

ВЛАСОВ Николай Евгеньевич,
магистрант,
Национальный исследовательский университет «МИЭТ»,
e-mail: kolawlas@yandex.ru

ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ КАК ОБЪЕКТ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Статья представляет собой комплексный аналитический обзор, посвящённый вопросам организации и проведения аудита информационной безопасности (ИБ) центров обработки данных в Российской Федерации. В условиях стремительного роста российского рынка ЦОД и увеличения числа кибератак данная тема приобретает особую актуальность.

Автор последовательно рассматривает ключевые аспекты темы. Статья открывается анализом динамики рынка ЦОД в России, подчёркивая его объём и возрастающую важность как элемента инфраструктуры. Далее приводится классификация ЦОД по различным параметрам: целям использования, назначению, размеру и уровням отказоустойчивости. Значительное внимание уделено детальному анализу актуальных угроз ИБ, включая DDoS-атаки, вредоносное ПО, внутренние угрозы, ошибки конфигурации и физические риски, с приведением статистических данных за 2023-2024 годы.

Ядром работы является систематизация нормативно-правовых требований, предъявляемых к аудиту. Автор детально разбирает роль основных регуляторов: ФСТЭК России, ФСБ России и Роскомнадзора, а также релевантные федеральные законы (№152-ФЗ и №149-ФЗ) и национальные стандарты (ГОСТ Р ИСО/МЭК 27001). В статье четко регламентируется рекомендуемая периодичность проведения аудитов для различных типов организаций и систем (персональные данные, КИИ, государственные системы) и определяется перечень ключевых объектов проверки: физическая, техническая и организационная безопасность.

Статья имеет практическую ценность и предназначена для широкого круга специалистов: руководителей, сотрудников служб ИБ, аудиторов, операторов ЦОД, а также студентов и исследователей в области информационной безопасности. Материал служит структурированным руководством, позволяющим понять полный цикл требований к аудиту ИБ ЦОД в России и обеспечить соответствие деятельности законодательству.

Ключевые слова: Аудит информационной безопасности, центр обработки данных (ЦОД), ФСТЭК России, Федеральный закон № 152-ФЗ, персональные данные, критическая информационная инфраструктура (КИИ), ГОСТ Р ИСО/МЭК 27001, DDoS-атаки, нормативно-правовое регулирование, периодичность проверок, средства защиты информации (СЗИ).

VLASOV Nikolay Evgenievich,
Master's student,
National Research University «MIET»

DATA CENTERS AS AN OBJECT OF INFORMATION SECURITY AUDIT

Annotation. The article presents a comprehensive analytical review dedicated to the organization and conduct of information security (IS) audits for data centers in the Russian Federation. In the context of the rapid growth of the Russian data center market and the increasing number of cyberattacks, this topic is gaining particular relevance.

The author sequentially examines key aspects of the subject. The article begins with an analysis of the dynamics of the data center market in Russia, highlighting its volume and growing importance as an infrastructure element. This is followed by a classification of data centers according to various parameters: purpose of use, function, size, and levels of fault tolerance. Significant attention is paid to a detailed analysis of current IS threats, including DDoS attacks, malware, internal threats, configuration errors, and physical risks, supported by statistical data for 2023-2024.

The core of the work is the systematization of regulatory requirements for such audits. The author provides a detailed breakdown of the role of key regulators: the Federal Service for Technical and Export Control (FSTEC) of Russia, the Federal Security Service (FSB) of Russia, and Roskomnadzor, as well as relevant federal laws (No. 152-FZ and No. 149-FZ) and national standards (GOST R ISO/IEC 27001). The

article clearly outlines the recommended frequency of audits for different types of organizations and systems (personal data, critical information infrastructure, state systems) and defines a list of key audit objects: physical, technical, and organizational security.

The article has practical value and is intended for a wide range of specialists: managers, information security personnel, auditors, data center operators, as well as students and researchers in the field of information security. The material serves as a structured guide to understanding the full cycle of requirements for IS audits of data centers in Russia and ensuring compliance with legislation.

Key words: Information security audit, data processing center (DPC), FSTEC of Russia, Federal Law No. 152-FZ, personal data, critical information infrastructure (CII), GOST R ISO/IEC 27001, DDoS attacks, regulatory framework, inspection frequency, information protection tools.

Введение

Центры обработки данных (ЦОД) являются критически важным элементом цифровой инфраструктуры, обеспечивающим хранение и обработку информации. В связи с этим обеспечение информационной безопасности (ИБ) ЦОД становится одной из приоритетных задач для организаций и государства. В России требования к аудиту ИБ ЦОД строго регламентированы законодательством и нормативными документами таких регуляторов, как ФСТЭК России, ФСБ России и Роскомнадзор [1]. Настоящая статья ставит целью не только описание и систематизацию этих требований, но и анализ их практической реализации, выявление возможных проблемных зон и противоречий в регулировании.

Динамика российского рынка ЦОД

Последние годы стали прорывными для российского рынка ЦОД. В 2023-2024 гг. отмечен рекордный ввод новых стойко-мест – более 12 тыс. единиц ежегодно [2]. Общий парк стойко-мест на конец 2024 года оценивается примерно в 82,4 тыс. единиц. Объем рынка за пять лет (2020-2024 гг.) вырос почти втрое – с 53,1 млрд до расчетных 156,5 млрд рублей, со среднегодовым темпом роста около 30% [2]. Параллельно с ростом рынка наблюдается беспрецедентный рост числа и сложности кибератак на объекты информационной инфраструктуры, включая ЦОД. В 2023 году было зафиксировано около 200 тысяч наиболее опасных компьютерных атак, при этом особое внимание злоумышленников было сосредоточено на объектах критической информационной инфраструктуры (КИИ) [3]. Такая динамика однозначно подтверждает высокую актуальность темы защиты информации в ЦОД и необходимость эффективного аудиторского контроля.

Классификация ЦОД

ЦОД можно классифицировать по различным параметрам: цели использования (хостинговые, корпоративные, смешанные), назначению (основные, резервные), размеру (микро, малые, средние, крупные) и уровню отказоустойчивости (Tier I-IV по классификации Uptime Institute) [4; 5; 6]. Эта классификация важна для аудита, так как определяет глубину и фокус проверки. Например, требования к хостинговому ЦОД, обрабатывающему персональные данные множества клиентов, будут строже, чем к внутреннему корпоративно-

му ЦОД малого предприятия. Аудит ЦОД уровня Tier IV должен уделять максимальное внимание резервированию всех систем, в то время как для Tier I этот аспект может быть менее критичным.

Актуальные угрозы ИБ ЦОД

Современные ЦОД сталкиваются с широким спектром угроз: Кибератаки: DDoS-атаки с пиковой мощностью до сотен Гбит/с [7], целевое вредоносное ПО (включая ransomware), эксплуатация уязвимостей в программном обеспечении. Внутренние угрозы: Умышленные или случайные действия инсайдеров. Ошибки конфигурации: Неверные настройки облачных хранилищ, серверов и сетевого оборудования, ведущие к утечкам данных. Физические угрозы: Отказы систем электропитания и охлаждения, несанкционированный физический доступ. Аудит ИБ должен быть сфокусирован на оценке эффективности мер противодействия именно этому спектру угроз.

Законодательные требования, требования регуляторов и национальные стандарты

ФСТЭК России: Ключевой регулятор. Устанавливает требования через приказы № 21 (защита ПДн), № 17 (госинформосистемы), № 235 и № 239 (объекты КИИ) [8; 9; 10; 11]. ФСБ России: Регулирует использование криптографических средств защиты информации (Приказ № 378) [12]. Роскомнадзор: Контролирует соблюдение Федерального закона № 152-ФЗ «О персональных данных» [13]. Законы: № 152-ФЗ (ПДн) и № 149-ФЗ (об информации) [13; 14]. Стандарты: ГОСТ Р ИСО/МЭК 27001 (системы менеджмента ИБ) и ГОСТ Р 57580 (для финансового сектора) [15; 16].

Несмотря на детальную проработку, существующая нормативная база имеет ряд особенностей и сложностей для практической реализации:

1. Множественность и потенциальная противоречивость требований. Организация, чей ЦОД одновременно обрабатывает персональные данные и является объектом КИИ, должна одновременно выполнять требования приказов ФСТЭК № 21 и № 235/239, которые могут иметь различия в подходах к классификации угроз, номенклатуре СЗИ или периодичности контроля. Это создает сложности при планировании и проведении комплексного аудита.

2. Многие требования носят формально-предписывающий характер (установи то, примени это), что может приводить к «галочному» подходу к аудиту, когда проверяется лишь наличие доку-

ментов и средств защиты, а не их реальная эффективность в конкретном технологическом контексте ЦОД. Международный стандарт ISO/IEC 27001, положенный в основу ГОСТ Р ИСО/МЭК 27001, в большей степени ориентирован на оценку и управление рисками, что создает методологический разрыв при попытке его совмещения с предписаниями отраслевых регуляторов.

3. Практические сложности при аудите распределенных и облачных моделей ЦОД. Традиционные нормативные акты зачастую ориентированы на классическую модель физически обособленного ЦОД. С распространением гибридных и облачных инфраструктур, где ресурсы распределены между несколькими площадками или провайдерами, возникает неопределенность в разграничении ответственности и применимости требований. Аудит в таких условиях требует оценки безопасности не только собственной инфраструктуры, но и цепочек поставщиков услуг, что нормативно регламентировано недостаточно четко.

4. Текущие требования и, как следствие, типовые программы аудита сосредоточены преимущественно на контроле состояния защищенности (есть/нет). При этом слабо развиты методики оценки зрелости процессов управления ИБ (например, по моделям типа CMMI), что позволило бы давать более содержательные рекомендации по их развитию, а не только по устранению конкретных нарушений.

Требования к периодичности аудита

Периодичность аудита законодательно дифференцирована: для операторов персональных данных и государственных информационных систем – не реже раза в год; для объектов КИИ – не реже раза в 3 года [13; 17]. Данный подход в целом логичен, однако фиксированные сроки могут не всегда соответствовать реальной динамике изменения рисков. Для быстроразвивающегося ЦОД, активно внедряющего новые услуги или технологии, годовой интервал может быть избыточным, в то время как для стабильной инфраструктуры с высоким уровнем угроз – недостаточным. Более гибкий, риск-ориентированный подход к определению периодичности (с учетом факторов изменений, результатов предыдущих проверок, текущей обстановки) повысил бы эффективность контроля. Ключевые объекты ауди-

та (физическая, техническая и организационная безопасность) охватывают основные аспекты. Однако на практике часто наблюдается дисбаланс: техническому аудиту (сканирование уязвимостей, анализ журналов) уделяется больше внимания, чем глубокой проверке организационных мер (эффективность политик, реальная культура безопасности среди персонала, процедуры реагирования на инциденты). Устранение этого дисбаланса – важная задача для повышения качества аудита.

Заключение

Аудит информационной безопасности ЦОД в России представляет собой сложный, жестко регламентированный процесс, необходимый для обеспечения защиты информации и соблюдения законодательства. Проведенный анализ позволяет сделать следующие выводы и предложения:

1. Существующая нормативная база является всеобъемлющей, но в ряде аспектов излишне формализованной и фрагментированной, что создает практические сложности для организаций со смешанным типом обрабатываемой информации.

2. Внедрение более последовательного риск-ориентированного подхода при согласовании требований разных регуляторов и определении периодичности аудита позволило бы повысить его практическую ценность и адаптивность к меняющимся условиям.

3. Требуется развитие методик аудита, учитывающих современные архитектуры (облачные, гибридные) и направленных на оценку не только состояния, но и зрелости процессов управления ИБ. 4. Для повышения объективности и глубины аудита целесообразно более активное сочетание процедур обязательного контроля с лучшими практиками, заложенными в стандартах семейства ISO/IEC 27000. Таким образом, дальнейшее совершенствование системы аудита ИБ ЦОД должно идти по пути гармонизации нормативных требований, внедрения гибких риск-ориентированных методик и развития компетенций аудиторов для работы со сложными распределенными инфраструктурами. Это будет способствовать не только формальному соответствию, но и реальному повышению устойчивости критически важных объектов информационной инфраструктуры России к современным угрозам.

Список литературы:

- [1] Обзор регуляторных требований к информационной безопасности в РФ (2023) // Информационная безопасность. – 2023. – № 4. – С. 12–18.
- [2] Исследование российского рынка ЦОД 2023-2024 / iKS-Consulting, CNews Analytics. – 2024. – URL: <https://iks-consulting.ru/> (дата обращения: 15.10.2024).
- [3] Обзор киберугроз для объектов критической информационной инфраструктуры Российской Федерации за 2023 год / Совет Безопасности Российской Федерации. – 2024. – URL: <https://www.scrf.gov.ru/> (дата обращения: 15.10.2024).
- [4] Петров А. В. Архитектура и классификация современных центров обработки данных. – М.: ИД

«Синергия», 2022. – 245 с.

[5] Смирнов С. И. Основные и резервные ЦОД: принципы построения отказоустойчивых систем // Труды научно-практической конференции «Инфофорум-2023». – М., 2023. – С. 45–52.

[6] Uptime Institute. Data Center Site Infrastructure Tier Standard: Topology. – 2021. – URL: <https://uptimeinstitute.com/tiers> (дата обращения: 15.10.2024).

[7] Анализ DDoS-атак в первом квартале 2024 года / Selectel: [технический отчет]. – 2024. – URL: <https://selectel.ru/blog/> (дата обращения: 15.10.2024).

[8] Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 11.11.2022) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

[9] Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 23.12.2020) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

[10] Приказ ФСТЭК России от 25.12.2017 № 235 (ред. от 26.06.2020) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

[11] Приказ ФСТЭК России от 22.12.2020 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

[12] Приказ ФСБ России от 10.07.2014 № 378 (ред. от 15.03.2021) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации».

[13] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

[14] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – 2006. – № 31 (1 ч.).

[15] ГОСТ Р ИСО/МЭК 27001-2021. Информационная безопасность, кибербезопасность и защита приватности. Системы менеджмента информационной безопасности. Требования. – Введ. 2022-07-01. – М.: Стандартинформ, 2021. – 32 с.

[16] ГОСТ Р 57580-2017. Защита информации. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – Введ. 2018-07-01. – М.: Стандартинформ, 2017. – 45 с.

[17] Федеральный закон от 30.12.2021 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» // Собрание законодательства РФ. – 2022. – № 1 (часть I).

References:

[1] Review of regulatory requirements for information security in the Russian Federation (2023) // Information Security. – 2023. – No. 4. – pp. 12–18.

[2] Research of the Russian data center market 2023–2024 / iKS-Consulting, CNews Analytics. – 2024. – URL: <https://iks-consulting.ru/> (date of access: 15 October 2024).

[3] Review of cyber threats to critical information infrastructure facilities of the Russian Federation for 2023 / Security Council of the Russian Federation. – 2024. – URL: <https://www.scrf.gov.ru/> (date of access: 15 October 2024).

[4] Petrov A. V. Architecture and classification of modern data processing centers. – Moscow: ID «Synergy», 2022. – 245 p.

[5] Smirnov, S. I. “Primary and Backup Data Centers: Principles of Building Fault-Tolerant Systems” // Proceedings of the Scientific and Practical Conference “Infoforum-2023”. Moscow, 2023, pp. 45–52.

[6] Uptime Institute. Data Center Site Infrastructure Tier Standard: Topology. 2021: <https://uptimeinstitute.com/tiers> (Accessed: October 15, 2024).

[7] Analysis of DDoS Attacks in the First Quarter of 2024 / Selectel: [technical report]. 2024: <https://selectel.ru/blog/> (Accessed: October 15, 2024).

[8] Order of the FSTEC of Russia dated February 18, 2013 No. 21 (as amended on November 11, 2022) «On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data When Processing It in Personal Data Information Systems.»

[9] Order of the FSTEC of Russia dated February 11, 2013 No. 17 (as amended on December 23, 2020) «On Approval of the Requirements for the Protection of Information That Does Not Constitute a State Secret, Contained in State Information Systems.»

[10] Order of the FSTEC of Russia dated December 25, 2017 No. 235 (as amended on June 26, 2020) «On Approval of the Requirements for the Creation of Security Systems for Significant Objects of the Critical

Information Infrastructure of the Russian Federation and Ensuring Their Functioning.» [11] Order of the FSTEC of Russia dated December 22, 2020 No. 239 «On Approval of the Requirements for Ensuring the Security of Significant Objects of the Critical Information Infrastructure of the Russian Federation.»

[12] Order of the FSB of Russia dated July 10, 2014 No. 378 (as amended on March 15, 2021) «On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data When Processing Them in Personal Data Information Systems Using Cryptographic Information Protection Tools.»

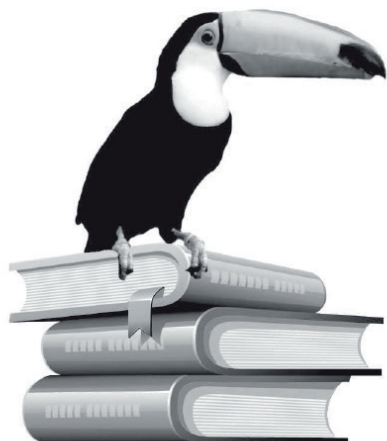
[13] Federal Law of July 27, 2006 No. 152-FZ (as amended on July 14, 2022) «On Personal Data» // Collected Legislation of the Russian Federation. - 2006. - No. 31 (part 1). - Art. 3451.

[14] Federal Law of July 27, 2006 No. 149-FZ (as amended on July 2, 2021) «On Information, Information Technologies, and Information Protection» // Collected Legislation of the Russian Federation. - 2006. - No. 31 (part 1).

[15] GOST R ISO/IEC 27001-2021. Information security, cybersecurity, and privacy protection. Information security management systems. Requirements. - Introduced on July 1, 2022. - Moscow: Standartinform, 2021. - 32 p.

[16] GOST R 57580-2017. Information protection. Ensuring information security of organizations of the banking system of the Russian Federation. General provisions. - Introduced on July 1, 2018. - M.: Standartinform, 2017. - 45 p.

[17] Federal Law of 30.12.2021 No. 266-FZ «On Amendments to the Federal Law «On Personal Data» // Collected Legislation of the Russian Federation. - 2022. - No. 1 (Part I).



ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.