 © Авторы статьи / Authors of the article

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ И АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ/COMPUTER MODELING AND DESIGN AUTOMATION

DOI: https://doi.org/10.60797/itech.2026.12.4 EDN: XEENHS

МЕТОДЫ И АРХИТЕКТУРА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В ОБЛАЧНЫХ BIM-СЕРВИСАХ НА ЭТАПЕ ЭКСПЛУАТАЦИИ

Научная статья

Вовчок С.С.[1, *]

[1] Российский университет транспорта (МИИТ), Москва, Российская Федерация

* Корреспондирующий автор (vov4ok2000[at]ya.ru)

Предложена: 29.06.2026; Принята: 01.09.2026; Опубликована: 14.10.2026

Аннотация

В статье рассматривается проблема обеспечения безопасности данных в облачных сервисах информационного моделирования (BIM), применяемых на этапе эксплуатации зданий и сооружений. Анализируется специфика этапа эксплуатации, отличающегося длительным жизненным циклом данных, множественностью участников с различными уровнями доступа и интеграцией с внешними системами мониторинга. Выявляются основные угрозы безопасности, характерные для данного этапа: несанкционированный доступ, нарушение целостности информационной модели, инсайдерские риски, атаки на каналы интеграции и программы-вымогатели. Систематизируются методы защиты данных, включая идентификацию и аутентификацию с применением многофакторного подтверждения, управление доступом на основе ролевых моделей с гранулярным разграничением прав, шифрование при хранении и передаче, контроль версий и аудит изменений, а также резервное копирование. Описывается типовая архитектура безопасности облачного BIM-сервиса, построенная по эшелонированному принципу с выделением внешнего и внутреннего контуров, изоляцией тенантов в многопользовательской среде и дифференцированным подходом к хранению различных типов эксплуатационных данных. Обосновываются рекомендации по выбору мер защиты в зависимости от масштаба и чувствительности объекта. Делается вывод о необходимости комплексного подхода к обеспечению безопасности как обязательного условия внедрения облачных технологий в практику управления объектами недвижимости.

Ключевые слова: информационное моделирование зданий (BIM), облачные технологии, безопасность данных, этап эксплуатации, защита информации, управление доступом, шифрование, аудит.

METHODS AND ARCHITECTURE FOR ENSURING DATA SECURITY IN CLOUD-BASED BIM SERVICES DURING THE OPERATIONAL PHASE

Research article

Vovchok S.S.[1, *]

[1] Russian University of Transport (MIIT), Moscow, Russian Federation

* Corresponding author (vov4ok2000[at]ya.ru)

Suggested: 29.06.2026; Accepted: 01.09.2026; Published: 14.10.2026

Abstract

The article examines the issue of ensuring data security in cloud-based Building Information Modelling (BIM) services used during the operational phase of buildings and structures. The specificity of the operational phase is analysed, characterised by a long data lifecycle, a multitude of stakeholders with varying levels of access, and integration with external monitoring systems. The main security threats characteristic of this phase are identified: unauthorised access, breaches of the information model's integrity, insider risks, attacks on integration channels and ransomware. Data protection methods are systematised, including identification and authentication using multifactor verification, access control based on role-based models with granular rights separation, encryption at rest and in transit, version control and change auditing, as well as backup. A typical security architecture for a cloud-based BIM service is described, built on a layered principle with distinct external and internal perimeters, tenant isolation in a multi-tenant environment, and a differentiated approach to the storage of various types of operational data. Recommendations are provided on the selection of security measures depending on the scale and sensitivity of the property. A conclusion is made about the need for a complex approach to ensuring security as a prerequisite for the implementation of cloud technologies in property management practice.

Keywords: Building Information Modelling (BIM), cloud technologies, data security, operational phase, information security, access control, encryption, audit.

Введение

Цифровая трансформация строительной отрасли и сферы управления недвижимостью привела к широкому внедрению технологий информационного моделирования. Если изначально технологии BIM применялись преимущественно на этапах проектирования и строительства, то сегодня наблюдается устойчивый тренд на использование информационных моделей (ИМ) на протяжении всего жизненного цикла объекта, ключевым и наиболее продолжительным этапом которого является эксплуатация. Облачные BIM-сервисы становятся основной средой для

 © Авторы статьи / Authors of the article

хранения и обработки данных об объекте, обеспечивая удаленный доступ всем участникам процесса: эксплуатирующим организациям, собственникам, подрядным службам, надзорным органам.

На этапе эксплуатации в облачной среде накапливаются значительные массивы данных, имеющих высокую коммерческую ценность и критическую значимость. Это не только сама информационная модель, отражающая текущее состояние здания, но и потоковые данные с датчиков Интернета вещей (IoT) о параметрах микроклимата, работе инженерных систем, показаниях счетчиков, а также юридически значимые документы: акты, договоры, отчеты об осмотрах и персональные данные арендаторов или жильцов. Проблема обеспечения безопасности этих данных становится первостепенной. Утечка или компрометация эксплуатационной информации несет в себе риски не только финансовых потерь, но и угрозы физической безопасности объекта. Несанкционированный вход в учетные записи облачных продуктов и заражение инфраструктуры программами-вымогателями являются практически значимыми сценариями угроз для организаций строительного профиля [5]. Требования российских регуляторов, в частности Федерального закона № 152-ФЗ «О персональных данных», обязывают операторов обеспечивать установленный уровень защиты обрабатываемой информации [1], [13].

Целью настоящей статьи является систематизация методов и архитектурных решений, применяемых для обеспечения безопасности данных в облачных BIM-сервисах на этапе эксплуатации зданий. В рамках работы решаются задачи анализа специфических угроз, обзора современных методов защиты, описания типовой архитектуры безопасной системы и выработки практических рекомендаций.

Методы и принципы исследования

Теоретико-методологическую основу исследования составили научные труды отечественных и зарубежных авторов в области защиты информации, облачных вычислений и технологий информационного моделирования, нормативные документы по защите персональных данных и критической информационной инфраструктуры, а также аналитические материалы отраслевых организаций по вопросам кибербезопасности в строительстве и сфере ЖКХ. Эмпирическую базу работы сформировали техническая документация и руководства по безопасности коммерческих облачных BIM-платформ, рекомендации по управлению криптографическими ключами и мобильными устройствами, а также открытые данные о киберинцидентах в отраслевых информационных системах. В процессе исследования применялись общенаучные методы: системный анализ для структурирования классов данных и угроз на этапе эксплуатации; сравнительный анализ для сопоставления методов защиты и архитектурных решений; метод классификации и типологизации для упорядочивания мер безопасности; метод анализа случаев для оценки последствий реальных инцидентов; а также метод моделирования при описании типовой архитектуры защищенной облачной среды. Кроме того, использовались методы декомпозиции и синтеза при рассмотрении комплексной системы обеспечения безопасности как совокупности взаимосвязанных компонентов.

Основные результаты

Как отмечают Гришина Н. М., Мицко Д. И., этап эксплуатации здания коренным образом отличается от этапов проектирования и строительства с точки зрения характера работы с данными и требований к их защите. Если на ранних этапах жизненного цикла информация имеет проектный, часто статичный характер, то эксплуатация порождает непрерывный поток операционных и ретроспективных данных [2].

Во-первых, эксплуатационные данные должны сохраняться и оставаться доступными для чтения в течение десятилетий. Поэтому системы хранения и резервного копирования должны обеспечивать долговременную целостность данных, совместимость форматов и контролируемую миграцию архивов. Во-вторых, для этапа эксплуатации характерно значительное разнообразие участников. В отличие от замкнутого круга проектировщиков, с моделью работают сотрудники эксплуатирующей организации, подрядчики, управляющие и ресурсоснабжающие организации, арендаторы и надзорные органы. Многие из этих субъектов имеют временный или ограниченный доступ, что требует гибкой и многоуровневой системы разграничения прав.

В-третьих, эксплуатационная информационная модель (ЭИМ) является динамической структурой. Она объединяет несколько классов данных, каждый из которых имеет свою критичность:

- базовая ИМ (архитектурные, конструктивные решения);
- данные мониторинга (телеметрия с IoT-датчиков, SCADA-систем);
- эксплуатационная документация (журналы осмотров, акты выполненных работ, паспорта систем);
- персональные данные (жильцов, арендаторов, сотрудников).

Исходя из этого, требования к безопасности на этапе эксплуатации формулируются в классической триаде CIA (конфиденциальность, целостность, доступность), но с определенными акцентами. Конфиденциальность необходима для защиты персональных данных и коммерческой информации. Целостность критически важна для ИМ и документов, так как внесение несанкционированных изменений в модель может привести к аварийным ситуациям при проведении ремонтных работ. Доступность означает, что сервис и данные должны быть доступны уполномоченным лицам в любое время для обеспечения непрерывного функционирования объекта. Дополнительным требованием является аудируемость — возможность точно определить, кто, когда и какие изменения внес в модель или данные [3].

Специфика этапа эксплуатации формирует особый ландшафт угроз. Помимо классических рисков, таких как несанкционированный доступ и утечки данных, характерных для любой облачной среды, возникают специфические вызовы. Ключевой угрозой является нарушение целостности информационной модели и связанной с ней документации. Преднамеренное или случайное изменение параметров инженерных систем, замена материалов в модели на менее прочные или удаление данных о скрытых коммуникациях могут привести к фатальным последствиям при проведении последующих ремонтов или модернизации [4].

Как верно подчеркивает Сафонов В. А., высокая ротация персонала и привлечение множества подрядных организаций порождают угрозы, связанные с человеческим фактором и инсайдерами. Бывшие сотрудники или

 © Авторы статьи / Authors of the article

недобросовестные подрядчики могут сохранить доступ к системе, если не настроены своевременная блокировка учетных записей и строгий контроль сессий. Особую опасность представляют атаки на каналы интеграции с внешними системами, такими как SCADA или «умные» счетчики. Скомпрометированный датчик или контроллер может стать точкой входа для злоумышленника во всю облачную инфраструктуру. Также актуальны атаки типа «отказ в обслуживании» (DDoS), способные нарушить работу диспетчерской службы. Программы-вымогатели, шифрующие базы договоров или архивы ИМ, могут остановить операционную деятельность эксплуатирующей организации [5].

Практическую реализуемость этих угроз показывают два типовых сценария. В первом случае злоумышленник использует ранее скомпрометированные реквизиты доступа для входа в учетную запись пользователя, не защищенную многофакторной аутентификацией. Полученные права позволяют просматривать или выгружать эксплуатационные документы и фрагменты информационной модели. Во втором случае программа-вымогатель проникает в инфраструктуру через унаследованную систему или рабочее место подрядчика, после чего шифрует цифровую документацию и пытается скопировать ее во внешнее хранилище. Эти сценарии показывают необходимость одновременно обеспечивать доступность и конфиденциальность данных с помощью MFA, контроля массовой выгрузки и изолированных резервных копий [5].

Противодействие описанным угрозам требует применения комплекса взаимодополняющих методов защиты, адаптированных к эксплуатационным сценариям.

Базовым уровнем защиты является надежная идентификация и аутентификация пользователей. В современных облачных BIM-решениях стандартом становится применение единой системы входа (SSO — Single Sign-On), что позволяет централизованно управлять жизненным циклом учетных записей и интегрироваться с корпоративными каталогами (например, Active Directory). Обязательным требованием является использование многофакторной аутентификации (MFA), которая существенно снижает риск компрометации учетной записи даже при утечке пароля.

Управление доступом к данным реализуется на основе ролевых моделей (RBAC — Role-Based Access Control) или моделей, учитывающих атрибуты (ABAC — Attribute-Based Access Control). В контексте BIM это означает разграничение прав не только на уровне разделов или папок проекта, но и на уровне отдельных элементов модели или даже их свойств. Например, подрядчик, выполняющий ремонт в конкретном помещении, может получить доступ к элементам модели только этого помещения и только на чтение, без права редактирования остальной части здания. Разграничение по типам операций (чтение, создание, изменение, удаление, утверждение) позволяет реализовать принцип минимальных привилегий [6], [7].

Защита данных при хранении и передаче обеспечивается криптографическими методами. Критически важные данные, включая файлы ИМ и базы данных, должны храниться в зашифрованном виде с использованием стойких алгоритмов, например AES-256, либо сертифицированных средств криптографической защиты, когда их применение предусмотрено моделью угроз и требованиями регуляторов. Передача данных между клиентом и сервером защищается актуальными версиями протокола TLS, гарантирующими конфиденциальность и целостность трафика.

В мультитенантной среде криптографическая изоляция должна дополнять логическое разделение данных. Для каждого тенанта целесообразно назначать отдельный ключ шифрования ключей (Key Encryption Key, KEK), защищенный в KMS или аппаратном модуле HSM. Данные шифруются одноразовыми или регулярно обновляемыми ключами данных (Data Encryption Key, DEK), а сами DEK хранятся только в зашифрованном виде, что соответствует принципу конвертного шифрования. При модели, управляемой провайдером, генерация, хранение и ротация корневых ключей находятся в зоне ответственности поставщика облачного сервиса. Модель Bring Your Own Key (BYOK) передает заказчику контроль над ключом тенанта: заказчик создает или импортирует его, устанавливает сроки ротации, получает независимый журнал операций и может отозвать доступ. BYOK повышает контролируемость обработки и поддерживает требования к суверенитету данных, но не освобождает оператора и провайдера от договорного закрепления ответственности за доступность KMS, резервирование ключей и восстановление после их утраты. Политика управления ключами должна охватывать генерацию, выдачу прав, ротацию, отзыв, архивирование и уничтожение ключевого материала [7].

Для обеспечения целостности информации необходимы механизмы контроля версий и журналирования изменений. Каждое изменение в ИМ должно фиксироваться как отдельная версия с возможностью возврата к предыдущему состоянию, что защищает от случайных или злонамеренных правок. Для юридически значимых документов (акты, договоры) рекомендуется применение хеширования или усиленной квалифицированной электронной подписи, что гарантирует их подлинность и неизменность. Аудит и мониторинг являются активными методами защиты. Система должна в автоматическом режиме собирать и анализировать события доступа и изменения данных. Выявление аномалий (например, массовая выгрузка документов или вход в систему в нерабочее время) позволяет оперативно реагировать на потенциальные инциденты. Наконец, политики резервного копирования и восстановления приобретают на этапе эксплуатации критическое значение. Регулярное создание резервных копий, их хранение в географически распределенных центрах обработки данных и, что самое важное, регулярное тестирование восстановления из «бэкапов» являются последней линией обороны против потери данных, в том числе вследствие атак программ-вымогателей [8].

Архитектура безопасности облачного BIM-сервиса строится по эшелонированному принципу. На внешнем контуре клиентские приложения взаимодействуют с системой через защищенный API-шлюз, обеспечивающий терминацию TLS-соединений и первичную фильтрацию трафика. Уровень сервисов приложения разделяется на внешний контур (DMZ), обрабатывающий запросы, и внутренний, где размещаются изолированные микросервисы безопасности: аутентификация, аудит и управление ключами. Такое разделение минимизирует поверхность атаки. В многопользовательской архитектуре критически важна изоляция тенантов на уровне баз данных, файловых хранилищ и криптографических ключей. Специфика эксплуатационных данных требует дифференцированного подхода к хранению: высоконагруженные потоки телеметрии обрабатываются через очереди сообщений и базы временных

 © Авторы статьи / Authors of the article

рядов, тогда как документооборот и информационная модель размещаются в объектных хранилищах с поддержкой версионности. Доступ к хранилищам строго соответствует ролевой модели приложения [10].

Отдельной точкой внешнего контура являются мобильные клиенты, используемые техническим персоналом при осмотрах и ремонте. Их доступ следует разрешать только с зарегистрированных устройств, соответствующих корпоративной политике безопасности. Средства MDM или EMM должны обеспечивать шифрование локального хранилища, разделение служебных и личных данных, контроль версий операционной системы, запрет небезопасного копирования и удаленное стирание служебного контейнера. Локальное кэширование фрагментов ИМ ограничивается сроком и объемом, а особо критичные операции подтверждаются повторной аутентификацией. При утрате устройства токены и сертификаты доступа должны быть немедленно отозваны; весь обмен выполняется по защищенному каналу и регистрируется в журнале аудита [7].

Обсуждение

Выбор модели использования облачной инфраструктуры определяется требованиями к суверенитету данных. Зарубежные платформы (Autodesk BIM 360) строятся на публичной облачной инфраструктуре, тогда как российские разработчики (АСКОН, G Tech) предлагают решения в защищенных контурах или частных облаках, ориентированные на исполнение требований законодательства РФ. При этом географическое размещение данных, юрисдикция провайдера и местонахождение ключевого материала должны оцениваться раздельно. Применение BYOK позволяет усилить контроль заказчика над доступом к данным, однако само по себе не заменяет требований к локализации, сертификации средств защиты и договорному распределению ответственности.

Новоселова И.В., Чернявский И.А. пишут о том, что выбор методов защиты должен основываться на анализе рисков конкретного объекта [11]. Для небольшого объекта, не отнесенного к значимым объектам критической информационной инфраструктуры (КИИ), минимальный набор включает SSO с MFA, ролевой доступ, шифрование данных при хранении и передаче, централизованный аудит и управляемые мобильные клиенты. Практически обоснованной отправной точкой является ежедневное инкрементное и еженедельное полное резервное копирование с одной изолированной неизменяемой копией; целевые значения допустимой потери данных (RPO) до 24 часов и времени восстановления (RTO) до 8 часов уточняются по результатам анализа влияния на деятельность. Восстановление необходимо проверять не реже одного раза в квартал.

Для средних и крупных объектов рекомендуются отдельные ключи тенантов, сегментация сети, централизованный сбор событий безопасности, резервирование KMS и сокращение RPO и RTO в соответствии с критичностью инженерных процессов. Унаследованные системы не следует подключать непосредственно к облачному хранилищу: их интеграция выполняется через выделенный шлюз в сегменте DMZ с инвентаризацией интерфейсов, фильтрацией команд, преобразованием устаревших протоколов и, где это возможно, доступом только на чтение. Для объектов, подпадающих под действие Федерального закона № 187-ФЗ, проводится категорирование и реализуются меры защиты, соответствующие значимости объекта [14]. При обработке персональных данных состав мер определяется с учетом требований Федерального закона № 152-ФЗ [13]. Для стратегических и иных высококритичных объектов необходима полноценная система с сегментированием сети, HSM, SIEM, изолированными контурами резервного копирования и непрерывным контролем каналов интеграции.

Основными ограничениями остаются зависимость от политик облачного провайдера, высокая стоимость частных облачных решений, сложность интеграции унаследованных систем и дефицит квалифицированных кадров. Дальнейшие исследования следует направить на разработку методов машинного обучения для выявления аномалий, оценку защищенности мобильного доступа и создание отраслевых стандартов обмена эксплуатационными данными [12].

Заключение

Таким образом, обеспечение безопасности данных в облачных BIM-сервисах на этапе эксплуатации является сложной многогранной задачей. Специфика этапа — длительный жизненный цикл, множество разнородных участников, высокая ценность и разнообразие данных — требует применения комплексного подхода к защите. Такой подход должен сочетать надежную идентификацию и управление доступом на гранулярном уровне, криптографическую защиту с разделением ключей тенантов и определенной моделью ответственности за KMS, обеспечение целостности через контроль версий и аудит, защиту мобильных клиентов, а также отказоустойчивую архитектуру хранения и резервного копирования. Архитектура современного защищенного BIM-сервиса строится по эшелонированному принципу с выделением контуров безопасности, логической и криптографической изоляцией тенантов и интеграцией с инфраструктурными сервисами облачных провайдеров. Состав мер должен определяться анализом рисков, чувствительностью данных и применимыми требованиями регуляторов, а их эффективность — подтверждаться проверками восстановления и анализом событий безопасности. Реализация этих принципов позволяет минимизировать риски утечек, нарушения целостности и потери данных. Практическая значимость работы заключается в создании основы для выбора и внедрения адекватных мер защиты при переходе к облачным технологиям управления эксплуатацией.

Конфликт интересов

Не указан.

Рецензия

Шайхулова А.Ф., Уфимский университет науки и технологий, Уфа Российская Федерация
DOI: https://doi.org/10.60797/itech.2026.12.4.1

Conflict of Interest

None declared.

Review

Shaykhulova A.F., Ufa University of Science and Technology, Ufa Russian Federation
DOI: https://doi.org/10.60797/itech.2026.12.4.1

 © Авторы статьи / Authors of the article

Список литературы / References

1. Федотова А.С. BIM на стадии эксплуатации / А.С. Федотова // E-Scio. — 2020. — № 12 (51). — URL: https://cyberleninka.ru/article/n/bim-na-stadii-ekspluatatsii (дата обращения: 14.02.2026).

2. Гришина Н.М. Разработка и внедрение BIM-стандарта: исследование методов управления в строительстве / Н.М. Гришина, Д.И. Мицко // Известия КазГАСУ. — 2017. — № 3 (41). — URL: https://cyberleninka.ru/article/n/razrabotka-i-vnedrenie-bim-standarta-issledovanie-metodov-upravleniya-v-stroitelstve (дата обращения: 14.02.2026).

3. Черникова А.А. Информационное моделирование на стадии эксплуатации здания / А.А. Черникова // Молодой ученый. — 2022. — № 49 (444). — С. 66–68.

4. Городнова Н.В. Применение BIM-технологий в цифровой экономике: мировой опыт и российская практика / Н.В. Городнова, В.А. Лемеза // Экономика, предпринимательство и право. — 2022. — Т. 12. — № 8. — С. 2241–2260. — DOI: 10.18334/epp.12.8.115082.

5. Сафонов В.А. Исследование уязвимостей и методов защиты данных в облачных информационных хранилищах / В.А. Сафонов // Актуальные исследования. — 2024. — № 22 (204). — Ч. I. — С. 51–54.

6. Абрамян С.Г. Интеграция BIM и ГИС технологий в целях обеспечения экологической безопасности строительства / С.Г. Абрамян, А.В. Котляревская, О.В. Оганесян [и др.] // Международный научно-исследовательский журнал. — 2020. — № 5 (95). — DOI: 10.23670/IRJ.2020.95.5.004.

7. Акбарова М.Р. Безопасность и защита данных в облачных технологиях / М.Р. Акбарова // Universum: технические науки: электрон. научн. журн. — 2022. — № 10 (103). — URL: https://7universum.com/ru/tech/archive/item/14427 (дата обращения: 14.02.2026).

8. Лустина О.В. Использование BIM-технологий в современном строительстве / О.В. Лустина, Н.А. Бикбаева, А.М. Купчеков // Молодой учёный. Международный научный журнал. — 2016. — Т. 2. — № 15. — С. 187–190.

9. Бейсембаева С.А. Применения БИМ-технологий на стадии эксплуатации в зданиях / С.А. Бейсембаева, А.Ш. Калмагамбетова, Б.С. Туралыкова // Эпоха науки. — 2021. — № 25. — URL: https://cyberleninka.ru/article/n/primeneniya-bim-tehnologiy-na-stadii-ekspluatatsii-v-zdaniyah (дата обращения: 14.02.2026).

10. Абалтусов Ю.А. BIM-технологии. Проблемы их внедрения и перспективы развития в строительстве и проектировании / Ю.А. Абалтусов, В.В. Чатуров // Молодой ученый. — 2019. — № 25 (263). — С. 151–153.

11. Новоселова И.В. Применение BIM-технологий на всех стадиях жизненного цикла строительного проекта / И.В. Новоселова, И.А. Чернявский // Современные тенденции в строительстве, градостроительстве и планировке территорий. — 2022. — № 1 (3). — С. 4–15. — DOI: 10.23947/2949-1835-2022-1-3-4-15.

12. Girya L. Organizational and technological computeraided process of real estate management / L. Girya, E. Zorenko, N. Ulianov [et al.] // E3S Web of Conferences. — 2021. — Vol. 263. — P. 04032.

13. Российская Федерация. Законы. О персональных данных : федер. закон : [от 27.07.2006 № 152-ФЗ].

14. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон : [от 26.07.2017 № 187-ФЗ].

Список литературы на английском языке / References in English

1. Fedotova A.S. BIM na stadii ekspluatatsii [BIM during the operational phase] / A.S. Fedotova // E-Scio. — 2020. — № 12 (51). — URL: https://cyberleninka.ru/article/n/bim-na-stadii-ekspluatatsii (accessed: 14.02.2026). [in Russian]

2. Grishina N.M. Razrabotka i vnedrenie BIM-standarta: issledovanie metodov upravleniya v stroitelstve [Development and Implementation of a BIM Standard: A study of management methods in the construction industry] / N.M. Grishina, D.I. Mitsko // Izvestiya KazGASU [Proceedings of KazSASU]. — 2017. — № 3 (41). — URL: https://cyberleninka.ru/article/n/razrabotka-i-vnedrenie-bim-standarta-issledovanie-metodov-upravleniya-v-stroitelstve (accessed: 14.02.2026). [in Russian]

3. Chernikova A.A. Informatsionnoe modelirovanie na stadii ekspluatatsii zdaniya [Information modelling during the operational phase of a building] / A.A. Chernikova // Molodoi uchenii [Young Scientist]. — 2022. — № 49 (444). — P. 66–68. [in Russian]

4. Gorodnova N.V. Primenenie BIM-tekhnologii v tsifrovoi ekonomike: mirovoi opit i rossiiskaya praktika [The application of BIM technologies in the digital economy: international experience and Russian practice] / N.V. Gorodnova, V.A. Lemeza // Ekonomika, predprinimatelstvo i pravo [Economics, Entrepreneurship and Law]. — 2022. — Vol. 12. — № 8. — P. 2241–2260. — DOI: 10.18334/epp.12.8.115082. [in Russian]

5. Safonov V.A. Issledovanie uyazvimostei i metodov zashchiti dannikh v oblachnikh informatsionnikh khranilishchakh [A study of vulnerabilities and data protection methods in cloud data storage systems] / V.A. Safonov // Aktualnie issledovaniya [Current Research]. — 2024. — № 22 (204). — Pt. I. — P. 51–54. [in Russian]

6. Abramyan S.G. integratsiya BIM i GIS tekhnologii v tselyakh obespecheniya ekologicheskoi bezopasnosti stroitelstva [The integration of BIM and GIS technologies to ensure environmental safety in construction] / S.G. Abramyan, A.V. Kotlyarevskaya, O.V. Oganesyan [et al.] // Mezhdunarodnii nauchno-issledovatelskii zhurnal [International Research Journal]. — 2020. — № 5 (95). — DOI: 10.23670/IRJ.2020.95.5.004. [in Russian]

7. Akbarova M.R. Bezopasnost i zashchita dannikh v oblachnikh tekhnologiyakh [Data security and protection in cloud technologies] / M.R. Akbarova // Universum: tekhnicheskie nauki: elektron. nauchn. zhurn. [Universum: Technical Sciences: electronic scientific journal] — 2022. — № 10 (103). — URL: https://7universum.com/ru/tech/archive/item/14427 (accessed: 14.02.2026). [in Russian]

 © Авторы статьи / Authors of the article

8. Lustina O.V. Ispolzovanie BIM-tekhnologii v sovremennom stroitelstve [The use of BIM technologies in modern construction] / O.V. Lustina, N.A. Bikbaeva, A.M. Kupchekov // Molodoi uchyonii. Mezhdunarodnii nauchnii zhurnal [Young Scientist. International Research Journal]. — 2016. — Vol. 2. — № 15. — P. 187–190. [in Russian]

9. Beisembaeva S.A. Primeneniya BIM-tekhnologii na stadii ekspluatatsii v zdaniyakh [Applications of BIM technologies during the operational phase of buildings] / S.A. Beisembaeva, A.Sh. Kalmagambetova, B.S. Turalikova // Epokha nauki [The Age of Science]. — 2021. — № 25. — URL: https://cyberleninka.ru/article/n/primeneniya-bim-tehnologiy-na-stadii-ekspluatatsii-v-zdaniyah (accessed: 14.02.2026). [in Russian]

10. Abaltusov Yu.A. BIM-tekhnologii. Problemi ikh vnedreniya i perspektivi razvitiya v stroitelstve i proektirovanii [BIM technologies. Challenges in their implementation and prospects for development in construction and design] / Yu.A. Abaltusov, V.V. Chaturov // Molodoi uchenii [Young Scientist]. — 2019. — № 25 (263). — P. 151–153. [in Russian]

11. Novoselova I.V. Primenenie BIM-tekhnologii na vsekh stadiyakh zhiznennogo tsikla stroitelnogo proekta [The use of BIM technologies at all stages of a construction project's life cycle] / I.V. Novoselova, I.A. Chernyavskii // Sovremennie tendentsii v stroitelstve, gradostroitelstve i planirovke territorii [Current Trends in Construction, Urban Development and Spatial Planning]. — 2022. — № 1 (3). — P. 4–15. — DOI: 10.23947/2949-1835-2022-1-3-4-15. [in Russian]

12. Girya L. Organizational and technological computeraided process of real estate management / L. Girya, E. Zorenko, N. Ulianov [et al.] // E3S Web of Conferences. — 2021. — Vol. 263. — P. 04032.

13. Rossiiskaya Federatsiya. Zakoni. O personalnikh dannikh [Russian Federation. Legislation. On Personal Data] : Federal Law: [No. 152-FZ of 27 July 2006]. [in Russian]

14. Rossiiskaya Federatsiya. Zakoni. O bezopasnosti kriticheskoi informatsionnoi infrastrukturi Rossiiskoi Federatsii [Russian Federation. Laws. On the Security of Critical Information Infrastructure of the Russian Federation] : Federal Law: [No. 187-FZ of 26 July 2017]. [in Russian]