Дипломная работа

По теме: Аудит информационной безопасности

Выполнил: Канунов Артём

Введение

Аудит информационной безопасности — один из важнейших этапов построения надежной системы защиты информации предприятия. Комплексная проверка позволяет увидеть полную картину состояния ИБ на предприятии, локализовать имеющиеся проблемы и слабые места системы защиты и разработать эффективную программу построения системы информационной безопасности предприятия

Актуальность

Актуальность выбранной темы дипломной работы обусловлена тем, чтобы показать на примере предприятия насколько недооценен аудит, подойдя комплексно к устранению утечек информации, несанкционированного доступа, а также к другим уязвимостям на предприятиях.

Цели и задачи дипломной работы

Цель дипломной работы – изучить аудит информационной безопасности и провести его на примере предприятия.

Для достижения цели поставлены следующие задачи:

- Изучить основные этапы проведения аудита
- Исследовать аудит на примере предприятия (ООО):
- Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- Оценка текущего уровня защищенности ИС;
- Локализация узких мест в системе защиты ИС;
- Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.
- Сформулировать выводы по проделанной работе.

Раздел 1. Законы и правовые нормы.

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В Гражданском кодексе Российской Федерации фигурируют такие понятия, как банковская, коммерческая и служебная тайна. Согласно статье 139, информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Раздел 2. Теоретическая часть темы диплома

Общепринятая методика аудита выделенных помещений условно разделяет действия по выявлению средств несанкционированного съема информации (НСИ) на три этапа:

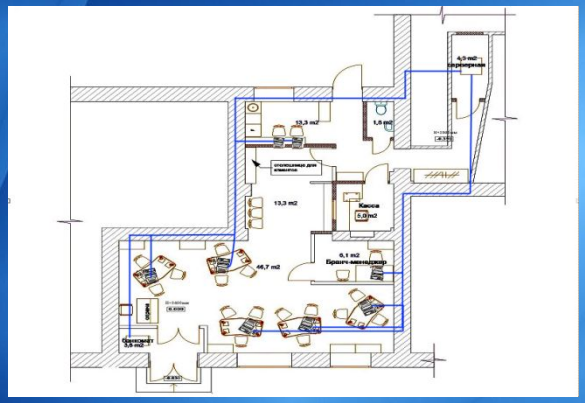
- Подготовительный этап;
- Этап непосредственного проведения аудита;
- Заключительный этап.

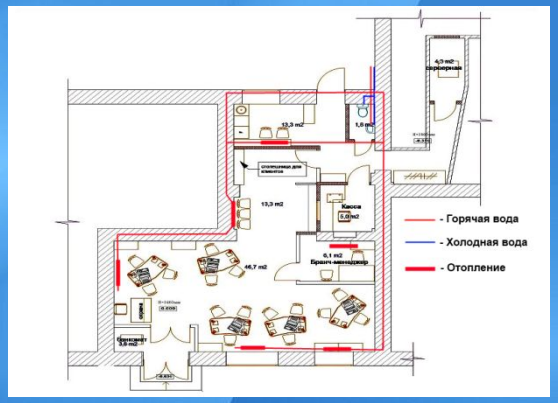
Раздел 3. Проведение аудита информационной безопасности на предприятии.

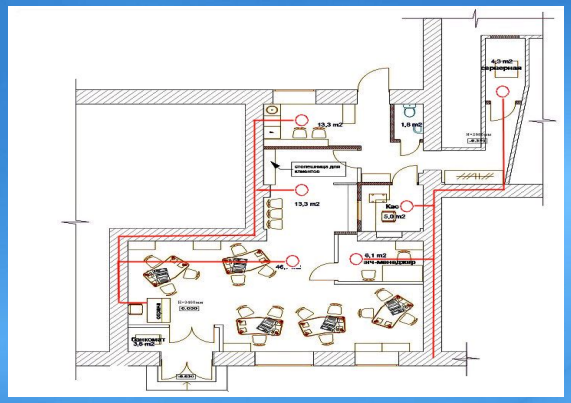
В практической части я проведу аудит информационной безопасности на примере коммерческого банка ООО “Должанский Банк”.

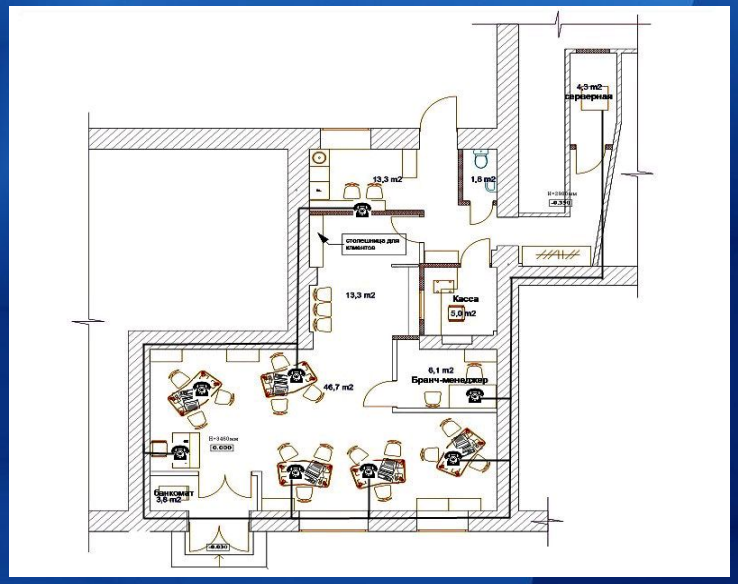
- Для проведения аудита информационной безопасности поставлены следующие задачи:
- Проанализировать риски, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- Оценить текущий уровень защищенности ИС;
- Устранить слабые места в системе защиты ИС;
- Разработать рекомендации по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

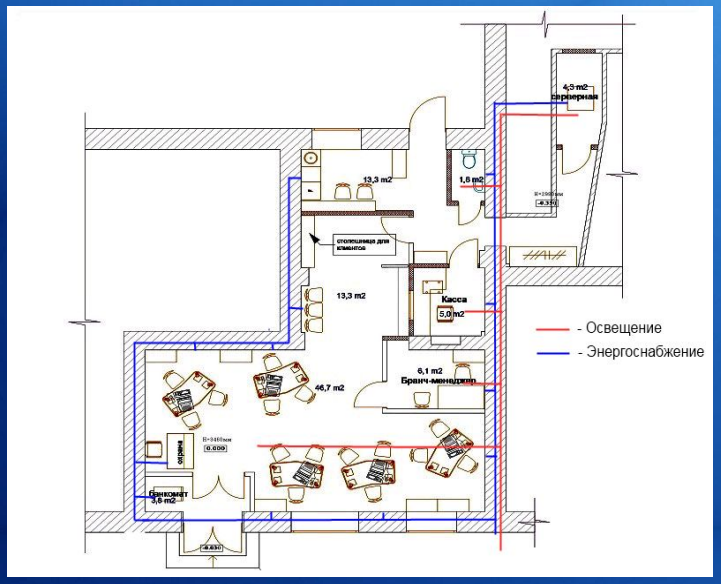
Подготовительный этап











Проведение аудита информационной безопасности

1. Аудит информационной безопасности начинается с осмотра ограждающих конструкций, мебели и других предметов интерьера.
2. Далее нужно произвести осмотр тех же предметов интерьера и мебели, только с помощью специальных поисковых технических средств.

Комплект
ПОИСК-2

Нелинейный локатор
NR-900EM

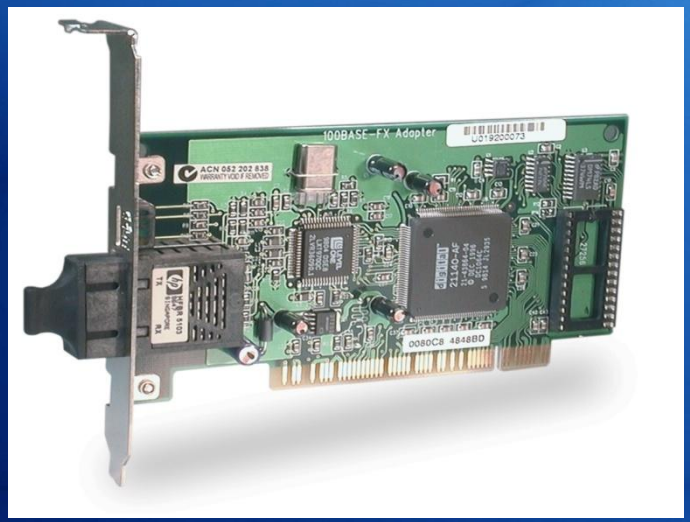
Проведение аудита информационной безопасности

3. Выполнение мер по активации внедренных средств НСИ (Негласный съём информации).

Комплекс обнаружения радиоизлучающих средств и радиомониторинга КРОНА-Про

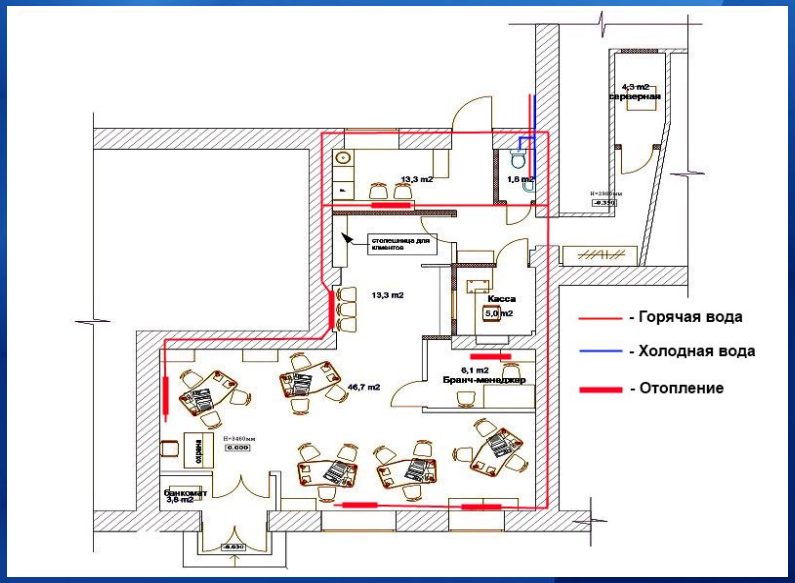
Проведение аудита информационной безопасности

4. Следующим этапом является проверка линий и оборудования проводных коммуникаций.
5. Поиск средств негласного съема и передачи информации, внедренных в электронные приборы.



Проведение аудита информационной безопасности

6. Исследование звукопроницаемости элементов конструкций, проверка трубопроводных и других технологических коммуникаций на наличие в них акустических и виброакустических сигналов из проверяемого помещения.



Многофункциональный поисковый прибор ST 031 Пиранья

Проведение аудита информационной безопасности

7. Исследование побочных электромагнитных излучений компьютеров, оргтехники, и другого оборудования для выявления в них ых сигнал

Программно-аппаратный комплекс Навигатор-П-3Г

Устройство "Октава-РС"

Заключительный этап проведения аудита информационной безопасности

Уровень защищенности данного предприятия не очень высок, несмотря на то, что у банка отсутствуют явные уязвимости. Риск довольно высок, допущены грубые грубые ошибки.

В ходе проведения аудита в банке ООО “Должанский банк” были детально изучены помещения и сформулированы следующие выводы по оценке информационной безопасности предприятия:

- Кабели телефонной связи проложены неправильно, имеют слишком большую длину, директору банка стоит обратить на это внимание;
- Сетевым кабелям не место в банке, скорость интернета значительно страдает из за этого, к тому же злоумышленник может снять побочные электромагнитные излучения, персональные данные клиентов, а также это может затронуть финансы банка;
- Исследование побочных электромагнитных излучений компьютеров показало высокий уровень информативных электромагнитных излучений, что может также привести к съему ПЭМИН.
- Отсутствие бесперебойного питания, что может привести к сбоям и потери информации.

Рекомендации по устранению уязвимостей.

D-Link DGE-560SX

ИБП APC BX650CI-RS

Устройство "Октава-РС"

Покупка	Количество (шт.)	Цена (руб.)
Сетевая карта D-Link DGE-	20	10140 руб
МГТС GPON	1	2000 руб./мес.
Устройство "Октава-РС"	1	33 925 руб
ИБП APC BX650CI-RS	20	5089 руб

Итог: 340 505 руб.

Заключение

Я выбрал данную тему дипломной работы из за её актуальности. Аудит информационной безопасности – неотъемлемая часть объективной оценки безопасности, без её помощи сложно представить комплексную защиту информации.

Цель настоящей работы заключается в изучении и демонстрации на примере предприятия, как проводится аудит информационной безопасности.

Для достижения указанной цели перед работой был поставлен ряд задач.

При решении задачи изучения аудита информационной безопасности, в работе были показаны правовые аспекты и основные этапы проведения аудита, были также показаны технические средства, с помощью которых проводится аудит.

При решении задачи исследования аудита информационной безопасности на примере предприятия ООО “Должанский Банк” мною были получены следующие результаты:

- Были проанализированы риски, связанные с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- Был оценен текущий уровень защищенности ИС;
- В ходе работы были локализованы узкие места в системе защиты ИС;
- Были выработаны рекомендации по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.
- Был проведён расчёт затрат на устранение уязвимостей;

Таким образом, задачи решены в полном объёме, цель достигнута – изучить аудит информационной безопасности и провести его на