Практическая работа №1

# АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

**Цель работы.** Изучить типовой алгоритм описания информационной системы. Приобрести практические навыки по его применению. Научиться идентифицировать угрозы информационной системы, их источники и методы парирования.

## Краткие сведения из теории

На этапе описания информационной системы (ИС) необходимо указать цели ее создания, границы, информационные ресурсы, требования в области информационной безопасности (ИБ) и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом:

– аппаратные средства ИС, их конфигурация;

– используемое программное обеспечение (ПО);

– интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии;

– типы данных и информации;

– персонал, работающий в данной ИС (обязанности);

– миссия данной ИС (основные цели);

– критичные типы данных и информационные процессы;

– функциональные требования к ИС;

– категории пользователей системы и обслуживающего персонала;

– формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и т. д.);

– архитектура подсистемы ИБ;

– топология локальной сети;

– программно-технические средства обеспечения ИБ;

– входные и выходные потоки данных;

– система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ);

– существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т. д.);

– организация физической безопасности;

– управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и т. д.).

**Активы организации** – все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении. К активам организации могут относиться:

– информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т. д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

– выпускаемая продукция и/или оказываемые услуги;

– аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы;

– программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;

– данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;

– пользователи, обслуживающий персонал;

– документация: по программам, по аппаратуре, системная, по административным процедурам;

– расходные материалы: бумага, формы, красящая лента, магнитные носители.

Для системы, находящейся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

**Анализ угроз информационной безопасности.** Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу. Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Уязвимость объекта – это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

Атака – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая 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). Угроза целостности – несанкционированное изменение, искажение, уничтожение информации;

– конфиденциальности (несанкционированное получение). Угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам;

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

– права собственности.

*По характеру:*

– случайные (отказы, сбои, ошибки, стихийные явления). 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 (злоумышленные действия людей). 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.

*По источникам:*

– человек;

– технические устройства;

– программное обеспечение;

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

Угроза, как следует из определения, – это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

Угрозами безопасности информации являются нарушения при обеспечении:

– конфиденциальности;

– доступности;

– целостности.

**Конфиденциальность информации** – это свойство информации быть

известной только аутентифицированным законным ее владельцам или пользователям. Нарушения при обеспечении конфиденциальности:

– хищение (копирование) информации и средств ее обработки;

– утрата (неумышленная потеря, утечка) информации и средств ее обработки.

**Доступность информации** – это свойство информации быть доступной для аутентифицированных законных ее владельцев или пользователей. Нарушения при обеспечении доступности:

– блокирование информации;

– уничтожение информации и средств ее обработки.

**Целостность информации** – это свойство информации быть неизменной в семантическом смысле при воздействии на нее случайных или преднамеренных искажений или разрушающих воздействий. Нарушения при обеспечении целостности:

– модификация (искажение) информации;

– отрицание подлинности информации;

– навязывание ложной информации.

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 необхо-

димы 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.

## Порядок выполнения работы

1 Описать информационную систему Белорусской железной дороги, выбранный из таблицы 1 в соответствии с предпоследней цифрой шифра.

*Таблица 1* – **Варианты информационных объектов Белорусской железной дороги**

| Цифра шифра | Информационный объект | Цифра шифра | Информационный объект |
|---|---|---|---|
| 0 | Испытательный центр объектов железнодорожного транспорта | 5 | Отдел управления сети связи |
| 1 | Транспортно-логистический центр | 6 | Служба сигнализации и связи |
| 2 | Служба организации труда и заработной платы | 7 | Главный расчетный информационный центр |
| 3 | Служба информационных технологий | 8 | Служба безопасности движения поездов |
| 4 | Служба бухгалтерского учета | 9 | Финансово-экономическая служба |

2 Конкретизировать род деятельности ИО, определить ее штат, структуру административного управления.

3 Категорировать информацию, с которой работают в данном ИО исходя из его рода деятельности.

4 Составить список необходимого оборудования для нормальной работы компании, включая, при необходимости, и бытовую технику.

5 Оценить свойства и стоимость информационных активов ИО. Работу выполнять в виде таблицы 2. Стоимость актива определять в зависимости от его свойств по таблице 3.

*Таблица 2* – **Перечень активов информационного объекта**

| Тип актива | Свойства информационного актива | | | Стоимость актива |
|---|---|---|---|---|
| | целостность | доступность | конфиденциальность | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

*Таблица 3* – **Определение стоимости актива в зависимости от его свойств**

| Стоимость актива, у. е. | Свойства актива | | |
|---|---|---|---|
| | целостность | доступность | конфиденциальность |
| 500 | – | – | – |
| 3 000 | – | – | + |
| 2 000 | – | + | – |

| | | | |
|---|---|---|---|
| 4 000 | – | + | + |
| 2 500 | + | – | – |
| 5 000 | + | – | + |
| 5 500 | + | + | – |
| 20 000 | + | + | + |

6 Определить не менее пяти угроз для выбранных активов, их источников и методов борьбы с ними, которые могут быть реализованы по отношению к информации, создаваемой, хранящейся и обрабатываемой на информационном объекте. Работу выполнять в виде таблицы 4.

*Таблица 4* – **Определение угроз, их источников и методов борьбы с данными угрозами**

| Уязвимость | Наименование угрозы | Источник угрозы | Возможный результат при реализации угрозы, какие активы могут быть повреждены |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Содержание отчета

1 Цель работы.

2 Результаты выполнения задания.

3 Описание информационного объекта.

4 Таблица перечня информационного объекта

5 Таблица угроз, их источников и методов борьбы с данными угрозами для информационного объекта.

6 Вывод по работе.

### Контрольные вопросы

1 Чем информационная система отличается от информационного объекта?

2 Что принято называть угрозой информационной безопасности?

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

4 Какова классификация угроз информационной безопасности?

5 Что понимается под термином «информационный объект»?

6 Что представляет собой угроза права собственности?