Содержание:

ВВЕДЕНИЕ

В настоящее время невозможно представить себе серьезную компанию, не использующую в своей работе современные информационные технологии для ведения бизнеса. Одной из непременных составляющих данных технологий является объединение вычислительных ресурсов компании в единую распределенную корпоративную сеть.

Проблема информационной безопасности в корпоративных сетях передачи данных сегодня очень остро стоит перед компаниями любого уровня. Утечка критически важной корпоративной информации, рост объемов паразитного трафика, вымогательство, шантаж и заказные атаки на информационные ресурсы стали в последнее время частым явлением.

Все это обуславливает актуальность темы данной магистерской диссертации, практическое значение которой заключается в разработке конкретных рекомендаций по повышению эффективности защиты информации в распределенной корпоративной сети производственного предприятия.

Объектом диссертации является корпоративная сеть передачи данных научно-производственного холдинга НПО «Ассоциация К».

Предметом диссертации являются методы и средства повышения эффективности защиты информации в распределенной сетевой инфраструктуре.

Цель работы — сформировать перечень конкретных рекомендаций, реализация которых позволит повысить уровень информационной безопасности исследуемого предприятия.

Для достижения поставленной цели в работе должны быть решены следующие задачи:

- раскрытие теоретических аспектов, понятий и методов, специфики защиты информации в корпоративных сетях передачи данных;
- построение модели безопасной корпоративной сетевой инфраструктуры;

- исследование существующей ИТ-инфраструктуры предприятия, используемых средств и методов ее защиты;
- проведение анализа рисков информационной безопасности;
- разработка рекомендацию по повышению уровня защищенности корпоративной сети и оценка их эффективности.

Для решения вышеупомянутых задач следует полагаться на литературу известных специалистов в области информационной безопасности, а также на рекомендации по построению защищенных инфраструктур мировых производителей сетевого оборудования и программного обеспечения.

Диссертация состоит из введения, четырех глав, имеющих подразделы, заключения и приложения, представляющего собой полный отчет MSAT.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

1.1 Принцип многоуровневой защиты в построении архитектур информационной безопасности

Непрерывно изменяющаяся ситуация в сфере информационной безопасности постоянно ставит перед организациями новые задачи. Быстрое распространение вирусов и шпионских программ, постоянное усложнение сетевых атак, тревожащий рост организованной киберпреступности и шпионажа с использованием Интернета, хищение персональных данных и конфиденциальной информации, более сложные способы инсайдерских атак, развитие новых форм угроз для мобильных систем — вот лишь несколько примеров многообразия и сложности реальных угроз, формирующих современный ландшафт безопасности.

Поскольку сети являются ключевым механизмом ведения бизнеса, при их проектировании и реализации необходимо учитывать проблемы безопасности, чтобы гарантировать конфиденциальность, целостность и доступность данных и системных ресурсов, поддерживающих основные бизнес-процессы компании.

В наши дни для достижения приемлемого уровня безопасности уже не достаточно развернуть точечные продукты на периметре сети. Сложность и изощренность современных угроз требует внедрения интеллектуальных совместно работающих механизмов безопасности во все элементы распределенной инфраструктуры. С учетом этих соображений все чаще используется подход глубокой многоуровневой (эшелонированной) защиты, согласно которому множество уровней защиты распределены по стратегически важным элементам по всей сети и действуют в рамках унифицированной стратегии[1]. Информация о событиях и состоянии систем согласованно используется различными элементами системы информационной безопасности, что позволяет обеспечить более надежный контроль состояния ИТ-инфраструктуры, а ответные действия координируются в рамках общей стратегии управления.

Этот подход предусматривает модульный принцип построения системы информационной безопасности, что позволяет ускорить развертывание и способствует внедрению новых решений и технологий по мере развития потребностей бизнеса. Такая модульность расширяет срок использования имеющегося оборудования и обеспечивает защиту произведенных капитальных вложений. В то же время предусмотрен набор инструментальных средств, упрощающих повседневную эксплуатацию и обеспечивающих снижение совокупных эксплуатационных расходов.

Вышеописанный модульный подход удобно рассмотреть на примере архитектуры безопасности корпоративных сетей — Security Architecture for Enterprise Networks (SAFE), разработанной компанией Cisco — крупнейшим производителем сетевого оборудования[2]. Эта архитектура основана на концепции Cisco Security Framework (CSF), которая обуславливает выбор продуктов и функций, обеспечивающих максимальный уровень безопасности, контроля и управления ИТ-инфраструктурой. Данная концепция предусматривает способы выявления текущих направлений угроз, а также отслеживания новых и развивающихся угроз за счет следования лучшим практическим рекомендациям и использования комплексных решений.

Согласно концепции CSF, необходимо по результатам анализа угроз и рисков разработать такие политики безопасности, которые будут способствовать достижению организацией поставленных бизнес-целей и плановых показателей. Алгоритм разработки таких политик следующий:

1. определить бизнес-цели и задачи организации;

2. выявить возможные угрозы для выделенных целей и задач (пример такого соответствия представлен в таблице 1.1);
3. выполнить более глубокий анализ угроз и рисков для определения важности ресурсов, используемых в среде;
4. проанализировать возможные риски безопасности для этих ресурсов;
5. оценить возможное действие нарушений безопасности на бизнес.

Таблица 1.1 - Бизнес-цели, задачи и возможные угрозы

Защита источников дохода	Прерывание бизнеса вследствие нарушения безопасности может повлечь за собой немедленные и долговременные потери доходов.
Соответствие требованиям заказчиков	Несоответствие ожиданиям заказчиков в части конфиденциальности, безопасности и уровней обслуживания может привести к серьезным убыткам.
Защита корпоративной идентификационной информации и бренда	Раскрытие конфиденциальных данных может разрушить тщательно спланированные маркетинговые кампании и повредить репутации бренда.
Соблюдение требований нормативных документов и стандартов	Недостаточное соответствие нормативно-правовым требованиям может привести к отзыву лицензий, потере бизнеса, денежным взысканиям и к более серьезным юридическим последствиям.

Результатом этих шагов является создание политик безопасности и формулирование принципов, которыми определяется приемлемое и безопасное использование каждого сервиса, устройства и системы в рамках ИТ-инфраструктуры организации. В свою очередь, политики безопасности определяют процессы и процедуры, необходимые для достижения бизнес-целей и выполнения задач. Совокупность процессов и процедур определяет операции по обеспечению безопасности. Схематическое изображение этого процесса представлено на рисунке 1.1.

Бизнес-релевантность

Политики безопасности

Факторы безопасности

Функции безопасности

Бизнес-цели и задачи

Угрозы достижению целей и задач

Действия в сфере безопасности

Анализ рисков и угроз

Управление

Контроль

Идентификация

Мониторинг

Корреляция

Повышение устойчивости

Изоляция

Обеспечение выполнения

Рис. 1.1. Графическое представление концепции CSF

Политики безопасности будут настолько эффективны, насколько они улучшают контроль и управление (безопасность — есть функция контроля и управления): без контроля невозможно управление, а без управления нет безопасности. На практике это выражается в выборе условий и методов развертывания платформ и функций для достижения требуемого уровня контроля и управления. В таблице 1.2 представлены шесть мер обеспечения безопасности, которые обеспечивают выполнение политик безопасности и расширяют возможности по контролю и управлению.

Таблица 1.2 - Меры обеспечения безопасности

Контроль	*Идентификация*	Идентификация и классификация пользователей, сервисов, трафика и оконечных устройств.
	Мониторинг	Мониторинг производительности, поведения, шаблонов использования, событий и соответствия политике.
	Выявление взаимозависимостей	Сбор, анализ и выявление взаимозависимостей событий в масштабе системы.
	Повышение устойчивости	Повышение устойчивости оконечных устройств, сервисов, приложений и инфраструктуры.
Управление	*Изоляция*	Изоляция пользователей, систем и сервисов для сдерживания и защиты.
	Обеспечение выполнения	Обеспечение выполнения политики разграничения доступа, политик безопасности и противодействие угрозам безопасности.

Вышеописанную концепцию следует использовать при создании каждого сегмента сети[3]. При этом определяются наиболее подходящие для конкретной среды технологии и практические рекомендации, чтобы можно было выполнить каждую из шести ключевых мер. Эти технологии и функции в масштабах всей сети обеспечивают контроль сетевых операций, реализуют сетевую политику и решают проблемы аномального трафика. Средствами мониторинга и обеспечения выполнения политик являются стандартные элементы сетевой инфраструктуры, такие как маршрутизаторы и коммутаторы.

1.2 Классификация сетевых атак и основные методы защиты от них

Каждую сетевую атаку можно в общем случае разбить на 5 этапов (таблица 1.3). В реальной ситуации некоторые шаги могут быть пропущены.

Таблица 1.3 - Основные классы сетевых атак

Класс сетевой атаки	**Описание класса**
1. Исследование	Получение общей информации о компьютерной системе (КС)
1.1 Социотехника	Получение информации посредством вежливого втирания в доверие по телефону, электронной почте и т.п.
1.2 Непосредственное вторжение	Получение информации посредством физического доступа к оборудованию сети
1.3 Разгребание мусора	Получение информации из мусорных корзин или архивов
1.4 Поиск в WEB	Получение информации из интернета посредством общедоступных поисковых систем
1.5 Изучение WHOIS	Получение информации из регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем
1.6 Изучение DNS зон	Получение информации посредством использования сервиса доменных имен

2. Сканирование	Получение информации об инфраструктуре и внутреннем устройстве КС
2.1 Поиск активных устройств	Получение информации об активных устройствах КС
2.2 Трассировка маршрутов	Определение топологии КС
2.3 Сканирование портов	Получение информации об активных сервисах, функционирующих в КС
3. Получение доступа	Получение привилегированных прав на управление узлами КС
3.1 Переполнение стека	Выполнение произвольного кода в результате вызванного злоумышленником сбоя в программном обеспечении
3.2 Атака на пароли	Подбор паролей из списка стандартных или по специально сгенерированному словарю, перехват паролей
3.3 Атаки на WEB - приложения	Получение доступа в результате эксплуатации уязвимостей в открытых WEB-приложениях КС
3.4 Сниффинг	Получение доступа посредством пассивного (прослушивание) и активного (подмена адресатов) перехвата трафика КС
3.5 Перехват сеанса связи	Получение доступа вследствие перехвата авторизационных данных текущих сеансов пользователей КС

4. Полезная нагрузка	Эксплуатация полученных прав для достижения целей взлома
4.1 Поддержание доступа	Установка систем удаленного администрирования
4.2 DOS-атаки	Вывод из строя устройств и отдельных сервисов КС
4.3 Обработка конфиденциальной информации	Перехват, копирование и/или уничтожение информации
5. Заметание следов	Сокрытие факта проникновения в КС от систем защиты
5.1 Стирание системных логов	Удаление данных архивов приложений и сервисов КС
5.2 Сокрытие признаков присутствия в сети	Туннелирование внутри стандартных протоколов (HTTP, ICMP, заголовков TCP и т.п.)

Рассмотрим основные способы и средства защиты от перечисленных сетевых угроз [4].

Социотехника. Наилучший метод защиты от социотехники — осведомленность пользователя. Необходимо сообщить всем сотрудникам о существовании социотехники и четко определить те виды информации, которые ни под каким предлогом нельзя разглашать по телефону. Если в организации предусмотрены варианты предоставления какой-либо информации по телефону (номеров телефонов, идентификационных данных и др.), то следует четко регламентировать данные процедуры, например, используя методы проверки подлинности звонящего.

Непосредственное вторжение:

- контрольно-пропускной режим (системы контроля доступа, журнал посетителей, бейджи и др.);
- физическая безопасность оборудования (механические, электронные замки);
- блокировка компьютера, хранители экрана;
- шифрование файловой системы.

Разгребание мусора. Хорошо известная всем бумагорезательная машина (шредер) — самая лучшая защита против тех, кто роется в мусорных корзинах. У сотрудников должен быть беспрепятственный доступ к таким машинам, чтобы они могли уничтожить всю сколько-нибудь ценную информацию. Другой вариант: каждому пользователю предоставляется отдельная урна для бумаг, содержащих важные сведения, откуда каждую ночь документы поступают на бумагорезательную машину. Сотрудники должны быть четко информированы о том, как обращаться с конфиденциальной информацией.

Поиск в WEB. Основной способ защиты — неразглашение информации. Нужно сделать необходимым и достаточным перечень информации, подлежащей размещению на публичных ресурсах в сети интернет. Избыточные данные о компании могут «помочь» злоумышленнику в реализации его намерений. Сотрудники должны нести ответственность за распространение конфиденциальной информации. Периодически следует проводить проверку публичной информации собственными силами или с привлечением сторонних компаний.

Изучение WHOIS. Не существует общих способов защиты от получения регистрационных данных злоумышленником. Существуют рекомендации, согласно которым информация в соответствующих базах должна быть как можно более точной и правдоподобной. Это позволяет администраторам различных компаний беспрепятственно связываться друг с другом и способствовать поиску злоумышленников.

Изучение DNS-зон. В первую очередь необходимо проверить, что на DNS-сервере нет утечки данных, которая возникает за счет наличия там лишних сведений. Такими сведениями могут быть имена, содержащие название операционных систем, записи типа HINFO или TXT. Во-вторых, необходимо корректно настроить DNS-сервер, чтобы ограничить передачу зоны. В-третьих, необходимо настроить граничный маршрутизатор таким образом, чтобы доступ к 53-му порту (TCP и UDP) имели только резервные серверы DNS, производящие синхронизацию с

центральным сервером. Также следует использовать разделение внешнего и внутреннего DNS-серверов. Внутренний сервер настраивается таким образом, чтобы он мог разрешать имена только внутренней сети, а для разрешения имен внешней сети используются правила пересылки. То есть внешний DNS-сервер не должен ничего «знать» про внутреннюю сеть.

Поиск активных устройств и трассировка маршрутов. Способ защиты — установка и настройка межсетевых экранов на фильтрацию пакетов таким образом, чтобы отсеивать запросы программ, используемых злоумышленником. Например, блокировка ICMP запросов от ненадежных источников сильно затруднит трассировку.

Сканирование портов. Первое и самое важное — закрытие всех неиспользуемых портов. Например, если вы не используете TELNET, то необходимо закрыть соответствующий порт. При развертывании новой системы, необходимо заранее выяснить используемые ей порты и открывать их по мере необходимости. В особенно важных системах рекомендуется удалить программы, соответствующие ненужным сервисам. Лучшей считается такая настройка систем, в которой число установленных сервисов и инструментов минимально. Второе — необходимо самостоятельно тестировать собственную систему на проникновение, тем самым предопределяя действия нарушителя. Для защиты от более совершенных сканеров рекомендуется применять пакетные фильтры с контролем состояния системы. Такие фильтры исследуют пакеты протоколов и пропускают только те из них, которые соответствуют установленным сессиям.

Общие рекомендации против сканирования — своевременное применение пакетов безопасности, использование для сети и для хостов систем обнаружения вторжений (IDS), систем предотвращения вторжений (IPS), своевременное их обновление.

Переполнение стека. Способы защиты от данного типа атак можно разделить на две категории.

1. Методы, которые применяют системные администраторы и сотрудники службы безопасности при эксплуатации, настройке и сопровождении систем: своевременное применение патчей к системам, отслеживание обновлений установленных продуктов, сервис-паков для них, удаление лишних программ и сервисов, контроль и фильтрация входящего/исходящего трафика, настройка неисполняемого стека. Многие IDS способны обнаруживать атаки

переполнения памяти по сигнатурам.
2. Методы, используемые разработчиками программного обеспечения в процессе создания программ: устранение ошибок программирования, путем проверки пространства доступной памяти, объема проходящей вводимой информации через приложение. Воздержание от использования проблемных функций с точки зрения безопасности; компиляция программ специальными средствами.

Вышеописанные методы помогают минимизировать количество атак на переполнение стековой памяти, но не гарантирует полную безопасность системы.

Атаки на пароли. Первое и самое главное — «сильные» пароли. Это пароли длиной не менее 9-и знаков и содержащие специальные символы. Далее — регулярная смена паролей. Чтобы это все корректно работало, рекомендуется выработать адаптированную под конкретную организацию политику паролей и довести ее содержание до всех пользователей. Не лишним будет предоставить сотрудникам конкретные рекомендации по созданию паролей. Второе — рекомендуется использовать системы со встроенной проверкой на «слабость» паролей. Если такой проверки нет, то следует развернуть дополнительное программное обеспечение, выполняющее имеющее схожий функционал. Самый эффективный способ — отказ от паролей и использование систем аутентификации (смарт-карты и др.). Рекомендуется регулярно производить тестовые «взломы» собственных паролей. Хорошей практикой является защита файлов с хешированными паролями, а также их теневых копий.

Атаки на WEB-приложения. Для того чтобы защититься от похищения учетных записей, необходимо выводить на экран одну и ту же ошибку при неправильном вводе логина или пароля. Это затруднит злоумышленнику перебор вашего ID или пароля. Лучшая защита от атак, отслеживающих соединение — хеширование передаваемой информации о соединении, динамическая смена сеансового ID, завершение неактивного сеанса. Самые опасные атаки — внедрение SQL-кода в приложение. Защита от них — разработка WEB-приложений таким образом, чтобы они могли тщательно фильтровать указанные пользователем данные. Приложение не должно слепо доверять вводимой информации, поскольку в ней могут содержаться символы, с помощью которых модифицируются SQL-команды. Приложение должно удалять специальные символы, прежде чем обработать запрос пользователя.

Следует отметить, что на сегодняшний день активно развивается направление WAF (Web Application Firewall) — файервол уровня приложений, предоставляющий

комплексные методы защиты WEB-ресурсов. К сожалению, эти решения ввиду высокой стоимости доступны в основном только крупным компаниям.

Сниффинг. Первое — шифрование данных, передаваемых по сети. Для этого используются протоколы — HTTPS, SSH, PGP, IPSEC. Второе — внимательное обращение с сертификатами безопасности, игнорирование сомнительных сертификатов. Использование современных коммутаторов, позволяющих настроить MAC-фильтрацию на портах, реализовать статическую ARP-таблицу. Использовать VLAN-ы.

IP-спуфинг. Данную угрозу можно минимизировать следующими мерами.

1. Контроль доступа. На границе сети устанавливаются пакетные фильтры, позволяющие отсеивать весь трафик внешней сети, где в пакетах исходным адресом указан один из адресов внутренней сети.
2. Фильтрация RFC2827. Она заключается в отсечении исходящего трафика внутренней сети, в котором исходным адресом не обозначен ни один из IP-адресов вашей организации.
3. Внедрение дополнительных видов аутентификации (двухфакторной) и криптографического шифрования делает такие атаки абсолютно неэффективными.

Перехват сеанса связи. Эффективно бороться с этим видом атак можно только с помощью криптографии. Это может быть SSL-протокол, VPN-сети и др. Для наиболее критичных систем целесообразно использовать шифрование и во внутренних сетях. Атакующий, перехвативший трафик зашифрованной сессии не сможет получить из него какой-либо ценной информации.

DOS-атаки. Для описания средств защиты от DOS-атак рассмотрим их классификацию. Эти атаки, как правило, разделяются на две категории: прекращение сервисов и истощение ресурсов (таблица 1.5). Прекращение сервисов — сбой или отключение конкретного сервера, используемого в сети. Истощение ресурсов — расходование компьютерных или сетевых ресурсов с целью помешать пользователям в получении атакуемого сервиса. Оба вида атак могут проводиться как локально, так и дистанционно (через сеть).

Таблица 1.5 - Категории DOS-атак

Категория атаки Тип атаки	Прекращение сервисов	Истощение ресурсов
Локальная	• прекращение процессов • реконфигурация системы • крушение процессов	• расщепление процессов для заполнения таблицы процессов • заполнение всей файловой системы
Дистанционная	• атаки битыми пакетами	• пакетные наводнения, • DDoS-атаки

Защита против прекращения локальных сервисов: актуальные патчи безопасности локальных систем, регулярное исправление ошибок, разграничение прав доступа, применение программ проверки целостности файлов.

Защита против локального истощения ресурсов: применение принципа наименьшего количества привилегий при назначении прав доступа, увеличение системных ресурсов (память, скорость процессора, пропускная способность каналов связи и т.д.), применение IDS.

Защита против дистанционного прекращения сервисов: применение патчей, быстрое реагирование.

Лучшей защитой от дистанционного истощения ресурсов является быстрое реагирование на атаку. В этом могут помочь современные IDS-системы, сотрудничество с провайдером. Как и в предыдущих пунктах, следует своевременно обновлять и исправлять системы. Использовать функции анти-спуфинга. Ограничивать объем трафика со стороны провайдера. Для наиболее критичных систем необходимо иметь адекватную пропускную способность и избыточные линии связи.

Поддержание доступа. Вирусы и «троянские кони». Лучшая защита — эффективное антивирусное программное обеспечение (ПО), работающее как на пользовательском уровне, так и на уровне сети. Для обеспечения высокого уровня

безопасностей от этих угроз требуется регулярное обновление антивирусного ПО и сигнатур известных вирусов. Вторым шагом является получение актуальных обновлений операционных систем, настройка политик безопасности приложений в соответствии с актуальными рекомендациями их разработчиков. Необходимо обучить пользователей навыкам «безопасной» работы в Интернете и с электронной почтой. Защита от «ROOTKIT» обеспечивается политиками разграничения доступа, антивирусным программным обеспечением, применением обманок и системами обнаружения вторжений.

Заметание следов. После атаки злоумышленник, как правило, пытается избежать ее обнаружения администраторами безопасности. Для этих целей он производит изменение или удаление лог-файлов, хранивших историю действий нарушителя. Создание эффективной защиты, предотвращающей изменение лог-файлов злоумышленником, является важнейшим условием безопасности. Количество усилий, которые необходимо затратить на защиту регистрационной информации данной системы, зависит от ее ценности. Первым шагом для обеспечения целостности и полноценности лог-файлов является включение регистрации в особо важных системах. Чтоб избежать ситуации, когда в случае форс-мажора оказывается, что журналы отключены, необходимо создать политику безопасности, в которой бы регламентировались процедуры ведения журналов. Рекомендуется регулярно проводить проверки систем на соответствие данной политики. Другой необходимой мерой защиты лог-файлов является разграничение прав доступа на эти файлы. Эффективным приемом защиты регистрационной информации является установка выделенного сервера регистрации событий, обеспечив соответствующий уровень безопасности. Также хороши такие способы защиты как шифрование лог-файлов и разрешение на запись только в конец файла. Использование систем IDS.

Защититься против туннелирования можно в двух местах: на конечном компьютере и в сети. На конечном компьютере защита обеспечивается правами доступа, антивирусным ПО, безопасной конфигурацией и установкой обновлений. На уровне сети туннелирование можно обнаружить системами обнаружения вторжений.

Выше были перечислены основные способы защиты от сетевых атак. На их основании строятся комплексные решения, которые могут совмещать в себе ряд функций по защите информации и использоваться в конкретном модуле сетевой инфраструктуры.

ГЛАВА 2. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

2.1 Краткая характеристика предприятия

НПО «Ассоциация К» — холдинговая компания, состоящая из группы научно-производственных предприятий различного профиля деятельности, но объединенных единой целью — разработкой, производством и продвижением на рынок огнезащиты высококачественных продукции и услуг для обеспечения пожарной безопасности зданий и сооружений промышленного и гражданского назначения и защиты людей от влияния вредных факторов техногенного характера.

Профили деятельности:

- организационно-методическое и научно-техническое сопровождение производственной деятельности подведомственных предприятий; их информационное и юридическое обеспечение, подбор и подготовка кадров, материально-техническое обеспечение, предоставление транспортных услуг;
- проектирование схем и систем противопожарной защиты, пассивных и активных средств пожаротушения, обеспечивающих пожарную безопасность зданий, сооружений; разработка новой продукции и услуг, проектов огнезащиты;
- производство и продажа противопожарных изделий, оборудования, составов, красок и пропиток;
- производство работ по повышению огнестойкости металлических, железобетонных и деревянных конструкций, электрических кабелей, воздуховодов, каналов дымоудаления, ковровых изделий и др., а также работ по монтажу пожарно-технических изделий и оборудований, систем пожарной и охранной сигнализации, установок пожаротушения и сервисному обслуживанию, проведению мониторинга смонтированного оборудования, как

собственного, так и других фирм;
- проектирование, разработка, изготовление противопожарных преград: противопожарных дверей, остекленных перегородок, окон, ворот и другого оборудования.

2.2 Бизнес-процессы верхнего уровня рассматриваемого предприятия

Ниже перечислены процессы верхнего уровня НПО «Ассоциация К».

Процессы управления:

1. управление ресурсами;
2. процессы менеджмента качества.

Основные процессы:

1. прохождение заказа;
2. проектирование и разработка;
3. управление производством;
4. контроль;
5. поставка и сервис.

Обеспечивающие процессы:

1. управление персоналом;
2. техническое обслуживание оборудования и средств механизации;
3. закупки;
4. управление контрольно-измерительными средствами.

Управление процессами осуществляется в направлении наибольшего удовлетворения потребителей как внешних, так и внутренних, поэтому производится мониторинг и оценка удовлетворённости потребителей, что является основой для улучшения (совершенствования) бизнес-процессов.

На рисунке 2.1 изображена диаграмма модели процессов холдинга согласно стандарту ГОСТ ISO 9001-2015.

Рис. 2.1 - Модель процессов НПО «Ассоциация К» согласно ГОСТ ISO 9001-2015

2.3 Основные этапы построения систем защиты информации

Для достижения цели повышения информационной безопасности на рассматриваемом предприятии, необходимо полностью или частично следовать нижеописанным этапам построения защищенных систем.

1. Выявление конфиденциальной информации, которую необходимо защищать, а также источников угроз (частных лиц и организаций), которых эти сведения могут интересовать.
2. Выявление возможных точек нападения.
3. Анализ уязвимостей (каналы утечки и НСД, вероятность реализации угроз, модель действий нарушителя, анализ и оценка рисков).
4. Выбор контрмер, обеспечивающих информационную безопасность.
5. Проверка системы защиты информации (оценка эффективности, тестирование).
6. Составление плана защиты информации.
7. Реализация плана защиты информации.

2.4 Конфиденциальная информация предприятия

Согласно действующему законодательству РФ организация — владелец информации вправе сама определять перечень отнесения тех или иных сведений к конфиденциальной информации. ФЗ «Об информации, информационных технологиях и защите информации» определяет лишь понятие «конфиденциальности». «Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя». Эта информация имеет действительную или потенциальную коммерческую ценность для предприятия в силу недоступности третьим лицам.

Перечень конфиденциальных сведений базируется на основных бизнес-процессах компании.

1. Данные о потребностях организации в персонале, составе и численности работников, уровне их квалификации, опыте работы.
2. Учебные пособия входящего в состав холдинга учебного центра по пожарной безопасности.
3. Информация о наличии и стоимости готовой продукции (остатки на складах, в цехе, в незавершенном производстве, прайс-листы и др.).
4. Информация об объемах работ, поставках, сроках исполнения по договорам.
5. Клиентская база.
6. Ценовая политика и порядок расчетов.
7. Проектная, конструкторская, сопроводительная документация.
8. Хранившаяся в базах данных информация о потенциальных или действительных заказах, коммерческих предложениях, договорах, проектах и др.
9. Полученная от клиентов информация о качестве выполненных работ и поставленной продукции, рекламации и другие претензии и замечания.
10. Проекты схем и систем противопожарной защиты, пассивных и активных средств пожаротушения, обеспечивающих пожарную безопасность зданий и сооружений.
11. Разработки новых и модифицированных видов огнезащитных составов, красок, пропиток.
12. Разработки новых изделий и пожарно-технического оборудования, технологий.
13. Результаты архитектурного и технологического проектирования объектов.
14. Технологические регламенты.
15. Информация о проведенных экспертизах проектов в пожарной безопасности.
16. Производственные прогнозы, планы развития и совершенствования производства.
17. Нормы расходов сырья, материалов, чертежи.
18. Информация о потребностях в сырье, материалах, полуфабрикатах и комплектующих изделиях.
19. Наличие и состояние производственных мощностей и возможностей производства.
20. Данные о поставщиках, заключенных с ними договорах и история взаимоотношений. Реестр утвержденных поставщиков.
21. Реестры (информационные базы) учета договоров и коммерческих предложений, сведения об их реализации.

22. Каталог комплектующих материалов (с характеристиками и модификациями), необходимый для формирования заказа на изготовление противопожарного оборудования.
23. Документы контроля качества изготовляемой продукции.
24. Схемы размещения сырья, материалов, готовой продукции на складах.
25. Документы системы менеджмента качества (Руководство по качеству, Положения об отделах, описание бизнес-процессов, структуры холдинга и т.д.).
26. Протоколы испытаний готовой продукции, данные о результатах контроля.
27. Документы внутренних аудитов, перспективный план развития компании.
28. Регламенты технического обслуживания и ремонта технологического оборудования.
29. Нормативно-техническая документация.
30. Финансовая информация: затраты на производство, себестоимость, накладные расходы, минимальные цены.
31. Маркетинговые исследования (технические возможности и цены конкурентов).
32. Конкурсная документация.
33. Платежные документы, данные об экономических показателях.
34. Приказы и поручения руководства компании, другие локальные нормативно-правовые акты.
35. Регистрируемая входящая и исходящая корреспонденция.
36. Бюджеты, бухгалтерские балансы, сведения об оплате труда, акты выполненных работ.
37. Первичные документы бухгалтерского учета.
38. Телефонные справочники.
39. Сведения об используемом программном обеспечении, средствах вычислительной техники, СКЗИ, средствах защиты информации.
40. Документы и сведения, содержащие данные о системе охранно-пожарной сигнализации, графике работы сотрудников охраны, схемы размещения камер видеонаблюдения, систем контроля доступа.

2.4 Территориальная структура предприятия

НПО «Ассоциация К» имеет следующую территориально-распределенную структуру (рисунок 2.2).

Рис. 2.2- Территориальная структура предприятия

1. Центральный офис — расположен на принадлежащей компании территории промышленной зоны в деревне Машково Московской области и представляет собой несколько офисных зданий. Здесь же располагается химическое производство огнезащитных составов, красок и пропиток. Территория огорожена по периметру и имеет круглосуточную охрану (сотрудники охраны, пропускной режим, система видеонаблюдения и контроля доступа, охранно-пожарная сигнализация). Вход и выход сотрудников предприятия осуществляется через систему контроля доступа с использованием именных электромагнитных пропусков. Проезд автотранспорта на территорию осуществляется через автоматические ворота. Электропитание на территорию подается по двум независимым линиям, основной и резервной, переключение между которыми осуществляется в ручном режиме в течение регламентированного времени (10 минут). Подключение к Интернету организовано по двум независимым каналам связи от разных провайдеров Интернета (основной канал — оптико-волоконная линия, резервный — направленный Wi-Fi). Переключение между ними в случае аварии осуществляется автоматическим способом. Доступ в серверные комнаты, а также в некоторые закрытые помещения осуществляется с использованием электронной системы контроля доступа с последующим дублированием механическими замками. Все серверы и сетевое оборудование уровней ядра и распределения расположены в серверных комнатах, сетевое оборудование уровня доступа — в открытом доступе в помещениях офиса (как правило, в одном из помещений этажа на стене). Офисные здания и производственные цеха соединены между собой оптико-волоконной линией связи. Количество рабочих мест (компьютер/ноутбук) в офисе — около 250.
2. Представительский офис в г. Москва — расположен на территории двухэтажного арендуемого здания и примыкающей к нему огороженной автомобильной стоянкой. Имеет два выхода из здания, один на городскую улицу, второй во внутренний двор со стоянкой, въезд и выезд с которой производится через автоматические ворота. Офис имеет круглосуточную охрану (сотрудники охраны, пропускной режим, система видеонаблюдения и контроля доступа, охранно-пожарная сигнализация). Вход и выход сотрудников предприятия осуществляется через систему контроля доступа с

использованием именных электромагнитных пропусков. Аналогично центральному офису доступ в серверную комнату и другие критически важные объекты осуществляется с помощью системы контроля доступа. Резервного электропитания в офисе нет, но имеется в наличие дизель-генератор, время на ввод в эксплуатацию которого составляет около 1-го часа. Подключение офиса к Интернету организовано по двум каналам связи, основному — по витой паре, и резервному — по технологии ADSL. Переключение осуществляется автоматическим способом. Все серверы и сетевое оборудование уровней ядра и распределения расположены в серверных комнатах, сетевое оборудование уровня доступа — в открытом доступе в помещениях офиса. Количество рабочих мест (компьютер/ноутбук) в офисе — около 50.

3. Региональный офис — расположен в г. Алексин Тульской области. Представляет собой огороженную территорию, на которой располагаются офисное здание и цех по производству противопожарных изделий и оборудования. Охрана и контроль доступа в офисе обеспечиваются по той же схеме, как и в центральном офисе. Есть резерв электропитания, два интернет-канала (основной — оптико-волоконный, резервный — ADSL). Серверная комната совмещена (смежное расположение) с кабинетом системного администратора, доступ в кабинет осуществляется только по электронным пропускам. Все серверы и сетевое оборудование уровней ядра и распределения расположены в серверной комнате, сетевое оборудование уровня доступа — в открытом доступе в помещениях офиса. Количество рабочих мест (компьютер/ноутбук) в офисе — около 70.
4. Представительство в г. Санкт-Петербург — располагается в нежилых (коммерческих) помещениях многоквартирного дома. Количество рабочих мест сотрудников представительства — около 10. Офис оборудован домофоном для обеспечения контроля доступа посторонних лиц, в нерабочее время закрывается на ключ и ставится под охрану. Электропитание подается от сети многоквартирного дома, Интернет проводной по выделенной линии, резерва нет. Серверное оборудование отсутствует.
5. Представительство в г. Сочи — располагается на территории офисного центра. Численный состав сотрудников представительства — 5 человек. Офис в нерабочее время закрывается на ключ, охраняется службой охраны бизнес-центра. Резерва электропитания и Интернета нет. Серверное оборудование отсутствует.

6. Филиалы в районах расположения объектов строительства. Представляют собой арендованные помещения или строительные «вагончики» с числом сотрудников от 1 до 5. Как правило, обеспечиваются мобильным интернетом, но может присутствовать и проводное подключение к Интернету (со статическим IP-адресом) для обеспечения IP-телефонией и программным VPN-туннелем с центральным офисом.

Весь информационный обмен между территориальными структурами холдинга производится через глобальные сети посредством защищенных VPN-туннелей, обеспечивающих инкапсуляцию, проверку подлинности и шифрование данных. Помимо этого в каждом подразделение развернута аналоговая телефония (количество линий зависит от размера филиала), обеспечивающая резервную телефонную связь между ними в случае возникновения проблем с Интернетом.

ГЛАВА 3. РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

1. Необходимо развернуть межсетевые экраны во всех офисах и подразделениях компании, где они еще не развернуты, а также регулярно проверять их работу. Согласно описанной выше инфраструктуре рассматриваемого предприятия допускается организация локальных сетей без сетевого экрана, что повышает риск нарушения безопасности данных. Следует избегать таких топологий и стараться размещать в филиалах как минимум экраны уровня «малого бизнеса», такие как D-Link NetDefend UTM Firewall.
2. Желательно развернуть межсетевые экраны для конкретных серверных ресурсов внутри сети и обеспечить фильтрацию трафика для предотвращения несанкционированных подключений. В настоящий момент в корпоративной сети межсетевые экраны размещаются только по периметру.
3. Необходимо выделить публичные ресурсы в DMZ-зону и ограничить к ней доступ из общей сети. Для рассматриваемого предприятия этими ресурсами

могу служить почтовый и терминальный сервер, а также сервер IP-телефонии.

4. Необходимо установить антивирусное программное обеспечение на все серверы и настольные компьютеры предприятия. В настоящий момент на почтовом сервере, шлюзе доступа, файловом сервере и сервере резервного копирования нет антивирусного ПО. Для этих серверов на операционной системе CentOS можно использовать, например, *Clam AntiVirus (ClamAV)* — свободно распространяемый антивирус, работающий в UNIX-подобных операционных системах. Также нужно регулярно обновлять сигнатуры вирусов и настроить централизованное управление.
5. Рекомендуется рассмотреть возможность развертывания многофакторной проверки подлинности для VPN-соединений. В настоящий момент используется доменная авторизация.
6. Необходимо обеспечить полную сегментацию сети посредством технологии VLAN. В рассматриваемой инфраструктуре VLAN не используется, хотя большая часть сетевого оборудования (производителя HP) эту функцию поддерживает. Необходимо выделить в отдельные VLAN-ы схожие ресурсы (серверные и другие), также целесообразно использовать сегментацию по подразделениям.
7. Необходимо рассмотреть возможность развертывания сетевых и узловых систем обнаружения вторжений (IDS) для определения и уведомления об атаках в корпоративной сети. Основная проблема заключается в том, что такие системы, как правило, слишком дороги и требуют более детальной проработки экономической целесообразности их применения, соотнося стоимость внедрения с возможными последствиями ущерба. Однако, можно попробовать использовать свободно распространяемые IDS/IPS. Примером такой системы может служить достаточно известная система *Snort.* Следует учитывать тот факт, что для развертывания и анализа полученной информации такой системы потребуются дополнительные компетенции.
8. Рекомендуется отключить широковещательную рассылку SSID в беспроводной сети (не отключено), проводить регулярную смену паролей и использовать стойкие алгоритмы шифрования (производится). Желательно рассмотреть возможность использования VPN и в беспроводной сети.
9. Для административных пользователей желательно рассмотреть возможность внедрения многофакторной проверки подлинности помимо использования сложного пароля.
10. Для удаленных пользователей сети необходимо рассмотреть возможность внедрения многофакторной проверки подлинности помимо использования

сложного пароля и предоставлять удаленный доступ только тем сотрудникам, которым он реально необходим.

11. Рекомендуется регулярно проводить аудит удаленных пользователей на предмет актуальных обновлений своих систем. В настоящий момент данная процедура не регламентирована.
12. Для создания безопасных рабочих станций рекомендуется создать уникальный образ для каждого типа рабочих станций. Следует регулярно следить за актуализацией этих образов.
13. Необходимо рассмотреть возможность установки персональных межсетевых экранов на рабочие станции пользователей. В настоящий момент такие экраны развернуты только на некоторых компьютерах сети.
14. Рекомендуется использовать программное обеспечение шифрования данных на диске для рабочих станций пользователей. В рассматриваемой сети целесообразно выделять ряд наиболее критичных с точки зрения безопасности рабочих станций и установить там данное программное обеспечение. Такими рабочими станциями могут быть, например, компьютеры научно-исследовательской лаборатории.
15. Рекомендуется рассмотреть возможность отказа от использования систем удаленного наблюдения и контроля.
16. Необходимо обеспечить размещение сетевого оборудования в закрытых шкафах/стойках. В настоящий момент оборудование уровня доступа располагается на этажах в открытом доступе. Для выполнения этого пункта достаточно в местах размещения произвести монтаж закрытых шкафов с доступом только для ИТ-персонала.
17. Рекомендуется использовать средства обеспечения физической безопасности для персональных компьютеров. Для переносных компьютеров использовать дополнительные кабельные замки.
18. Для серверов, расположенных в серверной комнате также рекомендуется использовать запираемые шкафы или стойки. Это позволит уменьшить риск несанкционированного использования.

ЗАКЛЮЧЕНИЕ

Результатом проведенной аналитической и практической работы стал перечень рекомендаций по повышению эффективности защиты информации в корпоративной сети передачи данных.

Анализ рисков текущего состояния информационной безопасности на предприятии дал неплохие результаты, но, несмотря на это, в некоторых направлениях защиты наблюдается недостаток передовых методик, к тому же итоговая диаграмма рисков иллюстрирует необходимость перегруппировки защитных действий между этими направлениями.

Разработанные рекомендации сгруппированы по четырем основным областям: инфраструктура, приложения, операции, персонал. В каждой группе описаны меры, которые необходимо предпринять в имеющейся среде для достижения требуемого результата. В дополнении к этому сформирован перечень приоритетных действий для отдела ИТ.

Анализ рисков информационной безопасности, проведенный с учетом предложенных рекомендаций, показал их предполагаемую эффективность.

Таким образом, делаю вывод о практической значимости полученных результатов для рассматриваемого предприятия.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А. Обеспечение информационной безопасности бизнеса. — Альпина Паблишерз, 2011. — 338 с.;
2. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009. № 1(49). С. 15–26;
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. — М.: РИОР: ИНФРА-М, 2015. — 315с.;
4. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии: учебное пособие. — М.: Издательский центр “Академия”, 2009. — 416 с.;
5. Лукацкий А.В. Обнаружение атак. — СПб.: БХВ — Петербург, 2016. — 624 с.;
6. Петренко С.А. Анализ рисков в области защиты информации: информационно-методическое пособие. — Издательский дом «Афина», 2012. — 153 с.;
7. Скудис Эд. Противодействие хакерам, полное руководство по компьютерным атакам и эффективной защите. — М.: ДМК-Пресс, 2013. — 502 с.;

8. Хоффман, Л. Д. Современные методы защиты информации. Под редакцией В.А. Герасименко. — М.: Сов. радио, 2016. – 264 с.;
9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М: ДМК Пресс, 2012. — 592 с.;
10. Обзор архитектуры безопасности. Информационный бюллетень. — Cisco Press, 2010. — 35 с.;
11. Пять шагов, которые необходимо предпринять для обеспечения безопасности беспроводной сети. — Cisco Press, 2013. — 10 с.;
12. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей (издание 4), составитель М. Кадер. — Cisco Press, 2013. — 100 с.;
13. Средство оценки безопасности Microsoft Security Assessment Tool (MSAT) [Электронный ресурс] — URL: http://technet.microsoft.com/ru-ru/security/cc185712.aspx (Дата обращения: 05.03.2017);
14. ГОСТ Р ИСО/МЭК 27000-2012 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология;
15. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности;
16. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 13.07.2015) “Об информации, информационных технологиях и о защите информации”;
17. Федеральный закон от 29.07.2004 №98-ФЗ (ред. от 12.03.2015) “О коммерческой тайне”;
18. Руководство по менеджменту качества НПО “Ассоциация К” (РК Асс К— 03): третья редакция, 2015. — 37с.;
19. The Bacula Open Source Network Backup Solution [Электронный ресурс] — URL: http://blog.bacula.org/ (Дата обращения: 05.03.2017);
20. OpenVPN [Электронный ресурс] — URL: https://openvpn.net/ (Дата обращения: 05.03.2017);
21. Samba. Opening Windows to a Wider World [Электронный ресурс] — URL: https://www.samba.org/ (Дата обращения: 05.03.2017);
22. ClamAV [Электронный ресурс] — URL: http://www.clamav.net/about (Дата обращения; 05.03.2017);
23. Zabbix. The Enterprise-class Monitoring Solution for Everyone [Электронный ресурс] — URL: http://www.zabbix.com/ru/ (Дата обращения; 05.03.2017).

1. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. — М: ДМК Пресс, 2012. — с.65 ↑

2. Обзор архитектуры безопасности. Информационный бюллетень. — Cisco Press, 2010. — с.12 ↑

3. *Грибунин В.Г., Чудовский В.В.* Комплексная система защиты информации на предприятии: учебное пособие. — М.: Издательский центр “Академия”, 2009. — с.65 ↑

4. *Баранова Е.К., Бабаш А.В.* Информационная безопасность и защита информации. — М.: РИОР: ИНФРА-М, 2015. — с.9 ↑