Ширяев Иван Сергеевич

студент

Князева Марина Данииловна

канд. техн. наук, доцент

ОАНО ВО «Московский институт технологий и управления»

г. Москва

КОМПЛЕКСНЫЙ ПРОЕКТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДЛЯ МОНИТОРИНГОВОГО ЦЕНТРА

Аннотация: *в статье рассматривается проблема построения комплексной системы защиты персональных данных на примере мониторингового центра частной охранной организации. Актуальность обусловлена ростом киберугроз и наличием типовых недостатков. Предложен проект создания интегрированной системы на базе трех компонентов: управление доступом, мониторинг инцидентов и защита от утечек. Обоснована целесообразность собственной разработки платформы вместо адаптации тиражных решений для обеспечения точного соответствия бизнес-процессам и требованиям законодательства. Реализация проекта позволит обеспечить соответствие 152-ФЗ, снизить риски утечек и перейти к проактивной модели управления информационной безопасностью.*

Ключевые слова: *защита данных, информационная безопасность, предотвращение утечек.*

По данным международного исследования IBM Security, каждую секунду крадут или теряют 59 записей персональных данных. Это средняя скорость утечек в секунду.

Актуальность данной проблемы обусловлена фундаментальными изменениями в цифровой среде, где персональные данные стали критически важным активом и одновременно ключевым источником рисков для организаций любой от-

расли. В условиях ужесточения законодательства в области защиты персональных данных, роста изощренности кибератак и повышенных ожиданий общества в части сохранения конфиденциальности, построение эффективной системы защиты информации перестает быть технической задачей и приобретает стратегическое значение для устойчивого развития любого бизнеса.

В качестве примера рассмотрим мониторинговый центр частной охранной организации, как оператора, который обрабатывает значительные объемы персональных и конфиденциальных данных клиентов и сотрудников. Обеспечение их безопасности является не только обязанностью, установленной Федеральным законом №152-ФЗ, но и императивом деловой репутации и конкурентного преимущества. Анализ текущего состояния системы, как правило, выявляет наличие типовых системных недостатков: фрагментированность процессов управления доступом, отсутствие централизованного мониторинга инцидентов безопасности, низкий уровень автоматизации выполнения требований законодательства и высокие операционные затраты на администрирование. Данные проблемы создают реальные риски финансовых потерь вследствие штрафных санкций, репутационного ущерба и потери доверия клиентов.

Обозначенная проблема обуславливает объективную необходимость в качественной трансформации подхода к защите персональных данных – от набора разрозненных технических средств к целостной, управляемой и эффективной системе. Для решения этих задач рассмотрим проект, решающий их за счет системного проектирования и внедрения комплекса взаимосвязанных организационно-технических решений. Его реализация позволит не только достичь формального соответствия требованиям регуляторов, но и перейти к проактивной модели управления рисками, обеспечить прозрачность и контролируемость бизнес-процессов, связанных с обработкой персональных данных, и, как следствие, создать прочный фундамент для цифровой устойчивости и дальнейшего роста.

В проекте представлен детальный пошаговый план построения комплексной системы информационной безопасности (СИБ). План учитывает экстремальную

чувствительность обрабатываемых данных (персональные данные, коммерческая тайна, данные охраняемых объектов) и критичность функционирования МЦ. Реализация программы позволит не только обеспечить соответствие требованиям законодательства (152-ФЗ), но и создать устойчивую к кибератакам и инсайдерским угрозам операционную среду, а также следующее.

1. Снизить операционные риски и минимизировать вероятность утечек конфиденциальной информации.

2. Сократить трудозатраты на администрирование и управление системой безопасности за счет автоматизации ключевых процессов.

Основные этапы работ.

1. Обследование и анализ информационных систем.

Выявление всех информационных систем, где обрабатываются персональные данные (1С, CRM, файловые хранилища и т. д.). С последующим анализом текущей архитектуры: как предоставляется и отзывается доступ, как реагируют на инциденты, как выполняются запросы субъектов ПДн. Выявление несоответствия требованиям 152-ФЗ.

2. Создание проекта архитектуры решений.

Разработка концепции и технического задания на создание Центра управления доступом (IAM Core) как единой точки управления правами пользователей.

Создание проекта системы мониторинга и реагирования на инциденты на базе SIEM-системы.

Разработка политик и правил DLP-системы для предотвращения утечек.

3. Разработка и внедрение технических средств.

Разработка и внедрение IAM-системы:

− создание единого каталога пользователей и ролей;

− внедрение workflow-движка для согласования заявок на доступ;

− интеграция ее со всеми ИСПДн (1С, CRM, сетевое хранилище) через API и скрипты.

Внедрение SIEM-системы:

− настройка сбора и централизованное хранение логов со всех критичных систем;

− разработка и настройка правил корреляции для обнаружения сложных атак и аномалий.

Внедрение DLP-системы:

− развертывание серверных компонентов и агентов на рабочих станциях;

− настройка политик контроля для веб-трафика, почты и USB-накопителей.

4. Разработка и внедрение организационных средств.

Разработка нового пакета организационно-распорядительных документов:

− регламент управления доступом;

− политика обработки персональных данных;

− положение об инцидентах и порядке реагирования;

− разработка программы и обучение по ней сотрудников, включая интерактивные курсы и тестирования на устойчивость к фишингу.

5. Интеграция компонентов в единую систему.

Настройка взаимодействие между IAM, SIEM и DLP. Например, при увольнении сотрудника IAM автоматически отзывает права, а SIEM и DLP получают сигнал для усиления мониторинга его активности. Инциденты от DLP автоматически регистрируются в SIEM для расследования.

Обеспечение сквозного аудита всех процессов.

Представленная диаграмма последовательности системных операций (Рисунок 1), отображает технологическое взаимодействие компонентов системы:

− взаимодействие между программными компонентами;

− протоколы и форматы обмена (http, LDAP, вызовы БД);

− последовательность технических операций при обработке запросов.

При создании глубоко интегрированной системы требуется провести сравнительный анализ возможностей тиражных решений и заложенной в проект целевой архитектуры. Для этого нужно рассмотреть, как международные, так и российские готовые решения для реализации проекта, которые теоретически могут

быть адаптированы под задачи проекта. Это зачастую не является экономически и технически целесообразным.

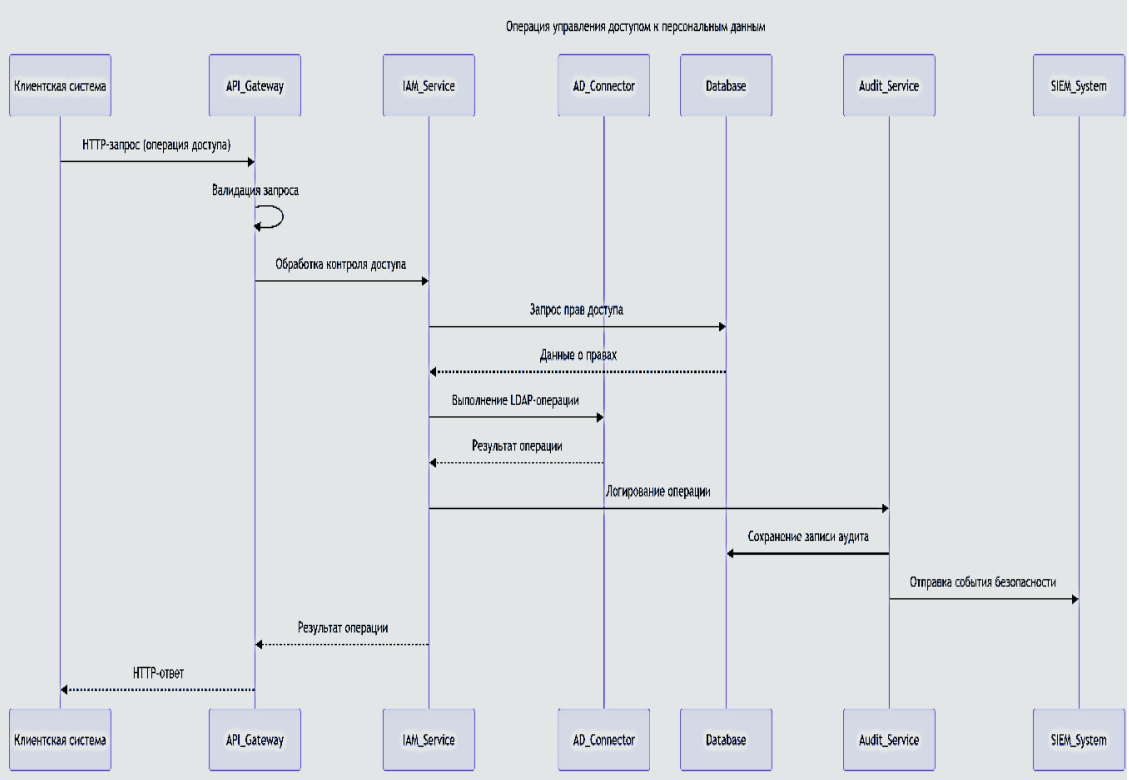

Рис. 1. Диаграмма последовательности системных операций

Затраты на лицензии, доработку и интеграцию превысят бюджет проекта, при этом не будет достигнуто полное соответствие уникальным бизнес-процессам и нормативным требованиям, предъявляемым к оператору ПДн в сфере охранной деятельности. Уникальность операционной деятельности организации может потребовать собственной разработки интегрированной платформы, а не адаптации тиражных решений. Это позволит создать целостную платформу безопасности, обеспечивающую соответствие требованиям законодательства о защите ПДн.

Собственная разработка позволит:

– реализовать только необходимый функционал, идеально соответствующий модели информационной системы;

– обеспечить глубинную интеграцию с существующей инфраструктурой (1С, AD, системы видеомониторинга) через собственные API;

− заложить соответствие 152-ФЗ и ФСТЭК на архитектурном уровне;

− снизить долгосрочные затраты на владение и получить полный контроль над системой.

Ключевым результатом и конкурентным преимуществом разработанного проекта будет является синергетический эффект, возникающий от интеграции трех ключевых компонентов – IAM, SIEM и DLP – в единый замкнутый контур безопасности. Их взаимодействие переводит систему защиты на качественно новый уровень, обеспечивая не просто суммирование функциональных возможностей, но и возникновение новых свойств, не присущих каждому компоненту в отдельности.

Реализация описываемого проекта позволит в полной мере достичь заявленных стратегических целей.

1. Повышение цифровой устойчивости. Создается управляемая, предсказуемая и адаптивная среда, устойчивая к широкому спектру угроз – от целевых кибератак до инсайдерских действий. Система приобретает способность не только противостоять известным угрозам, но и выявлять и блокировать новые, ранее не встречавшиеся атаки за счет анализа аномалий.

2. Обеспечение полного и доказуемого соответствия 152-ФЗ. Формальное соблюдение требований закона подкрепляется работающими техническими и организационными механизмами. При проверке регулятору можно продемонстрировать не только документы, но и действующие процессы автоматизированного управления доступом, регистрации инцидентов и выполнения запросов субъектов, что кардинально снижает риски штрафных санкций.

3. Снижение операционных рисков и затрат. Автоматизация рутинных процессов (назначение и отзыв прав, сбор логов, первичный анализ инцидентов) высвобождает значительные ресурсы IT- и security-подразделений, позволяя переориентировать их с оперативной деятельности на стратегическое развитие. Снижаются не только прямые затраты на администрирование, но и косвенные убытки от возможных инцидентов.

Таким образом представленная модель проекта по защите персональных данных для мониторингового центра ЧОО является реальным, имеющим способность к дальнейшему развитию и совершенствованию решением, учитывающим все аспекты проблемы сохранения персональных данных.

Список литературы

1. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

2. Барсуков В.С. Современные технологии информационной безопасности / В.С. Барсуков, Д.В. Михайлов. – М.: Солон-Пресс, 2019. – 256 с.

3. Запечников С.В. Криптографические методы и средства обеспечения информационной безопасности: учебное пособие / С.В. Запечников, Н.В. Дмитриевский. – М.: Горячая линия-Телеком, 2020. – 294 с.

4. Петренко С.А. Управление доступом в информационных системах / С.А. Петренко, А.А. Курбатов. – М.: ДМК Пресс, 2018. – 418 с.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW61798 (дата обращения: 03.05.2026).

6. Портал по информационной безопасности SecurityLab. – URL: https://www.securitylab.ru (дата обращения: 03.05.2026).