

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ/SYSTEM ANALYSIS, MANAGEMENT AND PROCESSING OF INFORMATION

DOI: https://doi.org/10.60797/IRJ.2026.168.34 EDN: HLAOFY

ЭМПИРИЧЕСКИЙ АНАЛИЗ РУКОВОДЯЩИХ ПРАКТИК И РЕГЛАМЕНТИРУЮЩИХ НОРМ ПРИМЕНИТЕЛЬНО К ПРОЦЕДУРАМ РЕЗЕРВНОГО КОПИРОВАНИЯ В КОРПОРАТИВНЫХ ХРАНИЛИЩАХ ПРОИЗВОДСТВА

Научная статья

Макаров А.О.[1,] *, Ломакин А.С.[2], Дорохов И.А.[3], Орлова Ю.А.[4]
[2] ORCID : 0009-0001-9340-1748;
[4] ORCID : 0000-0003-4854-7462;
[1, 2, 3, 4] Волгоградский государственный технический университет, Волгоград, Российская Федерация

* Корреспондирующий автор (a.o.makarov2003[at]gmail.com)

Предложена: 27.02.2026; Принята: 05.05.2026; Опубликована: 17.06.2026

Аннотация

Статья посвящена анализу практик и нормативных требований к резервному копированию в корпоративных хранилищах производственных предприятий Российской Федерации. В статье рассматриваются актуальные данные о кибератаках, а также подчёркивается серьёзная угроза ransomware-атак, и то, как они влияют на необходимость надёжной защиты данных. Детально проведён обзор ключевых нормативно-правовых актов, которые регламентируют правила резервного копирования и сроки восстановления ИТ-ландшафтов в зависимости от их классов защищённости. Подробно рассматриваются основные методы и архитектуры резервного копирования в корпоративных ИТ-инфраструктурах, включая полные, инкрементальные и дифференциальные копии, гибридные схемы хранения данных с использованием локальных и удаленных хранилищ, а также применение неизменяемых WORM-хранилищ для защиты от перезаписи. Выполнен сравнительный анализ отечественного ПО в сфере бэкапа по ключевым характеристикам, включая поддержку виртуализированных сред, совместимость с отечественными операционными системами, а также наличие в Едином реестре российских программ для ЭВМ и БД и сертификатов ФСТЭК. Обоснована потребность в создании автоматизированного агента, который позволит формировать индивидуальные рекомендации по построению планов резервного копирования и защите данных в WORM-хранилищах с учётом особенностей виртуализированных сред и существующего ИТ-ландшафта.

Ключевые слова: резервное копирование, корпоративные ИТ-инфраструктуры, ransomware-атаки, WORM-хранилища, виртуализированные среды, КИИ, ПДн, RPO, RTO, импортозамещение, системы бэкапа.

AN EMPIRICAL ANALYSIS OF BEST PRACTICES AND REGULATORY STANDARDS RELATING TO BACKUP PROCEDURES IN CORPORATE PRODUCTION STORAGE SYSTEMS

Research article

Makarov A.O.[1,] *, Lomakin A.S.[2], Dorokhov I.A.[3], Orlova Y.A.[4]
[2] ORCID : 0009-0001-9340-1748;
[4] ORCID : 0000-0003-4854-7462;
[1, 2, 3, 4] Volgograd State Technical University, Volgograd, Russian Federation

* Corresponding author (a.o.makarov2003[at]gmail.com)

Suggested: 27.02.2026; Accepted: 05.05.2026; Published: 17.06.2026

Abstract

The article analyses best practices and regulatory requirements for data backup in corporate storage systems at manufacturing enterprises in the Russian Federation. The paper examines current data on cyberattacks, highlights the serious threat posed by ransomware attacks, and how they impact the need for reliable data protection. A detailed review is provided of the key regulatory and legal acts governing backup procedures and recovery times for IT environments, depending on their security classifications. The main backup methods and architectures in corporate IT infrastructures are reviewed in detail, including full, incremental and differential backups, hybrid data storage schemes using local and remote storage, as well as the use of write-once, read-many (WORM) storage to protect against overwriting. A comparative analysis of domestic backup software is carried out based on key characteristics, including support for virtualised environments, compatibility with domestic operating systems, as well as inclusion in the Unified Register of Russian Computer and Database Programmes and FSTEC certificates. The need for an automated agent has been substantiated, which will enable the generation of customised recommendations for creating backup plans and protecting data in WORM storage, taking into account the specific traits of virtualised environments and the existing IT landscape.

Keywords: backup, corporate IT infrastructure, ransomware attacks, WORM storage, virtualised environments, CII, PD, RPO, RTO, import substitution, backup systems.

Введение

В существующей реальности, когда всё больше предприятий стремятся к цифровизации на рабочих местах, а объемы обрабатываемых данных неуклонно растут, корпоративные хранилища становятся центральными элементами информационной инфраструктуры большинства организаций. От их безопасности и стабильности работы зависит не только сохранность критически важной информации, но и непрерывное функционирование производственных процессов. По данным АО «Лаборатории Касперского», за первый квартал 2025 года зафиксировано свыше 629 миллионов кибератак, включая 21 миллион вредоносных файлов, а также 12 тысяч новых шифровальщиков [1]. Уже во втором квартале 18% компьютеров АСУ в России столкнулись с вредоносным ПО — особенно страдают строительная, нефтегазовая и энергетическая отрасли, где отказ ИТ-инфраструктуры может привести к серьезным экономическим потерям [2], [4]. По международным отчетам АО «Лаборатории Касперского», около 40–50% организаций сталкиваются с трудностями при восстановлении данных после атак, вследствие того что их бэкапы повреждены или устарели [3].

Технологии резервного копирования прошли путь от копий отдельных файлов и лент к виртуализированным средам, сетевым хранилищам данных и облакам. Современные подходы сочетают инкрементальные, дифференциальные и полные бэкапы, а также снапшоты и репликацию для того, чтобы минимизировать время восстановления [5].

В настоящее время резервное копирование сильно интегрировано с виртуализацией и инструментами оркестрации ИТ-ландшафтов. Корпоративные решения создают согласованные снимки ВМ и контейнеров, упрощая восстановление. Виртуализация повышает эффективность, но увеличивает риски, требуя особой защиты резервных копий.

На данный момент серьёзную угрозу для ИТ-ландшафтов представляют программы-шифровальщики (ransomware). Современные ransomware-атаки используют стойкие криптографические алгоритмы, поэтому расшифровать данные без ключа злоумышленника на заражённом устройстве невозможно [7], [11]. В результате чего, организации сталкиваются с длительными простоями ИТ-инфраструктур, значительными финансовыми потерями, а в некоторых случаях и с ущербом их репутации. Надёжное восстановление возможно только при наличии неизменяемых копий: WORM-хранилищ, логического или физического отделения бэкапов от основной сети и строгой проверки целостности [6], [8].

В производственных отраслях (промышленность, энергетика, нефтегаз) простои недопустимы, поэтому применяются репликация ВМ, сочетание локальных и удаленных резервных копий, контроль целостности с учётом длительных циклов и необходимости поддержания непрерывности.

Несмотря на развитые системы защиты и восстановления данных в масштабах предприятия, сохраняются определённые проблемы. Сложности с внутренними правилами, отсутствие единого стандарта для систем бэкапа, разные способы защиты копий и слабое включение нормативов в работу мешают эффективно защищать данные. Для устранения обозначенных проблем необходимы чётко регламентированные подходы и адаптивные средства, в том числе агентные решения, обеспечивающие выработку рекомендаций по стратегиям резервирования данных.

Научная новизна данного исследования заключается в том, что впервые был проведен сравнительный анализ 13 систем резервного копирования на основе 8 критериев оценки с особым акцентом на соответствие обновленным нормативным требованиям ФСТЭК России, а именно приказу № 117, а не только ранее установленным требованиям.

Оригинальность данной работы определяется выявлением несоответствий между формальными нормативными требованиями и фактическими возможностями большинства существующих решений для резервного копирования на рынке РФ.

Практическая значимость результатов обусловлена тем, что они могут быть применены ИТ-отделами и специалистами по информационной безопасности предприятий, работающих в условиях импортозамещения.

Целью исследования является систематизация существующих практик и нормативной базы по резервному копированию данных в современных корпоративных инфраструктурах РФ для дальнейшей разработки автоматизированного агента, способного формировать индивидуальные рекомендации по созданию планов резервного копирования и обеспечению защиты данных в WORM-хранилищах с учетом особенностей виртуализированных сред существующей ИТ-инфраструктуры.

Нормативно-правовые требования к резервному копированию данных в РФ

В Российской Федерации меры по созданию резервных копий и восстановлению данных определяются нормами федерального законодательства и подзаконных актов.

Основу регулирования составляют Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», в которых закреплена обязанность операторов информации и персональных данных обеспечивать их доступность, целостность и защиту от утраты, в том числе за счёт организации процессов резервного копирования и своевременного восстановления [12], [13].

Специальные технические и организационные требования к резервному копированию формализованы в приказах Федеральной службы по техническому и экспортному контролю (ФСТЭК) России.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (в редакции от 28 августа 2024 г.) для государственных информационных систем предписывает регулярное создание резервных копий, а также необходимость обеспечивать возможность восстановления сведений с резервных машинных носителей в пределах установленного временного интервала (меры ОДТ.2, ОДТ.3, ОДТ.4, ОДТ.5) [14]. Конкретные периодичности резервного копирования и предельное время восстановления не регламентированы жёстко и определяются оператором данных самостоятельно с учётом класса защищённости системы, значимости обрабатываемой информации и актуальной модели угроз, что закрепляется во внутренней документации. Приказ ФСТЭК России № 21 от 18.02.2013 также требует

систематического резервного копирования и обеспечения возможности восстановления информации с резервных носителей в установленные сроки (меры ОДТ.3, ОДТ.4, ОДТ.5) [15]. При этом периодичность копирования и предельные значения времени восстановления в нём также возлагаются на усмотрение оператора данных с учётом уровня защищённости персональных данных.

Приказ ФСТЭК России № 117 от 11.04.2025 (действует с 01.03.2026) актуализирует требования к резервному копированию и восстановлению информации в государственных и иных ведомственных информационных системах, впервые вводя конкретные предельные сроки восстановления работоспособности (не более 24 часов для систем 1-го класса защищённости, 7 календарных дней — для 2-го класса и 4 недель — для 3-го класса), которых ранее не содержали приказы ФСТЭК России от 11 февраля 2013 г. № 17 (в редакции от 28 августа 2024 г.) и ФСТЭК России № 21 от 18.02.2013, где регулирование этих параметров полностью ложилось на оператора [16].

Документ сохраняет принцип, по которому периодичность создания резервных копий и детальные процедуры определяются организацией самостоятельно, но обязывает закреплять их во внутренних организационно-распорядительных актах с учётом класса защищённости и принятой модели угроз. Указанный приказ признаёт утратившими силу приказ ФСТЭК России от 11 февраля 2013 г. № 17 (в редакции от 28 августа 2024 г.) с последующими изменениями (приказы № 27, 106 и 61), тем самым ужесточая нормативную базу [17], [18] в части обеспечения доступности информации через резервное копирование и оперативное восстановление [19].

Приказы ФСТЭК России (№ 17, 21, 117) реализуют положения Федеральных законов от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и от 27.07.2006 № 152-ФЗ «О персональных данных», устанавливая обязательный характер мер по резервированию и восстановлению для объектов КИИ и систем обработки персональных данных. Надзор за соблюдением требований в части ПДн возложен на Роскомнадзор, тогда как вопросы криптографической защиты копий находятся в компетенции ФСБ России. В условиях политики импортозамещения программные продукты, применяемые для резервного копирования, должны соответствовать отечественным требованиям сертификации ФСТЭК и ФСБ, что способствует обеспечению технологического суверенитета и устойчивости информационно-технологических инфраструктур.

Методы и архитектуры резервного копирования в корпоративных ИТ-инфраструктурах

В продолжении анализа нормативных аспектов резервного копирования стоит рассмотреть, какие именно подходы и инструменты создания резервных копий используются в корпоративных ИТ-средах.

В современных ИТ-инфраструктурах резервному копированию, как правило, подлежат пользовательские данные, СУБД, конфигурационные файлы, образы операционных систем, виртуальные машины и серверные сервисы. Конкретный способ организации копирования выбирают исходя из целевых показателей точки восстановления (RPO) и допустимого времени восстановления (RTO), которые обычно закрепляются во внутренней документации компании, регламентирующей процессы резервирования [20].

На практике используются полные, инкрементальные и дифференциальные типы резервного копирования. Полный вариант позволяет восстановить весь объём информации, но требует значительных ресурсов по объёму хранилища и времени выполнения операции. Инкрементальные и дифференциальные копии, напротив, уменьшают нагрузку на инфраструктуру и сокращают потребление ресурсов, однако усложняют процедуру восстановления и предъявляют более строгие требования к поддержанию целостности цепочки резервных версий.

Для резервного копирования используются локальные и сетевые хранилища, внешние носители, а также специализированные аппаратные комплексы и программные системы. Профильные программные продукты обеспечивают автоматизацию процессов резервирования, централизованное управление правилами создания копий, контроль целостности информации и управление жизненным циклом бэкапов, включая сроки хранения и схемы ротации.

В распределённых и виртуализированных ИТ-ландшафтах широкое распространение получили гибридные архитектуры бэкапа, при которых используются как локальные, так и удалённые хранилища. Подобное территориальное разнесение копий снижает риски от отказов оборудования, аварий и иных нештатных ситуаций. Для защиты бэкапов от несанкционированных изменений или удаления, в том числе при атаках типа ransomware, применяются неизменяемые хранилища по принципу WORM, а также логическую или физическую изоляцию среды резервного копирования [21].

Практика показывает, что эффективные стратегии резервного копирования строятся на использовании нескольких копий данных, размещённых на различных типах носителей и в разных местах. Такой подход предотвращает наличие единственной точки отказа и даёт уверенность в возможности восстановления информации. Для их успешной реализации необходимо чётко регламентировать процедуры создания и хранения копий, регулярно проводить тесты восстановления, а также фиксировать целевые показатели RPO и RTO в документах по защите информационных систем с учётом предъявляемых к ним требований.

Системы резервного копирования в РФ

В условиях ужесточения регулирования и роста числа инцидентов, связанных с нарушением доступности и целостности информации, результативность резервного копирования в значительной степени определяется функциональностью профильного программного обеспечения. Российский сегмент решений для резервирования данных характеризуется высоким уровнем импортозамещения и нацелен на соответствие требованиям ФСТЭК и ФСБ России. В рамках данной работы рассматриваются ключевые программные продукты, применяемые в корпоративных ИТ-ландшафтах и предлагаемые на рынке отечественными вендорами и дистрибьюторами.

"Altaro VM Backup" — решение для резервного копирования виртуальных машин на платформах Hyper-V и VMware. Позволяет выполнять создание копий без остановки работы ВМ, поддерживает механизмы дедупликации, сжатия, шифрования и централизованного управления задачами резервирования.

"Basis Virtual Protect" — система для защиты виртуальных машин и кластеров Kubernetes с упором на быстрое восстановление инфраструктуры после сбоев. Реализует полные и инкрементальные копии и умеет размещать данные в NFS- и S3-совместимых хранилищах.

"Beeline Cloud Backup" — облачный сервис для резервирования персональных данных и инфраструктур компании с поддержкой правила 3-2-1, обеспечивая защиту как локальных, так и размещённых в облаке ресурсов с возможностью организации аварийного восстановления.

"Handy Backup" — универсальное программное средство для автоматизации резервирования, восстановления и синхронизации данных в средах Windows и Linux, включающее функции «горячего» копирования баз данных, ведения версий, сжатия и шифрования.

«MWS Резервное копирование» — сервис от MTS Web Services для защиты разнотипных и разномасштабных данных, поддерживающий резервирование персональных данных в аттестованные хранилища и кроссплатформенную миграцию.

"Postgres Pro Backup Enterprise" — специализированный продукт для создания копий и восстановления кластеров PostgreSQL и Postgres Pro; поддерживает полный, дифференциальный и инкрементальный режимы, контроль целостности и гибкую настройку политик хранения.

"RuBackup" — модульная система с открытым API, нацеленная на построение импортонезависимых корпоративных решений; реализует поддержку электронной подписи резервных копий, работу с ленточными библиотеками и совместимость с отечественными операционными системами.

«Резервное копирование как услуга в Selectel» — облачный сервис, который предназначен для бэкапа физических серверов, приложений и виртуальных сред с размещением копий в географически распределённых дата-центрах уровня Tier III.

"VK Cloud Backup" предлагает средства для автоматизированного управления резервными копиями с использованием различных стратегий хранения, работает как с физическими, так и с виртуальными ресурсами, обеспечивая высокую скорость восстановления и масштабируемость.

"Yandex Cloud Backup" — платформа для резервного копирования и восстановления виртуальных машин и физических серверов, предоставляющая централизованный интерфейс управления, пофайловое восстановление и поддержку как полных, так и инкрементальных копий.

«Береста» — отечественное промышленное решение, ориентированное на задачи резервирования и восстановления данных в условиях политики импортозамещения. Предусматривает централизованное администрирование, дедупликацию на уровне хранилища и интеграцию с внешними системами аутентификации.

«Кибер Бэкап» позиционируется как корпоративная платформа для защиты ИТ-инфраструктур высокой сложности, поддерживает широкий спектр сценариев резервирования и размещение данных как на дисковых, так и на ленточных носителях.

«Хайстекс Акура» — программное обеспечение для резервного копирования и аварийного восстановления приложений и рабочих нагрузок в физических и виртуальных средах, обеспечивающее кроссплатформенное восстановление и гибкую настройку политик хранения.

Сравнительный анализ отечественных платформ резервного копирования

Анализ отечественного рынка систем резервирования данных, выполненный независимым информационно аналитическим центром Anti Malware.ru (зарегистрированное отраслевое СМИ, специализирующееся на ИБ и ИТ рынке), в обзоре за 2025 год показывает, что отечественные решения полностью покрывают задачи корпоративного бэкапа. Речь идет о защите физических и виртуальных серверов, создание бэкапов баз данных и приложений, совместимость с контейнерами, а также взаимодействии с неизменяемыми и изолированными хранилищами [22]. Большинство ПО обеспечивают централизованное управление политиками, дедупликацию, сжатие данных, контроль целостности данных, а также тестирование восстановления.

Обзор функциональности отечественных систем (см. Таблицу 1) выделяет основные сравнительные характеристики (СХ), а именно:

1) поддержка резервирования отдельных файлов и папок;
2) возможность создания бэкапов СУБД;
3) поддержка резервного копирования виртуализированных сред;
4) возможность хранения бэкапов в облачных хранилищах;
5) совместимость с отечественными ОС;
6) возможность поддержки или интеграции с программно-аппаратными комплексами;
7) наличие сертификации ФСТЭК России;
8) наличие продукта в Едином реестре российских программ для ЭВМ и БД.

Таблица 1 - Сравнение базовых возможностей российских систем резервного копирования

DOI: https://doi.org/10.60797/IRJ.2026.168.34.1

Продукт	СХ-1	СХ-2	СХ-3	СХ-4	СХ-5	СХ-6	СХ-7	СХ-8
Altaro VM Backup	Нет	Нет	Да	Да	Нет	Нет	Нет	Нет
Basis	Нет	Нет	Да	Нет	Да	Нет	Нет	Нет

Продукт	СХ-1	СХ-2	СХ-3	СХ-4	СХ-5	СХ-6	СХ-7	СХ-8
Virtual Protect								
Beeline Cloud Backup	Да	Да	Да	Да	Нет	Нет	Нет	Нет
Handy Backup	Да	Да	Да	Да	Нет	Нет	Нет	Да
MWS Резервное копирование	Да	Да	Да	Да	Да	Нет	Нет	Нет
Postgres Pro Backup Enterprise	Нет	Да	Нет	Да	Да	Нет	Нет	Да
RuBackup	Да	Да	Да	Да	Да	Да	Нет	Да
Selectel Резервное копирование как услуга	Да	Да	Да	Да	Да	Нет	Да	Нет
VK Cloud Backup	Да	Да	Да	Да	Да	Нет	Да	Нет
Yandex Cloud Backup	Да	Нет	Да	Да	Да	Нет	Нет	Нет
Береста	Да	Да	Да	Да	Да	Нет	Нет	Да
Кибер Бэкап	Да	Да	Да	Да	Да	Нет	Да	Да
Хайстекс Акура	Да	Да	Да	Да	Да	Нет	Нет	Да

Представленные сведения показывают, что большинство отечественных систем резервного копирования ориентированы на работу в гибридных ИТ-инфраструктурах с возможностью хранения бэкапов как локально, так и на удалённых площадках. Подобная архитектура снижает риски отказов и позволяет соблюдать требования по целевому времени восстановления (RTO), установленные нормативными актами ФСТЭК России. Основные различия между продуктами касаются уровня автоматизации жизненного цикла бэкапов, гибкости политик хранения, а также совместимости с российскими ОС и ПАК, сертификации ФСТЭК и включения в реестр российского ПО, что критически важно в первую очередь для государственного сектора.

По данным ведущего российского ИТ-издания Cnews, на 2025 год лидером среди российских систем резервного копирования стала компания «Киберпротект», одним из продуктов которой, является «Кибер Бэкап» [23]. Её решения популярны в корпоративном и госсекторе благодаря широкой функциональности и соответствию нормативным требованиям.

Таким образом, анализ отечественного рынка систем резервного копирования показывает, что представленные решения обеспечивают необходимую функциональность для корпоративных и государственных ИТ-ландшафтов. Большинство продуктов поддерживают виртуализацию, базы данных и облачные хранилища, однако существенно различаются по совместимости с российскими ОС и ПАК, сертификации ФСТЭК и включению в реестр российского ПО.

Результаты исследования

В результате проведённого исследования установлено, что вступление в силу с 01.03.2026 приказа ФСТЭК России № 117 значительно меняет подход к организации резервного копирования. Впервые вводятся конкретные сроки восстановления работоспособности информационных систем, зависящие от их класса защищённости. В отличие от предыдущих нормативных актов, данные параметры утрачивают рекомендательный характер и требуют обязательного оформления и практической реализации в инфраструктуре организаций.

Проведённый анализ показывает, что лишь небольшая часть систем резервного копирования (3 из 13 рассмотренных) имеют встроенные механизмы, которые теоретически удовлетворяют новым требованиям к срокам восстановления, установленные приказом ФСТЭК России № 117. При этом большинство проанализированных решений ориентированы в первую очередь на функциональную полноту (поддержку виртуализации, облачных сред, баз данных), но не обеспечивают необходимого уровня соответствия новым регуляторным требованиям.

В отличие от обзора, подготовленного Anti-Malware.ru, который фокусируется в основном на функциональных возможностях продуктов, в данном исследовании выявляется разрыв между нормативными требованиями и реальными возможностями систем.

Также с учётом данных АО «Лаборатория Касперского», согласно которым лишь 40–50% организаций в состоянии корректно восстановить данные после инцидентов, можно говорить о системной проблеме, обусловленной не только выбором технологий резервного копирования, но и организацией хранения, проверки целостности и актуальности резервных копий.

Таким образом, результаты свидетельствуют о существенном несоответствии между ожиданиями регулирующих органов, реальной практикой внедрения и техническими возможностями распространённых решений для резервного копирования на отечественном рынке.

Заключение

В рамках исследования проведена систематизация нормативно-правовых требований к резервному копированию данных в Российской Федерации, включая актуализированные положения ФСТЭК России. Рассмотрены современные методы и архитектуры резервного копирования, применяемые в корпоративных ИТ-инфраструктурах, и выполнен сравнительный анализ отечественных программных решений по ключевым критериям.

Установлено, что несмотря на высокий уровень функциональной зрелости существующих систем резервного копирования, большинство из них не соответствует новым нормативным требованиям, в частности по времени восстановления, установленным приказом ФСТЭК России № 117. Выявлен явный разрыв между нормативными требованиями и фактическими возможностями большинства коммерческих решений на рынке РФ, что свидетельствует о необходимости пересмотра подходов к проектированию и внедрению систем резервирования.

Сравнительный анализ показал различия в уровне поддержки отечественных операционных систем, наличии сертификации ФСТЭК, интеграции с ПАК и возможностях организации неизменяемого хранения данных, критически важных для защиты от современных киберугроз.

Таким образом, полученные результаты обосновывают целесообразность разработки автоматизированного агента, формирующего индивидуальные рекомендации по построению стратегий резервного копирования и организации защиты данных в WORM-хранилищах с учётом требований действующей нормативной базы и особенностей виртуализированных сред.

Конфликт интересов

Не указан.

Рецензия

Белашова Е.С., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.168.34.2

Conflict of Interest

None declared.

Review

Belashova E.S., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.168.34.2

Список литературы / References

1. Развитие информационных угроз в первом квартале 2025 года. Статистика по ПК // АО «Лаборатория Касперского». — URL: https://securelist.ru/malware-report-q1-2025-pc-iot-statistics/112821/ (дата обращения: 13.11.2025).

2. В Kaspersky ICS CERT рассказали о динамике киберугроз для российской промышленности во втором квартале 2025 года // АО «Лаборатория Касперского». — URL: https://www.kaspersky.ru/about/press-releases/v-kaspersky-ics-cert-rasskazali-o-dinamike-kiberugroz-dlya-rossijskoj-promyshlennosti-vo-vtorom-kvartale-2025-goda (дата обращения: 13.11.2025).

3. Incident Response аналитический отчёт за 2024 год // АО «Лаборатория Касперского». — URL: https://content.kaspersky-labs.com/fm/site-editor/18/18b11446b26bf9d75192859778e9a9de/source/report-ir2024.pdf (дата обращения: 13.11.2025).

4. Динамика внешних и внутренних угроз АСУ. Второй квартал 2025 года // Kaspersky ICS CERT. — URL: https://ics-cert.kaspersky.ru/publications/reports/2025/09/10/dynamics-of-external-and-internal-threats-to-industrial-control-systems-q2-2025/ (дата обращения: 13.11.2025).

5. Бопп В.А. Особенности выбора систем резервного копирования / В.А. Бопп // Известия ТулГУ. Технические науки. — 2019. — № 10. — С. 297–300.

6. Черкесова Л.В. Механизм восстановления данных в результате их повреждения, заражения и/или несанкционированного изменения / Л.В. Черкесова, В.А. Савельев, Е.А. Ревякина [и др.] // Вестник ДГТУ. Технические науки. — 2025. — № 1. — С. 134–146.

7. Elkhail A.A. Seamlessly safeguarding data against ransomware attacks / A.A. Elkhail, N. Lachtar, D. Ibdah [et al.] // IEEE Transactions on Dependable and Secure Computing. — 2023. — Vol. 20, № 1. — P. 1–16. — DOI: 10.1109/TDSC.2022.3214781.

8. Guardiola Múzquiz G. The Reverse File System: Towards open cost-effective secure WORM storage devices for logging / G. Guardiola Múzquiz, J. González-Gómez, E. Soriano-Salvador. — 2025. — DOI: 10.48550/arXiv.2509.17969.

9. Бударный Г.С. Разновидности нарушений безопасности и типовые атаки на операционную систему / Г.С. Бударный // АПИНО 2022. — 2022. — С. 406–411.

10. Абраменко Г.Т. Анализ особенностей субъектов критической информационной инфраструктуры РФ / Г.Т. Абраменко, Н.Н. Лансере, И.И. Фадеев // АПИНО 2022. — 2022. — С. 49–54.

11. Allagulyyev B. Ransomware attacks: evolution, defense strategies, and future mitigation techniques / B. Allagulyyev // Innovacionnaja nauka [Innovative Science]. — 2025. — № 5-1-1.

12. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. I). — Ст. 3448.

13. Российская Федерация. Законы. О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации. — 2006. — № 31 (ч. I). — Ст. 3451.

14. Федеральная служба по техническому и экспортному контролю. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 28 августа 2024 г.) // Зарегистрировано в Минюсте России 31 мая 2013 г. № 28608. — 23 с.

15. Федеральная служба по техническому и экспортному контролю. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 14 мая 2020 г.) // Зарегистрировано в Минюсте России 14 мая 2013 г. № 28375. — 17 с.

16. Федеральная служба по техническому и экспортному контролю. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : приказ ФСТЭК России от 11 апреля 2025 г. № 117 // Зарегистрировано в Минюсте России 16 июня 2025 г. № 82619. — 35 с.

17. Федеральная служба по техническому и экспортному контролю. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 : приказ ФСТЭК России от 15 февраля 2017 г. № 27 // Зарегистрировано в Минюсте России 14 марта 2017 г. № 45933. — 15 с.

18. Федеральная служба по техническому и экспортному контролю. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 : приказ ФСТЭК России от 28 мая 2019 г. № 106 (ред. от 27 апреля 2020 г.) // Зарегистрировано в Минюсте России 13 сентября 2019 г. № 55924. — 30 с.

19. Федеральная служба по техническому и экспортному контролю. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 : приказ ФСТЭК России от 27 апреля 2020 г. № 61 // Зарегистрировано в Минюсте России 12 мая 2020 г. № 58322. — 2 с.

20. Питкевич П.И. Методы резервного копирования данных для критически важных ИТ-систем предприятия / П.И. Питкевич // Universum: технические науки. — 2021. — № 10-1 (91).

21. Шайтура С.В. Методы резервирования данных для критически важных информационных систем предприятия / С.В. Шайтура, П.Н. Питкевич // Russian Technological Journal. — 2022. — Т. 10, № 1. — С. 28–34. — DOI: 10.32362/2500-316X-2022-10-1-28-34

22. Ли Д. Обзор российского рынка резервного копирования и восстановления данных – 2025 / Д. Ли // Anti-Malware.ru. — URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-BackUp-systems-2025 (дата обращения: 15.01.2026).

23. Млечко В. Доля российских решений на рынке средств резервного копирования / В. Млечко // CNews. — URL: https://www.cnews.ru/reviews/rynok_reshenij_rezervnogo_kopirovaniya_1/articles/dolya_rossijskih_reshenij_na_rynke (дата обращения: 03.02.2026).

24. Натров В.В. Оценка общего объема архива при организации системы резервного копирования / В.В. Натров // Защита информации. Инсайд. — 2007. — № 1(13). — С. 70–72.

25. Екубджонов Д.И. Исследование производительности технологий объектно-реляционного отображения при взаимодействии с Microsoft SQL Server / Д.И. Екубджонов, Р.Ф. Гибадуллин // Международный научно-исследовательский журнал. — 2024. — № 10(148). — DOI: 10.60797/IRJ.2024.148.145

Список литературы на английском языке / References in English

1. Razvitie informacionnyh ugroz v pervom kvartale 2025 goda. Statistika po PK [Development of information threats in the first quarter of 2025. Statistics on PCs] // // AO «Laboratorija Kasperskogo» [Kaspersky Lab]. — URL: https://securelist.ru/malware-report-q1-2025-pc-iot-statistics/112821/ (accessed: 13.11.2025). [in Russian]

2. V Kaspersky ICS CERT rasskazali o dinamike kiberugroz dlja rossijskoj promyshlennosti vo vtorom kvartale 2025 goda [Kaspersky ICS CERT spoke about the dynamics of cyber threats for Russian industry in the second quarter of 2025] // AO «Laboratorija Kasperskogo» [Kaspersky Lab]. — URL: https://www.kaspersky.ru/about/press-releases/v-kaspersky-ics-cert-rasskazali-o-dinamike-kiberugroz-dlya-rossijskoj-promyshlennosti-vo-vtorom-kvartale-2025-goda (accessed: 13.11.2025). [in Russian]

3. Incident Response analiticheskij otchjot za 2024 god [Incident Response analytical report for 2024] // AO «Laboratorija Kasperskogo» [Kaspersky Lab]. — URL:

https://content.kaspersky-labs.com/fm/site-editor/18/18b11446b26bf9d75192859778e9a9de/source/report-ir2024.pdf (accessed: 13.11.2025). [in Russian]

4. Dinamika vneshnih i vnutrennih ugroz ASU. Vtoroj kvartal 2025 goda [Dynamics of external and internal threats to industrial control systems. Second quarter of 2025] // Kaspersky ICS CERT. — URL: https://ics-cert.kaspersky.ru/publications/reports/2025/09/10/dynamics-of-external-and-internal-threats-to-industrial-control-systems-q2-2025/ (accessed: 13.11.2025). [in Russian]

5. Bopp V.A. Osobennosti vybora sistem rezervnogo kopirovanija [Features of choosing backup systems] / V.A. Bopp // Izvestija TulGU. Tehnicheskie nauki [Proceedings of Tula State University. Technical Sciences]. — 2019. — № 10. — P. 297–300. [in Russian]

6. Cherkesova L.V. Mehanizm vosstanovlenija dannyh v rezul'tate ih povrezhdenija, zarazhenija i/ili nesankcionirovannogo izmenenija [Data recovery mechanism as a result of their damage, infection and/or unauthorized modification] / L.V. Cherkesova, V.A. Savel'ev, E.A. Revjakina [et al.] // Vestnik DGTU. Tehnicheskie nauki [Bulletin of DSTU. Technical Sciences]. — 2025. — № 1. — P. 134–146. [in Russian]

7. Elkhail A.A. Seamlessly safeguarding data against ransomware attacks / A.A. Elkhail, N. Lachtar, D. Ibdah [et al.] // IEEE Transactions on Dependable and Secure Computing. — 2023. — Vol. 20, № 1. — P. 1–16. — DOI: 10.1109/TDSC.2022.3214781.

8. Guardiola Múzquiz G. The Reverse File System: Towards open cost-effective secure WORM storage devices for logging / G. Guardiola Múzquiz, J. González-Gómez, E. Soriano-Salvador. — 2025. — DOI: 10.48550/arXiv.2509.17969.

9. Budarnyj G.S. Raznovidnosti narushenij bezopasnosti i tipovye ataki na operacionnuju sistemu [Types of security breaches and typical attacks on the operating system] / G.S. Budarnyj // APINO 2022. — 2022. — P. 406–411. [in Russian]

10. Abramenko G.T. Analiz osobennostej sub"ektov kriticheskoj informacionnoj infrastruktury RF [Analysis of the features of subjects of critical information infrastructure of the Russian Federation] / G.T. Abramenko, N.N. Lansere, I.I. Fadeev // APINO 2022. — 2022. — P. 49–54. [in Russian]

11. Allagulyyev B. Ransomware attacks: evolution, defense strategies, and future mitigation techniques / B. Allagulyyev // Innovacionnaja nauka [Innovative Science]. — 2025. — № 5-1-1.

12. Rossijskaja Federacija. Zakony. Ob informacii, informacionnyh tehnologijah i o zashhite informacii [Russian Federation. Laws. On information, information technologies and information protection] : federal law No. 149-FZ of July 27, 2006 (last edition) // Sobranie zakonodatel'stva Rossijskoj Federacii [Collection of Legislation of the Russian Federation]. — 2006. — № 31 (pt. I). — Art. 3448. [in Russian]

13. Rossijskaja Federacija. Zakony. O personal'nyh dannyh [Russian Federation. Laws. On personal data] : federal law No. 152-FZ of July 27, 2006 (last edition) // Sobranie zakonodatel'stva Rossijskoj Federacii [Collection of Legislation of the Russian Federation]. — 2006. — № 31 (pt. I). — Art. 3451. [in Russian]

14. Federal'naja sluzhba po tehnicheskomu i jeksportnomu kontrolju. Ob utverzhdenii Trebovanij o zashhite informacii, ne sostavljajushhej gosudarstvennuju tajnu, soderzhashhejsja v gosudarstvennyh informacionnyh sistemah [Federal Service for Technical and Export Control. On approval of Requirements for the protection of information not constituting a state secret contained in state information systems] : order of FSTEC of Russia No. 17 of February 11, 2013 (as amended on August 28, 2024) // Registered with the Ministry of Justice of Russia on May 31, 2013, № 28608. — 23 p. [in Russian]

15. Federal'naja sluzhba po tehnicheskomu i jeksportnomu kontrolju. Ob utverzhdenii Sostava i soderzhanija organizacionnyh i tehnicheskih mer po obespecheniju bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh [Federal Service for Technical and Export Control. On approval of the Composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems] : order of FSTEC of Russia No. 21 of February 18, 2013 (as amended on May 14, 2020) // Registered with the Ministry of Justice of Russia on May 14, 2013, № 28375. — 17 p. [in Russian]

16. Federal'naja sluzhba po tehnicheskomu i jeksportnomu kontrolju. Ob utverzhdenii Trebovanij o zashhite informacii, soderzhashhejsja v gosudarstvennyh informacionnyh sistemah, inyh informacionnyh sistemah gosudarstvennyh organov, gosudarstvennyh unitarnyh predprijatij, gosudarstvennyh uchrezhdenij [Federal Service for Technical and Export Control. On approval of Requirements for the protection of information contained in state information systems, other information systems of state bodies, state unitary enterprises, state institutions] : order of FSTEC of Russia No. 117 of April 11, 2025 // Registered with the Ministry of Justice of Russia on June 16, 2025, № 82619. — 35 p. [in Russian]

17. Federal'naja sluzhba po tehnicheskomu i jeksportnomu kontrolju. O vnesenii izmenenij v Trebovanija o zashhite informacii, ne sostavljajushhej gosudarstvennuju tajnu, soderzhashhejsja v gosudarstvennyh informacionnyh sistemah, utverzhdennye prikazom Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju ot 11 fevralja 2013 g. № 17 [Federal Service for Technical and Export Control. On amendments to the Requirements for the protection of information not constituting a state secret contained in state information systems, approved by order of the Federal Service for Technical and Export Control No. 17 of February 11, 2013] : order of FSTEC of Russia No. 27 of February 15, 2017 // Registered with the Ministry of Justice of Russia on March 14, 2017, № 45933. — 15 p. [in Russian]

18. Federal'naja sluzhba po tehnicheskomu i jeksportnomu kontrolju. O vnesenii izmenenij v Trebovanija o zashhite informacii, ne sostavljajushhej gosudarstvennuju tajnu, soderzhashhejsja v gosudarstvennyh informacionnyh sistemah, utverzhdennye prikazom Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju ot 11 fevralja 2013 g. № 17 [Federal Service for Technical and Export Control. On amendments to the Requirements for the protection of information not constituting a state secret contained in state information systems, approved by order of the Federal Service for Technical and Export Control No. 17 of February 11, 2013] : order of FSTEC of Russia No. 106 of May 28, 2019 (as amended on April 27, 2020) // Registered with the Ministry of Justice of Russia on September 13, 2019, № 55924. — 30 p. [in Russian]

19. Federal'naja sluzhba po tehnicheskomu i jeksportnomu kontrolju. O vnesenii izmenenij v Trebovanija o zashhite informacii, ne sostavljajushhej gosudarstvennuju tajnu, soderzhashhejsja v gosudarstvennyh informacionnyh sistemah,

utverzhdennye prikazom Federal'noj sluzhby po tehnicheskomu i jeksportnomu kontrolju ot 11 fevralja 2013 g. № 17 [Federal Service for Technical and Export Control. On amendments to the Requirements for the protection of information not constituting a state secret contained in state information systems, approved by order of the Federal Service for Technical and Export Control No. 17 of February 11, 2013] : order of FSTEC of Russia No. 61 of April 27, 2020 // Registered with the Ministry of Justice of Russia on May 12, 2020, № 58322. — 2 p. [in Russian]

20. Pitkevich P.I. Metody rezervnogo kopirovanija dannyh dlja kriticheski vazhnyh IT-sistem predprijatija [Data backup methods for critical IT systems of an enterprise] / P.I. Pitkevich // Universum: tehnicheskie nauki [Universum: Technical Sciences]. — 2021. — № 10-1 (91). [in Russian]

21. Shajtura S.V. Metody rezervirovanija dannyh dlja kriticheski vazhnyh informacionnyh sistem predprijatija [Data redundancy methods for critical information systems of an enterprise] / S.V. Shajtura, P.N. Pitkevich // Russian Technological Journal. — 2022. — Vol. 10, № 1. — P. 28–34. — DOI: 10.32362/2500-316X-2022-10-1-28-34 [in Russian]

22. Li D. Obzor rossijskogo rynka rezervnogo kopirovanija i vosstanovlenija dannyh – 2025 [Review of the Russian data backup and recovery market – 2025] / D. Li // Anti-Malware.ru. — URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-BackUp-systems-2025 (accessed: 15.01.2026). [in Russian]

23. Mlechko V. Dolja rossijskih reshenij na rynke sredstv rezervnogo kopirovanija [Share of Russian solutions in the backup market] / V. Mlechko // CNews. — URL: https://www.cnews.ru/reviews/rynok_reshenij_rezervnogo_kopirovaniya_1/articles/dolya_rossijskih_reshenij_na_rynke (accessed: 03.02.2026). [in Russian]

24. Natrov V.V. Ocenka obshhego ob'ema arhiva pri organizacii sistemy rezervnogo kopirovanija [Estimation of the total archive volume when organizing a backup system] / V.V. Natrov // Zashhita informacii. Insajd [Information Security. Insight]. — 2007. — № 1(13). — P. 70–72. [in Russian]

25. Ekubdzhonov D.I. Issledovanie proizvoditel'nosti tehnologij ob'ektno-reljacionnogo otobrazhenija pri vzaimodejstvii s Microsoft SQL Server [Performance study of object-relational mapping technologies when interacting with Microsoft SQL Server] / D.I. Ekubdzhonov, R.F. Gibadullin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Research Journal]. — 2024. — № 10(148). — DOI: 10.60797/IRJ.2024.148.145 [in Russian]