**Практическая работа № 2**

**«Анализ угроз информационной безопасности»**

**Цели:**

1. **Изучить угрозы информационной безопасности**
2. **Научиться определять угрозы и способы их предотвращения**

**1.1 Краткие теоретические сведения**

Информационный объект – это среда, в которой информация создается, обрабатывается, хранится и передается.

Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу.

К настоящему времени известно большое количество угроз информационной безопасности.

Рассмотрим их классификацию по различным классификационным признакам.

По виду:

– физической и логической целостности (уничтожение или искажение информации);

– конфиденциальности (несанкционированное получение);

– доступности;

– права собственности.

По характеру:

– случайные (отказы, сбои, ошибки, стихийные явления);

– преднамеренные (злоумышленные действия людей);

По источникам:

– человек;

– технические устройства;

– программное обеспечение;

– внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам.

Угроза целостности – несанкционированное изменение, искажение, уничтожение информации.

Угроза доступности (отказ в обслуживании) – нарушение работоспособности объекта, доступ к которому получил злоумышленник.

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются, как правило, в теории надежности, программировании, инженерной психологии.

Преднамеренные угрозы связаны с действиями людей (работники спецслужб либо самого объекта, хакеры). Для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если по отношению к ним не предприняты никакие меры защиты, либо нештатными каналами доступа, к которым принято относить:

– побочное электромагнитное излучение информации с аппаратуры системы;

– побочные наводки информации по сети электропитания и заземления;

– побочные наводки информации на вспомогательных коммуникациях;

– подключение к внешним каналам связи.

Таблица 1.1 – Возможная подробная классификация угроз информационной безопасности в зависимости от их источника и происхождения

|  |  |  |
| --- | --- | --- |
| Природные угрозы | Угрозы техногенного характера | Угрозы, созданные людьми |
| – магнитные бури;  – радиоактивные излучения и осадки;  – стихийные бедствия. | – сбои в работе компьютерной сети (КС), вызванные отключением или колебанием электропитания либо другими средствами функционирования КС;  – отказы и сбои КС вследствие её ненадёжности;  – электромагнитные излучения и наводки;  – утечки через каналы связи – электрические, акустические, оптические и др. | – непреднамеренные либо преднамеренные действия:  а) обслуживающего персонала;  б) пользователей;  в) архивной службы;  г) службы безопасности;  д) управленческого персонала;  – хакерские атаки; |

Все методы защиты информации по характеру проводимых действий можно разделить на:

– законодательные (правовые);

– организационные;

– технические;

– комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

**1.2 Практическое задание**

Выполните задание

1. Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации,
2. методы борьбы с данными угрозами.
3. Обозначить источник каждой из приведенных угроз

|  |  |
| --- | --- |
| Вариант | Объект |
|  | Банковская карта |
|  | Учебная аудитория 226 |
|  | Банкомат |
|  | Автоматизированное рабочее место в больнице |
|  | Домашний ПК |
|  | Смартфон |
|  | Цифровая банковская карта |
|  | Домашний ПК |
|  | Рабочее место в банке |
|  | Рабочее место преподавателя университета |
|  | Банкомат |
|  | Цифровая банковская карта |
|  | Учебная аудитория 224 |
|  | Автоматизированное рабочее место в фирме по разработке ПО |
|  | Автоматизированное рабочее место в больнице |
|  | Автоматизированное рабочее место в строительной компании |
|  | Банкомат |
|  | Учебная аудитория 228 |
|  | Цифровая банковская карта |
|  | Учебная аудитория 300 |
|  | Автоматизированное рабочее место бухгалтера |
|  | Автоматизированное рабочее место учителя в школе |
|  | Библиотечный архив |
|  | Автоматизированное рабочее место в детском саду |
|  | Банкомат |

Ответ оформить в виде таблицы

Объект\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Область деятельности\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Характеристики объекта\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Уязвимость | Наименование угрозы | Как избежать угрозы |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |

**1.3 Контрольные вопросы.**

1. Что принято называть угрозой информационной безопасности?

2. Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?

3. Какова классификация угроз информационной безопасности?

4. Что понимается под термином информационный объект?

5. Что представляет собой угроза права собственности?

|  |  |  |
| --- | --- | --- |
| **Угроза информационной безопасности** | **Источник угроз** | **Способы реализации угроз** |
| I. Получение информации | 1. Антропогенный | а) Разглашение, передача или утрата атрибутов  разграничения доступа |
| б) Внедрение агентов в число персонала системы |
| в) Хищение носителей информации |
| г) Незаконное получение паролей и других  реквизитов разграничения доступа |
| д) Несанкционированная модификация  программного обеспечения |
| е) Перехват данных, передаваемых по каналам  связи |
| ж) Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих  устройств |
| II. Анализ характеристик информации | 1. Антропогенный | а) Хищение носителей информации  хищение производственных отходов |
| б) чтение остаточной информации из оперативной памяти и с внешних запоминающих  устройств |
| в) Несанкционированная модификация  программного обеспечения |
| г) Перехват данных, передаваемых по каналам связи, и их анализ |

|  |  |  |
| --- | --- | --- |
| **Угроза информационной**  **безопасности** | **Источник угроз** | **Способы реализации угроз** |
| III. Изменение (искажение, подмена)  информации | 1. Антропогенный | а) Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию  носителей информации, удаление данных и т.п.) |
| б) Непреднамеренное заражение компьютера  вирусами |
| в) Ввод ошибочных данных |
| г) Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных |
| 2. Техногенный | а) аварии в системах электропитания |
| б) нарушение температурного режима в помещениях с критическим оборудованием  (серверы, узлы связи) в результате неисправности систем кондиционирования |
| IV. Нарушение информации | 1. Антропогенный | а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или  программных средств |
| б) Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не  являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.) |
| в) Непреднамеренное заражение компьютера  вирусами |
| г) Игнорирование организационных ограничений  (установленных правил) при работе в системе |
| д) Ввод ошибочных данных |
| 2. Техногенный | а) аварии в системах электропитания |
| б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате  неисправности систем кондиционирования |
| V. Нарушение  работоспособности систем | 1. Антропогенный | а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или  программных средств |
| б) Физическое разрушение или вывод из строя всех или отдельных наиболее важных  компонентов автоматизированной системы |

|  |  |  |
| --- | --- | --- |
| **Угроза информационной**  **безопасности** | **Источник угроз** | **Способы реализации угроз** |
|  | 2. Техногенный | а) закупки несовершенных, устаревших или неперспективных средств информатизации и  информационных технологий; |
| б) аварии в системах электропитания; |
| в) аварии в системах отопления и водоснабжения в непосредственной близости к техническим  средствам обработки информации; |
| г) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате  неисправности систем кондиционирования; |
| д) неумышленное повреждения внешних кабельных систем связи строительными  организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи; |
| е) возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил  противопожарной безопасности. |
| 3. Стихийный | а) Разрушение зданий, отдельных помещений |
| б) воздействие атмосферного электричества |
| в) возникновение стихийных очагов пожаров |