Дата поступления рукописи в редакцию: 15.05.2026 г.
Дата принятия рукописи в печать: 30.06.2026 г.
DOI: 10.24412/3034-4271-2026-3-22-27

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

АДАПТАЦИЯ МЕР КОНТРОЛЯ ПРИЛОЖЕНИЯ А ISO/IEC 27001:2022 К СТРУКТУРЕ ЦОД

Аннотация. *Статья посвящена методическим аспектам адаптации мер контроля Приложения А стандарта ISO/IEC 27001:2022 к специфике аудита центров обработки данных (ЦОД). Обосновывается необходимость глубинной контекстуализации общих требований информационной безопасности для преодоления поверхностной проверки и фокусировки на уникальных рисках инженерной, физической и операционной среды дата-центра.*

Представлена детальная адаптация ключевых мер контроля для наиболее уязвимых доменов безопасности ЦОД. В рамках физической и экологической безопасности акцент сделан на проверке отказоустойчивости систем жизнеобеспечения, включая анализ нагрузочных тестов дизель-генераторных установок и систем прецизионного кондиционирования. В области управления доступом рассмотрены требования к ужесточению контроля над административными сессиями через бастион-хосты и двухфакторную аутентификацию, а также к архитектурной сетевой сегментации и изоляции клиентских сред. Операционная безопасность раскрывается через необходимость корреляции цифровых и физических событий в SIEM-системах. Требования к непрерывности бизнеса проверяются через призму практических учений с анализом фактического времени восстановления и объема потерянных данных.

Практическая значимость работы заключается в формировании технико-организационной карты проверки, позволяющей оценивать не формальное соответствие, а реальную способность инфраструктуры дата-центра противостоять уникальному сочетанию угроз. Материал предназначен для внутренних и внешних аудиторов, специалистов служб информационной безопасности, операторов ЦОД, а также технических экспертов, участвующих в подготовке инфраструктуры к сертификации.

Ключевые слова: *ISO/IEC 27001:2022, аудит информационной безопасности, центр обработки данных (ЦОД), адаптация мер контроля, Приложение А, физическая безопасность, управление доступом, непрерывность бизнеса, сетевая сегментация, SIEM.*

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

ADAPTATION OF ANNEX A CONTROL MEASURES OF ISO/IEC 27001:2022 TO THE DATA CENTER STRUCTURE

Annotation. *This article is devoted to the methodological aspects of adapting the control measures of Annex A of ISO/IEC 27001:2022 to the specifics of data center (DC) auditing. It substantiates the need for deep contextualization of general information security requirements in order to overcome superficial verification and focus on the unique risks of the engineering, physical, and operational environment of a data center.*

A detailed adaptation of key control measures for the most vulnerable data center security domains is presented. Within the domain of physical and environmental security, the emphasis is placed on verifying the fault tolerance of life support systems, including the analysis of load tests for diesel generator sets and precision cooling systems. In the area of access management, the requirements for tightening control over administrative sessions through bastion hosts and two-factor authentication, as well as for architectural network segmentation and isolation of client environments, are examined. Operational security is addressed through the need for correlation of digital and physical events within SIEM systems. Business continuity requirements are verified through practical drills, with analysis of actual recovery time and data loss volume.

The practical significance of this work lies in the formation of a technical and organizational verification framework that allows for the assessment not of formal compliance, but of the actual ability of a data center's infrastructure to withstand a unique combination of threats. The material is intended for internal and external

auditors, information security professionals, data center operators, and technical experts involved in preparing infrastructure for certification.

Key words: *ISO/IEC 27001:2022, information security audit, data center (DC), control adaptation, Annex A, physical security, access management, business continuity, network segmentation, SIEM.*

Введение

Разработка методики аудита, ориентированной на специфику центра обработки данных, требует не простого перечисления требований стандарта ISO/IEC 27001:2022 [1], а их глубокой трансформации и контекстуализации. Адаптация мер контроля Приложения А является критически важным этапом, поскольку именно она позволяет перевести универсальные принципы информационной безопасности в конкретный язык проверок, релевантных для технологической, физической и операционной среды ЦОД. Без такой адаптации аудитор рискует проводить поверхностную проверку, игнорируя ключевые риски, связанные с гипервизорами, системами жизнеобеспечения и физическим периметром. Данный процесс предполагает интеграцию требований базового стандарта с положениями специализированных нормативных документов, таких как ISO/IEC 27017 для облачной безопасности [3] и отраслевых стандартов типа TIA-942 для инженерной инфраструктуры [4], а также с современными научными подходами к оценке рисков ЦОД [8], аудиту непрерывности бизнеса [9] и корреляции событий безопасности [10]. Ниже представлена детальная адаптация ключевых мер контроля для наиболее уязвимых доменов безопасности дата-центра, а также результаты её апробации в ходе практических аудитов 2024 – 2025 гг.

Адаптация мер контроля физической и экологической безопасности (A.7)

В рамках домена «Физическая и экологическая безопасность» (A.7) общие требования о защите от внешних угроз приобретают для ЦОД характер инженерной дисциплины, где на первый план выходит обеспечение бесперебойного функционирования систем жизнеобеспечения. Как отмечают Белов Е.Б. с соавторами [8], специфика оценки рисков ЦОД требует учета не только киберугроз, но и отказов инженерной инфраструктуры, что часто игнорируется в традиционных подходах.

Контроль A.7.4 «Защита от внешних и экологических угроз» [1] трансформируется из задачи поддержания базовых параметров среды в комплексный процесс управления отказоустойчивостью. Для аудита это означает необходимость проверки не только показаний датчиков температуры и влажности, но и всей цепочки обеспечения этих параметров. Аудитор должен запрашивать и анализировать детальные отчеты о плановых нагрузочных тестах систем аварийного электропитания. Критически важно, чтобы такие тесты не сводились к кратковременному запуску дизель-генераторных установок (ДГУ) на холостом ходу, а предполагали реальное переключение нагрузки серверных стоек на резервные источники с фиксацией времени выхода на номинальный режим, стабильности выходных параметров и корректности обратного переключения. Новиков А.П. и Федоров И.С. [11] подчеркивают, что формальное тестирование без нагрузочных испытаний создает иллюзию надежности, тогда как реальные отказы происходят именно при переходе на резервные источники под нагрузкой. Соответствие заявленному в SLA уровню доступности должно подтверждаться схемами резервирования (конфигурации N+1, 2N) и актами выполненных работ по техническому обслуживанию каждого компонента цепи: вводных распределительных устройств, модулей ИБП, самих ДГУ и систем автоматического ввода резерва. Указанные требования согласуются с положениями стандарта TIA-942 [4], регламентирующего категории надежности инженерной инфраструктуры ЦОД.

Аналогичный подход применяется к системам прецизионного кондиционирования. Аудит должен включать проверку не только текущей температуры, но и регламентов обслуживания чиллеров, градирен и внутренних блоков, наличия запаса хладагента, чистоты воздушных фильтров и корректности настройки воздушных потоков в подпольном пространстве и горячих/холодных коридоров.

Отдельным объектом проверки становятся системы раннего обнаружения угроз: датчики протечки воды, установленные под фальшполом и в дренажных системах, аспирационные системы обнаружения задымления, позволяющие выявить возгорание на самой ранней стадии тления изоляции кабелей. Аудит должен верифицировать, что события от этих систем интегрированы в общую систему мониторинга и управления с настроенными процедурами оперативного реагирования.

Контроль A.7.13 «Оборудование» [1] в контексте ЦОД, предоставляющего услуги колокации или IaaS, смещает фокус с инвентарного учета на гарантированное уничтожение данных и защиту активов клиентов. Аудитор обязан проверить наличие и практическое применение формализованного регламента вывода из эксплуатации носителей информации. Ключевым доказательством здесь выступают не сами политики, а конкретные артефакты: акты на уничтожение с указанием моделей, серийных номеров дисков и примененного метода. Приемлемыми методами являются криптографическое стирание для самозакодированных накопителей (с верификацией успешности операции) или физическое разру-

шение с использованием шредера, соответствующего стандартам безопасности. Для дисков, принадлежащих клиентам, должен существовать четкий процесс их возврата или предоставления подтверждающих документов об уничтожении. Кроме того, адаптация данного контроля требует проверки физической безопасности клиентских стоек: наличия индивидуальных замков, ведения журналов вскрытия по запросу клиента и контроля доступа к ним со стороны персонала ЦОД.

Адаптация мер контроля управления доступом (A.9)

В среде ЦОД система «управление доступом» (A.9) разделяется на два мощных, но взаимосвязанных потока: физический и логический, причем последний для облачных услуг усложняется моделью разделенной ответственности, описанной в ISO/IEC 27017 [3].

Контроль A.9.4.2 «Безопасный вход в систему» [1] для административного доступа к платформенным системам требует максимального ужесточения. Аудит должен подтвердить, что любой доступ к системам управления гипервизорами, сетевым контроллерам, системам хранения и другим критичным компонентам осуществляется исключительно через выделенные бастион-хосты. Эти хосты должны быть максимально облегчены, подвергнуты харденингу и выступать в роли единственного контролируемого шлюза. На них в обязательном порядке должна быть внедрена двухфакторная аутентификация, причем использование SMS или голосовых звонков как второго фактора считается недостаточным; предпочтение отдается криптографическим токенам или аппаратным ключам. Каждая сессия администратора на бастион-хосте и на конечных системах управления должна подвергаться полной записи с защитой логов от модификации и обеспечением их целостности для последующего расследования. Абсолютно недопустимым является наличие и использование общих или служебных учетных записей с привилегиями, не привязанных к конкретному сотруднику. Аудит должен включать выборочную проверку журналов аутентификации на предмет использования таких аккаунтов.

Контроль A.9.1.2 «Доступ к сетям и сетевым службам» [1] адаптируется в задачу проверки архитектурной сетевой сегментации. Аудитор должен анализировать не абстрактные политики, а конкретные конфигурации. Это включает проверку схемы сети, демонстрирующей логическое разделение на сегменты: управляющая сеть инфраструктуры, сеть хранения данных, внутренняя сеть сервисов ЦОД и изолированные сегменты клиентов. Для клиентских сегментов в услугах IaaS критически важно подтверждение технической реализации изоляции. Аудитор проверяет настройки Private VLAN на коммутаторах уровня доступа или в распределенных виртуальных портах, конфигурации групп безопасности в платформах виртуализации или облачных платформах, которые предотвращают прямой сетевой трафик между виртуальными машинами разных клиентов. Эта проверка напрямую связана с требованием ISO/IEC 27017 [3], который предписывает провайдеру облачных услуг обеспечивать изоляцию на уровне инфраструктуры. Отдельно проверяется изоляция сети управления аппаратными интерфейсами серверов, которые должны быть полностью вынесены в отдельную, строго контролируемую сеть с доступом только для уполномоченного персонала.

Адаптация мер контроля операционной безопасности (A.12)

Операционная безопасность ЦОД (A.12) характеризуется необходимостью анализа событий не только из цифрового, но и из физического мира, а также управления динамичными облачными средами. Как указывает Михайлов Д.В. [10], эффективная корреляция событий физической и логической безопасности является критическим фактором обнаружения инсайдерских угроз в ЦОД, однако на практике реализуется менее чем в 30% объектов.

Контроль A.12.4.1 «Анализ журналов событий» [1] расширяется до концепции централизованного мониторинга безопасности всей гетерогенной среды. Аудитор должен убедиться, что в систему SIEM поступают и коррелируются события с сетевых устройств, серверов, систем виртуализации, межсетевых экранов, а также, что критически важно, с систем контроля доступа (СКУД), видеонаблюдения и систем управления зданием. Например, корреляционное правило должно детектировать сценарий: «Неудачная попытка доступа по карте к двери серверного зала в нерабочее время — Спустя 5 минут успешная аутентификация в систему vCenter с рабочей станции в этом же зале». Тихонов В.А. [12] отмечает, что большинство инцидентов в ЦОД остаются необнаруженными именно из-за отсутствия корреляции между физическими и цифровыми событиями. Качество работы SOC оценивается не по количеству собранных логов, а по анализу правил корреляции, отчетов об инцидентах, инициированных по событиям из SIEM, и скорости их закрытия. Аудитор может запросить для анализа несколько кейсов, чтобы оценить глубину расследования и результативность предпринятых действий.

Контроль A.12.6.2 «Ограничения на установку программного обеспечения» [1] в модели IaaS претерпевает значительную трансформацию. Ответственность провайдера смещается с запрета установки ПО на серверы (которые являются виртуальными и принадлежат клиенту) на управление жизненным циклом предоставляемых клиенту строительных блоков. Аудит фокусируется на проверке процесса управления базовыми образами виртуальных машин. Должен существовать

каталог таких образов, прошедших процесс харденинга (отключение ненужных служб, настройка брандмауэра, установка базовых агентов мониторинга), и регламент их регулярного обновления и проверки на наличие уязвимостей.

Адаптация мер контроля непрерывности бизнеса (A.17)

Для ЦОД, чья основная ценность заключается в гарантированной доступности, требования к непрерывности бизнеса носят не рекомендательный, а императивный характер.

Контроль A.17.1.1 «Планирование непрерывности информационной безопасности» [1] проверяется исключительно через призму доказательств практической работоспособности. Аудитор должен запрашивать и скрупулезно анализировать отчеты о проведении последних комплексных учений. Критерием качества учения является его приближенность к реальному сценарию: не имитация, а реальное (плановое) отключение одного из центров питания с переводом нагрузки на второй; запуск и проверка работы резервной системы охлаждения; отработка процедуры восстановления из резервных копий не на тестовом, а на выделенном аварийном оборудовании. В отчетах должны быть зафиксированы ключевые метрики: фактическое время восстановления для каждой критичной службы и объем потерянных данных. Особое внимание уделяется безопасности в режиме аварийного функционирования: проверяются процедуры аутентификации администраторов на резервной площадке, порядок восстановления систем шифрования и журналирования, чтобы исключить потерю контроля в процессе восстановления. По итогам учений должны быть оформлены выводы и обновлены планы, что также подлежит проверке.

Для обеспечения практической применимости разработанной методики в таблице 1 представлена технико-организационная карта проверки (чек-лист), содержащая ключевые объекты и методы верификации для каждого из рассмотренных доменов безопасности.

Таблица 1. Чек-лист ключевых объектов

Домен безопасности	Контроль ISO/IEC 27001:2022	Объект проверки	Метод верификации
Физическая и экологическая безопасность (A.7)	A.7.4 Защита от внешних и экологических угроз	Системы аварийного электропитания (ДГУ, ИБП), системы кондиционирования, датчики протечки и задымления	Анализ протоколов нагрузочных тестов с фиксацией времени переключения и параметров нагрузки; проверка схем резервирования (N+1, 2N)
	A.7.13 Оборудование	Процедуры вывода из эксплуатации носителей	Проверка актов уничтожения с указанием серийных номеров; верификация методов криптографического стирания или физического разрушения
Управление доступом (A.9)	A.9.4.2 Безопасный вход в систему	Административный доступ к гипервизорам, сетевым контроллерам, СХД	Проверка наличия бастион-хостов, двухфакторной аутентификации (токены/аппаратные ключи), отсутствия общих учетных записей; анализ журналов сессий
	A.9.1.2 Доступ к сетям и сетевым службам	Сетевая сегментация, изоляция клиентских сред	Анализ конфигураций Private VLAN, групп безопасности; проверка изоляции сети управления серверами
Операционная безопасность (A.12)	A.12.4.1 Анализ журналов событий	SIEM, корреляция цифровых и физических событий	Проверка поступления событий от СКУД, видеонаблюдения; анализ правил корреляции и отчетов об инцидентах
	A.12.6.2 Ограничения на установку ПО	Управление базовыми образами ВМ (IaaS)	Проверка каталога образов, процедур харденинга, регламентов обновления и сканирования уязвимостей
Непрерывность бизнеса (A.17)	A.17.1.1 Планирование непрерывности	Комплексные учения, фактическое время восстановления (RTO), объем потерянных данных (RPO)	Анализ отчетов об учениях с реальным отключением питания, восстановлением на резервном оборудовании; проверка обновления планов по итогам учений

Мной предложена апробация настоящей методики на Кейсе . «Корреляция событий SIEM и СКУД (контроль А.12.4.1 «Анализ журналов событий», ЦОД «Южный», г. Москва, ноябрь 2024 г.)».

Исходные данные: ЦОД, предоставляющий услуги IaaS для 45 клиентов. В ходе аудита была предоставлена документация о внедрении SIEM-системы (сбор логов с 1200 источников, включая сетевые устройства, серверы и гипервизоры). Отчеты об инцидентах за последние 6 месяцев отсутствовали, что было интерпретировано оператором как «отсутствие инцидентов».

Примененная процедура адаптированного аудита: в соответствии с разработанной методикой (таблица 1) аудитор:

1. Запросил схему потоков событий в SIEM.

2. Проверил наличие источников событий от системы контроля доступа (СКУД) и видеонаблюдения.

3. Инициировал тестовый сценарий (с согласия руководства ЦОД) для проверки корреляции физических и цифровых событий.

Тестовый сценарий:

Сотрудник, например, инженер ЦОД, не имеющий допуска в серверный зал в ночное время) пытается пройти по чужой карте доступа в серверную зону в 23:30 (неудачная попытка).

Через 7 минут тот же сотрудник осуществляет вход в панель управления гипервизором (vCenter) с рабочей станции, расположенной в зоне свободного доступа (успешная аутентификация).

Выявленное несоответствие: события от СКУД не интегрированы в SIEM (поступают только в локальную систему мониторинга охраны). В SIEM отсутствуют правила корреляции, связывающие физический и логический доступ. Тестовый инцидент не был зафиксирован как событие безопасности; SOC не получил никаких уведомлений.

Принятые меры: По результатам аудита выдано несоответствие категории «значительное». Разработан план корректирующих действий:

Интеграция СКУД в SIEM (срок — 3 месяца).

1. Разработка не менее 10 корреляционных правил для детектирования аномалий доступа (включая описанный сценарий).

2. Проведение обучения персонала SOC по работе с межсистемной корреляцией.

Данный пример эмпирически подтверждает выводы Михайлова Д.В. [10] и Тихонова В.А. [12] о критическом дефиците корреляции физических и цифровых событий в реальных ЦОД, а также демонстрирует необходимость адаптации контроля А.12.4.1.

Заключение

Таким образом, адаптация мер контроля Приложения А ISO/IEC 27001:2022 [1] к структуре центра обработки данных представляет собой не механический перенос требований, а процесс их глубокой трансформации и насыщения специфическим содержанием, релевантным для технологической, физической и операционной среды ЦОД. Проведенный анализ ключевых доменов безопасности — физической и экологической (А.7), управления доступом (А.9), операционной безопасности (А.12) и непрерывности бизнеса (А.17) — демонстрирует, что универсальные формулировки стандарта приобретают практический смысл только при их интерпретации через призму инженерной инфраструктуры, архитектурных решений и эксплуатационных процессов дата-центра.

Предложенный подход позволяет трансформировать общее руководство по менеджменту информационной безопасности в детальную технико-организационную карту проверки, где каждый контроль получает конкретное проверочное действие: от анализа нагрузочных тестов дизель-генераторных установок и конфигураций сетевой сегментации до корреляции событий SIEM с физическими системами контроля доступа и оценки результатов комплексных учений по восстановлению. Такая контекстуализация дает возможность аудитору оценивать не формальное наличие документированных процедур, а реальную способность сложной инфраструктуры дата-центра противостоять уникальному сочетанию угроз, включая отказы инженерных систем, инсайдерские риски и целевые кибератаки.

Кроме того, интеграция требований ISO/IEC 27001:2022 с положениями специализированных стандартов, таких как ISO/IEC 27017 (облачная безопасность) и отраслевых документов типа TIA-942 (инженерная инфраструктура ЦОД), позволяет сформировать комплексную методологию аудита, учитывающую как управленческие, так и технические аспекты функционирования дата-центра. Сформулированные в работе проверочные действия служат непосредственной основой для проектирования последующих элементов методологии: специализированных чек-листов, сценариев тестирования и процедур анализа свидетельств аудита. Разработанный подход может быть адаптирован для различных моделей обслуживания (колокация, IaaS, PaaS) и типов ЦОД (корпоративные, коммерческие, распределенные), что определяет его практическую ценность для специалистов в области аудита и управления информационной безопасностью.

Список литературы:

[1] Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Geneva : ISO, 2022. — 22 с.

[2] ISO/IEC 27002:2022. Информационная технология. Методы обеспечения безопасности. Правила практики менеджмента информационной безопасности. — Geneva : ISO, 2022. — 78 с.

[3] ISO/IEC 27017:2015. Информационная технология. Методы обеспечения безопасности. Правила практики для защиты информации в об-

лачных сервисах. — Geneva : ISO, 2015. — 32 с.

[4] TIA-942-B. Telecommunications Infrastructure Standard for Data Centers. — Arlington : Telecommunications Industry Association, 2017. — 214 p.

[5] ГОСТ Р ИСО/МЭК 27001—2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Москва : Российский институт стандартизации, 2021. — 32 с.

[6] ГОСТ Р ИСО/МЭК 27017—2021. Информационная технология. Методы и средства обеспечения безопасности. Правила практики менеджмента информационной безопасности для облачных сервисов. — Москва : Российский институт стандартизации, 2021. — 28 с.

[7] ГОСТ Р 56550—2015. Защита информации. Центры обработки данных. Модель обеспечения безопасности. — Москва : Стандартинформ, 2016. — 16 с.

[8] Белов Е.Б., Лось В.П., Мещеряков Р.В. Методология оценки рисков информационной безопасности центров обработки данных // Вопросы кибербезопасности. — 2023. — № 4 (52). — С. 42–53.

[9] Куприянов А.А., Сергеев С.С. Аудит систем непрерывности бизнеса в ЦОД: от формальной проверки к практическим учениям // Информационная безопасность регионов. — 2024. — № 1 (46). — С. 27–35.

[10] Михайлов Д.В. Корреляция событий физической и логической безопасности в центрах обработки данных // Защита информации. Инсайд. — 2024. — № 2 (98). — С. 60–66.

[11] Новиков А.П., Федоров И.С. Анализ методов тестирования отказоустойчивости инженерной инфраструктуры ЦОД // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». — 2025. — № 1 (138). — С. 88–102.

[12] Тихонов В.А. Практика внедрения SIEM-систем в центрах обработки данных: проблемы корреляции и инциденты // Cloud & Data Center. — 2024. — № 3 (41). — С. 34–41.

References:

[1] Information technology. Security techniques. Information security management systems. Requirements. — Geneva : ISO, 2022. — 22 p.

[2] ISO/IEC 27002:2022. Information technology. Security techniques. Code of practice for information security management. — Geneva : ISO, 2022. — 78 p.

[3] ISO/IEC 27017:2015. Information technology. Security techniques. Code of practice for protecting information in cloud services. — Geneva : ISO, 2015. — 32 p.

[4] TIA-942-B. Telecommunications Infrastructure Standard for Data Centers. — Arlington : Telecommunications Industry Association, 2017. — 214 p.

[5] GOST R ISO/IEC 27001—2021. Information technology. Security Methods and Tools. Information Security Management Systems. Requirements. Moscow: Russian Institute of Standardization, 2021. 32 p.

[6] GOST R ISO/IEC 27017—2021. Information Technology. Security Methods and Tools. Information Security Management Practice Rules for Cloud Services. Moscow: Russian Institute of Standardization, 2021. 28 p.

[7] GOST R 56550—2015. Information Protection. Data Processing Centers. Security Model. Moscow: Standartinform, 2016. 16 p.

[8] Belov E.B., Los V.P., Meshcheryakov R.V. Information Security Risk Assessment Methodology for Data Processing Centers // Cybersecurity Issues. 2023, No. 4 (52), pp. 42–53.

[9] Kupriyanov A.A., Sergeev S.S. Audit of business continuity systems in data centers: from formal verification to practical exercises // Information security of regions. - 2024. - No. 1 (46). - P. 27-35.

[10] Mikhailov D.V. Correlation of physical and logical security events in data processing centers // Information protection. Inside. - 2024. - No. 2 (98). - P. 60-66.

[11] Novikov A.P., Fedorov I.S. Analysis of methods for testing the fault tolerance of data center engineering infrastructure // Bulletin of Bauman Moscow State Technical University. Series «Instrument engineering». - 2025. - No. 1 (138). - P. 88-102.

[12] Tikhonov V.A. Practice of implementing SIEM systems in data processing centers: problems of correlation and incidents // Cloud & Data Center. - 2024. - No. 3 (41). - P. 34–41.