

Слайд 1

Здравствуйте, уважаемые члены аттестационной комиссии!

Тема моей дипломной работы - **«Обеспечение информационной безопасности на предприятии»**.

Актуальность темы обусловлена тем, что проблема обеспечения защиты информации является одной из важнейших для устойчивого функционирования информационной структуры предприятия, а также для минимизации рисков на предприятии.

Слайд 2

Целью выпускной квалификационной работы является разработка политики информационной безопасности и организационно-распорядительной документации в области информационной безопасности для предприятия ФКУ «Налог-Сервис» ФНС России в Тюменской области.

Слайд 3

Для достижения поставленной цели, в работы производится Анализ информационной системы в организации ФКУ «Налог-Сервис».

Слайд 4

Общая схема циркуляции информации в системе документооборота организации представлена на Рисунке.

Слайд 5

Анализ Структуры и особенностей сети предприятия позволил выявить Ключевые особенности сети:

- 1) Локальная вычислительная сеть (ЛВС) налогового органа и Интернет-сегмент реализованы в различных структурированных кабельных системах (СКС);
- 2) Подключение к сети Интернет ЛВС налогового органа допускается осуществлять только с использованием средств шифрования трафика (в виде VPN-туннеля);
- 3) Взаимодействие между внутренним сегментом ЛВС и интернет-сегментом запрещено;
- 4) и другие особенности

Слайд 6

Далее в работе осуществлена разработка частной модели угроз.

ИСПДн предприятия представляет собой распределенную информационную систему, состоящую из рабочих станций и серверов. ИСПДн имеет подключения к сетям связи общего пользования. Обработка ПДн производится в многопользовательском режиме с разграничением прав доступа, речевая обработка ПДн не производится. Технические средства ИСПДн находятся в пределах Российской Федерации.

Описание объектов безопасности, требующих защиты, представлены на слайде.

Слайд 7

Анализ источников угроз информации, циркулирующей на объекте, позволил выявить Антропогенные и Техногенные источники угроз.

В качестве антропогенных источников угроз выступают субъекты, имеющие санкционированный/несанкционированный доступ к работе со штатными средствами

объекта информатизации, действия которых могут быть распознаны, как умышленные или совершенные по неосторожности.

Техногенные источники угроз характеризуются технократической деятельностью человека и развитием техники.

Слайд 8

Все нарушители делятся на две основные группы: внутренние и внешние. Под внутренними нарушителями подразумеваются все работники объекта информатизации, имеющие санкционированный доступ на территорию объекта к ресурсам автоматизированной системы (АС). Под внешними нарушителями подразумеваются все остальные лица.

На слайде номер 8 представлен перечень возможных нарушителей.

Анализ предполагаемой квалификации потенциального нарушителя проводится по классификационным признакам. Кто бы ни был источником нарушения, какое бы оно не было, все нарушители имеют одну общую черту - доступ к объекту информатизации.

Слайд 9

Далее в работе осуществлена разработка мер по определению актуальных угроз безопасности ПДн в ИСПДн. При определении актуальности угроз и их описании используются два методических документа, разработанных и утвержденных ФСТЭК России:

- Базовая модель угроз безопасности ПДн при их обработке в ИСПДн;
- Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн.

Составлена сводная таблица, содержащая расчет исходной защищенности.

Проведенный анализ защищенности показал, что ИСПДн имеет низкий уровень исходной защищенности.

Слайд 10

Основываясь на результатах анализа, была осуществлена Разработка политики информационной безопасности и организационно-распорядительной документации.

Для каждого из этапов функционирования компонентов АС предъявляются требования к реализации мер по планированию обеспечения информационной безопасности. Так, был составлен перечень мер для следующих стадий:

- Предпроектной
- Стадия разработки
- Стадии установки.
- Стадии списания.

Слайд 11

Физические меры защиты предназначены для создания физических препятствий на возможных путях проникновения потенциальных нарушителей на территорию предприятия, к компонентам АС и доступа к защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физические меры защиты данных касаются таких параметров, как:

1. Защита центров данных и компьютерных залов
2. Правила использования рабочего стола
3. Источники электропитания
4. Защита оборудования, используемого за пределами предприятия

Слайд 12

Разработка мер безопасности, применительно к техническим средствам, касается таких направлений, как:

1. Требования к подсистеме идентификации
2. Требования к подсистеме аутентификации
3. Требования к парольной подсистеме
4. Требования к системам регистрации сетевых событий

Слайд 13

Также в работе обозначены требования безопасности к Функциональным средствам. Под функциональными средствами понимаются методы обеспечения безопасности АС, имеющие отношение, прежде всего, к механизмам, выполняемым при непосредственном участии работников предприятия (человеческого фактора).

Например, Документирование механизмов безопасности является средством защиты, позволяющим формализовать защитные и функциональные процедуры обеспечения информационной безопасности, характерные для данной системы.

Слайд 14

По итогам проведенной работы можно сделать следующие выводы:

1. Разработаны необходимые организационно-методические документы и политика информационной безопасности на основе методических рекомендаций.
2. Сотрудники предприятия были должным образом проинструктированы.
3. Организован процесс реагирования на инциденты по фактам нарушений защиты информации на предприятии в виде Технического регламента.
4. На предприятии была проведена внутренняя проверка.
5. Выявлены и классифицированы защищаемые информационные ресурсы, классифицированы предполагаемые нарушители безопасности информации.
6. Разработана политика информационной безопасности и организационно-распорядительная документация в области информационной безопасности.

Слайд 15

Таким образом, Цель работы - разработка политики информационной безопасности и организационно-распорядительной документации в области информационной безопасности для предприятия ФКУ «Налог-Сервис» ФНС России в Тюменской области – **достигнута.**

Спасибо за внимание! Доклад окончен.