Проектирование защищенной информационной системы с использованием программного комплекса ViPNet

Андреев А.Н.
информатика
3 курс, Многопрофильный колледж ФГБОУ ВО «ТГТУ», г.Тамбов, Тамбовской области
Научный Руководитель: Мосягина Н.Г., Многопрофильный колледж ФГБОУ ВО «ТГТУ», г. Тамбов, Тамбовской области

ВВЕДЕНИЕ

В современном цифровом пространстве даже небольшие организации, такие как индивидуальные предприниматели, сталкиваются с необходимостью обеспечения надёжной защиты информации. Коммерческие данные, персональные данные сотрудников и клиентов, финансовая документация и доступ к государственным сервисам требуют создания безопасной информационной системы. Одним из наиболее распространённых решений для построения защищённой сетевой инфраструктуры является комплекс программно-аппаратных средств ViPNet от компании «ИнфоТеКС».

Цель данного технологического проекта – разработать и описать технологическое решение по внедрению защищённой ИС в небольшой компании на примере условной ИП «Авангард», оказывающей услуги по бухгалтерскому сопровождению малых предприятий. Организация использует один офис, три рабочих места и удалённый доступ к бухгалтерским сервисам и клиентским базам, расположенным в облаке. Основная задача – обеспечить защищённый обмен данными между офисом и удалёнными ресурсами, а также организовать безопасную внутреннюю сеть с контролируемым доступом.

1.Основная часть

1.1 Анализ защищённости информационной системы

Анализ защищённости информационной системы небольшой организации всегда начинается с оценки того, какие данные обрабатываются, какие операции выполняются и какие технологические процессы наиболее критичны. В случае ИП «Авангард», занимающегося бухгалтерским сопровождением, ключевыми активами являются персональные данные клиентов, финансовая документация, учетные базы, а также доступ к облачным сервисам и государственным информационным ресурсам. Именно они формируют ядро информационной системы, и любые нарушения их целостности, доступности или конфиденциальности могут привести к серьёзным последствиям: нарушениям законодательства, утрате доверия клиентов или остановке деятельности.

Угрожающие факторы для ИП условно делятся на три группы: внешние, внутренние и технологически обусловленные. Внешние угрозы для малой организации, несмотря на компактность инфраструктуры, остаются значимыми: злоумышленники используют автоматизированные сканеры уязвимостей, массовые атаки через интернет, фишинговые рассылки и подбор слабых паролей. Поскольку ИП активно работает с облачными сервисами, одним из вероятных каналов атаки является перехват трафика или попытка подмены удалённого ресурса. Отсутствие защищённого канала между офисом и облаком создаёт пространство для MITM-атак (атак «человек посередине»), внедрения вредоносного кода или перехвата аутентификационных данных.

Не менее важную роль играют внутренние угрозы. В малых организациях нередко отсутствует полноценное разделение доступа, сотрудники используют одинаковые или слабые пароли, а файлы могут перемещаться на личные устройства. Это повышает вероятность случайной утечки данных. Помимо непреднамеренных действий персонала, существует и риск злоумышленного поведения, например попытка копирования клиентской базы перед увольнением. Отдельно стоит учитывать угрозы, связанные с внешними подрядчиками – мастерами по обслуживанию компьютеров, временными работниками или

сторонними бухгалтерами, которые получают доступ к информации в период выполнения задач.

Технологические угрозы возникают из-за особенностей ИТ-инфраструктуры. Даже небольшая компания использует офисную сеть, точки Wi-Fi, а также персональные компьютеры, которые могут содержать уязвимости. Неправильная конфигурация роутера, отсутствие обновлений Windows или устаревшие антивирусные базы создают благоприятные условия для внедрения вредоносных программ. Одним из частых сценариев атак на малый бизнес является шифрование данных вымогателями, которые проникают в систему через электронную почту. В ИП «Авангард» такая угроза особенно критична, поскольку потеря бухгалтерских баз приведёт к полной невозможности ведения деятельности.

Анализируя источники угроз, можно выделить несколько наиболее вероятных. Прежде всего, это внешние злоумышленники, осуществляющие автоматизированные сетевые атаки. Их цель – получить доступ к корпоративной сети или украсть учетные данные. Второй источник – недобросовестные сотрудники или лица, имеющие ограниченный физический доступ к технике. Третий – случайные пользователи или посетители офиса, которые могут подключиться к незащищённой сети Wi-Fi или получить доступ к незаблокированному ПК. Кроме того, источником угроз являются поставщики программного обеспечения и облачных сервисов, если их инфраструктура или политика безопасности недостаточно надёжна.

По характеру происхождения угрозы делятся на техногенные, антропогенные и природные. Для ИП техногенные включают аппаратные отказы – сбой жесткого диска, выход из строя сетевого оборудования, повреждение файлов вследствие критических ошибок. Антропогенные угрозы – это ошибки пользователей, фишинг, неправильная настройка устройств, халатность при работе с конфиденциальными данными. Природные угрозы (пожары, затопления, перепады напряжения) менее вероятны, но для малого офиса без

качественного электропитания риски повреждения техники остаются актуальными.

Идентифицированные слабые места ИС: отсутствие защищённых каналов к облаку, слабые и единые учётные данные сотрудников, недостаточное разграничение доступа, уязвимые рабочие станции, риск фишинга/вредоносного ПО, отсутствие централизованного контроля и логирования, а также риски аппаратных отказов и физического доступа.

1.2 Разработка системы защиты информации с использованием программно- аппаратных средств защиты информации

Выстроим последовательную стратегию закрытия выявленных проблем средствами программного комлекса ViPNet и сопутствующей практикой.

1.2.1 Защита каналов связи

Это предотвращение MITM, перехвата трафика и незашифрованного доступа к облаку

Решение строится на развёртывании ViPNet Coordinator в офисе и организации защищённых «доменных» туннелей между Coordinator и удалёнными узлами провайдера / облака. Coordinator выполняет роль криптографического шлюза и централизованного элемента управления, что позволяет обеспечить взаимную аутентификацию узлов и шифрование всего трафика между доверенными точками. Практические шаги: установить Coordinator (физический HW- или виртуальный образ), создать защищённый домен, включить генерацию и распространение регистрационных пакетов для каждого удалённого узла; на стороне облака развёрнуть ViPNet-узел провайдера и подписать его в том же домене. После этого все соединения между офисом и облачными сервисами проходят через криптотуннель ViPNet, что исключает простую подмену сервера или перехват сессий. Это решение – базовая контрмера против MITM и сетевого прослушивания (рисунок 1).

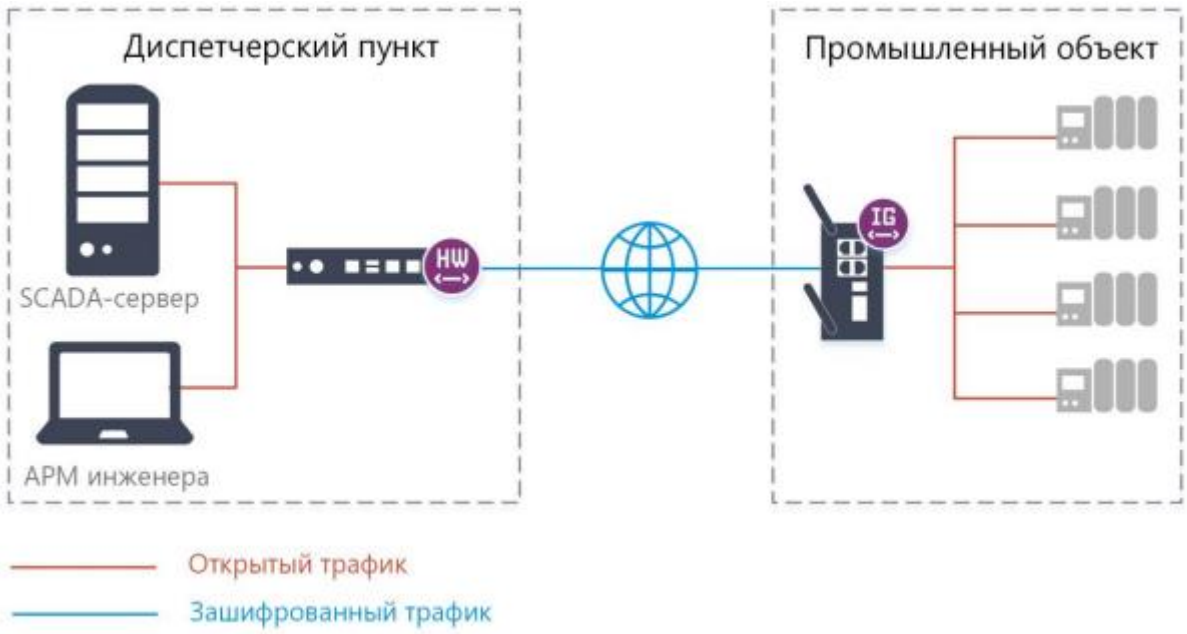

Рисунок 1 – Схема туннелирования

Практическая конфигурация (пример для бухгалтера): сгенерировать регистрационный файл на Coordinator → передать сотруднику (через защищённый переносной носитель или защищённый e-mail) → импорт в ViPNet Client → в Coordinator создать политику доступа, ограничивающую маршруты только к IP/домену бухгалтерского облака и протоколам (например, HTTPS). В результате трафик к облаку идёт исключительно по защищённому туннелю. [2]

1.2.2 Аутентификация и управление ключами

Исключаем «подбор пароля» и уязвимости учётных записей.

ViPNet использует централизованное управление ключами и сертификатами (CSP/Coordinator) – это позволяет перевести аутентификацию пользователей с паролей на криптографические идентификаторы (ключи/контейнеры), которые сложнее украсть или подобрать. Практика: запретить доступы по простым паролям к критическим ресурсам, выдать каждому пользователю уникальный криптоконтейнер (PKI/ключ), настроить политику срока действия ключей и процедуру отзыва при увольнении. Включение взаимной аутентификации (cert-based) делает невозможным подмену узлов без действительного ключа. Для соответствующих утверждений и процедур опираемся на документацию и политику безопасности ViPNet Crypto Core. [2]

Практическое правило: при приеме сотрудника генерируем ключ на Coordinator, оформляем регистрацию и загружаем в клиент; при увольнении – немедленно аннулируем ключ на Coordinator и удаляем ключевой контейнер (через политику удаления/блокировки), тем самым закрывая доступ в течение минут – без смены паролей на всех ресурсах (рисунок 2).

Рисунок-схема создания ключей шифрования и идентификации ViPNet

1.2.3 Разграничение доступа и сегментация сети

ViPNet позволяет задавать политики доступа между узлами/группами (зоны/роли). Для ИП «Авангард» целесообразно создать как минимум две зоны: «бухгалтерия» и «руководство», а также отдельную гостевую зону для интернета/посетителей. На Coordinator создаются политики, разрешающие только необходимые соединения: бухгалтерам – доступ к бухгалтерскому облаку и внутренним финансовым ресурсам; руководителю – расширенный набор. Дополнительно на Coordinator можно ограничивать маршруты и сервисы (белые списки IP/портов), чтобы даже в случае заражения рабочей станции вредоносный трафик не уходил в произвольном направлении. [3]

Практическая мера: реализовать «принцип наименьших привилегий» через политики ViPNet, прописав explicit allow-only правила и запретив межзоновые

соединения по умолчанию. Это уменьшает последствия компрометации одного узла для всей ИС (рисунок 3).

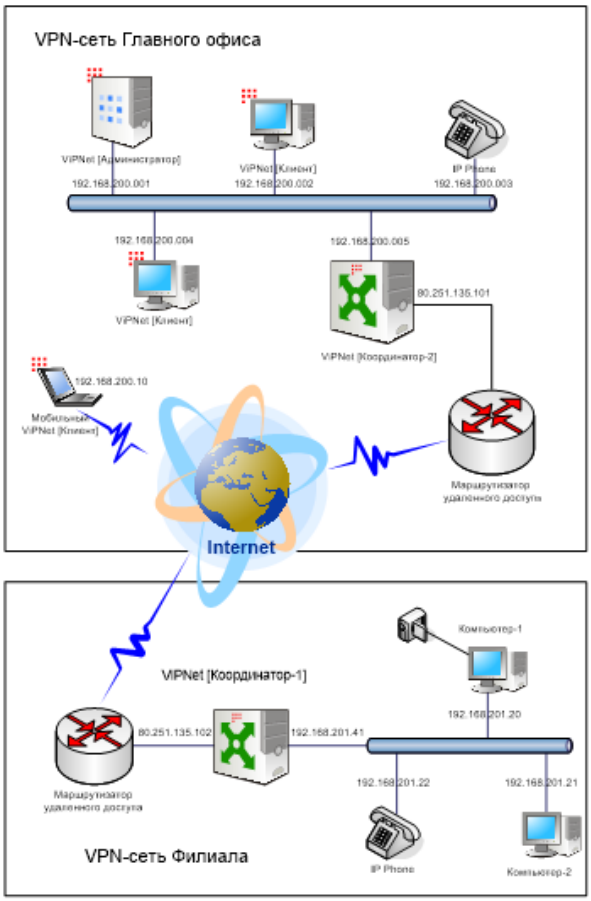

Рисунок 3 – Примерная схема сегментации сети

1.2.4 Борьба с фишингом и кражей учётных данных

Фишинг на уровне почты нельзя полностью закрыть только VPN-мирами, но ViPNet снижает риск успешной атаки: во-первых, за счёт того, что доступ к критичным ресурсам возможен только через криптотуннель и по сертификату; во-вторых, при использовании дополнительных корпоративных политик (например, доступ к бухгалтерскому облаку только с защищённых машин, привязка ключей к устройствам). Практические шаги: запретить доступ к внутренним сервисам извне без ViPNet (закрыть публичные порты), включить контроль списка устройств (Device-binding) – т.е. ключи привязывать к конкретным рабочим станциям, и обязать сотрудников использовать двухфакторную аутентификацию для порталов, где это возможно. Также важно

обучение персонала (phishing tests) и централизованное обновление почтовых фильтров (рисунок 4). [3]

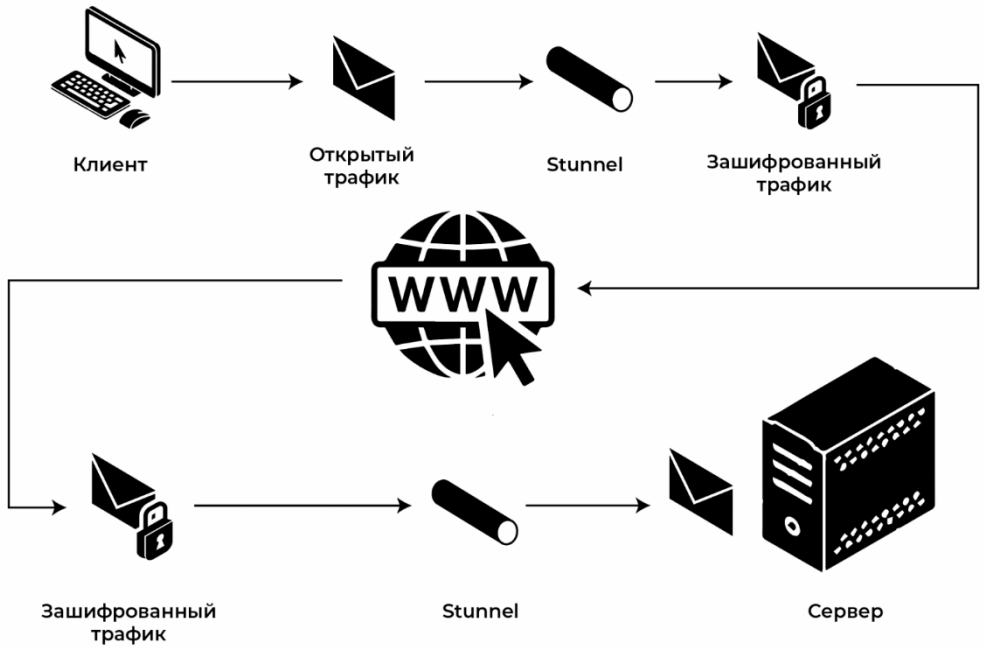

Рисунок 4 – Принцип крипто туннелирования

1.2.5 Защита рабочих станций от вредоносного ПО

ViPNet Client предоставляет дополнительные функции шифрования локальных областей и работы с защищёнными контейнерами; это помогает ограничить доступ вредоносного ПО к хранилищу чувствительных данных. Для уменьшения риска шифрования баз данных рекомендуется комбинировать ViPNet с полноценным EDR/антивирусом: настроить политику, при которой критичные серверы и рабочие станции доступны в сеть только при наличии актуального статуса защиты (интеграция с SIEM/EDR). Практический набор мер: включить контроль обновлений ОС, централизованно управлять антивирусом, ограничить права пользователей (не давать административных прав), запретить запуск неизвестного ПО (whitelisting). ViPNet поможет тем, что даже при заражении внешняя передача данных будет ограничена политиками туннеля (рисунок 5). [1]

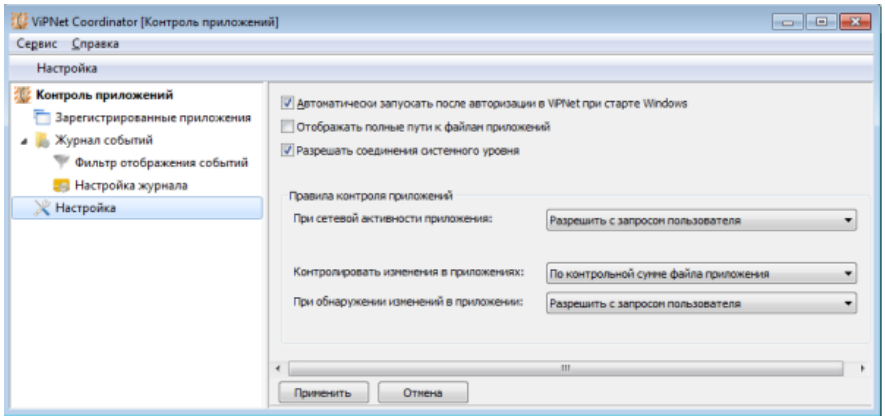

Рисунок 5 – Контроль приложений ViPNet

1.2.6 Логирование, мониторинг и реагирование

ViPNet генерирует события безопасности (TIAS/системные логи), которые можно экспортировать в централизованную систему мониторинга/SIEM по протоколу syslog. Для ИП достаточно настроить автоматический экспорт логов событий доступа, отказов аутентификации, ошибок ключей и изменений политик на локальный SIEM или даже на облачный лог-менеджер. Это позволит фиксировать попытки несанкционированного доступа и быстро реагировать (аннулировать ключи, заблокировать узел). Практическая последовательность: на Coordinator включаем экспорт TIAS/syslog → настроить прием в SIEM/KUMA/другой лог-сервис → создать простые корреляции (повторные неуспешные аутентификации, изменение конфигурации) (рисунок 6). [1]

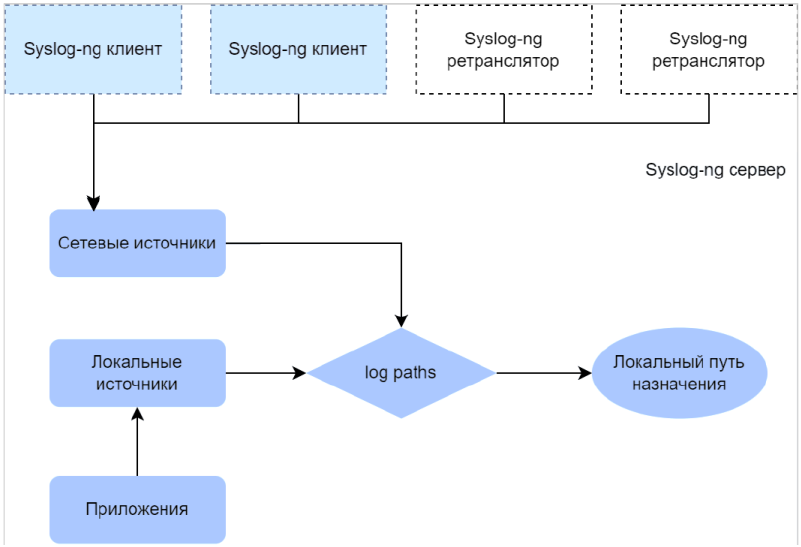

Рисунок 6 – Syslog-ng клиент и его схема

1.2.7 Защита от аппаратных отказов и обеспечение резервирования

Чтобы снизить риск потери данных из-за отказа диска или сетевого оборудования, ViPNet-координатор можно развернуть с резервированием (если оборудование/лицензия позволяют – настроить отказоустойчивость). Там, где Coordinator развёрнут в облаке или у провайдера, учесть ограничения (некоторые облачные VA имеют функциональные ограничения по экспорту/функциям). Практические рекомендации: регулярное резервное копирование конфигурации Coordinator и ключевых контейнеров в защищённое хранилище; настройка failover/MultiWAN (если поддерживается моделью Coordinator) для обеспечения связи через альтернативный канал. Это критично для поддержания доступности сервисов. [4]

1.3 Политики обновлений и поддержка актуальности криптографии

Регулярно обновлять версии ViPNet Client/Coordinator и следить за рекомендациями по криптополитикам (включая требования к алгоритмам и параметрам). ViPNet имеет документированную политику криптографии и механизмы инициализации ключей – следовать ей при ротации ключей и резервном копировании.

Практическое требование: установить график обновлений (минимум ежемесячный контроль патчей), автоматизировать обновления клиента (если возможно), тестировать обновления в тестовой среде перед внедрением в продуктив. [1]

ViPNet эффективно закрывает каналы и обеспечивает криптографическое разграничение, но для комплексной защиты требуется «слоевая» архитектура: интегрировать ViPNet с EDR/антивирусом, внедрить MFA для административных порталов, организовать регулярные бэкапы баз и конфигураций, прописать регламенты на случай инцидента (роли/ответственности, чек-листы). Это уменьшит как вероятность инцидента, так и время восстановления. [4]

ЗАКЛЮЧЕНИЕ

Современные информационные системы даже небольших организаций и индивидуальных предпринимателей требуют надёжной защиты, так как число киберугроз постоянно растёт. ViPNet предоставляет комплексный и удобный инструментарий для построения безопасной инфраструктуры: защищённые каналы связи, шифрование данных, контроль доступа и централизованное управление. Благодаря готовым шаблонам, понятным интерфейсам и сертифицированным криптографическим алгоритмам система позволяет эффективно защищать трафик, рабочие станции и серверы без необходимости глубоких технических знаний.

Использование ViPNet обеспечивает предпринимателю соответствие требованиям законодательства, минимизирует риски несанкционированного доступа и упрощает администрирование сети. Решение легко масштабируется, работает устойчиво даже при распределённой структуре и обеспечивает сквозную защиту между всеми узлами. В результате ViPNet выступает как надёжная, современная и достаточно простая в эксплуатации основа для построения информационной безопасности в малом бизнесе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. InfoTeCS. Официальный сайт — материалы, описания и документация по ViPNet. — Режим доступа: https://www.infotecs.ru/

2. Криптографические методы защиты информации / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва: Юрайт, 2024. — 309 с. — ISBN 978-5-534-02574-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536453

3. Криптографические методы защиты информации для изучающих компьютерную безопасность / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., Москва: Юрайт, 2024. — 473 с. — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132

4 Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва: Юрайт, 2025. — 312 с. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562070