Исследование методов защиты информации в автоматизированных системах обработки конфиденциаьных данных и информационных системах управления процессами предприятия

ПАО «Мобильные ТелеСистемы» Макро-регион «Урал»

Студент: Ялунин М. Р.
Группа: РИ-510702

ПАО «МТС»

Год основания:	1993
Продукция:	Сотовая связь, проводная телефонная связь, широкополосный доступ в Интернет, телевидение

- Порядка 100 миллионов абонентов
- Услуги по всей России, Украине, Беларуси и странам СНГ
- Самый дорогой российский телекоммуникационный бренд по данным рейтинга BRANDZ™

Нормативно-методическая документация

1. Система управления информационной безопасностью «Базовый уровень информационной безопасности операторов связи» - Международный союз электросвязи от 4 октября 2007 г.
2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных»
3. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.12.2014) «Об информации, информационных технологиях и о защите информации»
4. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 13.07.2015) «О связи»
5. Стандарты и политики компании по безопасности ОАО «МТС»

Защита информации в ПАО «МТС»

У любого предприятия, дорожащего своей репутацией и прибылью, должна быть чётко сформирована система защиты, как информации, так и предприятия в целом. На таком предприятии, как ОАО «Мобильные ТелеСистемы» утечка данных может привести не только к краху корпорации, но и нанести ущерб клиентам компании, так как в автоматизированной системе организации находятся персональные данные клиентов, включающие паспортные данные, которые должны храниться в секрете от посторонних лиц.

Компания ОАО «Мобильные ТелеСистемы» хранит персональные данные своих клиентов, сотрудников, вкладывая немалые средства в обеспечение своей защиты и защиты клиентов.

Базовый уровень информационной безопасности операторов связи

Стандарт разработан Международным Союзом Электросвязи, а в России наибольший вклад в его развитие внесла Ассоциация Документальной Электросвязи.

«Базовый уровень ИБ операторов связи» представляет собой минимальный набор рекомендаций, реализация которых должна гарантировать определенный уровень ИБ коммуникационных услуг, позволяя при этом обеспечить баланс интересов операторов, пользователей и государства. Разработка этого норматива обусловлена развитием телекоммуникационной отрасли: операторы связи вынуждены объединять свои сети, чтобы предоставлять необходимый набор услуг, но при этом сами операторы не знают, с кем они имеют дело и кому они могут доверять, чтобы избежать угроз ИБ. Для этих целей и вводится «Базовый уровень».

Исследование средств защиты данных

Для исследования средств ИБ рассмотрим:

1. «*АРМ Конфиденциальная связь*» - объект информатизации, предназначенный для обработки конфиденциальной информации

1. ИСПДн «*QuotA*» - информационная система управления технологическими процессами предприятия

«АРМ Конфиденциальная связь»

Предназначение: обработка конфиденциальной информации.

Перечень защищаемых информационных ресурсов автоматизированной системы «АРМ Конфиденциальная связь».

1. Перечень информационных задач, материалов, обрабатываемых на объекте ВТ:
   - создание и обработка текстовых документов;
   - вывод документов на печать;
   - сохранение документов на ГМД;
   - сохранение документов на оптических носителях;
   - сохранение документов на USB flash-накопителях.

2. Перечень информационных ресурсов объекта ВТ ограниченного доступа:
   - конфигурационные файлы СЗИ НСД;
   - каталоги, содержащие конфиденциальные документы:
     - D:\Документы\конфиденциально (конфиденциально);
     - на съемных носителях.

«АРМ Конфиденциальная связь»: средства защиты

1. Физическая защита:
   - физическая охрана объектов;
   - наличие СКД;
   - видеонаблюдение.

«АРМ Конфиденциальная связь»: средства защиты

2. Защита от несанкционированного доступа.
   - СЗИ НСД «Аккорд-NT/2000»:
     - ✔ доверенная загрузка (загрузка ОС происходит после авторизации на СЗИ с помощью ключа);
     - ✔ на прикладном уровне осуществляется разграничение доступа.
   - Парольная защита ОС.

«АРМ Конфиденциальная связь»: средства защиты

3. Антивирусная защита.
4. Защита от ПЭМИН
5. Сетевая защита
6. Лицензионное ПО (системное и прикладное)

ИСПДн «QuotA»

«Quota» - информационная система, в которой регистрируют заявки абонентов на обслуживание (фиксированная связь):

- интернет;
- телевидение;
- телефония (проводная);

Предназначение: система предоставляет возможность в канале продаж в режиме онлайн назначать время выхода монтажника при подключении клиентов и при решении Trouble Tickets (сообщения о неисправности или снижении параметра качества)

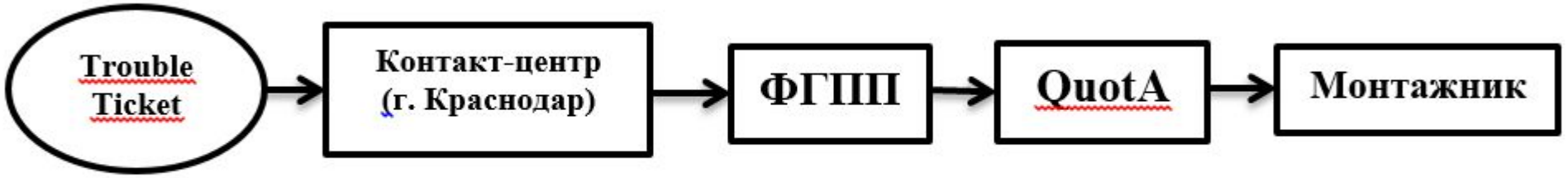
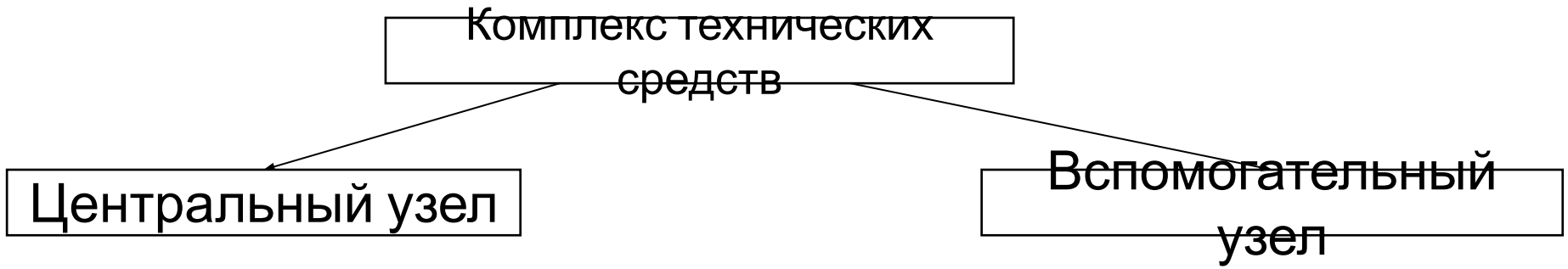


Рисунок 2.1 – Схема движения Trouble Ticket

ИСПДн «QuotA»



КТС Центрального узла состоит из:

- 1-го виртуального сервера;
- 1-ой системы хранения данных (СХД).

КТС Вспомогательного узла состоит из:

- 1-го виртуального сервера;
- 2-х СХД.

ИСПДн «QuotA»: средства защиты

1. Физическая защита:
   - физическая охрана объектов;
   - наличие СКД;
   - видеонаблюдение.
2. Парольная защита ОС
3. Антивирусная защита
4. Лицензионное ПО
5. Сетевая безопасность

Аудит удаленного доступа

Цель: выявить и устранить удаленные доступы непривилегированным сотрудникам.

Этапы работы.

1. Получение информации об уволенных и переведенных сотрудниках ОАО «МТС» Макро-регион «Урал» за 2014-2015 гг.
2. Получение информации о сотрудниках, имеющих удаленный доступ к VPN-шлюзу ОАО «МТС» Макро-регион «Урал».
3. Сопоставление полученных данных, составление таблицы сотрудников, у которых удаленный доступ необходимо устранить.

Аудит удаленного доступа

В компании существует 2 способа удаленной авторизации:

- с помощью RSA-токена;
- через FreeRadius-сервера (SMS-авторизация)

Аудит удаленного доступа: Результаты

1. Выявлены и аннулированы учетные записи сотрудников, которые были переведены или уволены, но имели удаленный доступ к VPN-шлюзу через RSA-сервера.
2. Выявлены и аннулированы учетные записи сотрудников, которые были переведены или уволены, но имели удаленный доступ к VPN-шлюзу через FreeRadius-сервера (SMS-авторизация).
3. Выявлены и аннулированы удаленные доступы сотрудников, которые авторизовались удаленно на VPN-шлюзе более 3-х месяцев назад.

Аудит соответствия стандартам

Цель: сравнить сведения о конфигурации всех рабочих серверов ОАО «МТС» Макро-регион «Урал» с сведениями из внутренних стандартов политики безопасности предприятия; устранить все несоответствия.

Этапы работы.

1. Изучение внутренних стандартов политики безопасности.
2. Получение информации о конфигурации рабочих серверов:
    - сервера контроллеров домена;
    - файловые сервера;
    - сервера печати;
    - сервера приложений.
3. Сравнение полученной информации со стандартами.
4. Формирования итогового документа с выявленными несоответствиями.

Заключение

В ходе выполнения задания на научно-исследовательскую практику получены следующие результаты.

1. Изучены основные стандарты и политики информационной безопасности предприятия.
2. Исследованы методы защиты информации на объекте информатизации «АРМ Конфиденциальная связь» и на ИСПДн «QuotA».
3. Проведены аудит на соответствие сведений о конфигурациях внутренних серверов стандартам политики безопасности предприятия и аудит на удаленный доступ в корпоративную сеть непривилегированных сотрудников.

Спасибо за внимание!