DOI 10.37882/2223-2966.2025.06.33

КОМПЛАЕНС, КАК ВАЖНАЯ СОСТАВЛЯЮЩАЯ ПРОЦЕССОВ ИБ

COMPLIANCE AS AN IMPORTANT COMPONENT OF INFORMATION SECURITY PROCESSES

V. Litvinov
A. Pavlov

Summary. The article analyzes the role of compliance in ensuring the information security of organizations against the backdrop of a tightening regulatory environment and growing cyber threats. The main regulations, standards and approaches to information security risk management are considered, such as GDPR, NIST Cybersecurity Framework and Russian standards (GOST R 57580-2017, Federal Law No. 152). The importance of implementing comprehensive measures to comply with legislation is emphasized: audit, monitoring, personnel training, and automation of compliance processes. It also examines the practical challenges organizations face, including a lack of resources and skilled professionals, and the need to adapt to new threats. It analyzes the growth trends in data protection breaches for 2021–2023, confirming the increase in regulatory pressure. It concludes by emphasizing that effective compliance not only helps reduce risks and fines, but also builds trust in the organization in the context of rapid digitalization.

Keywords: compliance, compliance, legal framework, standards, practices, audit, security, regulations, monitoring.

Литвинов Всеволод Вячеславович
РГУ нефти и газа (НИУ) имени И.М. Губкина
lvsevolod10@gmail.com
Павлов Алексей Константинович
Аспирант, Московский финансовый юридический университет (МФЮА)
lexus3@mail.ru

Аннотация. Статья посвящена анализу роли комплаенса в обеспечении информационной безопасности организаций на фоне ужесточения регуляторной среды и роста киберугроз. Рассматриваются основные нормативные акты, стандарты и подходы к управлению рисками информационной безопасности, такие как GDPR, NIST Cybersecurity Framework и российские стандарты (ГОСТ Р 57580–2017, ФЗ № 152). Подчёркивается важность внедрения комплексных мер для соблюдения законодательства: аудита, мониторинга, обучения персонала и автоматизации процессов комплаенса. Также рассматриваются практические сложности, с которыми сталкиваются организации, включая нехватку ресурсов и квалифицированных специалистов, а также необходимость адаптации к новым угрозам. Анализируются тенденции роста нарушений в области защиты данных за 2021–2023 годы, подтверждающие увеличение регуляторного давления. В заключение подчёркивается, что эффективный комплаенс способствует не только снижению рисков и штрафов, но и укреплению доверия к организации в условиях стремительной цифровизации.

Ключевые слова: комплаенс, соответствие требованиям, нормативно-правовая база, стандарты, практики, аудит, безопасность, положения, мониторинг.

Введение

Комплаенс в сетевой безопасности — это соблюдение установленных правил и стандартов, направленных на защиту конфиденциальной информации и обеспечение подотчетности организации перед лицом киберугроз. По мере того, как утечки данных и кибератаки становятся все более распространенными, эффективные механизмы обеспечения соответствия критически важны для защиты персональных и корпоративных данных, тем самым поддерживая доверие заинтересованных сторон и репутацию организации. Соответствие нормативным требованиям подразумевает не только выполнение юридических обязательств, но и проактивный подход к обеспечению кибербезопасности в соответствии с лучшими отраслевыми практиками, например, изложенными в Общем регламенте защиты данных (GDPR) и Федеральный законе «Об информации, информационных технологиях и о защите информации». [1][2]

Важность соблюдения требований сетевой безопасности подчеркивается значительными юридическими и финансовыми последствиями, которые грозят организациям за их несоблюдение. Например, нарушение GDPR может привести к штрафам в размере до 20 миллионов евро или 4 % годового мирового оборота, что подчеркивает необходимость создания надежных программ обеспечения соответствия.[1][3] Более того, такие системы, как NIST Cybersecurity Framework, предлагают структурированные подходы, которые организации могут использовать для эффективного управления и снижения рисков кибербезопасности.[4]

Однако обеспечение соответствия является постоянной проблемой. В условиях меняющегося ландшафта угроз, сложных нормативных требований и нехватки ресурсов, это особенно важно для небольших организаций.[5][6]

Споры вокруг соблюдения норм сетевой безопасности часто разворачиваются вокруг эффективности и практичности различных нормативно-правовых актов. Критики утверждают, что чрезмерно строгие нормы могут подавлять инновации и налагать неоправдан-

ное бремя на предприятия, в то время как сторонники утверждают, что такие меры необходимы для защиты данных потребителей и создания безопасной цифровой среды.[7][8] Кроме того, быстрый темп технологического прогресса вызывает вопросы о том, насколько существующие нормы адекватно учитывают новые риски.

В целом, соблюдение требований сетевой безопасности — это многогранная проблема, требующая от организаций баланса между юридическими обязательствами и практическими мерами безопасности.

Методы

Исследование основывалось на анализе нормативных актов, стандартов и практик в области сетевой безопасности. Рассматривались такие международные стандарты, как GDPR, NIST Cybersecurity Framework, и российские ГОСТ Р 57580–2017, Федеральный закон № 152-ФЗ «О персональных данных».

Ход исследования включал следующий пункты.

1. Сравнительный анализ стандартов и требований сетевой безопасности.
2. Изучение методов внедрения стандартов, включая аудит, мониторинг, и адаптацию к изменениям нормативных требований.
3. Сравнение отечественных и зарубежных инструментов для обеспечения комплаенса.

Применялись практические стратегии, такие как документирование регламентов, обучение сотрудников и использование программных решений для управления соответствием.

Результаты

Нормативно-правовые акты в области сетевой безопасности устанавливают рекомендации и лучшие практики, которым должны следовать организации для обеспечения соответствия различным законодательным требованиям для повышения уровня кибербезопасности. Эти рамки имеют решающее значение для управления сложным ландшафтом нормативных актов, регулирующих защиту данных, конфиденциальность и кибербезопасность в разных юрисдикциях.

Основные положения в Мире. Несколько важных нормативных актов формируют ландшафт соответствия для организаций, особенно в отношении обработки персональных данных и информационной безопасности.

Общий регламент по защите данных (GDPR) — это всеобъемлющий закон, который применяется к любой организации, обрабатывающей персональные данные физических лиц на территории Европейского союза (ЕС), независимо от местонахождения организации[1][3]. Введенный в действие в мае 2018 года, GDPR устанавливает строгие требования к сбору, обработке и хранению данных, стремясь предоставить людям больший контроль над своими персональными данными. Несоблюдение требований может привести к крупным штрафам, достигающим 20 миллионов евро или 4 % от мирового годового оборота, в зависимости от того, какая сумма больше [1][3]. Ключевыми компонентами GDPR являются минимизация данных, прозрачность обработки данных и требование явного согласия на обработку персональных данных[13].

Калифорнийский закон о защите частной жизни потребителей (CCPA) — предоставляет жителям особые права в отношении их личной информации, включая право знать, какие данные о них собираются, и право требовать удаления своих данных [2]. Как и GDPR, CCPA делает акцент на прозрачности и правах потребителей, но при этом адаптирован к уникальному правовому ландшафту Калифорнии.

NIST Cybersecurity Framework (NIST CSF) предоставляет организациям структурированный подход управлению рисками кибербезопасности. В ней описаны пять основных функций: идентификация, защита, обнаружение, реагирование и восстановление[4].

В России существует своя нормативно-правовая база для организаций.

ГОСТ Р 57580–2017 — этот закон является аналогом подхода NIST CSF, Этот стандарт предоставляет аналогичный структурированный подход к управлению рисками информационной безопасности, охватывая такие же функции, как идентификация, защита, обнаружение, реагирование и восстановление.

Федеральный закон № 152-ФЗ «О персональных данных» — этот закон регулирует обработку персональных данных в России и устанавливает требования для операторов данных в отношении их сбора, хранения, обработки и защиты. Он соответствует многим положениям GDPR, например, требованию о получении согласия на обработку данных, установлению целей обработки и защите прав субъектов данных. Важно, что для международных компаний, работающих с данными российских граждан, закон предусматривает необходимость локализации хранения персональных данных на территории России.

Стандарт ГОСТ Р 57580–2017 «Система менеджмента информационной безопасности. Требования» является российским аналогом международных стандартов ISO 27001 и ISO 27002 и предоставляет организацию с требованиями к созданию и поддержанию системы управления информационной безопасностью (СМИБ).

Федеральный закон № 126-ФЗ «О связи» регулирует вопросы безопасности телекоммуникационных сетей и защиты информации, передаваемой через эти сети.

В России существуют также нормативно-правовые акты, касающиеся защиты информации в контексте национальной безопасности (Документы Федеральной службы безопасности (ФСБ)). Например, Приказ ФСБ России № 378 и Федеральный закон «О техническом обеспечении безопасности критической информационной инфраструктуры Российской Федерации» устанавливают требования по защите информации, передаваемой через каналы связи, и управление угрозами в области кибербезопасности в критической инфраструктуре.

Рамки для кибербезопасности в России (РКК). Российская система стандартов и норм в области кибербезопасности, такие как ГОСТ Р 51583–2014 «Средства защиты информации. Оценка соответствия средств защиты информации» и ГОСТ Р 57580–2017, направлены на улучшение системы защиты информации в России.

Стандарт безопасности данных индустрии платежных карт (PCI DSS) — это набор стандартов безопасности, разработанных для того, чтобы гарантировать, что компании, которые принимают, обрабатывают, хранят или передают информацию о кредитных картах, поддерживают безопасную среду [14]. Для российского контекста аналогом PCI DSS является несколько нормативных актов и стандартов, регулирующих безопасность данных в сфере финансов и платежных систем

ГОСТ Р 57334–2016 «Система защиты информации. Требования безопасности для платежных карт» — этот стандарт, аналогичный PCI DSS, устанавливает требования безопасности для защиты данных при работе с платежными картами. Он охватывает аспекты, связанные с обработкой, хранением и передачей данных платёжных карт, а также с защитой транзакционных данных в финансовых учреждениях. В нем прописаны меры, направленные на предотвращение утечек данных, а также контроль за соблюдением стандартов безопасности.

Федеральный закон № 161-ФЗ «О национальной платежной системе» регулирует деятельность в области платежных систем и устанавливает требования к защите данных в процессе выполнения платежных операций.

Рекомендации Центрального банка России (ЦБ РФ) для организаций, работающих в сфере платежных систем, таких как банки и процессинговые компании. Одним из таких актов является Положение о защите информации при осуществлении платежных операций.

Приказ ФСБ России № 378 — нормативный акт, регулирующий вопросы безопасности информации, также затрагивает аспекты защиты данных при работе с финансовыми операциями и транзакциями.

Важность соответствия требованиям нормативно-правовой базы

Стандарты соответствия в области сетевой безопасности — это установленные правила и протоколы, которым должны придерживаться организации для обеспечения безопасности, целостности и эффективности своей сетевой инфраструктуры. Эти стандарты помогают снизить риски, связанные с утечкой данных и несанкционированным доступом и способствуют укреплению доверия со стороны заинтересованных сторон и клиентов, сохраняя при этом операционную целостность [5] [11]. Приведем ключевые стандарты соответствия.

ISO/IEC 27001 — это признанный во всем мире стандарт управления информационной безопасностью, в котором изложены требования к системе управления информационной безопасностью (СУИБ). Он подчеркивает системный подход к управлению конфиденциальной информацией компании, охватывающий людей, процессы и технологии.

ГОСТ Р 57580–2017 «Система менеджмента информационной безопасности. Требования» — это российский стандарт, который является аналогом ISO/IEC 27001 и устанавливает требования к созданию и поддержанию СУИБ. Он охватывает все важнейшие аспекты информационной безопасности, включая анализ рисков, управление доступом, защиту данных и защиту от угроз, что соответствует принципам ISO/IEC 27001.

NIST Cybersecurity Framework представляет собой набор добровольных рекомендаций для организаций по управлению и снижению рисков кибербезопасности. Она состоит из пяти ключевых функций: Идентификация, Защита, Обнаружение, Реагирование и Восстановление. Эта система помогает организациям выработать комплексный подход к кибербезопасности, затрагивая различные аспекты, такие как управление активами и планирование реагирования на инциденты[17].

ГОСТ Р 51901.1–2014 «Информационные технологии. Методы и средства обеспечения безопасности. Основные положения» представляет собой набор рекомендаций для обеспечения безопасности в сфере информационных технологий, аналогичных компонентам NIST Cybersecurity Framework. В нем описаны меры, связанные с идентификацией, защитой, обнаружением и реагированием на угрозы информационной безопасности. Он помогает организациям формировать структуру управления рисками, что аналогично принципам NIST CSF.

Исследование базировалось на изучении нарушений в области обеспечения безопасности персональных

данных Российскими компаниями за период 2021–2023 года.

Для подведения статистики выделим количество общих нарушений, а также те положения законодательства, по которым были зафиксированы нарушения, и соответственно обозначим количество штрафов, наложенных на компании, в зависимости от количества нарушений.

Таблица 1.

Сводная таблица нарушений за указанный период

Год	Общее количество нарушений	Нарушения по конкретным статьям	Количество штрафов
2021	51	Ч. 1 ст. 8: 19	15
		Иные: 32	
2022	120	Ч. 3 ст. 6: 22	40
		Иные:98	
2023	151	Ч. 3 ст. 6: 34	50
		Ч. 3 ст. 6 (волеизъявление): 43	
		Иные:74	

График роста количества нарушений за указанный период демонстрируется на рисунке 1 и 2.

По приведённым данным прослеживается закономерность роста количество нарушений в сфере защиты прав субъектов персональных данных с каждым годом. Так, в 2021 году зафиксировано 51 нарушение, в 2022 году — 120, а в 2023 году эта цифра возросла до 151.

Это увеличение нарушений непосредственно коррелирует с ростом вероятности наложения санкций. Чем больше нарушений, тем выше вероятность того, что регуляторы применят меры по обеспечению соблюдение законодательства. В приведённой таблице для каждого года указано количество штрафов. Количество штрафных санкций составляет примерно 30 % от общего числа нарушений.

На основании проведенного исследования можно сделать вывод, что количество применённых штрафных санкций со стороны регуляторов в области защиты персональных данных напрямую связано с числом нарушений, которое, в свою очередь, растёт из года в год, что в свою очередь подчеркивает важность соблюдения норм законодательства и необходимости для компаний иметь надлежащие механизмы, в частности механизмы комплаенса для обеспечения исполнения требований законодательства в области защиты персональных данных, а также норм иных законодательных актов в целях избежания наложения на них штрафных санкций.

Обсуждение

Чтобы эффективно поддерживать соответствие вышеперечисленным стандартам, организациям следует внедрить следующие практики.

Регулярный мониторинг и отчетность позволяют интегрировать соблюдение нормативных требований в стандартные бизнес-операции, превращая их в непрерывный процесс, а не в разовую задачу [7].

Обучение и информирование сотрудников. Формирование культуры соблюдения требований включает в себя регулярные программы обучения. Хорошо подготовленные сотрудники могут обнаружить уязвимости и значительно снизить вероятность несоблюдения требований[11][8].

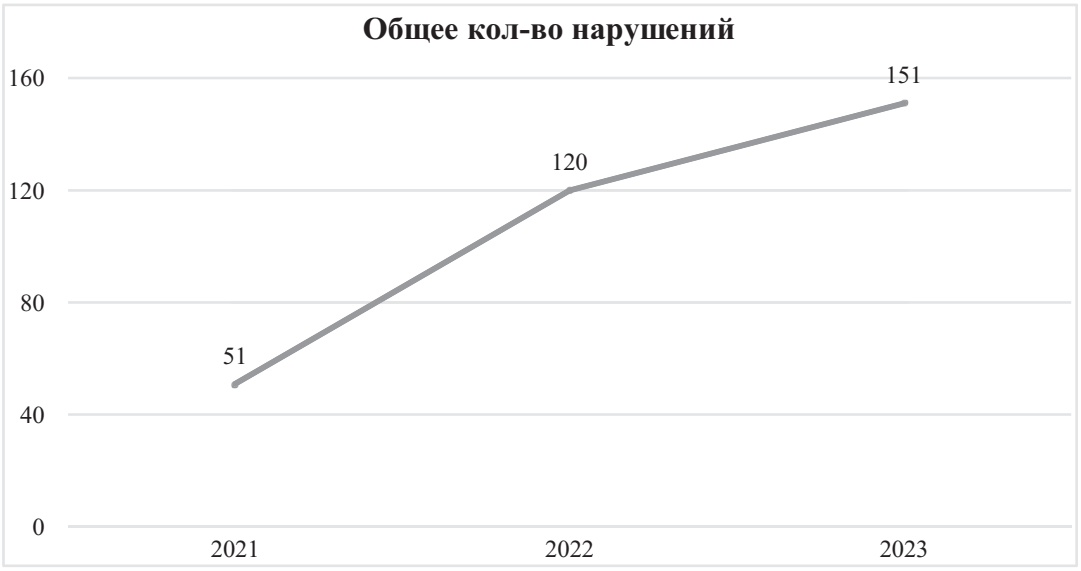

Рис. 1. График роста количества нарушений за период 2021–2023 гг.

Рис. 2. График роста количества штрафов за нарушения за период 2021–2023 гг.

Использование программного обеспечения для управления соответствием позволяет оптимизировать процессы, связанные с нормативными требованиями. Автоматизация задач, связанных с соблюдением нормативных требований, обеспечивает постоянный мониторинг и способность быстро адаптировать их к изменениям в законодательстве[11][8].

Внедрение комплексных процессов документирования необходимо для обеспечения четкого соблюдения требований. Документирование политик, процедур и обновлений обеспечивает информированность и подотчетность всех заинтересованных сторон, что помогает продемонстрировать соответствие требованиям во время аудитов и проверок[11][8].

Следуя этим стандартам и передовым практикам, организации могут защитить конфиденциальную информацию, снизить риски и укрепить доверие клиентов и партнеров в условиях цифрового взаимодействия.

Оценка соответствия и аудит являются важнейшими компонентами для обеспечения соблюдения нормативных требований в области сетевой безопасности.

Регулярные аудиты соответствия требованиям необходимы для выявления областей, требующих обеспечения соответствия организаций отраслевым нормам, перечисленным ранее[5].

Процесс аудита обычно включает в себя несколько основных этапов:

Планирование: определение масштаба аудита, цели и методологии, которые будут использоваться.

Сбор данных: сбор необходимой информации, включая сведения о конфигурации, журналы и сетевые карты.

Анализ: оценка собранных данных в соответствии с установленными политиками безопасности и стандартами соответствия.

Тестирование: проведение оценок, которые могут включать имитацию атак для выявления уязвимостей .

Отчетность: документирование результатов, включая обнаруженные уязвимости и рекомендации по корректирующим действиям.

Устранение: Устранение результатов аудита путем внедрения рекомендованных корректирующих мер.

Непрерывный мониторинг в режиме реального времени соответствует требованиям и становится все более важным, поскольку позволяет организациям осуществлять надзор за своей сетевой безопасностью. Для этого необходимо использовать автоматизированные инструменты, которые непрерывно сканируют систему на соответствие различным нормативным стандартам и автоматически документируют любые несоответствия.

Чтобы максимально повысить эффективность аудита соответствия, организациям следует придерживаться нескольких лучших практик:

— Разработать и внедрить комплексные политики безопасности и регламенты реагирования на инциденты [17].
— Проводить регулярные внутренние и внешние аудиты, чтобы обеспечить постоянное соблюдение требований и выявить области для улучшения [17].
— Обучение сотрудников по вопросам соблюдения требований.[5].
— Документирование регламентов по исполнению политик и процедур и по реагированию на события и инциденты ИБ. [17].

Соблюдая эти правила, организации смогут более эффективно справляться со сложностями оценки соответствия и аудита, тем самым повышая общий уровень безопасности и снижая риски, связанные с несоблюдением требований.

Поддержание соответствия стандартам сетевой безопасности ставит перед организациями ряд серьезных задач, в основном обусловленных динамичным ландшафтом угроз и ограниченностью ресурсов.

Развивающийся ландшафт угроз. Постоянно меняющийся характер киберугроз представляет собой серьезное препятствие для соблюдения нормативных требований. По мере того как киберпреступники совершенствуют свои методы и разрабатывают все более изощренные векторы атак, организации должны постоянно адаптировать свои стратегии соблюдения нормативных требований, чтобы противостоять меняющимся рискам[6]. Эта постоянная задача требует необходимости интеграции передовых технологий, таких как искусственный интеллект (ИИ) и машинное обучение, для повышения уровня безопасности [5][9].

Ограниченность ресурсов существенно влияет на способность организации соответствовать стандартам сетевой безопасности. Многие компании, особенно небольшие, сталкиваются с бюджетными ограничениями, которые лишают возможности инвестиции в необходимые технологии, квалифицированный персонал и программы обучения [5]. Нехватка ресурсов может привести к появлению критических уязвимостей и препятствовать принятию надежных мер безопасности, необходимых для соблюдения стандартов [5].

Кроме того, нехватка квалифицированных специалистов по кибербезопасности усугубляет эти проблемы, поскольку организациям трудно нанять и удержать талантливых сотрудников, способных эффективно выполнять требования по соблюдению нормативных требований [8].

Существующая сложность и сегодняшнее быстрое развитие нормативно-правовой базы еще сильнее усложняют работу по обеспечению соответствия. Организациям приходится ориентироваться в огромном количестве инструкций, которые могут меняться так же быстро, как появляются новые угрозы ИБ[7][8]. Такая динамичная нормативная среда требует от компаний внедрения гибких методов обеспечения соответствия требованиям нормативно правовой базы ИБ, что может быть затруднительно без наличия соответствующих ресурсов и опыта [7][8].

В каждом сегменте рынка информационной безопасности существуют разнообразные инструменты, которые способны существенно ускорить и упростить процессы аудита, выявления уязвимостей и обеспечения соответствия стандартам. Ниже представлен краткий сравнительный обзор как отечественных, так и зарубежных решений в каждой из ключевых категорий.

1. Сканирование на уязвимости

Отечественные разработки:

Российский рынок представлен комплексными системами многоуровневого сканирования, обеспечивающими всестороннюю оценку состояния защищенности информационных систем. Наиболее технологически продвинутые отечественные решения поддерживают широкий спектр платформ и обеспечивают детальное сканирование внутренних сетей, веб-приложений и критической инфраструктуры. Следует отметить наличие в российском сегменте как масштабируемых корпоративных платформ глубокого анализа, так и более доступных решений для оперативной оценки сетевых уязвимостей с акцентом на безопасность веб-ресурсов.

Зарубежные разработки:

Иностранные сканеры уязвимостей характеризуются высокой степенью интеграции с международными базами данных угроз и обширными каталогами уязвимостей. Особое внимание уделяется автоматизации процессов верификации и валидации обнаруженных слабых мест. Преимуществами зарубежных решений являются облачная архитектура развертывания, возможность динамического масштабирования и регулярное обновление базы сигнатур в соответствии с актуальной моделью угроз.

2. Мониторинг сети

Отечественные разработки:

Российские системы мониторинга сетевой инфраструктуры специализируются на глубинном анализе сетевого трафика и детектировании аномальной активности. Существенным преимуществом отечественных

решений является адаптированность к особенностям национальной нормативно-правовой базы и учет специфических требований регуляторов. Функциональность данных систем включает в себя комплексный анализ сетевой активности и превентивную защиту от несанкционированного доступа к конфиденциальным данным.

Зарубежные разработки:

Зарубежные платформы мониторинга отличаются высокопроизводительной обработкой значительных массивов гетерогенных данных, что обеспечивает эффективный анализ как в режиме реального времени, так и при ретроспективном исследовании инцидентов безопасности. Модульная архитектура иностранных решений позволяет интегрировать дополнительные функциональные блоки посредством специализированных плагинов, что существенно расширяет аналитические возможности систем мониторинга.

3. Тестирование на проникновение

Отечественные разработки:

В российском сегменте представлены комплексные платформы для автоматизированного моделирования угроз и эмуляции атак на инфраструктуру. Отечественные решения в данной категории интегрируют функции имитации действий злоумышленников с элементами обучения специалистов по информационной безопасности. Особую ценность представляют технологические решения, обеспечивающие возможность верификации защищенности инфраструктуры в условиях, приближенных к реальным сценариям кибератак.

Зарубежные разработки:

Иностранные средства для автоматизированного моделирования угроз и эмуляции атак на инфраструктуру характеризуются универсальностью применения и обширным инструментарием для разработки и эксплуатации уязвимостей. Зарубежные решения демонстрируют высокую степень автоматизации процессов тестирования безопасности веб-приложений с интегрированными механизмами анализа исходного кода и взаимодействия с тестируемыми системами.

4. Оценка соответствия

Отечественные разработки:

Российские системы оценки соответствия ориентированы на автоматизацию процессов верификации защищенности информационных систем согласно требованиям национальных регуляторов (ФСТЭК, ФСБ, Центробанк). Отечественные решения в данном сегменте характеризуются интуитивно понятным интерфейсом и предустановленными шаблонами проверок в соответствии с актуальными нормативными документами, что существенно упрощает процедуру подготовки к сертификации информационных систем.

Зарубежные разработки:

Зарубежные платформы управления соответствием предлагают интегрированные механизмы анализа рисков и контроля исполнения политик информационной безопасности в масштабах глобальных корпораций. Международные решения данного класса отличаются возможностью одновременного соответствия нормативным требованиям различных юрисдикций и отраслевым стандартам (ISO 27001, GDPR, HIPAA, PCI DSS).

По мере развития нормативно-правовой базы организации должны вкладывать средства в программы непрерывного обучения и повышения осведомленности своих сотрудников, чтобы они всегда были в курсе всех изменений в нормативно-правовой базе.

Заключение

В заключение, важность комплаенса безопасности сети становится все более очевидной на фоне быстрого развития цифровых технологий и актуальных угроз в области информационной безопасности. Эффективное интегрирование соблюдения нормативных требований в повседневные бизнес-операции не только повышает уровень защищенности организаций, но и способствует устойчивому функционированию отдела информационной безопасности. Анализ зарубежной и отечественной нормативно-правовой базы, а также представленные практики и инструменты для достижения соответствия стандартам, подчеркивают необходимость разработки комплексного подхода к комплаенсу. В условиях стремительных изменений в цифровом пространстве организации должны признавать комплаенс как неотъемлемую часть своей стратегии, что обеспечит их долгосрочную защиту и конкурентоспособность на рынке.

ЛИТЕРАТУРА

1. «6 Security Controls You Need for GDPR Compliance.» — Text: electronic // Creative Networks: [website]. — URL: https://www.creative-n.com/blog/6-security-controls-for-gdpr-compliance/ (access date: 13.03.2025).: The Best Cybersecurity Standards and Frameworks — RiskSight.
2. «GDPR Compliance for Network Security.» — Text: electronic // codingdrills: [website]. — URL: https://www.codingdrills.com/tutorial/network-security-tutorial/gdpr-network-security (access date: 13.03.2025).
3. «10 Data Security Challenges Met by Organizations and CISOs.» — Text: electronic // sealpath: [website]. — URL: https://www.sealpath.com/blog/data-security-issues/ (access date: 13.03.2025).
4. George Mutune. «23 Top Cybersecurity Frameworks.» / Mutune George. — Text: electronic // cyberexperts: [website]. — URL: https://cyberexperts.com/cybersecurity-frameworks/ (access date: 13.03.2025).
5. Antti Pekkala. «Practical Strategies to Overcome Cybersecurity Challenges.» / Pekkala Antti. — Text: electronic // nomentia: [website]. — URL: https://www.nomentia.com/blog/practical-cybersecurity-strategies-to-overcome-challenges (access date: 13.03.2025).
6. «What is a Compliance and Regulatory Framework?» — Text: electronic // rapid7: [website]. — URL: https://www.rapid7.com/fundamentals/compliance-regulatory-frameworks/ (access date: 13.03.2025).
7. Editorial Staff. «Essential Guide to Network Security Compliance Standards.» / Staff Editorial. — Text: electronic // The Tech Artist: [website]. — URL: https://thetechartist.com/network-security-compliance-standards/ (access date: 13.03.2025).
8. Editorial Staff. «Understanding Network Compliance Standards for Enhanced Security.» / Staff Editorial. — Text: electronic // The Tech Artist: [website]. — URL: https://thetechartist.com/network-compliance-standards/ (access date: 13.03.2025).
9. «Common IT Security Standards, Regulations, And Frameworks.» — Text: electronic // jones it: [website]. — URL: https://www.itjones.com/blogs/common-it-security-standards-regulations-and-frameworks (access date: 13.03.2025).
10. «Compliance and Legal Considerations in Network Security.» — Text: electronic // CYB Software — Network Security & Securing Digital Transformation: [website]. — URL: https://cybsoftware.com/compliance-and-legal-considerations-in-network-security/ (access date: 13.03.2025).
11. Ryerse Jay. «Top 11 Cybersecurity Frameworks.» / Jay Ryerse. — Text: electronic // connectwise: [website]. — URL: https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks (access date: 13.03.2025).
12. Mainse Noah. «Top 5 Best Network Security Audit Tools to Safeguard Your Data.» / Noah Mainse. — Text: electronic // cybermatters: [website]. — URL: https://cybermatters.info/security-tools/best-network-security-audit-tools/ (access date: 13.03.2025).
13. «Comprehensive Guide to Network Compliance for IT Professionals.» — Text: electronic // eoxs: [website]. — URL: https://eoxs.com/new_blog/comprehensive-guide-to-network-compliance-for-it-professionals/ (access date: 13.03.2025).
14. Nagaraj Kuppuswamy. «Cyber Security Audit and Compliance: A Complete Guide to Safeguarding Your Network.» / Kuppuswamy Nagaraj. — Text: electronic // Beaconer: [website]. — URL: https://beaconer.io/cyber-security-audit-and-compliance-a-complete-guide-to-safeguarding-your-network/ (access date: 13.03.2025).
15. Developments Pepper. «Key Challenges in Cybersecurity Compliance and How to Overcome Them.» / Developments Pepper. — Text: electronic // datagr8: [website]. — URL: https://datagr8.com/blogs/information/key-challenges-in-cybersecurity-compliance-and-how-to-overcome-them (access date: 13.03.2025).
16. Fitzgerald Anna. «5 Hardest Things About Security Compliance and How Technology Can Help.» / Anna Fitzgerald. — Text: electronic // secureframe: [website]. — URL: https://secureframe.com/blog/security-compliance-challenges (access date: 13.03.2025).
17. Nigam Nidhi. «The Role of Artificial Intelligence and Machine Learning in Enhancing Cybersecurity Against Cybercrime.» / Nidhi Nigam. — Text: electronic // EC-Council CYBERSECURITY EXCHANGE: [website]. — URL: https://www.eccouncil.org/cybersecurity-exchange/network-security/role-of-ai-ml-in-enhancing-cybersecurity-against-threats/ (access date: 13.03.2025).

Журнал «Современная наука: актуальные проблемы теории и практики»