений. Однако такого рода затраты следует рассматривать как стратегические инвестиции в устойчивость бизнеса и повышение капитализации, поскольку ущерб от успешной кибератаки может многократно превысить расходы на превентивную защиту, приводя не только к прямым финансовым потерям, но и к репутационному дефолту, срыву сроков реализации проектов и кратному превышению первоначальных плановых смет.

Внедрение цифровых технологий в сфере девелопмента направлено на формирование новой автоматизированной среды взаимодействия стейкхолдеров в цепочках поставок и создает виртуальную среду, включая системы класса BIM – цифровых двойников сложных строительных объектов.

Эффект от цифровизации заключается в повышении синхронности работы над проектом, сокращении числа ошибок, увеличении количества заимствований при создании модели объекта на основе типовых проработанных решений или лучших отраслевых практик и способствует непрерывному обмену цифровыми ресурсами.

Обеспечение информационной безопасности в строительном девелопменте представляет собой непрерывный и динамичный процесс, требующий адаптации к меняющимся цифровым технологиям с учетом изменения нормативных требований и к новым, всё более развитым методам кибератак, взломов и действий злоумышленников.

Таким образом, информационная безопасность в сфере строительного девелопмента достигается за счет синергетического эффекта внедряемых технологических решений, рационально выстроенных процессов и осознания важности защиты конфиденциальных данных на всех уровнях управления компанией, комплексного подхода при защите информационных активов и цепочек создания стоимости, превращения безопасности в конкурентное преимущество, повышения доверия инвесторов, заказчиков, регуляторов и контрагентов.

СПИСОК ЛИТЕРАТУРЫ

1. *Клименко К.Е., Котляревский А.А.* Информационные системы как основа современного строительства // Инновации и инвестиции. – 2023. – № 5. – URL: https://cyberleninka.ru/article/n/informatsionnye-sistemy-kak-osnova-sovremennogo-stroitelstva (дата обращения: 25.02.2026). – EDN: WNCLGR.

2. *Норец Н.К.* Обеспечение кибербезопасности в строительной отрасли // Проблемы информационной безопасности социально-экономических систем: труды IX Международной научно-практической конференции, Гурзуф, 02–04 марта 2023 г. – Симферополь, 2023. – С. 148–150. – EDN: UXMDRS.

3. *Стрункина М.С., Воробьева А.В.* Разработка системы информационной безопасности для строительной компании // Международный научно-исследовательский журнал. – 2016. – № 10-2 (52). – URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-informatsionnoy-bezopasnosti-dlya-stroitelnoy-kompanii (дата обращения: 25.02.2026). – EDN: WWSDEF.

4. *Цыпылова Р.Н.* Цифровая трансформация строительной отрасли: преимущества и вызовы // Научный аспект. – 2024. – Т. 55, № 6. – С. 7107–7114. – EDN: YGOCEB.

5. *Шевко Н.Р., Коростиева В.С.* Кибербезопасность в строительстве // Информационные технологии в строительных, социальных и экономических системах. – 2025. – № 2 (36). – С. 172–175. – EDN: KCNVJX.

6. *Щепкина Н.Н.* Оценка рисков информационной безопасности строительных предприятий // Вестник МГСУ. – 2022. – Т. 17, № 11. – URL: https://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-stroitelnyh-predpriyatiy (дата обращения: 25.02.2026). – EDN: RQDDOZ.

7. *Ovsiannikova T.Yu., Patsukov A.A.* Building information modelling systems: strategic objectives and realities of digital transformation in construction // Недвижимость: экономика, управление. – 2022. – № 1. – С. 13–18. – DOI: 10.22337/2073-8412-2022-1-13-18. – EDN: VJSJCW.

8. *Колычев В.Д., Буданов Н.А.* Комплексная методика оценки рисков информационной безопасности в коммерческом банке // Безопасность информационных технологий. – 2021. – Т. 28, № 2. – С. 83–97. – DOI: 10.26583/bit.2021.2.08. – EDN: MHMRJK.

9. *Kolychev V.D., Shebotinov A.A.* Application of business intelligence instrumental tools for visualization of key performance indicators of an enterprise in telecommunications // Научная визуализация. – 2019. – Т. 11, № 1. – С. 20–37. – DOI: 10.26583/sv.11.1.03. – EDN: CZNAPN.

10. *Копалеишвили М.Д.* Цифровая трансформация девелопмента: инновационные технологии и маркетинговые стратегии как фактор устойчивости в условиях экономической нестабильности // Актуальные проблемы экономики и управления в строительстве: материалы III Национальной (Всероссийской) научно-практической конференции с международным участием. – СПб., 2025. – С. 368–375. – EDN: CGAKZG.

11. *Кисель Т.Н., Прохорова Ю.С.* Исследование уровня цифровизации на российских предприятиях инвестиционно-строительной сферы: монография. – М.: Изд-во МИСИ – МГСУ, 2023. – DOI: 10.22227/978-5-7264-3243-4.2023.53.

12. *Субботина Н.А., Нам Г.Е., Георгиади В.В.* BIM-моделирование как инструмент внедрения принципов OH&S в строительство // BIM-моделирование в задачах строительства и архитектуры: материалы II Международной научно-практической конференции. – СПб., 2019. – С. 91–95. – DOI: 10.23968/BIMAC.2019.016.

13. *Сулимова Е.А., Новицкая Д.А.* Развитие цифровой экономики в сфере строительства // Экономика строительства. – 2022. – № 10. – С. 89–95. – EDN: JIFDVM.

14. *Куровский С.В., Мишин Д.А., Самойленко А.В.* Методические и системные решения управления строительными проектами: проблемы их практического применения и направления их предотвращения // Экономика и управление: проблемы, решения. – 2025. – Т. 10, № 6 (159). – С. 42–54. – DOI: 10.36871/ek.up.p.r.2025.06.10.005.

15. *Рябоконь А.И., Черканов Н.С.* Особенности цифровизации процессов девелопмента недвижимости // Передовые технологии и инновации в образовании и науке для улучшения качества жизни и стимулирования устойчивого экономического роста: сборник статей VIII Международной научно-технической конференции. В 3-х томах. Минск, 2025. – Т. 2. – С. 327–330. – EDN: XZKHJW.

DOI: 10.17212/2782-2230-2026-2-9-36

Security factors of information systems in the construction development sphere*

I.A. Plotnikov[1], V.D. Kolychev [2]

[1] *National Research Nuclear University MEPhI, 31 Kashirskoye Shosse, Moscow, 115409, Russian Federation, second-year Master's student of the Department of Business Project Management (No. 72), Faculty of Business Informatics and Integrated Systems Management. E-mail: megavanek18@list.ru*
[2] *National Research Nuclear University MEPhI, 31 Kashirskoye Shosse, Moscow, 115409, Russian Federation, Candidate of Technical Sciences, Associate Professor of the Department of Financial Monitoring (No. 75), Institute of Financial Technologies and Economic Security. E-mail: kolychev@mephi.ru*

The research is devoted to the problems of information security in the field of construction development in the context of digitalization of the industry. The purpose of the work is to systematize information security factors for construction development, identify the main threats and develop recommendations for the protection of information assets. The methodology includes an analysis of the regulatory framework (FZ-152 "On Personal Data Protection", GOST R 58439.1–2019, GOST R 71452–2024), an assessment of current cyber threats, and a study of the specifics of information systems of development companies (including using BIM technologies), as well as the development of a system of key performance indicators (KPIs) and an algorithm for monitoring them. Results: the main threats have been identified: insider attacks, supply chain compromise, cloud infrastructure vulnerabilities, phishing; an information security methodology has been developed, adapted to industry specifics (long-term projects, multiple participants, voluminous BIM models); A KPI system has been formed, covering technical (incident detection time, percentage of protected systems), organizational (staff training, implementation of the action plan) and regulatory indicators (compliance with Federal Law and GOST); An integrated information security performance indicator and the concept of a dashboard for data visualization have been proposed. Scope of application: the results can be used by development companies to build and evaluate information security systems, make management decisions, predict risks and minimize damage from cyber attacks. Conclusions: an integrated approach combining technical measures (DLP, IDS, encryption), organizational measures (training, audit of partners) and continuous monitoring of KPIs allows for sustainable protection of information assets and turn security into a competitive advantage.

Keywords: security indicators panel, construction development, cyber threats, access control, data protection, information systems, key performance indicators

REFERENCES

1. Klimenko K.E., Kotlyarevskii A.A. Informatsionnye sistemy kak osnova sovremennogo stroitel'stva [Information systems as the backbone of modern construction]. *Innovacii i investicii*, 2023, no. 5. (In Russian). Available at:

* *Received 14 April 2026.*

https://cyberleninka.ru/article/n/informatsionnye-sistemy-kak-osnova-sovremennogo-stroitelstva (accessed 25.02.2026).

2. Norets N.K. [Ensuring cybersecurity in the construction industry]. *Problemy informatsionnoi bezopasnosti sotsial'no-ekonomicheskikh sistem* [Problems of information security of socio-economic systems]. Proceedings of the IX International Scientific and Practical Conference, Gurzuf, March 02–04, 2023. Simferopo, 2023, pp. 148–150. (In Russian).

3. Strunkina M.S., Vorobyeva A.V. Razrabotka sistemy informatsionnoi bezopasnosti dlya stroitel'noi kompanii [Development of an information security system for a construction company]. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal = International Research Journal*, 2016, no. 10-2 (52). Available at: https://cyberleninka.ru/article/n/razrabotka-sistemy-informatsionnoy-bezopasnosti-dlya-stroitelnoy-kompanii (accessed 25.02.2026).

4. Tsypylova R.N. Tsifrovaya transformatsiya stroitel'noi otrasli: preimushchestva i vyzovy [Digital transformation of the construction industry: advantages and challenges]. *Nauchnyi aspect*, 2024, vol. 55, no. 6, pp. 7107–7114. (In Russian).

5. Shevko N.R., Korostieva V.S. Kiberbezopasnost' v stroitel'stve [Cybersecurity in construction]. *Informatsionnye tekhnologii v stroitel'nykh, sotsial'nykh i ekonomicheskikh sistemakh*, 2025, no. 2 (36), pp. 172–175.

6. Shchepkina N.N. Otsenka riskov informatsionnoi bezopasnosti stroitel'nykh predpriyatii [Assessment of information security risks for construction enterprises]. *Vestnik MGSU = Monthly Journal on Construction and Architecture*, 2022, vol. 17, no. 11. Available at: https://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-stroitelnyh-predpriyatiy (accessed 25.02.2026).

7. Ovsiannikova T.Yu., Patsukov A.A. Building information modelling systems: strategic objectives and realities of digital transformation in construction. *Nedvizhimost': ekonomika, upravlenie = Real Estate: Economics, Management*, 2022, no. 1, pp. 13–18. DOI: 10.22337/2073-8412-2022-1-13-18.

8. Kolychev V.D., Budanov N.A. Kompleksnaya metodika otsenki riskov informatsionnoi bezopasnosti v kommercheskom banke [Development of a comprehensive methodology for assessing information security risks in a commercial bank]. *Bezopasnost' informatsionnykh tekhnologii = IT Security*, 2021, vol. 28, no. 2, pp. 83–97. DOI: 10.26583/bit.2021.2.08

9. Kolychev V.D., Shebotinov A.A. Application of business intelligence instrumental tools for visualization of key performance indicators of an enterprise in telecommunications. *Nauchnaya vizualizatsiya = Scientific Visualization*, 2019, vol. 11, no. 1, pp. 20–37.

10. Kopaleishvili M.D. [Digital transformation of real estate development: innovative technologies and marketing strategies as a factor of sustainability in conditions of economic instability]. *Aktual'nye problemy ekonomiki i upravleniya v*

stroitel'stve [Current Issues in Economics and Management in Construction]. Materials of the III National (All-Russian) Scientific and Practical Conference with International Participation, St. Petersburg, 2025, pp. 368–375. (In Russian).

11. Kisel' T.N., Prokhorova Yu.S. *Issledovanie urovnya tsifrovizatsii na rossiiskikh predpriyatiyakh investitsionno-stroitel'noi sfery* [A study of the level of digitalization in Russian enterprises of the investment and construction sector]. Moscow, MISI – MGSU Publ., 2023. DOI: 10.22227/978-5-7264-3243-4.2023.53.

12. Subbotina N.A., Nam G.E., Georgiadi V.V. [BIM-modeling as a tool for the implementation of OH&S principles in construction]. *BIM-modelirovanie v zadachakh stroitel'stva i arkhitektury* [BIM in construction & architecture]. Materials of the II International Scientific and Practical Conference, St. Prtrsburg, 2019, pp. 91–95. DOI: 10.23968/BIMAC.2019.016. (In Russian).

13. Sulimova E.A., Novitskaya D.A. Razvitie tsifrovoi ekonomiki v sfere stroitel'stva. [Development of the digital economy in the construction industry]. *Ekonomika stroitel'stva = Economics of Construction*, 2022, no. 10, pp. 89–95.

14. Kurovsky S.V., Mishin D.A., Samoylenko A.V. Metodicheskie i sistemnye resheniya upravleniya stroitel'nymi proektami: problemy ikh prakticheskogo primeneniya i napravleniya ikh predotvrashcheniya [Methodological and system solutions for managing construction projects: problems of their practical application and directions for their prevention]. *Ekonomika i upravlenie: problemy, resheniya = Economics and Management: Problems, Solutions*, 2025, vol. 10, no. 6 (159), pp. 42–54. DOI: 10.36871/ek.up.p.r.2025.06.10.005.

15. Ryabokon A.I., Cherkanov N.S. [Features of digitalization in real estate development processes]. *Peredovye tekhnologii i innovatsii v obrazovanii i nauke dlya uluchsheniya kachestva zhizni i stimulirovaniya ustoichivogo ekonomicheskogo rosta* [Advanced technologies and innovations in education and science for improving the quality of life and stimulating sustainable economic growth]. Collection of Articles of the VIII International Scientific and Technical Conference. Minsk, 2025, vol. 2, pp. 327–330.

Для цитирования:

Плотников И.А., Колычев В.Д. Факторы безопасности информационных систем в сфере строительного девелопмента // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 9–36. – DOI: 10.17212/2782-2230-2026-2-9-36.

For citation:

Plotnikov I.A., Kolychev V.D. Faktory bezopasnosti informatsionnykh sistem v sfere stroitel'nogo developmenta [Security factors of information systems in the construction development sphere]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 9–36. DOI: 10.17212/2782-2230-2026-2-9-36.