БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра информатики

Факультет НиДО

Специальность ИиТП

Контрольная работа № 1

по дисциплине «Основы защиты информации»

Выполнил студент: Дегтярев А.А.

группа 393551

Зачетная книжка № 902021-26

Минск 2016

~15 страниц печатного текста (несколько источников блабла)  
10 и 24

1. Указ Президента РБ “Вопросы ГЦБИ при Президенте РБ”. Концепция национальной безопасности РБ.
2. Электромагнитные каналы утечки информации.

**Практическая часть**

**Контрольное задание.** Анализ угроз информационной безопасности

Для трех информационных объектов **у**казать 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.

Дано 3 информационных объекта:

– локальная вычислительная сеть;

– банковская карточка;

– банкомат.

Работу рекомендуется выполнять в таблице вида:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование угрозы | Источник | Метод парирования угрозы |
| Компьютерный класс | | | |
| 1. | ... | ... | ... |
| Банковская карточка | | | |
| 1. | ... | ... | ... |
| Банкомат | | | |
| 1. | ... | ... | ... |

***Методические указания***

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.