Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Институт электронной техники и приборостроения

Кафедра Информационная безопасность автоматизированных систем

Направление 10.05.03 Информационная безопасность автоматизированных систем

Практическая работа №3

по дисциплине «Угрозы информационной безопасности»

по теме «Анализ источников, каналов распространения и каналов утечки информации»

Выполнил: студент 4 курса
учебной группы с-ИБС42
очной формы обучения
Солодилов В.В.
Проверил: аспирант каф. ИБС
Шелудяков Д.А.

Саратов 2022

Цель работы: формирование навыка работы с нормативными документами по вопросу; анализ угроз информационной безопасности.

Задание

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Контрольные вопросы

1. Что такое информационный риск?
2. В чем заключается задача управления информационными рисками?
3. Какие существуют методики оценки рисков и управления ими?
4. Какие формулы используются при количественной оценке информационных рисков?

Задание

В качестве объекта, для которого можно провести анализ защищенности, была выбрана локальная сеть СГТУ.

1) Для данного объекта могут быть присущи следующие виды угроз:
    a. *Нарушение физической целостности* – поломка отдельных частей локальной сети, не влияющих на её работоспособность (например, отдельного компьютера), или нарушение работы участков или целой сети в случае выхода из строя основополагающих компонентов (коммутаторов, маршрутизаторов или отдельного сервера), например, в результате сбоя аппаратуры или влияния природных факторов.
    b. *Нарушение логической целостности* – разрушение построенных логических связей между участками локальной сети. Возможно при неправильной настройке новых, только добавленных в сеть компонентов.
    c. *Нарушение содержания* – нарушение целостности информации, возникающее при переносе или изменении целых блоков информации, а также добавлении заведомо ложной информации. Маловероятно внутри сети, так как настроено разделение прав доступа для отдельных ПК. Возможно осуществить при атаках извне.
    d. *Нарушение конфиденциальности* – происходит при значительном изменении компонентов защиты, например, при устаревании антивирусного ПО. В результате этого становится более вероятным успех при атаке извне.
    e. *Нарушение прав собственности* – включает несанкционированные копирование и использование информации. Возможен как изнутри, так извне.

2) Опираясь на виды угроз, которые возможно осуществить в отношении данного объекта, можно выделить характер происхождения данных угроз:
    a. Случайные факторы. К ним относятся:
        i. *Несчастные случаи и стихийные бедствия.* В результате данных факторов уничтожится вся информация, которая хранится на твердых и/или электронных носителях. Данных исход маловероятен, но возможен.
        ii. *Ошибки в процессе обработки информации.* Они могут привести к искажению достоверной информации. Являются более вероятными событиями.
    b. Умышленные факторы. Наступление данных факторов наиболее вероятно по сравнению со случайными факторами, что требует повышенного внимания для недопущения их реализации.

    К умышленным факторам можно отнести:

        i. Хищение носителей информации
        ii. Несанкционированный доступ
        iii. Копирование данных
        iv. Разглашение информации.
3) Каналы несанкционированного доступа можно разделить на 2 группы:
    a. *Каналы от источника информации при несанкционированном доступе к нему.* К ним относятся:
        i. Хищение носителей информации (как на твердых, так и на электронных носителях).
        ii. Копирование информации с носителей.
        iii. Подслушивание разговоров и установка закладных устройств в помещение и съем информации с них.
    b. *Каналы со средств обработки информации при несанкционированном доступе к ним.* К ним относятся:
        i. Снятие информации с устройств электронной памяти.

ii. Установка закладных устройств в средства обработки информации (характерно для электронных носителей).
iii. Ввод программных продуктов, позволяющих злоумышленнику снимать информацию.

4) Источники появления угроз. Основными источниками появления угроз являются:
   a. *Люди* – посторонние лица, пользователи (студенты) или персонал. При внедрении злоумышленника из числа данных лиц вполне возможна утечка информации, модификация, хищение или уничтожение.
   b. *Технические устройства* – закладные, шпионские устройства. Возможна их установка при проникновении на территорию университета посторонних лиц.
   c. *Модели, алгоритмы, программы* – характерны для электронных носителей злоумышленника. В результате реализации данных действий с носителя возможно получение несанкционированного доступа к информации.
   d. *Технологические схемы обработки* – модификация или удаление поступающей информации при внедрении вредоносного ПО.
5) Причины нарушения целостности информации можно разделить на *преднамеренные* и *непреднамеренные*.
   a. Первые происходят в результате действия злоумышленников, которые попытаются получить несанкционированный доступ к информации практически любым способом.
   b. Вторые происходят в результате или стихийных угроз, которые сложно контролировать и сложно ликвидировать их последствия, или в результате случайных, без злого умысла действий сотрудников.
6) Для несанкционированного доступа к информации злоумышленник может:

a. Осуществить атаку на сервера автоматизированной системы из внешней сети, в том числе с использованием значительного объема вычислительных средств.
b. Проникнуть на охраняемую территории с целью получения доступа как к отдельным персональным компьютерам, так и к целым серверам.
c. Влиться в доверие к сотруднику или студенту, предлагая денежное или иное вознаграждение.
d. Установить прослушивающее/шпионское устройство или использовать устройство для улавливания шумов/вибраций/ЭМИ.

7) На основе всей изученной информации, можно сделать вывод, что класс защищенности данной автоматизированной системы – К2.

Контрольные вопросы

1. Информационным риском называют опасность возникновения убытков или ущерба в результате обработки, хранении и передачи информации с помощью автоматизированных информационных систем, а также сбоев в работе этих систем.
2. Задача управления информационными рисками заключается в своевременном обнаружении всех существующих рисков, оценка вероятности, материальности и последствий их наступления, создание систем и принятие мер по минимизации негативных и увеличению положительных последствий их наступления.
3. Существуют следующие методы анализа рисков:
   - статистический
   - оценки целесообразности затрат
   - экспертных оценок
   - аналитический
   - метод использования аналогов
   - оценки финансовой устойчивости и платёжеспособности
   - анализ последствий накопления риска
   - комбинированный метод
4. Формулу для оценки количественных рисков можно представить в следующем виде:

Величина Риска = Вероятность События * Размер Ущерба, где *Вероятность События* = Вероятность Угрозы * Величина Уязвимости.

Вывод

В результате выполнения практической работы были изучены основные критерии оценки защищенности информации автоматизированной системы, а также проведён анализ защищенности на основе локальной сети СГТУ.