УДК 004.89:69

РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ НЕЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В СТРОИТЕЛЬСТВЕ

Гулякин Д.В.
доктор педагогических наук, профессор,
Кубанский государственный технологический университет,
Краснодар, Россия

Мариёв А.А.
студент,
Кубанский государственный технологический университет,
Краснодар, Россия

Аннотация

В статье проанализированы ключевые риски, возникающие при использовании нелицензионного программного обеспечения (ПО) в строительной отрасли: правовые, финансовые, кибербезопасностные, операционные и репутационные. Рассмотрены особенности уязвимости строительных информационных экосистем (BIM-платформы, системы управления стройплощадкой, SCADA для строительной техники) при наличии пиратских или неподдерживаемых версий ПО, а также предложены практические меры по снижению рисков: менеджмент программных активов (SAM), внедрение политик лицензирования, технические и организационные мероприятия. Материал опирается на нормативные документы и отечественную и зарубежную практику.

Ключевые слова: нелицензионное программное обеспечение, риски, строительство, кибербезопасность, менеджмент программных активов, ГОСТ, BIM, SCM.

RISKS ASSOCIATED WITH THE USE OF UNLICENSED SOFTWARE IN CONSTRUCTION

Gulyakin D.V.
Doctor of Pedagogical Sciences, Professor,
Kuban State University of Technology,
Krasnodar, Russia

Mariev A.A.
student,
Kuban State University of Technology,
Krasnodar, Russia

Abstract
The article analyzes the key risks that arise when using unlicensed software in the construction industry: legal, financial, cybersecurity, operational and reputational. The features of vulnerability of construction information ecosystems (BIM platforms, site management systems, SCADA for construction equipment) in the presence of pirated or unsupported software versions are considered, and practical risk mitigation measures are proposed: software asset management (SAM), implementation of licensing policies, technical and organizational measures. The material is based on regulatory documents and domestic and foreign practice.

Keywords: unlicensed software, risks, construction, cybersecurity, software asset management, GOST, BIM, SCM.

Цифровая трансформация строительного комплекса сопровождается активным внедрением специализированных программных решений — от BIM-платформ и систем планирования ресурсов до цифровых инструментов удалённого контроля и программного обеспечения для управления строительной техникой и инженерными системами. Применение

нелицензионных копий программ в такой технологически насыщенной среде существенно увеличивает вероятность сбоев производственных процессов, утечки данных проектной документации и возникновения юридических и экономических последствий для участников строительного проекта. Практические исследования подтверждают устойчивую зависимость между уровнем использования пиратского ПО и частотой киберинцидентов, включая заражения вредоносными кодами и утраты критической информации. Эти факторы определяют особую актуальность рассматриваемой темы для компаний, внедряющих цифровые технологии в управление строительством [1,4].

Настоящее исследование сочетает анализ отраслевой специфики (в частности, особенностей применения BIM и систем управления проектами) с рассмотрением проблем нелицензионного программного обеспечения. В отличие от традиционных правовых и экономических оценок, в работе акцентируется внимание на технологических последствиях: нарушениях взаимодействия между форматами IFC, ошибках интеграции с инженерными системами, сбоях сенсорных устройств при применении модифицированных версий программ. В заключительной части сформулированы практические рекомендации для подрядных организаций, технических заказчиков и служб эксплуатации, включающие меры по управлению программными активами (Software Asset Management) и обеспечению кибербезопасности цифровой инфраструктуры [2].

Исторически строительная отрасль отличалась высокой консервативностью в вопросах автоматизации. Однако за последние годы наблюдается стремительное распространение комплексных цифровых решений — от проектных BIM-комплексов до облачных платформ для координации

проектов и IoT-систем для мониторинга объектов. В таких условиях законность и актуальность программных продуктов становятся не только правовой обязанностью, но и ключевым элементом технологической надёжности. Некорректные, изменённые или не обновляемые версии программ нередко становятся причиной сбоев при обмене данными, несовместимости модулей и нарушения целостности проектной информации, что в условиях междисциплинарного взаимодействия в строительстве может привести к критическим последствиям.

Использование нелицензионного ПО является прямым нарушением авторских прав и может повлечь административную или даже уголовную ответственность согласно действующему законодательству Российской Федерации (КоАП РФ, Уголовный кодекс РФ, а также нормы гражданского права в части защиты интеллектуальной собственности). Помимо санкций, правообладатели имеют законное основание требовать возмещения ущерба или компенсации, эквивалентной двукратной стоимости лицензии. Подобные споры часто завершаются судебными исками, изъятием нелегальных копий и финансовыми потерями организаций [8].

Результаты независимых аудитов и отчёты международных ассоциаций (в частности, BSA | The Software Alliance) указывают на то, что предприятия, использующие пиратское программное обеспечение, сталкиваются с кратным ростом вероятности кибератак и потери данных. Взломанные версии часто содержат вредоносный код, не имеют встроенных средств обновления и создают угрозу целостности информационной среды. Для строительных компаний это особенно критично: повреждение BIM-модели, нарушение связей геоданных или искажение параметров материалов способно привести к

инженерным ошибкам, перерасходу ресурсов и увеличению сроков строительства [4].

Кроме киберрисков, нелицензионные продукты нарушают совместимость программных сред. Применение несертифицированных версий часто делает невозможной корректную интеграцию с ERP-системами, сервисами облачного хранения и средствами обмена моделями (IFC, BCF). Потеря совместимости приводит к искажению данных, ошибкам при экспорте и импорте, нарушению синхронизации с инженерным оборудованием (например, с системами ЧПУ, IoT-датчиками или механизмами автоматической укладки), что напрямую отражается на качестве проектных и строительных работ [2].

Факт использования пиратского ПО подрывает доверие заказчиков, инвесторов и контролирующих органов. Внешние проверки со стороны поставщиков (Autodesk, Graphisoft, Trimble и др.) или специализированных организаций (BSA, Revenera) нередко выявляют нарушения и влекут за собой крупные штрафы, вынужденную покупку лицензий по завышенным тарифам и репутационные потери [5].

Особую опасность представляет применение нелегального программного обеспечения в системах, обеспечивающих функциональную безопасность: управлении строительной техникой, мониторинге нагрузок, геодезическом контроле и автоматизированных системах предупреждения аварий. Ошибки в работе таких систем вследствие изменения программного кода или отсутствия обновлений могут привести к сбоям оборудования и угрозе жизни работников. В соответствии с ГОСТ Р 56939-2024 и международными стандартами ISO/IEC 61508, ПО, участвующее в обеспечении безопасности, должно проходить обязательную сертификацию и регулярное обновление.

Одной из наиболее проблемных областей при использовании нелицензионного ПО является отсутствие сопровождения и технической поддержки. Такие версии программ не получают патчей, консультаций и обновлений, что приводит к накоплению уязвимостей и нестабильности систем. Особенно остро это проявляется в интеграционных BIM- и ERP-средах, где даже незначительные ошибки могут вызвать рассогласование моделей, сбои обмена данными и потерю проектных связей. Использование пиратских версий программных комплексов, таких как Autodesk Revit или ArchiCAD, неизбежно ведёт к несовместимости с официальными сервис-паками и нарушению работы совместных моделей [7,9].

Отсутствие обновлений безопасности также делает строительные ИТ-системы уязвимыми для внешних атак. В последние годы зафиксированы инциденты компрометации корпоративных сетей строительных компаний через заражённые версии программ для расчёта смет, что вызывало полную остановку производственных процессов и потерю данных. Кроме того, отсутствие SDK и официальных API делает невозможной адаптацию программ к корпоративным нуждам, снижая эффективность цифровой среды и повышая риски конфликтов при интеграции [5].

Хотя отказ от лицензий позволяет временно снизить прямые расходы, в долгосрочной перспективе это приводит к росту совокупной стоимости владения (TCO). Расходы на устранение ошибок, простои и восстановление информации превышают экономию от отсутствия лицензий. Исследования показывают, что уровень производственных потерь у компаний, применяющих пиратское ПО, достигает 15–25 % [3].

Кроме того, использование нелицензионных продуктов делает невозможным прохождение сертификаций по стандартам качества и

информационной безопасности (ГОСТ Р ИСО/МЭК 19770-1-2014, ГОСТ Р ИСО 9001-2015), что ограничивает участие таких организаций в государственных и международных тендерах. Отсутствие официального подтверждения соблюдения стандартов управления программными активами (SAM) снижает доверие заказчиков и партнёров, а также препятствует цифровой трансформации компании [6].

Меры по снижению рисков:

1. Внедрение системы менеджмента программных активов (SAM) на основе ISO/IEC 19770 и соответствующих российских ГОСТов.

2. Разработка корпоративных политик по лицензированию, контролю и обновлению программного обеспечения.

3. Централизованное управление установками, мониторинг целостности и применение антивирусных и EDR-систем.

4. Обучение сотрудников принципам безопасного использования программных продуктов и ответственности за нарушения.

5. Включение требований по легальности ПО в договоры с подрядчиками и проведение регулярных аудитов.

Использование нелицензионного программного обеспечения в строительстве формирует комплекс рисков — от юридических санкций до угроз кибербезопасности и сбоев производственных процессов. В условиях активной цифровизации, интеграции BIM, IoT и автоматизированных систем, надёжность и законность программных средств становятся стратегическим фактором устойчивого развития отрасли. Применение системного подхода, основанного на управлении программными активами, стандартах безопасности и развитии

культуры правомерного использования ПО, позволит минимизировать угрозы и повысить эффективность строительных организаций [2].

Использование нелицензионного программного обеспечения в строительстве формирует комплекс взаимосвязанных рисков, затрагивающих технологические, правовые и организационные аспекты. В условиях внедрения BIM-технологий, IoT-систем и цифровых платформ любые сбои в работе программных средств ведут к нарушению целостности проектных данных, ошибкам интеграции и увеличению вероятности киберинцидентов. Отсутствие обновлений, уязвимости и потенциальное наличие вредоносного кода в нелегальных версиях серьёзно подрывают стабильность производственных процессов и создают угрозы безопасности.

С точки зрения управления строительными организациями, применение пиратского ПО приводит к юридическим санкциям, финансовым потерям, утрате доверия заказчиков и невозможности соответствовать требованиям международных и российских стандартов. Для минимизации рисков необходимо внедрение системного управления программными активами, развитие корпоративной политики лицензирования и усиление мер кибербезопасности. Соблюдение лицензионной чистоты становится важным условием устойчивого развития и успешной цифровой трансформации строительного комплекса.

Библиографический список:

1. ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования.

2. ГОСТ Р ИСО/МЭК 19770-1-2014 (ISO/IEC 19770-1). Менеджмент программных активов (SAM).

3. ГОСТ Р 58439.1—2018. Организация информации об объектах капитального строительства. Информационный менеджмент в строительстве с использованием технологии информационного моделирования. Часть 1.

4. BSA | The Software Alliance. Study: The connection between unlicensed software and malware incidents.

5. Revenera. Software Piracy Statistics — 2024. (Отчёт по уровню нелицензионного ПО в мире).

6. Тихонов А.В. Использование искусственного интеллекта для контроля качества строительных работ // Вестник строительных наук. 2023.

7. Delo-Press. Нелицензионное программное обеспечение: риски и ответственность (обзор юридических последствий) // Информационные технологии.

8. Грахов В.П. Обзор современных строительных технологий и анализ рисков их внедрения / В. П. Грахов, З. С. Саидова, К. П. Мельниченко, А. Ф. Ангелич // Экономика и предпринимательство. – 2023. – № 2(151). – С. 633-639. – DOI 10.34925/EIP.2023.151.2.121. – EDN SCWMXG.

9. Кушнерев, Н. Ю. Эффективность и безопасность использования лицензированного по в строительстве / Н. Ю. Кушнерев // Будущее науки - 2025 : Сборник научных статей 12-й Международной молодежной научной конференции. В 5-х томах, Курск, 17–18 апреля 2025 года. – Курск: ЗАО "Университетская книга", 2025. – С. 162-165. – EDN FUGHMA.

Оригинальность 75%