Министерство науки и высшего образования Российской Федерации

[Название университета]

[Название факультета / института]

[Название кафедры]

КУРСОВАЯ РАБОТА

по дисциплине «Информационная безопасность»

на тему: «Современные методы защиты информации в корпоративных системах»

Выполнил(а): студент(ка)

[группа, курс]

Gabriel

Научный руководитель:

[должность, ФИО преподавателя]

[Город]

2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современная корпоративная среда всё сильнее зависит от информационных систем, которые обеспечивают работу бизнес-процессов, взаимодействие с клиентами и партнёрами, хранение и обработку данных, а также удалённый доступ сотрудников. На фоне цифровизации растёт и уровень киберугроз: атакующие активно используют фишинг и социальную инженерию, эксплуатируют уязвимости в публичных сервисах, атакуют цепочки поставок, применяют вредоносное ПО-вымогатели. Дополнительную сложность создают гибридные инфраструктуры (облако и локальные ресурсы), развитие мобильных рабочих мест и повышение требований регуляторов к защите персональных данных и значимых информационных ресурсов. Поэтому тема современных методов защиты информации в корпоративных системах остаётся актуальной как с теоретической точки зрения, так и для практики управления безопасностью в организациях.

Объектом исследования выступают корпоративные информационные системы организации, включающие сетевую инфраструктуру, серверы и рабочие станции, прикладные сервисы, средства хранения данных, а также процессы администрирования и эксплуатации. Предметом исследования являются современные методы и средства защиты информации, применяемые в корпоративной среде, а также организационные и технические меры, позволяющие снизить риски нарушения конфиденциальности, целостности и доступности данных.

Целью работы является обоснование и проектирование комплекса мер защиты информации для корпоративной системы с учётом актуальных угроз, требований нормативно-правовой базы и практик отраслевых стандартов. Для достижения поставленной цели необходимо решить ряд задач: рассмотреть корпоративную информационную систему как объект защиты, выделив ключевые активы, типовые угрозы и модель нарушителя; проанализировать

нормативно-правовые и организационные основы обеспечения информационной безопасности в организации, включая требования к защите персональных данных и подходы к управлению безопасностью; систематизировать современные методы защиты, охватывающие управление доступом, криптографическую защиту, мониторинг, обнаружение и реагирование на инциденты; выполнить анализ исходного состояния и оценку рисков на основе инвентаризации активов и классификации данных; разработать архитектуру комплекса защитных мер, включающую сетевую сегментацию, защиту конечных устройств, средства предотвращения утечек и резервное копирование; предложить план внедрения и подход к оценке эффективности, включая регламенты, обучение персонала, показатели результативности и аудит.

В работе используются методы анализа и обобщения научной и учебной литературы, сравнительный анализ стандартов и требований регуляторов, риск-ориентированный подход к выбору мер безопасности, моделирование угроз и построение логической архитектуры защиты. Также применяются элементы системного подхода, поскольку корпоративная информационная безопасность рассматривается как совокупность взаимосвязанных процессов, технологий и человеческого фактора.

Теоретическая значимость работы заключается в структурировании современных методов защиты и увязке их с моделью угроз, рисками и нормативными требованиями, что позволяет целостно рассматривать безопасность корпоративных систем. Практическая значимость состоит в том, что предложенный комплекс мер и план внедрения могут быть использованы как основа для разработки внутренних документов организации и проектирования защитных решений на уровне инфраструктуры и процессов, включая контроль доступа, криптографию, мониторинг и реагирование, а также меры по снижению вероятности утечек и простоя.

Работа состоит из двух глав. В первой главе рассматриваются теоретические основы защиты информации в корпоративных системах: раскрывается понятие корпоративной информационной системы как объекта защиты, анализируются активы, угрозы и модель нарушителя, приводятся нормативно-правовые и организационные основы обеспечения безопасности, а также описываются современные подходы и методы защиты, включая идентификацию и управление доступом, криптографическую защиту, мониторинг и реагирование на инциденты. Во второй главе выполняется проектирование комплекса мер защиты в корпоративной среде: проводится анализ исходного состояния и оценка рисков на базе инвентаризации и классификации данных, разрабатывается архитектура защиты (сегментация сети, защита конечных устройств, DLP, резервное копирование), а также формируется план внедрения и подход к оценке эффективности через регламенты, обучение персонала, метрики и аудит. Такой подход позволяет последовательно перейти от теоретической базы к практическому проектированию и получить обоснованные рекомендации по построению современной системы защиты информации в организации.

ГЛАВА 1 Теоретические основы защиты информации в корпоративных системах

1.1 Корпоративная информационная система как объект защиты: активы, угрозы и модель нарушителя

Корпоративная информационная система (КИС) в современной организации давно перестала быть «набором компьютеров и серверов». По сути, это среда, в которой выполняются ключевые операции бизнеса: от бухгалтерии и документооборота до клиентских сервисов, аналитики и управления производственными процессами. Поэтому при построении защиты важно рассматривать КИС как совокупность активов, процессов и участников, где уязвимость в одном звене быстро превращается в проблему для всей компании. Такой системный взгляд соответствует логике менеджмента информационной безопасности, принятой в международных стандартах, где объектом управления является не отдельное средство защиты, а риски для информации и сервисов [1].

В практическом смысле КИС включает несколько уровней. На инфраструктурном уровне находятся сеть (локальная, беспроводная, каналы связи с филиалами и облаком), серверные мощности (физические и виртуальные), системы хранения и резервного копирования, а также инженерные компоненты, влияющие на доступность (электропитание, климат, помещения). На прикладном уровне располагаются корпоративные сервисы: электронная почта, системы управления документами, ERP/CRM, базы данных, веб-приложения, средства удалённого доступа, каталоги пользователей и сервисы аутентификации. Отдельно стоит выделить конечные устройства: рабочие станции, ноутбуки, мобильные устройства, тонкие клиенты, а также специализированные устройства (например, терминалы, сканеры, кассовое оборудование). Наконец, есть организационно-

процессный уровень: регламенты, роли, процедуры администрирования, договоры с поставщиками, обучение сотрудников и культура работы с данными. Именно на этом уровне часто возникают условия для инцидентов, потому что даже сильная техническая защита не компенсирует ошибки в процессах [7].

Ключевой шаг в понимании КИС как объекта защиты связан с выделением активов. В подходах ISO/IEC активом считается всё, что имеет ценность для организации и требует защиты: информация, программное обеспечение, оборудование, услуги, персонал, репутация [2]. На практике удобно группировать активы по нескольким категориям. Первая категория, наиболее очевидная, это данные: персональные данные клиентов и сотрудников, коммерческая тайна, финансовая отчётность, договоры, переписка, техническая документация, исходные коды, результаты исследований, а также эксплуатационные данные (логи, конфигурации, учётные записи). Вторая категория это сервисы и процессы: доступность корпоративной почты, работоспособность ERP, возможность проводить платежи, выпускать документы, обслуживать клиентов. Третья категория это инфраструктура: сетевое оборудование, серверы, виртуализация, облачные ресурсы, средства резервного копирования. Четвёртая категория это люди и их полномочия: администраторы, пользователи, подрядчики, а также механизмы управления идентичностью. В современных атаках компрометация учётной записи часто равнозначна компрометации части инфраструктуры, поэтому «идентичность» фактически становится отдельным активом [3].

Когда активы определены, логично перейти к угрозам, то есть к возможным событиям, способным нанести ущерб конфиденциальности, целостности или доступности. В российской практике полезно опираться на терминологию и общую логику технической защиты информации, закреплённую в профильных рекомендациях [23], а также на банк данных

угроз ФСТЭК, который отражает актуальные сценарии и типовые векторы атак [19]. При этом важно не превращать анализ угроз в формальный перечень. Для корпоративной среды характерны несколько устойчивых классов угроз, которые встречаются независимо от отрасли.

Во-первых, это угрозы, связанные с человеческим фактором. Сюда относятся фишинг, компрометация учётных данных через социальную инженерию, ошибки при отправке писем и файлов, использование слабых паролей, игнорирование обновлений, подключение личных устройств без контроля. Отчёты по инцидентам регулярно показывают, что именно человеческий фактор остаётся одним из главных «входов» для атакующих [6]. Во-вторых, это уязвимости программного обеспечения и неправильные настройки. Уязвимости веб-приложений, ошибки авторизации, небезопасная обработка данных, открытые административные панели и неверно настроенные облачные хранилища формируют большой слой рисков, особенно для компаний, активно развивающих цифровые сервисы [5]. В-третьих, это вредоносное ПО, включая вымогателей, трояны для удалённого управления и средства кражи данных. Вымогатели особенно опасны тем, что одновременно бьют по доступности (шифрование) и по конфиденциальности (эксфильтрация и шантаж публикацией) [6]. В-четвёртых, это угрозы инсайдеров. Инсайдер не обязательно действует злонамеренно; часто речь идёт о «неосторожном инсайдере», который нарушает правила из удобства или незнания, но последствия для организации сопоставимы с целевой атакой [7]. В-пятых, это угрозы цепочки поставок: компрометация подрядчика, внедрение вредоносного обновления, использование уязвимого компонента. В корпоративных системах, где много внешних интеграций и сервисных контрактов, этот класс угроз становится всё более заметным [3].

Чтобы перейти от общего перечня угроз к проектированию защиты, требуется модель нарушителя. Модель нарушителя описывает, кто может атаковать, какими ресурсами обладает, какие цели преследует и каким

образом может действовать. В учебной и практической литературе обычно выделяют внешнего нарушителя (киберпреступники, конкуренты, хактивисты) и внутреннего (сотрудник, администратор, подрядчик) [8]. Однако для корпоративной среды полезнее рассматривать нарушителя по уровню возможностей: низкий (массовые атаки, готовые инструменты), средний (целенаправленный подбор уязвимостей, эксплуатация типовых ошибок конфигурации, использование утёкших учётных данных), высокий (целевая атака, длительное скрытное присутствие, использование 0-day или сложных техник уклонения). Такой подход помогает сопоставить угрозы с реальными сценариями и не «перекладывать» на организацию избыточные требования, если они не соответствуют её профилю рисков [13].

Важная часть модели нарушителя связана с точками входа и путями развития атаки. В корпоративной среде типичный сценарий начинается с компрометации учётной записи через фишинг или утечку пароля, затем следует закрепление в инфраструктуре (например, через доступ к почте, VPN или облаку), повышение привилегий, перемещение по сети и воздействие на критические сервисы. Такой «цепочный» характер атаки подтверждается практиками расследования инцидентов и рекомендациями по реагированию [4]. Поэтому при описании модели нарушителя полезно фиксировать не только «кто атакует», но и «как он будет развивать успех»: какие сегменты сети станут целью, где хранятся наиболее ценные данные, какие сервисы дают административные полномочия, какие журналы событий могут выдать присутствие атакующего.

Отдельно стоит обсудить критерии ущерба, поскольку угрозы сами по себе не определяют приоритеты защиты. Для бизнеса ущерб выражается не только в утечке данных, но и в простое сервисов, штрафах, потере доверия клиентов и партнёров, нарушении договорных обязательств. В российском контексте дополнительным фактором является соблюдение требований законодательства о персональных данных и безопасности значимых объектов,

если организация подпадает под соответствующие нормы [27], [28]. Даже если компания формально не относится к критической инфраструктуре, требования к защите персональных данных и к организационным мерам всё равно задают минимальный «порог» безопасности и влияют на архитектуру доступа, хранение данных и процессы реагирования [21].

Таким образом, рассмотрение КИС как объекта защиты начинается с инвентаризации активов и понимания их ценности, затем переходит к анализу актуальных угроз и построению модели нарушителя, ориентированной на реальные сценарии атак. Это создаёт основу для следующего шага: определения нормативно-правовых и организационных рамок, в которых организация должна выстраивать систему информационной безопасности, чтобы защита была не только технически сильной, но и управляемой.

В конце главы можно сделать вывод, что корпоративная информационная система является сложным объектом защиты, где критичны не только технические компоненты, но и данные, идентичности пользователей, процессы и взаимодействие с подрядчиками. Основные угрозы для КИС формируются на стыке человеческого фактора, уязвимостей ПО, вредоносных программ и ошибок конфигурации, а также инсайдерских и цепочных сценариев. Модель нарушителя позволяет связать эти угрозы с конкретными векторами атак и определить, какие активы и процессы требуют первоочередной защиты.

1.2 Нормативно-правовые и организационные основы обеспечения информационной безопасности в организации

Система защиты информации в корпоративной среде не может строиться только на «лучшем наборе средств». Она должна опираться на нормативные требования и на внутреннюю организацию работы с безопасностью, иначе меры будут разрозненными и плохо управляемыми. Нормативно-правовая база задаёт обязательные рамки и ответственность, а

организационные основы определяют, кто и как принимает решения, контролирует выполнение, реагирует на инциденты и улучшает защиту. В результате безопасность становится не разовой закупкой решений, а постоянным процессом управления рисками, что соответствует подходу систем менеджмента информационной безопасности [11].

В российской практике базовым законодательным актом в сфере информации является Федеральный закон № 149-ФЗ, который закрепляет общие положения о защите информации и принципах её обработки [26]. Для большинства организаций ключевым является также Федеральный закон № 152-ФЗ «О персональных данных», поскольку почти любая компания обрабатывает персональные данные сотрудников, клиентов или контрагентов [27]. Закон устанавливает обязанности оператора по обеспечению безопасности персональных данных, включая необходимость принятия правовых, организационных и технических мер. В прикладном смысле это означает, что организация должна понимать, какие персональные данные она обрабатывает, где они хранятся, кто имеет доступ, какие угрозы актуальны, и какие меры защиты применяются. Требования к составу и содержанию мер конкретизируются в нормативных документах, среди которых заметную роль играет приказ ФСТЭК № 21, устанавливающий набор мер защиты для информационных систем персональных данных [21]. Для государственных информационных систем действует приказ ФСТЭК № 17, который также часто используется как ориентир по построению защиты по уровням и мерам, даже если организация не относится к госструктурам [20].

Если организация относится к субъектам критической информационной инфраструктуры, то добавляется отдельный контур требований по 187-ФЗ [28]. На практике это означает необходимость категорирования объектов, выполнения требований по безопасности значимых объектов и взаимодействия с уполномоченными органами. Даже когда компания не является субъектом КИИ, сама логика 187-ФЗ подчёркивает важность

защищённости критичных сервисов и устойчивости к инцидентам, что полезно учитывать при проектировании корпоративной защиты.

Нормативная база включает не только законы и приказы, но и документы стратегического уровня, которые задают понимание угроз и приоритетов. Доктрина информационной безопасности Российской Федерации фиксирует актуальность угроз в информационной сфере и необходимость развития мер защиты на уровне государства и организаций [14]. Для курсовой работы важно не пересказывать Доктрину, а показать, что корпоративная безопасность вписывается в общую картину: рост киберугроз, зависимость экономики от ИТ, необходимость защищать информационные ресурсы и инфраструктуру.

Отдельный блок требований связан с криптографической защитой информации. В корпоративных системах криптография используется для защиты каналов связи, хранения, электронной подписи и аутентификации. При этом применение сертифицированных средств и соблюдение требований к криптографическим средствам в ряде случаев регулируется документами ФСБ России, в частности приказом № 796 [22]. На практике организация должна определить, где криптография является обязательной (например, при защите определённых категорий данных или при выполнении требований регуляторов), а где допустимы иные меры, исходя из модели угроз и рисков. В любом случае криптография не заменяет организационные меры, а работает вместе с ними, закрывая конкретные технические риски [17].

Помимо российской нормативной базы, в корпоративной среде широко применяются международные стандарты и лучшие практики, особенно если компания работает с партнёрами, проходит аудит или стремится к зрелому управлению безопасностью. Центральным стандартом является ISO/IEC 27001, который описывает требования к системе менеджмента информационной безопасности (СМИБ) и задаёт цикл постоянного улучшения [1]. В российской системе стандартизации ему соответствует ГОСТ Р

ИСО/МЭК 27001 [11]. Важно подчеркнуть, что ISO/IEC 27001 не диктует конкретные технические решения, а требует выстроить управляемую систему: определить контекст, оценить риски, выбрать меры, назначить ответственность, контролировать выполнение и улучшать. Набор типовых мер и практик раскрывается в ISO/IEC 27002 и его российском аналоге ГОСТ Р ИСО/МЭК 27002 [2], [12]. Эти документы удобны как «каталог» контролей: управление доступом, криптография, физическая безопасность, управление инцидентами, безопасность поставщиков, резервное копирование и т.д.

Для проектирования корпоративной безопасности полезны и документы NIST, поскольку они дают практическую детализацию контролей и процессов. NIST SP 800-53 предлагает структурированный набор мер безопасности и приватности, который помогает не забыть важные области и выстроить контрольную матрицу [3]. NIST SP 800-61 описывает процесс реагирования на инциденты и подчёркивает, что успешное реагирование начинается задолго до самого инцидента, с подготовки, ролей, процедур и инструментов [4]. В курсовой работе такие источники уместны как подтверждение «общепринятой» логики построения процессов, особенно когда нужно обосновать необходимость мониторинга, реагирования и обучения персонала.

Однако нормативные и стандартные требования работают только тогда, когда в организации есть организационная структура безопасности. В типовом варианте выделяют владельцев активов (обычно руководители подразделений), службу информационной безопасности, ИТ-службу, подразделения по внутреннему контролю и аудит (если они есть), а также пользователей и администраторов. Важно чётко разграничить ответственность: кто утверждает политику безопасности, кто отвечает за внедрение технических мер, кто контролирует соблюдение, кто проводит расследования и кто принимает решения при инциденте. В литературе по управлению ИБ подчёркивается, что размытая ответственность приводит к «серым зонам», где инциденты неизбежны, а контроль формален [7].

Организационные основы обычно начинаются с политики информационной безопасности. Политика задаёт цели, принципы, область действия, общие требования к доступу, работе с данными, использованию устройств, взаимодействию с подрядчиками. Далее политика раскрывается в регламентах: управление учётными записями, порядок предоставления доступа, требования к паролям и многофакторной аутентификации, порядок обновления ПО, резервное копирование, реагирование на инциденты, порядок работы с носителями, правила удалённой работы. В контексте персональных данных также формируются документы оператора: перечни ИСПДн, модели угроз, организационные меры, журналы учёта и т.д., что прямо связано с требованиями регулятора и практикой проверок [21], [25]. При этом важно, чтобы документы не существовали «ради документов». Они должны быть встроены в реальные процессы: например, регламент управления доступом должен быть связан с кадровыми событиями (приём, перевод, увольнение), иначе учётные записи будут оставаться активными и создавать риск [13].

Ещё один важный организационный аспект связан с управлением рисками. В российских рекомендациях по управлению рисками ИБ подчёркивается необходимость систематического подхода: идентификация активов, угроз, уязвимостей, оценка вероятности и ущерба, выбор мер обработки риска [24]. Аналогичная логика заложена и в ISO/IEC 27001, где оценка рисков является центральным элементом СМИБ [1]. Для организации это означает, что выбор мер защиты должен быть обоснован: не «поставили потому что модно», а «поставили потому что это снижает конкретный риск до приемлемого уровня». Такой подход особенно важен при ограниченном бюджете, когда нужно выбирать меры, дающие максимальный эффект.

Отдельно стоит выделить вопрос соответствия отраслевым стандартам. Например, для финансовых организаций в России действует ГОСТ Р 57580.1, который определяет базовый состав организационных и технических мер [10]. Даже если компания не относится к финансовому сектору, сам документ

полезен как пример зрелого подхода к построению защиты и к проверке полноты мер, особенно в части контроля доступа, журналирования, мониторинга и управления уязвимостями.

В завершение важно подчеркнуть, что нормативно-правовые требования и организационные основы не противостоят техническим мерам, а задают им рамки и смысл. Если в организации есть понятные роли, документы, процедуры и риск-ориентированный выбор контролей, то технические решения (сетевые экраны, EDR, DLP, SIEM, резервное копирование) становятся частью управляемой системы. Это логично подводит к следующему подразделу, где рассматриваются современные методы защиты как набор практик и технологий, которые применяются в корпоративной среде для реализации требований и снижения рисков.

В конце главы можно сделать вывод, что обеспечение информационной безопасности в организации опирается на сочетание обязательных требований законодательства (149-ФЗ, 152-ФЗ, приказы ФСТЭК, при необходимости 187-ФЗ) и на практики стандартов (ISO/IEC 27001/27002, NIST), которые помогают выстроить управляемую систему. Организационные меры, включая политику ИБ, регламенты, распределение ответственности и управление рисками, являются основой, без которой технические средства не дают устойчивого результата. Следующий шаг заключается в рассмотрении конкретных современных методов защиты, которые реализуют эти требования на уровне доступа, криптографии и процессов мониторинга и реагирования.

1.3 Современные подходы и методы защиты: идентификация и доступ, криптография, мониторинг и реагирование

Современная защита корпоративных систем всё больше строится по принципу «слоёв», когда разные меры перекрывают друг друга и снижают вероятность того, что одна ошибка приведёт к критическому инциденту. Это связано с тем, что атаки стали комплексными: злоумышленники используют

несколько техник одновременно, комбинируют социальную инженерию, уязвимости, компрометацию учётных данных и скрытное перемещение внутри сети. Поэтому эффективная защита должна объединять управление идентичностью и доступом, криптографические меры, а также мониторинг и реагирование, которые позволяют обнаружить атаку и ограничить ущерб [3].

Одним из центральных подходов последних лет является концепция Zero Trust, которая исходит из идеи «не доверять по умолчанию» ни внутренней сети, ни пользователю, ни устройству. Практически это означает постоянную проверку контекста доступа: кто обращается к ресурсу, с какого устройства, из какой сети, насколько безопасно устройство, какой уровень риска у сессии. В материалах крупных вендоров Zero Trust описывается как архитектурный принцип, который объединяет идентичность, устройства, приложения и данные в единую модель контроля [29], [30]. Для корпоративной среды это особенно актуально из-за удалённой работы и гибридных инфраструктур, где граница «периметра» размыта.

В рамках управления идентичностью и доступом (IAM) ключевой задачей остаётся обеспечение того, чтобы каждый субъект имел ровно те права, которые необходимы для выполнения работы, и не более. Здесь важны несколько практик. Первая практика это централизованная система учётных записей и ролей, когда управление пользователями, группами и правами происходит через единый каталог и согласованные процедуры. Вторая практика это принцип наименьших привилегий и разделение обязанностей, особенно для администраторов и критичных операций. Третья практика это многофакторная аутентификация, которая заметно снижает риск компрометации при утечке пароля или успешном фишинге. В современных условиях MFA становится фактически стандартом для удалённого доступа, облачных сервисов и привилегированных учётных записей [2]. Четвёртая практика это управление привилегированным доступом (PAM), когда администраторские права выдаются временно, с контролем и

журналированием, а сами административные сессии могут записываться и анализироваться. Такая мера важна, потому что компрометация администраторской учётной записи часто приводит к быстрому захвату домена и массовому распространению вредоносного ПО [4].

Отдельное внимание в управлении доступом уделяется жизненному циклу учётных записей. На практике многие инциденты происходят из-за «забытых» аккаунтов уволенных сотрудников, общих учётных записей, отсутствия контроля сервисных аккаунтов и ключей доступа. Поэтому организация должна связать кадровые процессы с ИТ-процедурами: приём и увольнение автоматически запускают создание или блокировку учётной записи, пересмотр групп, отзыв токенов и сертификатов. Такой подход соответствует управлению рисками и требованиям к организационным мерам, которые фигурируют в российских нормативных документах по защите персональных данных [21].

Криптографическая защита является следующим важным слоем. Её роль состоит в том, чтобы даже при перехвате трафика или доступе к носителю злоумышленник не смог прочитать данные или подменить их незаметно. В корпоративной среде криптография применяется в нескольких типовых сценариях: защита каналов связи (VPN, TLS), шифрование данных на носителях и дисках, шифрование резервных копий, электронная подпись для юридически значимого документооборота, защита ключей и секретов. Учебные материалы по криптографической защите подчёркивают, что эффективность криптографии зависит не только от алгоритмов, но и от управления ключами, процедур их хранения, ротации и контроля доступа [17]. Если ключи хранятся небезопасно или доступны слишком широкому кругу лиц, криптография превращается в «декорацию».

В российском контексте применение криптографических средств может требовать соблюдения требований к СКЗИ, особенно когда речь идёт о защите информации определённых категорий или о выполнении требований

регуляторов. Приказ ФСБ № 796 задаёт требования к средствам криптографической защиты, используемым для защиты информации, не содержащей гостайну [22]. На практике это означает, что при выборе решений организация должна учитывать не только функциональность, но и соответствие требованиям, если деятельность компании или тип обрабатываемой информации подпадает под такие правила. При этом важно понимать, что криптография не решает проблему фишинга или вредоносного ПО, поэтому она должна сочетаться с контролем доступа и мониторингом [2].

Мониторинг и реагирование на инциденты становятся третьим ключевым направлением современных методов защиты. Причина проста: полностью предотвратить атаки невозможно, а значит, критически важно быстро обнаруживать подозрительную активность и ограничивать последствия. NIST SP 800-61 рассматривает реагирование как цикл: подготовка, обнаружение и анализ, сдерживание и устранение, восстановление, а затем извлечение уроков [4]. Для корпоративной организации это означает, что должны быть заранее определены роли (кто принимает решение об отключении сервиса, кто общается с руководством, кто собирает доказательства), каналы связи, порядок эскалации, а также минимальный набор инструментов для расследования.

Практически мониторинг строится вокруг журналирования событий и их анализа. Источниками событий являются серверы, сетевые устройства, средства защиты, доменные контроллеры, почтовые системы, облачные сервисы, приложения и конечные устройства. Важно не просто собирать логи, а обеспечивать их целостность, достаточную детализацию и синхронизацию времени, иначе расследование будет затруднено. В корпоративной среде для корреляции событий часто применяются SIEM-системы, а на уровне рабочих станций и серверов всё чаще используются EDR-решения, которые фиксируют поведение процессов и помогают выявлять сложные атаки. Сами по себе названия классов решений не гарантируют безопасность, но отражают тренд:

смещение от «периметра» к наблюдаемости и контролю конечных точек, где часто начинается атака [3].

С мониторингом тесно связана тема обнаружения атак и аномалий. В научной и прикладной литературе подчёркивается, что современные атаки могут обходить простые сигнатурные механизмы, поэтому важны поведенческие методы, корреляция событий и анализ сетевого трафика [16]. Однако для корпоративной организации критично найти баланс: слишком чувствительные правила дают поток ложных срабатываний, и служба безопасности перестаёт реагировать. Поэтому мониторинг должен быть настроен под реальные активы и риски, а также поддерживаться процедурами: кто проверяет алерты, какие события считаются критическими, какие действия выполняются автоматически, а какие требуют согласования [7].

Отдельно стоит упомянуть безопасность веб-приложений и публичных сервисов, поскольку именно они часто становятся точкой входа. OWASP Top 10 даёт удобную классификацию наиболее критичных рисков веб-приложений: ошибки контроля доступа, уязвимости инъекций, небезопасная конфигурация, проблемы аутентификации, уязвимые компоненты [5]. Для корпоративной защиты это означает необходимость сочетать организационные меры (процессы разработки и тестирования) с техническими (WAF, сканирование уязвимостей, контроль конфигураций). Важно, что безопасность приложений не может быть «добавлена в конце», она должна быть встроена в жизненный цикл разработки, иначе уязвимости будут появляться быстрее, чем их успевают закрывать [18].

Если обобщить, современные методы защиты в корпоративной среде складываются в связанный набор: управление доступом ограничивает возможности злоумышленника, криптография защищает данные и каналы, мониторинг и реагирование позволяют обнаружить инцидент и минимизировать ущерб. Концепции вроде Zero Trust помогают объединить эти меры в единую архитектуру, особенно в условиях гибридной

инфраструктуры и удалённого доступа [29]. Такой теоретический обзор логично подводит к практической части работы: чтобы выбрать и обосновать конкретный набор мер, нужно оценить исходное состояние организации и риски, а затем на этой основе спроектировать комплекс защиты.

В конце главы можно сделать вывод, что современные подходы к защите корпоративных систем опираются на многоуровневую модель и риск-ориентированное применение мер. Управление идентичностью и доступом остаётся базовым механизмом снижения риска компрометации, криптография обеспечивает защиту данных и каналов при корректном управлении ключами, а мониторинг и реагирование позволяют выявлять атаки, которые всё же преодолели профилактические барьеры. Далее необходимо перейти от общих методов к оценке текущего состояния и рисков конкретной корпоративной среды, чтобы проектирование защиты было обоснованным и практичным.

ГЛАВА 2 Проектирование комплекса мер защиты информации в корпоративной среде

2.1 Анализ исходного состояния и оценка рисков: инвентаризация, классификация данных, выбор критериев

Проектирование комплекса мер защиты в корпоративной среде логично начинать не с выбора конкретных продуктов, а с анализа исходного состояния и оценки рисков. Это позволяет ответить на два практических вопроса: что именно нужно защищать в первую очередь и какие меры дадут наибольший эффект при разумных затратах. Риск-ориентированный подход закреплён в стандартах менеджмента информационной безопасности и в методических подходах к управлению рисками [1], [24]. Он помогает избежать ситуации, когда организация вкладывается в модные решения, но при этом оставляет без внимания базовые уязвимости, которые и становятся причиной инцидента.

Первый этап анализа это инвентаризация активов и понимание границ системы. В корпоративной среде границы редко совпадают с физическим периметром офиса. Обычно есть локальная сеть, филиалы, удалённые пользователи, облачные сервисы, внешние подрядчики и интеграции. Поэтому инвентаризация должна включать не только «железо», но и сервисы, учётные записи, данные и связи между системами. В рамках стандартного подхода ISO/IEC важно определить контекст и область применения системы менеджмента, то есть какие подразделения, процессы и ИТ-компоненты входят в контур управления безопасностью [1]. На практике это означает, что в перечень активов нужно включить критичные сервисы (например, почта, ERP, файловые хранилища, системы кадрового учёта), ключевые базы данных, инфраструктурные узлы (контроллер домена, шлюзы доступа, гипервизоры), а также облачные ресурсы, если они используются для хранения или обработки данных.

Инвентаризация обычно проводится в несколько проходов. Сначала формируется базовый реестр: список серверов, рабочих станций, сетевого оборудования, виртуальных машин, аккаунтов администраторов, используемых приложений и внешних сервисов. Затем уточняется, какие данные где хранятся и какие потоки данных существуют между системами. На этом шаге часто выявляются «теневые» сервисы, которые появились по инициативе отдельных подразделений, а также неучтённые каналы обмена данными, например пересылка документов через личную почту или мессенджеры. Подобные практики увеличивают риск утечек и усложняют выполнение требований по защите персональных данных [27]. Поэтому инвентаризация должна включать не только технический опрос ИТ-службы, но и взаимодействие с бизнес-подразделениями, которые реально используют данные.

Следующий этап это классификация данных и определение их критичности. Классификация нужна для того, чтобы задать приоритеты защиты и выбрать адекватные меры. В корпоративной практике обычно выделяют данные по уровню конфиденциальности (публичные, внутренние, конфиденциальные, строго конфиденциальные) и по критичности для бизнеса (насколько серьёзны последствия потери доступности или целостности). При этом персональные данные выделяются в отдельную категорию, поскольку к ним применяются специальные требования закона и регуляторов [27], [25]. Для персональных данных важно определить состав, цели обработки, категории субъектов, а также оценить, какие угрозы актуальны для конкретной информационной системы. Это напрямую связано с требованиями по выбору мер защиты для ИСПДн [21].

Классификация данных должна быть не формальной, а практичной. Например, коммерческая тайна в виде финансовых моделей или условий договоров может быть критичнее, чем часть персональных данных, если утечка приведёт к прямым конкурентным потерям. С другой стороны, утечка

персональных данных может привести к штрафам, судебным спорам и репутационному ущербу. Поэтому в классификации важно учитывать несколько измерений: юридические последствия, финансовый ущерб, влияние на репутацию и влияние на непрерывность бизнеса. Такая постановка вопроса соответствует идее, что безопасность должна защищать бизнес-ценность активов, а не абстрактные «файлы» [7].

После инвентаризации и классификации данных можно перейти к анализу угроз и уязвимостей в конкретной среде. Здесь полезно опираться на банк данных угроз ФСТЭК как на источник типовых сценариев, но адаптировать их под реальную архитектуру и процессы организации [19]. Например, если в компании широко используется удалённый доступ, то в число приоритетных угроз попадут компрометация VPN-учётных данных, атаки на почтовые аккаунты и фишинг. Если есть публичные веб-сервисы, то повышается значимость уязвимостей приложений и ошибок конфигурации, описываемых в отраслевых практиках [5]. Если есть критичные файловые хранилища и слабая сегментация сети, то риск вымогателей становится особенно высоким, потому что шифрование может затронуть сразу большую часть инфраструктуры [6].

Уязвимости в корпоративной среде обычно распределяются по нескольким типам. Это технические уязвимости (необновлённые системы, устаревшие протоколы, слабые настройки), организационные (отсутствие регламентов, неразграниченные права, отсутствие контроля подрядчиков), процессные (нет управления изменениями, нет контроля резервного копирования), а также уязвимости, связанные с человеческим фактором (низкая осведомлённость, отсутствие обучения, привычка обходить правила). В управлении рисками важно фиксировать не только наличие уязвимости, но и условия её эксплуатации: насколько легко атакующему получить доступ, какие привилегии можно получить, как быстро можно распространиться по

сети [13]. Это помогает оценить вероятность реализации угрозы, а не ограничиваться общими словами.

Далее определяется методика оценки рисков и критерии. В рамках курсовой работы целесообразно использовать качественную или полуколичественную оценку, где риск рассматривается как комбинация вероятности и ущерба. Подходы к управлению рисками ИБ допускают различные шкалы, главное, чтобы они были согласованы и применялись единообразно [24]. Например, вероятность можно оценивать по трёх- или пятибалльной шкале с учётом доступности вектора атаки (публичный сервис или внутренний), наличия известных уязвимостей, частоты подобных инцидентов в отрасли и уровня защищённости. Ущерб можно оценивать по влиянию на конфиденциальность, целостность и доступность, а также по финансовым и репутационным последствиям. При этом важно заранее определить, что считается «неприемлемым» риском, то есть где организация обязана внедрить меры, а где риск может быть принят или перенесён (например, через страхование или договорные условия).

Отдельный вопрос это критерии эффективности защиты и целевые показатели. Уже на этапе оценки рисков полезно определить, какие метрики будут использоваться далее: допустимое время простоя критичных сервисов, целевой уровень покрытия MFA, доля устройств с актуальными обновлениями, время обнаружения инцидента. Такие метрики потом можно связать с планом внедрения и аудитом, что соответствует логике постоянного улучшения в ISO/IEC 27001 [1]. Кроме того, ориентация на метрики делает проект более «управляемым», потому что можно показать прогресс не общими фразами, а измеримыми изменениями.

Результатом подраздела является понимание текущего профиля рисков. Например, для типичной компании со смешанной инфраструктурой часто выявляются следующие приоритеты: защита учётных данных и удалённого доступа, снижение риска вымогателей через сегментацию и резервное

копирование, повышение контролируемости конечных точек, устранение критичных уязвимостей в публичных сервисах, а также снижение риска утечек через контролируемые каналы обмена данными. Эти приоритеты должны быть увязаны с классификацией данных и критичностью сервисов, а также с обязательными требованиями по персональным данным [21], [27].

В конце главы можно сделать вывод, что анализ исходного состояния начинается с инвентаризации активов и уточнения границ корпоративной системы, затем включает классификацию данных и сервисов по критичности, после чего проводится оценка угроз и уязвимостей с опорой на актуальные источники. Выбор критериев риска и целевых метрик позволяет перейти от описания проблем к управляемому плану улучшений. Далее, имея картину приоритетных рисков, можно проектировать архитектуру комплекса защитных мер, чтобы закрыть наиболее значимые сценарии атак и обеспечить соответствие требованиям.

2.2 Разработка архитектуры защиты: сегментация сети, защита конечных устройств, DLP и резервное копирование

Разработка архитектуры защиты в корпоративной среде по сути является переводом результатов оценки рисков в конкретную систему мер и технических решений. Важно, чтобы архитектура не была набором несвязанных средств. Она должна отражать логику: какие активы защищаются, от каких угроз, какими контролями, и как эти контроли поддерживаются процессами. Такой подход соответствует идее «контролей» в ISO/IEC 27002 и структуре мер безопасности в NIST, где важна согласованность технических и организационных элементов [2], [3]. В рамках данной работы ключевыми компонентами архитектуры выступают сегментация сети, защита конечных устройств, предотвращение утечек (DLP) и резервное копирование как основа устойчивости.

Сетевая сегментация является одним из наиболее эффективных способов снизить ущерб от инцидентов. В корпоративной сети без сегментации компрометация одной рабочей станции может быстро привести к доступу к файловым серверам, базам данных и административным узлам. Это особенно опасно при атаках вымогателей, когда злоумышленники стремятся распространиться максимально широко и зашифровать как можно больше ресурсов [6]. Сегментация строится на принципе разделения сети на зоны безопасности с контролируемыми межзонными взаимодействиями. Типовая схема включает пользовательский сегмент, серверный сегмент, сегмент управления (администрирование), сегмент гостевого Wi-Fi, а также отдельные зоны для критичных систем и для внешних сервисов (DMZ). Между зонами устанавливаются правила доступа на межсетевых экранах, а также включается журналирование и контроль аномалий [9].

При проектировании сегментации важно учитывать не только IP-подсети, но и логические границы на уровне идентичности и приложений. Современные подходы, связанные с Zero Trust, предлагают строить доступ к ресурсам через проверку пользователя и устройства, а не через «доверенную внутреннюю сеть» [30]. На практике это означает, что даже внутри корпоративной сети доступ к критичным сервисам должен быть ограничен по принципу «разрешено только необходимое». Например, рабочие станции бухгалтерии не должны иметь прямого доступа к интерфейсам управления гипервизорами, а доступ администраторов к контроллерам домена должен осуществляться только с выделенных административных рабочих мест. Такая логика снижает риск lateral movement, то есть перемещения атакующего внутри сети после первичного проникновения [4].

Следующий элемент архитектуры это защита конечных устройств, потому что именно они чаще всего становятся точкой входа через фишинг, вредоносные вложения и эксплуатацию уязвимостей. Современный корпоративный подход включает несколько уровней. Базовый уровень это

управление конфигурациями и обновлениями: централизованная установка патчей ОС и приложений, контроль версий, запрет устаревших протоколов, минимизация локальных администраторских прав. Эти меры кажутся «рутинными», но именно их отсутствие часто делает атаку простой и дешёвой [7]. Следующий уровень это антивирусная защита и, по возможности, EDR, который позволяет видеть поведение процессов, выявлять попытки закрепления и подозрительные действия. В контексте NIST набор контролей для конечных устройств рассматривается как часть общей системы обнаружения и реагирования, где важны и технические средства, и процедуры обработки событий [3], [4].

Отдельно в архитектуре защиты конечных устройств следует учитывать мобильные устройства и удалённые рабочие места. Здесь важны шифрование дисков, управление политиками (MDM), контроль доступа к корпоративным ресурсам по состоянию устройства, а также многофакторная аутентификация. В условиях гибридной работы нельзя исходить из того, что устройство всегда находится в защищённой офисной сети, поэтому контроль должен переноситься на уровень идентичности и устройства, что соответствует принципам Zero Trust [29]. При этом организационные меры, такие как правила использования личных устройств и ответственность сотрудников, остаются обязательной частью, иначе технические меры будут обходиться [21].

Третьим компонентом архитектуры выступают меры предотвращения утечек данных, то есть DLP и связанные с ним механизмы контроля каналов. Утечки в корпоративной среде происходят не только из-за внешних атак, но и из-за ошибок сотрудников или злоупотреблений. DLP помогает контролировать передачу конфиденциальной информации по типовым каналам: электронная почта, веб-загрузки, облачные хранилища, внешние носители, печать. С практической точки зрения DLP должен опираться на классификацию данных, иначе система будет либо «молчать», либо мешать

работе из-за большого числа ложных блокировок. Поэтому архитектурно DLP связан с тем, как организация маркирует документы, какие шаблоны и словари использует, как определяет критичные типы данных (например, персональные данные, реквизиты договоров, финансовые отчёты) [2]. Важно также предусмотреть процесс обработки срабатываний: кто рассматривает инциденты DLP, как отличают ошибку от нарушения, какие меры применяются. Без этого DLP превращается в источник конфликтов и быстро отключается «ради удобства» [7].

Четвёртый ключевой элемент архитектуры это резервное копирование и восстановление, которое обеспечивает устойчивость к инцидентам и снижает ущерб от атак вымогателей и сбоев. Здесь важно уйти от упрощённого понимания «бэкап есть, значит всё хорошо». Вымогатели часто атакуют резервные копии в первую очередь, пытаясь удалить или зашифровать их, либо получить доступ к репозиторию через доменные учётные записи. Поэтому архитектура резервного копирования должна включать изоляцию резервных копий, ограничение доступа, раздельные учётные записи, а также регулярные тесты восстановления. В современных рекомендациях по реагированию на инциденты подчёркивается, что восстановление является частью процесса реагирования и должно быть заранее отработано, иначе в кризисный момент организация теряет время и увеличивает простой [4].

Практически разумно применять принцип 3-2-1: три копии данных, на двух разных типах носителей, одна копия вне основной инфраструктуры. В корпоративной среде «вне» может означать отдельный изолированный сегмент, облачное хранилище с отдельными ключами, или офлайн-носитель, если это обосновано. При этом важно шифровать резервные копии и защищать ключи, иначе резервное копирование создаёт новый риск утечки. Криптографические меры и требования к СКЗИ, если они применимы, должны учитываться и в контуре резервного копирования [17], [22]. Также необходимо определить RPO и RTO для критичных сервисов, то есть допустимую потерю

данных и допустимое время восстановления, чтобы архитектура бэкапов соответствовала реальным требованиям бизнеса [7].

В архитектуре защиты важно связать перечисленные компоненты между собой через единые принципы. Например, сегментация сети должна поддерживать защиту конечных устройств, ограничивая их доступ к серверным зонам. DLP должен опираться на классификацию данных и на управление доступом, чтобы не пытаться «компенсировать» избыточные права. Резервное копирование должно быть защищено от компрометации учётных записей, что снова возвращает к IAM и к разделению привилегий [2]. Для контроля целостности и расследований необходимо журналирование, а значит, архитектура должна предусматривать сбор логов с ключевых узлов и их хранение в защищённом виде, что соответствует подходам NIST к мониторингу и реагированию [3], [4].

Важным архитектурным решением является выделение критичных «опорных» систем, компрометация которых приводит к масштабным последствиям. Обычно это контроллеры домена, системы виртуализации, почтовая инфраструктура, системы управления доступом, репозитории резервных копий. Для них должны применяться усиленные меры: отдельные административные сегменты, строгая MFA, ограничение доступа по устройствам, повышенное журналирование и мониторинг. Такой подход соответствует идее, что защита должна быть пропорциональна критичности активов и рискам [13].

В конце главы можно сделать вывод, что архитектура защиты корпоративной среды должна строиться как связанная система мер, где сегментация сети ограничивает распространение атак, защита конечных устройств снижает вероятность первичного проникновения и закрепления, DLP уменьшает риск утечек через типовые каналы, а резервное копирование обеспечивает устойчивость и возможность восстановления после инцидентов. Согласование этих компонентов с управлением доступом, криптографией и

журналированием позволяет создать целостную модель защиты. Далее необходимо перейти к плану внедрения, поскольку даже хорошо спроектированная архитектура не будет работать без регламентов, обучения персонала, метрик эффективности и регулярного аудита.

2.3 План внедрения и оценка эффективности: регламенты, обучение персонала, показатели результативности и аудит

Переход от архитектуры защиты к реальной системе безопасности всегда связан с внедрением, а внедрение в корпоративной среде почти никогда не бывает «быстрым и идеальным». Ограничения бюджета, сопротивление изменениям, зависимость от подрядчиков и устоявшиеся привычки сотрудников делают этот этап самым сложным. Поэтому план внедрения должен быть поэтапным, ориентированным на риски и подкреплённым организационными документами. Такой подход соответствует идее постоянного улучшения в системах менеджмента информационной безопасности: меры вводятся, проверяются, корректируются и развиваются [1]. Кроме того, внедрение должно учитывать нормативные требования, особенно если организация обрабатывает персональные данные и обязана документировать часть процессов [27], [21].

Логично начинать внедрение с организационного «каркаса», потому что без него технические решения будут работать непредсказуемо. В первую очередь утверждается политика информационной безопасности и определяется ответственность: кто является владельцем системы, кто отвечает за администрирование, кто за контроль, кто за реагирование на инциденты. Далее разрабатываются регламенты, которые непосредственно поддерживают выбранную архитектуру. Например, для управления доступом нужен регламент предоставления и отзыва прав, включая сроки, согласования и контроль привилегий. Для сегментации сети нужен порядок управления правилами межсетевого взаимодействия и процедура внесения изменений.

Для резервного копирования нужен регламент периодичности, состава копируемых данных, хранения, контроля успешности и тестов восстановления. Для DLP нужен порядок обработки срабатываний и классификации инцидентов. Эти документы не должны быть чрезмерно объёмными, но обязаны быть понятными и применимыми, иначе они останутся «на бумаге» [7].

Далее внедрение целесообразно выстроить по приоритетам риска. На практике первым этапом часто становится усиление контроля учётных записей и удалённого доступа. Сюда относится включение многофакторной аутентификации для критичных сервисов и администраторов, пересмотр групп и прав, запрет общих аккаунтов, внедрение базовых принципов PAM хотя бы на уровне процедур (выделенные админ-аккаунты, отдельные рабочие места администраторов, запрет использования админ-прав для повседневной работы). Этот этап даёт быстрый эффект, потому что большое число атак начинается с компрометации учётных данных [6]. Параллельно стоит наладить управление обновлениями и устранение критичных уязвимостей, особенно в публичных сервисах и в удалённом доступе, поскольку эксплуатация известных уязвимостей остаётся распространённым сценарием [5].

Второй этап логично посвятить сетевой сегментации и защите критичных узлов. Обычно сегментация внедряется постепенно: сначала выделяются серверные зоны и зоны управления, затем ограничиваются межсегментные доступы, после чего вводится более детальная микросегментация для критичных сервисов. Важно, чтобы изменения сопровождались тестированием и взаимодействием с бизнес-подразделениями, иначе можно нарушить работу приложений и получить негатив к службе безопасности. Здесь особенно важен процесс управления изменениями: кто инициирует, кто согласует, как проводится тест, как откатываются изменения при проблемах. Надёжность и управляемость программных и инфраструктурных изменений рассматривается как

существенный фактор функциональной безопасности, поскольку ошибки изменений сами по себе могут стать причиной инцидента или простоя [18].

Третий этап включает внедрение и настройку средств мониторинга и реагирования. Практически это означает определение перечня источников логов, настройку журналирования на серверах и сетевых устройствах, организацию централизованного хранения и базовую корреляцию событий. Даже если полноценная SIEM недоступна, можно начать с централизованного сбора логов и настройки ключевых оповещений: подозрительные входы, множественные ошибки аутентификации, создание новых привилегированных аккаунтов, отключение средств защиты, массовое изменение файлов. Параллельно разрабатывается план реагирования на инциденты: каналы связи, роли, порядок эскалации, шаблоны отчётов и минимальный набор действий для типовых сценариев (фишинг, заражение рабочей станции, подозрение на утечку, вымогатель). Такая подготовка прямо соответствует рекомендациям по incident handling, где подчёркивается ценность заранее отработанных процедур [4].

Четвёртый этап связан с DLP и управлением данными. Здесь важно внедрять контроль аккуратно, начиная с режима мониторинга и анализа реальных потоков данных. Затем вводятся политики для наиболее критичных категорий данных, например персональных данных и коммерческой тайны. Одновременно стоит пересмотреть права доступа к файловым ресурсам и внедрить понятные правила хранения документов, иначе DLP будет «ловить» последствия хаоса, а не предотвращать утечки. В контексте 152-ФЗ и практики Роскомнадзора важно, чтобы организация могла показать, какие меры применяются для защиты персональных данных и как контролируются инциденты, связанные с их обработкой [27], [25]. Поэтому DLP и регламенты обработки инцидентов логично увязывать с контуром защиты персональных данных.

Пятый этап, который должен идти параллельно почти со всеми предыдущими, это развитие резервного копирования и устойчивости. Здесь внедрение включает не только настройку расписаний, но и изоляцию репозиториев, ограничение доступа, контроль целостности, шифрование и регулярные тесты восстановления. Тесты восстановления особенно важны, потому что «успешный бэкап» в отчёте не гарантирует, что система реально поднимется после инцидента. В рекомендациях по реагированию подчёркивается, что восстановление и возврат к нормальной работе должны быть заранее спланированы и проверены [4]. Для бизнеса это выражается в достижении согласованных RTO/RPO для критичных сервисов.

Отдельным блоком плана внедрения должно быть обучение персонала и повышение осведомлённости. Практика показывает, что значительная доля инцидентов начинается с фишинга или ошибок сотрудников, а значит, обучение даёт прямой эффект на снижение вероятности реализации угроз [6]. Обучение должно быть регулярным и прикладным: как распознавать фишинг, как проверять ссылки и вложения, как работать с корпоративными данными, что делать при подозрительном письме или при потере устройства. Для ИТ-администраторов и разработчиков обучение должно быть глубже и включать вопросы безопасной конфигурации, управления обновлениями, логирования, безопасной разработки. Уязвимости приложений, описываемые в OWASP, часто возникают из-за недостатка практик безопасной разработки и контроля изменений, поэтому обучение разработчиков и внедрение проверок в жизненный цикл разработки являются важной частью общей защиты [5].

Чтобы внедрение было управляемым, необходимо заранее определить показатели результативности и эффективности. В ISO/IEC 27001 подчёркивается необходимость мониторинга и измерения, а также оценки эффективности мер [1]. В корпоративной практике можно использовать несколько групп показателей. Первая группа отражает состояние базовой гигиены: доля устройств с актуальными обновлениями, доля пользователей с

MFA, количество учётных записей с привилегиями, процент успешных резервных копий и результаты тестов восстановления. Вторая группа отражает операционную безопасность: время обнаружения инцидента, время реакции, количество критичных уязвимостей, среднее время их устранения. Третья группа отражает человеческий фактор: результаты фишинговых тестов, доля сотрудников, прошедших обучение, количество обращений в ИБ по подозрительным событиям. Четвёртая группа может отражать соответствие требованиям: наличие актуальных моделей угроз и документов по ИСПДн, результаты внутренних проверок, выполнение обязательных мер [21]. Важно, чтобы показатели не превращались в «отчёт ради отчёта», а использовались для корректировки мер и планирования следующего цикла улучшений.

Завершающим элементом является аудит и контроль. Аудит можно рассматривать на двух уровнях: внутренний контроль и внешние проверки. Внутренний аудит включает регулярную проверку выполнения регламентов, анализ прав доступа, проверку журналов, контроль резервного копирования, тестирование процедур реагирования. Внешний аудит может быть связан с сертификацией по ISO/IEC 27001 или с проверками регуляторов по персональным данным. В любом случае аудит важен как механизм обратной связи: он выявляет разрыв между тем, что «задумано», и тем, что реально выполняется [11], [25]. Особенно полезны практические проверки, например учения по реагированию на инциденты и тестовые восстановления из резервных копий, потому что они показывают реальную готовность, а не формальное наличие документов [4].

В конце главы можно сделать вывод, что план внедрения комплекса мер защиты должен быть поэтапным и риск-ориентированным, начиная с усиления контроля доступа и базовой гигиены, затем переходя к сегментации и защите критичных узлов, мониторингу и реагированию, DLP и управлению данными, а также устойчивости через резервное копирование. Эффективность внедрения обеспечивается регламентами, обучением персонала, измеримыми

показателями результативности и регулярным аудитом, который позволяет корректировать систему и поддерживать её актуальность. Такой подход завершает практическую часть работы и позволяет перейти к обобщающим выводам.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы была рассмотрена тема современных методов защиты информации в корпоративных системах с акцентом на сочетание нормативных требований, управленческих подходов и практических технических решений. Актуальность темы подтверждается тем, что корпоративные инфраструктуры усложняются за счёт гибридных моделей, удалённой работы и роста числа цифровых сервисов, а характер угроз смещается в сторону комплексных атак, использующих компрометацию учётных данных, уязвимости публичных компонентов и вредоносное ПО, включая вымогателей [6]. В результате защита должна строиться не как единичная мера, а как управляемая система, ориентированная на риски и непрерывное улучшение [1].

По результатам первой главы было показано, что корпоративная информационная система является многокомпонентным объектом защиты, включающим данные, сервисы, инфраструктуру и идентичности пользователей. Определение активов, анализ угроз и построение модели нарушителя позволяют перейти от общего понимания «опасностей» к конкретным сценариям атак и к приоритизации мер. Было также обосновано, что существенную роль играют не только внешние атакующие, но и внутренние факторы, включая ошибки сотрудников и инсайдерские риски, что требует сочетания технических и организационных мер [7]. Нормативно-правовые основы, включая требования 149-ФЗ и 152-ФЗ, а также подзаконные акты и методические документы, задают минимальные обязательные рамки защиты, особенно в части обработки персональных данных [27], [21]. Дополнительно стандарты ISO/IEC 27001/27002 и рекомендации NIST помогают выстроить управляемую систему мер и процессов, включая оценку рисков и реагирование на инциденты [2], [4].

Во второй главе был предложен практический подход к проектированию комплекса мер защиты, начинающийся с анализа исходного состояния: инвентаризации активов, классификации данных и определения критериев риска. Обосновано, что именно риск-ориентированная оценка позволяет выбрать меры, которые дают максимальный эффект для конкретной организации и её критичных сервисов [24]. На основе этого была разработана логическая архитектура защиты, включающая сетевую сегментацию как средство ограничения распространения атак, защиту конечных устройств как ключевого «фронта» против фишинга и вредоносного ПО, DLP как инструмент снижения риска утечек, а также резервное копирование и восстановление как основу устойчивости к инцидентам и сбоям [3], [4]. Отдельно подчёркнута необходимость увязки технических решений с управлением доступом и криптографической защитой, а также с журналированием и мониторингом.

В рамках плана внедрения показано, что успешная реализация комплекса мер требует поэтапного подхода, разработки регламентов, обучения персонала и внедрения измеримых показателей результативности. Регулярный аудит и практические проверки, включая тесты восстановления и учения по реагированию, рассматриваются как механизм поддержания актуальности защиты и устранения разрыва между формальными требованиями и реальной практикой [1], [4]. Таким образом, ответ на исследовательский вопрос о том, какие современные методы защиты наиболее целесообразны для корпоративных систем и как их обосновать, заключается в следующем: наибольший эффект даёт комплексная модель, где управление идентичностью и доступом, криптография, сегментация, защита конечных устройств, контроль утечек, мониторинг и реагирование объединены в единую архитектуру и поддерживаются организационными процессами управления рисками и постоянного улучшения. Такой подход позволяет одновременно повысить устойчивость корпоративной системы к актуальным угрозам,

выполнить требования нормативной базы и обеспечить управляемость безопасности на уровне организации.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.

2. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO, 2022.

3. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.

4. NIST Special Publication 800-61 Rev. 2. Computer Security Incident Handling Guide. Gaithersburg: NIST, 2012.

5. OWASP Top 10:2021. The Ten Most Critical Web Application Security Risks [Электронный ресурс]. URL: https://owasp.org/www-project-top-ten/ (дата обращения: 03.04.2026).

6. Verizon. Data Breach Investigations Report 2024 [Электронный ресурс]. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата обращения: 03.04.2026).

7. Астахов А. М. Искусство управления информационной безопасностью. 2-е изд., перераб. и доп. М.: ДМК Пресс, 2020. 512 с.

8. Белов В. А., Лось В. П. Информационная безопасность: учебник для вузов. М.: Юрайт, 2021. 530 с.

9. Гайкович В. Ю. Основы построения защищённых корпоративных сетей. СПб.: Питер, 2019. 384 с.

10. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. М.: Стандартинформ, 2017.

11. ГОСТ Р ИСО/МЭК 27001–2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.

12. ГОСТ Р ИСО/МЭК 27002–2021. Информационные технологии. Методы и средства обеспечения безопасности. Кодекс практик по мерам информационной безопасности. М.: Стандартинформ, 2021.

13. Гребенников А. В. Управление рисками информационной безопасности: подходы, методы, практика. М.: КНОРУС, 2020. 256 с.

14. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646.

15. Касперский. Отчёты о киберугрозах и аналитика (Threat Research) [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases (дата обращения: 03.04.2026).

16. Котенко И. В., Саенко И. Б. Интеллектуальные технологии обнаружения атак в компьютерных сетях. СПб.: Наука, 2018. 368 с.

17. Криптографическая защита информации: учебное пособие / под ред. В. В. Лаврова. М.: Горячая линия — Телеком, 2020. 312 с.

18. Липаев В. В. Надёжность и функциональная безопасность программных средств. М.: СИНТЕГ, 2019. 432 с.

19. Методические документы ФСТЭК России. Банк данных угроз безопасности информации [Электронный ресурс]. URL: https://bdu.fstec.ru/ (дата обращения: 03.04.2026).

20. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

21. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

22. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам криптографической защиты информации,

используемым для защиты информации, не содержащей сведения, составляющие государственную тайну».

23. Р 50.1.056–2005. Техническая защита информации. Основные термины и определения. М.: Стандартинформ, 2005.

24. Р 50.1.053–2005. Информационная технология. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности. М.: Стандартинформ, 2005.

25. Роскомнадзор. Требования и разъяснения по вопросам обработки персональных данных [Электронный ресурс]. URL: https://rkn.gov.ru/personal-data/ (дата обращения: 03.04.2026).

26. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

27. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

28. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

29. Cisco. Zero Trust Security: Principles and Architecture [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/products/security/zero-trust.html (дата обращения: 03.04.2026).

30. Microsoft. Zero Trust guidance and resources [Электронный ресурс]. URL: https://www.microsoft.com/security/business/zero-trust (дата обращения: 03.04.2026).