ЗАЩИТА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРЕДПРИЯТИЯ

Р.Х.БАЛТАЕВ

Пермский государственный национальный исследовательский университет, 614990, Пермь, Букирева, 15

Задачи работы:

1. Определение исходных данных для построения частной модели угроз.

2. Разработка частной модели угроз безопасности персональных данных.

3. Разработка системы защиты персональных данных.

В информационной системе предприятия обрабатываются персональные данные работников предприятия.

В обработке персональных данных участвует следующий персонал:

1. Администратор БД ПДн
2. Сетевые администраторы
3. Инженеры-электроники (отвечают за тех. обслуживание АРМ)
4. Пользователи ИСПДн (имеют доступ к ПДн только для чтения)
5. Привилегированные пользователи ИСПДн (имеют доступ к ПДн для чтения, записи, изменения)

Схема информационной системы персональных данных предприятия представлена на рис. 1.

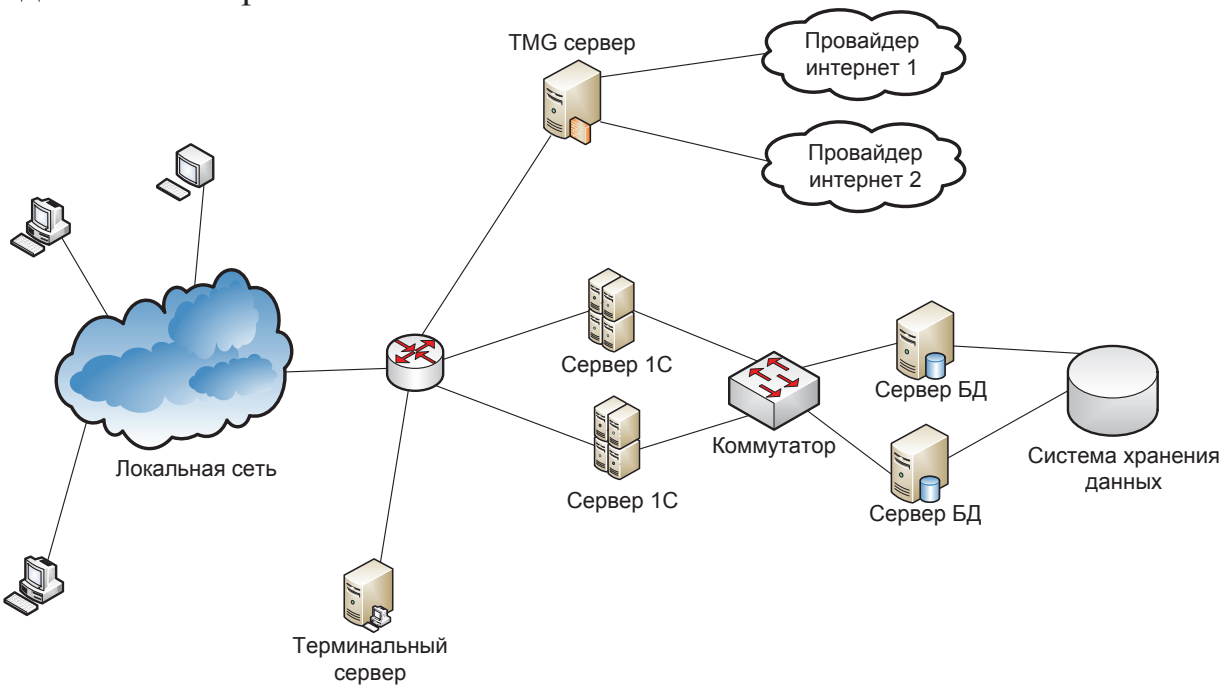

Рис. 1. *Схема ИСПДн предприятия*

В качестве средства разграничения сети предприятия от сети Интернет используется прокси-сервер MS TMG. ИСПДн построена на основе трехзвенной архитектуры клиент-сервер. Доступ пользователей к персональным данным осуществляется с помощью “тонких” клиентов и “нулевых” клиентов. В качестве сервера приложений используется кластер серверов 1С. Персональные данные обрабатываются в СУБД MS SQL-server. Данные в СУБД MS SQL-server передаются из системы хранения данных по протоколу iSCSI. В системе хранения данных находятся не только персональные данные, но и общие данные.

В частной модели угроз безопасности персональных данных были определены вероятные нарушители безопасности персональных данных, возможные угрозы безопасности персональных данных, уровень исходной защищенности ИСПДн, вероятность реализации угроз в ИСПДн, возможность реализации угроз в ИСПДн, опасность угроз в ИСПДн и актуальные угрозы безопасности персональных данных.

Вероятные нарушители безопасности ПДн:

- Внешние нарушители

1. Недобросовестные партнеры

2. Внешние субъекты (осуществление НСД через сеть Интернет)

- Внутренние нарушители

1. Инженеры-электроники

2. Пользователи ИСПДн

3. Привилегированные пользователи ИСПДн

Возможные угрозы безопасности ПДн [1]:

- Утечка видовой информации

- Перехват управления загрузкой ОС

- Вызов штатного или специального ПО реализующих НСД

- Угрозы внедрения вредоносных программ

- Угроза “анализ сетевого трафика”

- Угроза сканирования сети

- Угрозы внедрения ложного объекта сети

- Угрозы типа “отказ в обслуживании”

- Угрозы выявления паролей

- Угрозы удаленного запуска приложений

- Угрозы внедрения по сети вредоносных программ

- Искажение или уничтожение информации в результате ошибок пользователей

Уровень исходной защищенности ИСПДн определен как “средний”. [2]

Актуальность угроз безопасности персональных данных определяется на основании возможности реализации угроз ИСПДн и опасности угроз в ИСПДн. [2]

Актуальные угрозы безопасности ПДн:

- Угроза внедрение в ИСПДн вредоносных программ

- Угроза сканирования сети

- Угрозы выявления паролей

- Угрозы внедрения по сети вредоносных программ

Защита информационной системы персональных данных реализуется на основании требований ФСТЭК по обеспечению безопасности персональных данных и должна обеспечивать нейтрализацию актуальных угроз безопасности ПДн. [3] Реализация защиты персональных данных представлена на рис. 2.

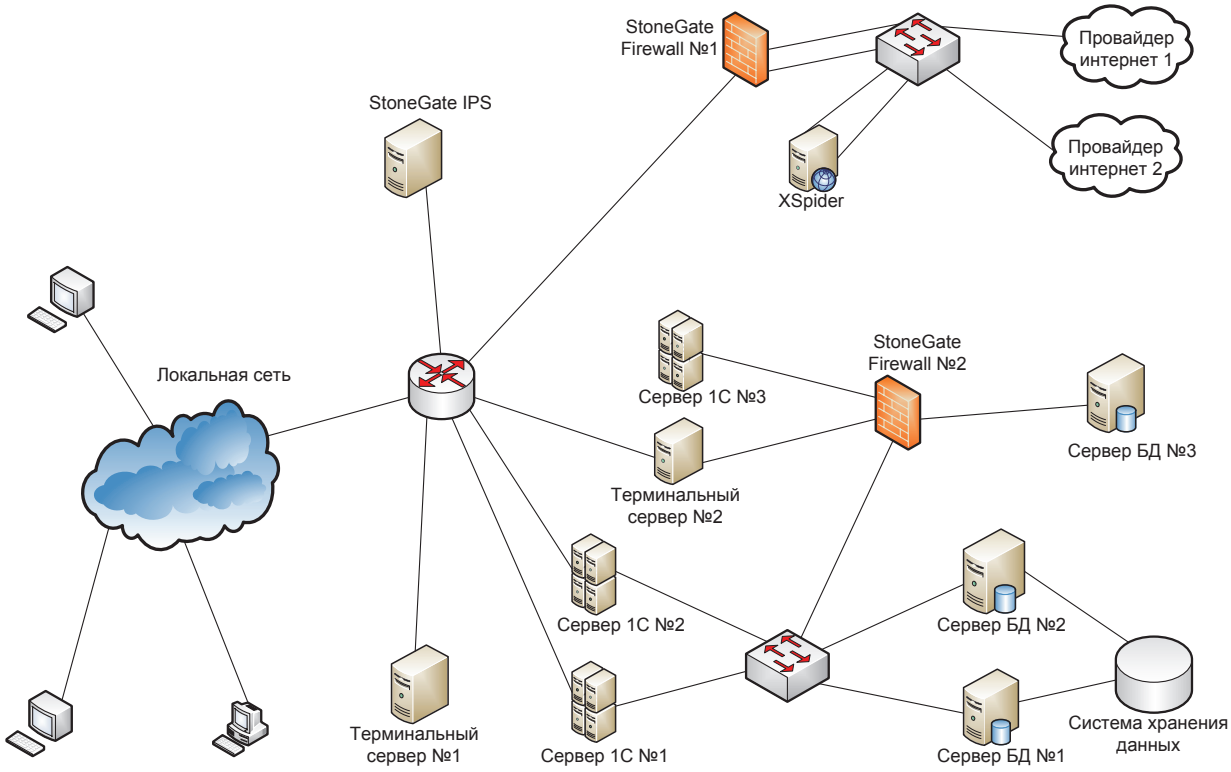

Рис. 2. *Схема системы защиты ИСПДн*

Безопасность межсетевого взаимодействия обеспечивается с помощью межсетевого экрана StoneGate Firewall №1, средства анализа защищенности XSpider и системы обнаружения вторжений StoneGate IPS.

Информационная система персональных данных делится на две подсистемы с помощью межсетевого экрана StoneGate Firewall №2. Первая подсистема содержит обезличенные персональные данные, которые располагаются в системе хранения данных. Доступ к обезличенным ПДн через Сервер БД №1 и Сервер БД №2, Сервер 1С №1 и Сервер 1С №2. Требования к защите обезличенных персональных данных не предъявляются. [3]

Во второй подсистеме доступ к персональным данным осуществляется только через “тонкие” и “нулевые” клиенты, в которых реализована доверенная загрузка образов операционных систем. Аутентификация пользователей ПДн происходит в СЗИ от НСД Dallas Lock, установленное на терминальном сервере №2. В качестве средства антивирусной защиты используется Dr.Web, который установлен на серверах БД, серверах 1С, терминальных серверах и ПЭВМ.

СПИСОК ЛИТЕРАТУРЫ

1. “Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных” (выписка) ФСТЭК России от 15 февраля 2008 г.

2. “Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных” ФСТЭК России от 14 февраля 2008 г.

3. Приказ ФСТЭК России от 5 февраля 2010 г. N 58 “Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных”