



Обеспечение информационной безопасности на предприятии

Выполнил:

ФИО

Научный руководитель проекта:

ФИО



ЦЕЛЬ, ЗАДАЧИ

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

Задачи:

1. анализ информационной системы;
2. анализ и классификация источников угроз информации;
3. разработка частной модели угроз информационной безопасности;
4. разработка политики информационной безопасности;
5. разработка регламентов, положений и инструкций в области информационной безопасности.

Анализ информационной системы

Описание предприятия:



ФКУ
НАЛОГ-СЕРВИС
ФНС РОССИИ

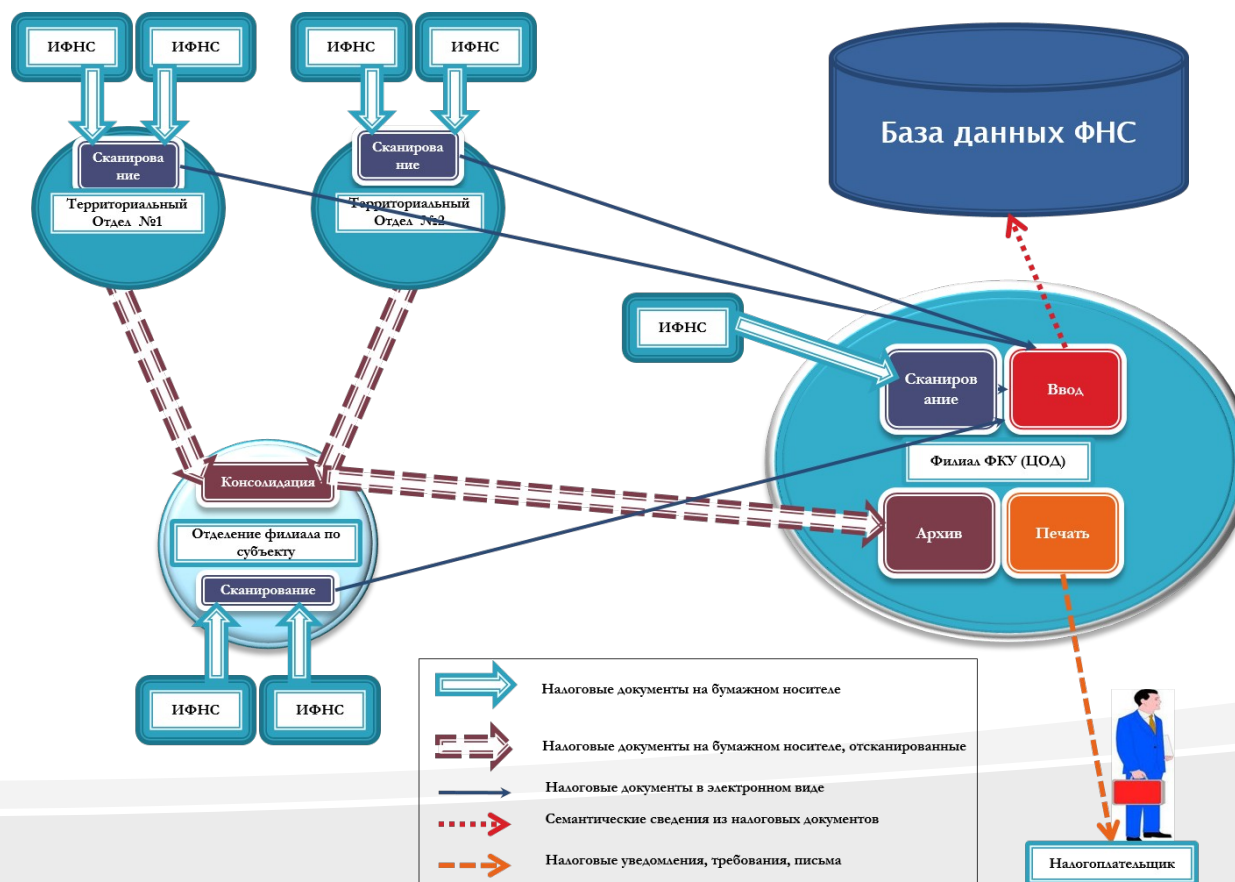
Основная цель - организационно-техническое и информационное обеспечение деятельности Федеральной налоговой службы России и ее территориальных органов

Основные виды деятельности ФКУ «Налог-Сервис»:

1. централизованный ввод в систему электронной обработки данных (ЭОД) данных, поступивших в налоговую инспекцию на бумажном носителе .
2. централизованная печать и/или массовая рассылка налогоплательщикам налоговых документов.
3. централизованное архивное хранение .
4. формирование архивных фондов.
5. обеспечение мероприятий по защите информации.

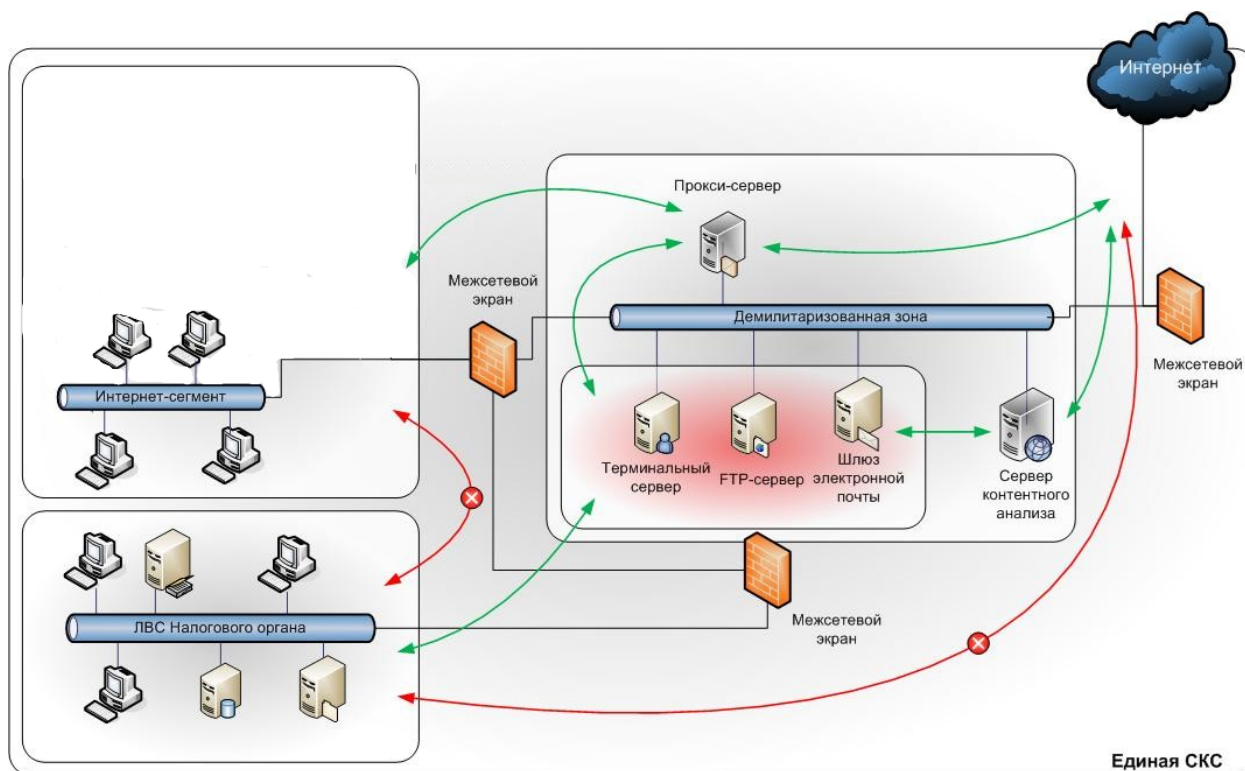
Анализ информационной системы

Схема системы документооборота:



Анализ информационной системы

Структура и особенности сети предприятия:





Разработка частной модели угроз

Описание ИСПДн:

Содержание объектов защиты для ИСПДн предприятия:

Описание объекта безопасности	Примечание
ПДн в виде акустических (речевых) сигналов.	В организации не производится голосовая обработка ПДн.
ПДн на средствах отображения графической, видео- и буквенно-цифровой информации.	В организации применяются СВТ, обрабатывающие видовую информацию: мониторы АРМ и серверов.
ПДн в виде побочных информативных электромагнитных полей и электрических сигналов.	В ИСПДн применяются средства вычислительной техники, обладающие свойствами излучения ПЭМИ: (системные блоки, мониторы и т.п.).
АРМ пользователя ИСПДн.	В ИСПДн имеются рабочие станции пользователей, на которых производится обработка персональных данных.
Серверы ИСПДн.	В ИСПДн имеются серверы, на которых производится обработка персональных данных.



Разработка частной модели угроз

Описание ИСПДн:

Антропогенные источники угроз:

Внешние антропогенные источники	Внутренние антропогенные источники
Криминальные группы и отдельные преступные субъекты	Работники предприятия (Основной персонал)
Потенциальные преступники (недобросовестные налогоплательщики) и хакеры	Администраторы АС, ЛВС, ТКУ, Администратор безопасности, программисты, администратор домена
Персонал поставщиков телематических услуг (Провайдеры)	Технический персонал
Представители надзорных организаций и аварийных служб	Работники отдела безопасности

Техногенные источники угроз:

Внешние техногенные источники угроз	Внутренние техногенные источники угроз
Средства связи, промышленные установки ионизирующего излучения, системы энергообеспечения	Некачественные технические средства обработки информации
Сети инженерных коммуникаций (водоснабжения, канализации)	Некачественные программные средства обработки информации
Транспорт (авиационный, железнодорожный, автомобильный,	Вспомогательные средства (охраны, сигнализации, телефонии, видеонаблюдения, СКУД)



Разработка частной модели угроз

Модель нарушителя:

Описание модели нарушителя для ИСПДн предприятия

1. Лица, не имеющие права доступа в контролируемую зону информационной системы.
2. Лица, имеющие санкционированный доступ к ИСПДн, но не имеющие доступа к ПДн.
3. Зарегистрированные пользователи ИСПДн, осуществляющие ограниченный доступ к ресурсам ИСПДн с рабочего места.
4. Зарегистрированные пользователи ИСПДн, осуществляющие удаленный доступ к ПДн по локальным и (или) распределенным информационным системам.
5. Зарегистрированные пользователи ИСПДн с полномочиями администратора безопасности сегмента (фрагмента) ИСПДн.
6. Зарегистрированные пользователи с полномочиями системного администратора ИСПДн.
7. Зарегистрированные пользователи с полномочиями администратора безопасности ИСПДн.
8. Программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на защищаемом

Разработка частной модели угроз

Определение актуальных угроз безопасности ПДн в

Расход исходной защищенности ИСПДн предприятия (фрагмент)

Показатели защищенности	Уровень защищенности		
	Высокий	Средний	Низкий
Технические и эксплуатационные характеристики ИСПДн			
По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования:	–	–	+



Разработка политики информационной безопасности и организационно-распорядительной документации

Планирование мероприятий по информационной безопасности для компонент автоматизированной системы:

1. Предпроектная стадия
2. Стадия разработки/приобретения
3. Стадия установки
4. Стадия функционирования и поддержки
5. Стадия списания



Разработка политики информационной безопасности и организационно-распорядительной документации

Физическая безопасность:

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



Разработка политики информационной безопасности и организационно-распорядительной документации

Технические средства:

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



Разработка политики информационной безопасности и организационно-распорядительной документации

Функциональные средства:

1. Работа с персоналом
2. Планирование непрерывной работы
3. Средства поддержки программных приложений
4. Средства обеспечения целостности информации
5. Документирование
6. Осведомлённость и обучение специалистов
7. Осведомлённость и обучение специалистов
8. Действия в случаях возникновения происшествий



Разработка политики информационной безопасности и организационно-распорядительной документации

Выводы:

1. Разработаны необходимые организационно-методические документы и политика информационной безопасности на основе методических рекомендаций.
2. Сотрудники предприятия были должным образом проинструктированы и осведомлены об особенностях защиты информации на предприятии.
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-распорядительную документацию в области



Обеспечение информационной безопасности на предприятии

СПАСИБО ЗА ВНИМАНИЕ!