**РАЗРАБОТКА СТРУКТУРЫ ЗАЩИЩЕННОЙ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ**

Е.Б. Романова, Н.Ю.Иванова, Н.М. Алексанков

**Аннотация**

В статье проанализированы риски информационной безопасности корпоративной сети. Проведен анализ деятельности, организационной структуры и дано функциональное назначение подразделений компании. Разработана структура защищенной корпоративной информационной сети, обеспечивающая: безопасность рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Разработка проводилась для конкретного общества с ограниченной ответственностью, но в рамках конфиденциальности название не упоминается.

**Ключевые слова**

Информационная безопасность, корпоративная сеть, Secret NET Studio

**Введение**

Корпоративные сети являются важной частью инфраструктуры современных компаний. Вся информация, а также конфиденциальная, передается по корпоративной сети. Но вместе с этим темпы развития, масштабы и сложность атак растут в геометрической прогрессии. Из-за этого обеспечение безопасности информации, которая передается по корпоративной сети, является, одной из самых важных проблем, которые стоят перед современными организациями.

Целью статьи является повышение уровня защищенности корпоративной информационной структуры компании.

Задачами работы является:

- Анализ корпоративной информационной структуры.

- Анализ и выделение важных для компании активов.

- Анализ и выделение актуальных угроз.

- Выбор средств защиты информации корпоративной информационной сети компании и разработка структуры защищенной корпоративной информационной сети компании, обеспечивающая: безопасность рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.

**1. Анализ корпоративной информационной структуры**

В ходе анализа корпоративной информационной структуры была разработана схема организационной структуры, которая представлена на рисунке 1.

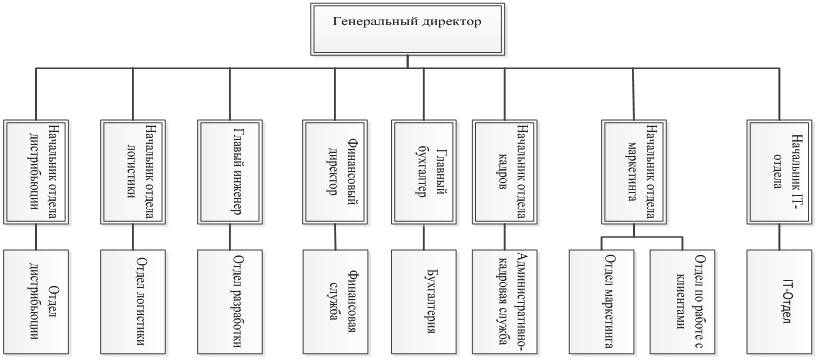


Рис.1. Схема организационной структуры

В рамках компании функционирует единая корпоративная информационная система, удовлетворяющая основные информационные потребности всех сотрудников, служб и подразделений, которая состоит из ЛВС и прикладного ПО. Техническая структура предприятия представлена на рисунке 2.

На всех автоматизированных рабочих местах компании (АРМ), кроме IT-отдела установлена операционная система MS Windows 8 и защита от вредоносного ПО осуществляется с помощью встроенной в операционную систему программы «Защитник Windows». В IT-отделе АРМы работают на операционной системе Mac OS Sierra.

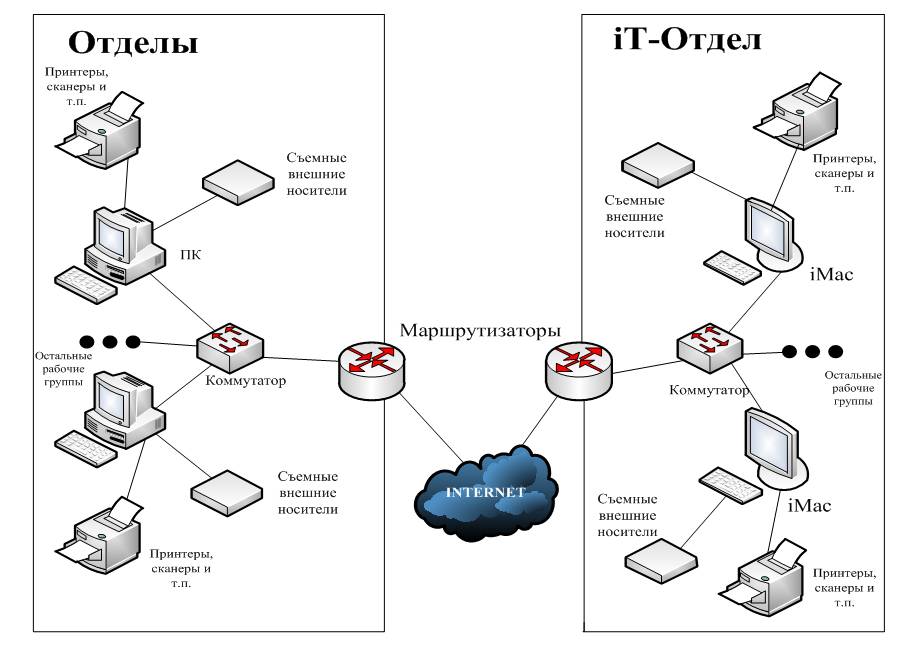


Рис.2. Структурная схема технической архитектуры предприятия

**2. Анализ активов и угроз**

В процессе анализа активов компании фиксируется, как вводится, хранится, обрабатывается и передается информация в системе. Главным результатом процесса выявления активов является получение детальной информационной структуры организации и способы работы с информацией. Были проанализированы все активы компании и активы, имеющие наибольшую ценность, приведены в таблице 1.

Есть обширный банк угроз информационной безопасности автоматизированных систем, который содержит сотни различных угроз. Рассмотрение всех этих угроз информационной безопасности выполняется для определения полного набора требований к проектируемой системе защиты информации. Вероятность угрозы будет считаться высокой, если есть предпосылки для реализации угрозы и нет никаких мер по обеспечению ИБ. Средняя вероятность, это когда есть предпосылки для реализации угрозы, но уже приняты меня по обеспечению ИБ. Низкая же вероятность, это когда отсутствуют предпосылки и меры по обеспечению ИБ уже предприняты.

Табл.1. Результаты ранжирования активов

| Наименование актива | Ранг актива |
| --- | --- |
| Протоколы Совета Компании. | 5 |
| Данные маркетинговых и статистических исследований | 5 |
| Сведения о контрагентах компании факт существования и условия заключенных или планируемых к заключению договоров. | 5 |
| Разработки, макеты, проекты | 4 |
| Ежемесячные, ежеквартальные, ежегодные планы и прогнозы продаж | 4 |
| Пароли, ключи для баз данных | 3 |
| Структура системы защиты информации | 2 |

Анализ угроз осуществлен на основе коэффициента реализуемости угрозы Y, который рассчитывается по формуле:

Y=(Y1+Y2)/20,

Где, при 0 ≤ Y ≤ 0,3 - вероятность реализации угрозы признается низкой;

0,3 < Y ≤ 0,6 - вероятность реализации угрозы признается средней;

0,6 < Y ≤ 0,8 - вероятность реализации угрозы признается высокой;

Y > 0,8 - вероятность реализации угрозы признается очень высокой».

Актуальные угрозы для предприятия: кража носителей информации; действия вредоносных программ (вирусов); установка ПО, которое не связано с исполнением служебных обязанностей; утрата ключей доступа; ненамеренная модификация или уничтожение информации сотрудниками; угрозы выявления паролей по сети; угрозы удаленного запуска приложений; перехват информации за переделами контролируемой зоны; угроза сбоя электроснабжения; доступ к информации лиц, которые не к ее обработке.

Далее разработка системы защиты конфиденциальной информации в корпоративной сети компании будет основываться на выявленных актуальных угрозах.

**3. Разработка структуры защищенной корпоративной информационной сети**

Для разработки защиты корпоративной сети потребуется использование аппаратных, технических, организационных, программных и программно-аппаратных средств защиты. Кроме СЗИ в сети будут необходимы дополнительные компоненты, которые обеспечат слаженную работу всей сети.

Так как все АРМ компании управляются под одной ОС, которой является ОС Windows, в качестве средства объединения АРМ была выбрана служба каталогов Active Directory. Для этого на одном из локальных хостов необходимо развернуть саму службу Active Directory, и этот хост будет считаться контроллером домена. В качестве такого хоста чаще всего выбирается сервер. На нем будут храниться все учетные записи пользователей и устройств, которые входят в эту сеть, а также правила, которые к этим устройствам и пользователям будут применяться. Active Directory не будет работать без сервера DNS, так как изначально на устройстве нет адреса контроллера домена. За получением этого адреса устройство должно обратиться к DNS-серверу.

Было решено выбрать NAS-устройство, как главный файловый сервер компании. Также в It-отделе, было решено использовать NAS-устройство с расчетом не дальнейшее увеличение числа сотрудников. На почтовые серверы необходимо выделить примерно 3 ТБ, а на файловые хранилища примерно около 10 ТБ. Для файлового хранилища стоит предусмотреть дополнительные слоты, чтобы в дальнейшем была возможность масштабирования сети. А для почтового сервера будет достаточно устройства с двумя слотами. Выбор пал NAS-устройства марки «Synology». Это «Synology DS918+» и «Synology DS718+»

Так как физический канал технически неосуществим, а аренда выделенной линии у провайдера очень дорогая, то связь между объектами было решено сделать при помощи создания сетевого туннеля. Такой туннель можно осуществить при помощи инкапсуляции протоколов. VPN-туннель можно организовать аппаратными средствами, так как он должен объединять две локальные сети, а программный способ не сможет обеспечить нужной скорости. Было решено приобрести межсетевой экран «WatchGuard Firebox M200». Эта модель разработана специально для защиты предприятий малого бизнеса от атак, которые могут быть не менее яростными, чем на крупные компании. Даже при всех включенных сервисах защиты, пропускная способность будет не менее 800Мб. Так же эта модель поддерживает политики безопасности Active Directory, а это упрощает централизованное управление.

Антивирусные программы отличаются по функциональным группам. Сканирующие антивирусные программы делают поиск вирусов с помощью сравнения компонентов с базой вирусов или с помощью эвристического анализа и при нахождении вируса или вредоносной программы сообщают об этом. Основными требованиями, которые требуются от антивирусной программы это: эффективная защита, быстродействие, минимальное количество ложных срабатываний, минимальная загрузка процессорной памяти, полный охват ИС (почтовый и файловый сервера, рабочие станции, а также сеть)

При выборе антивирусной программы, рассматривались только те, которые сертифицированы ФСТЭК. На NAS-устройствах присутствуют встроенные антивирусные средства, поэтому антивирусная защита необходима на АРМ и между узлами сети. Был выбран антивирус «ESET NOD32 Secure Enterprise Pack 5». Он сертифицирован ФСТЭК России.

Далее был осуществлен выбор СЗИ от НСД - Secret NET Studio. СЗИ Secret Net Studio – это комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Комплексное решение Secret NET Studio закрывает сразу несколько областей по защите ИСПДн и лишено проблем совместимости различных типов защиты. Однако, в связи с тем, что компоненты Secret NET Studio «Персональный межсетевой экран» и «Антивирусная защита» ещё не получили сертификат ФСТЭК ранее были выбраны сертифицированные СЗИ. Работа с Secret NET Studio осуществляется с помощью специального окна. Это окно состоит из нескольких вкладок, каждая из которых посвящена тому или иному инструменту защиты. На заглавной странице выводится состояние всех компонентов

Также были выбраны физические средства защиты. Физическая защита информации – это применение различных механических, также технических и электрических средств, которые будут препятствовать уничтожению или хищению информации на предприятии. В компании нужно выделать помещение, где будут располагаться сервера, коммутаторы и машрутизаторы. Такое, отдельно выделенное помещение даст безопасность и стабильность работы оборудования. Необходимо сделать две таких комнаты, для всего офиса и для IT-отдела. Наилучшие условия для такого помещения: помещение без каких-либо окон; надежная дверь с несколькими замками; помещение нельзя размещать под кухней, прачечной или любым другим источником возможного затопления, что выведет из строя всю серверную систему; обязательно нужно сделать систему кондиционеров, чтобы поддерживала температуру не выше 20 ºC, так как работа серверов и остального оборудования подвержена большому выделению тепла; нужны датчики, которые будут следить за относительной влажностью в помещении, она не должна превышать 50%, так как это может плохо сказаться на работе оборудования; необходимо установить несколько блоков розеток, которые будут запитаны от разных кабелей; и, конечно, нужно установить источники бесперебойного питания. Ключи от обеих серверных комнат хранятся у начальника IT-отдела.

Разработав модель угроз, была определена новая структура сети и ее компоненты. Как уже говорилось ранее, полностью обезопасить ИС невозможно. Но для лучшей безопасности и меньшей вероятности реализации той или иной угрозы, в рамках рассматриваемой ИС, необходимо приобрести NAS устройства, межсетевой экран и источники бесперебойного питания. Что касается программных средств, необходимо использовать Secret Net Studio, антивирусную защиты и службу каталогов Acive Directory. Чтобы обеспечить разграничение прав доступа, было необходимо разбить пользователей на группы при помощи Active Directory. Так же сеть необходимо сегментировать. Почтовый сервер было решено выделить в ДМЗ, а бухгалтерию и отдел кадров выделить в отдельную логическую сеть с отдельным сервером. Разработанная структура системы защиты корпоративной информационной сети представлена на рисунке 3.

Меры по противодействию ко всем актуальным угрозам представлены в таблице 2.

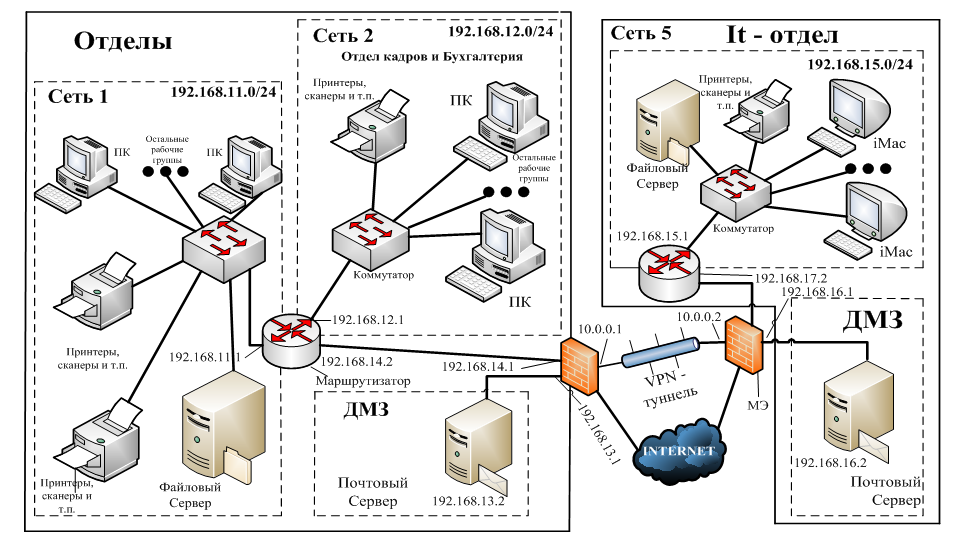


Рис.3. Структура системы защиты корпоративной информационной сети

Табл.2. Актуальные угрозы и средства защиты

|  |  |
| --- | --- |
| **Угроза** | **Мера/Решение** |
| Кража или утрата носителей информации | **NAS-Сервер и active directory**: централизованный файловый сервер;  **Secret Net Studio**: защита от копирования и контроль печати. |
| Вредоносное ПО и вирусы | **ESET NOD 32.** |
| Потеря ключей доступа | **Active directory:** Управление учетными записями;  **ESET NOD 32:** Менеджер паролей. |
| Модификация или уничтожение информации | **NAS-сервер:** централизованная резервная копия; **ESET NOD 32:** контроль целостности. |
| Выявление паролей по сети | **WatchGuard Firebox M200:** межсетевой экран; **ESET Gateway Security:** обеспечение защити HTTP и FTP шлюзов. |
| Удаленный запуск приложений | **WatchGuard Firebox M200:** межсетевой экран;  **ESET NOD 32:** Ограничение на установку приложений. |
| Перехват информации за пределами контролируемой зоны | Использование собственного **почтового сервера;**  **WatchGuard Firebox M200:** Организация VPN |
| Сбой электроснабжения | Использование **источника бесперебойного питания** |
| Несанкционированный доступ к информации | **Active directory и Secret Net Studio**: разграничение доступа и контроль пользователей, которые допущены к ресурсам системы. |

**Заключение**

В статье проанализированы риски информационной безопасности корпоративных сетей России. Проведен анализ его деятельности, организационной структуры, дано функциональное назначение подразделений компании. Дана характеристика программной и технической архитектур компании. Разработана структура защищенной корпоративной информационной сети, обеспечивающая: безопасность рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования. Выбрано конкретное оборудование и программное обеспечение сертифицированное ФСТЭК. Аналогичный подход может применяться для разработки защищенной структуры других обществ с ограниченной ответственностью.

**Список использованной литературы**

1. Об обществах с ограниченной ответственностью: федер. закон Рос. Федерации от 8 февраля 1998 г. №14-ФЗ.
2. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации ред. от 18 декабря 2018 г. №149-ФЗ.
3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных // ФСТЭК России, 2015 г.
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных // ФСТЭК России, 2008 г.
5. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России ред. от 23 марта 2017 г. №2.

**© Е.Б. Романова, Н.Ю.Иванова, Н.М. Алексанков 2019**