

Практическая работа № 2

Тема Выявление угроз информационной безопасности в конкретных ситуациях

Цели:

- изучить угрозы информационной безопасности
- научиться определять угрозы и способы их предотвращения

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.

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.

В таблице 2 представлена подробная классификация угроз информационной безопасности в зависимости от их источника и происхождения

Таблица 2

Классификация угроз информационной безопасности

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;	– непреднамеренные либо преднамеренные действия: а) обслуживающего персонала; б) пользователей;

	– отказы и сбои КС вследствие её ненадёжности; – электромагнитные излучения и наводки; – утечки через каналы связи – электрические, акустические, оптические и др.	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.

Методические указания

1. Заполните таблицу 3.

Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами.

Обозначить источник каждой из приведенных угроз.

Таблица 3

Анализ примеров нарушений информационной безопасности

№	Объект защиты	Наименование угрозы	Источник угрозы	Последствия	Как избежать угрозы
1	Банковская карта				
2	Рабочее место директора				
3	Домашний компьютер				
4	Рабочее место в больнице				
5	Фирма по разработке ПО				
6	Банкомат				

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?