УДК 004.056.53

МОДЕЛЬ УГРОЗ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Гончаренко Е.В., Галушко С.А.
ГВУЗ «Национальный горный университет», http://nmu.org.ua, vk-dnepr-1@mail.ru

В статье анализируются свойства защищенной информации, пути реализации действий, которые считаются опасными. Защита АС от несанкционированного доступа и ее потенциальных угроз. Также рассматривается потенциальные объекты атак нарушителя ТЗИ.

Ключевые слова – защита информации, угроза, модель угроз.

ВВЕДЕНИЕ

Для обеспечения защиты информации необходимо знать, какие убытки можно понести в случае потери информации. Очевидно, что затраты на защиту не должны превышать возможных убытков при потере информации. Таким образом, необходимо ввести меру ценности информации, то есть определить, в каком смысле следует понимать ее ценность.

СВОЙСТВА ЗАЩИЩЕННОЙ ИНФОРМАЦИИ

Конфиденциальность определяется как свойство информации, которое состоит в том, что она не может быть доступной для ознакомления пользователям и/или процессам, не имеющим на это соответствующих полномочий.

Целостность информации – это свойство, которое состоит в том, что она не может быть доступной для модификации пользователям и/или процессам, не имеющим на это соответствующих полномочий. Целостность информации может быть физической и/или логической.

Доступность информации – это свойство, которое состоит в возможности ее использования по требованию пользователя, имеющего соответствующие полномочия.

Наблюдаемость – это свойство информации, которое состоит в том, что процесс ее обработки может беспрерывно находиться под контролем органа, руководящего защитой.

Под угрозами понимаются пути реализации действий, которые считаются опасными. Например, угроза снятия информации и перехват излучения с дисплея ведет к потере конфиденциальности, угроза пожара ведет к нарушению целостности и доступности информации, угроза разрыва канала передачи информации может привести к потере доступности.

Угрозы могут осуществляться:

- по техническим каналам, которые включают акустические, оптические, радио-, радиотехнические и другие каналы утечки;
- по каналам специального влияния путем формирования полей и сигналов с целью разрушения системы защиты или нарушения целостности информации;
- благодаря НСД путем подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоления средств защиты для использования информации или навязывания ложной информации, применением закладных устройств или программ, использованием компьютерных вирусов.

Все потенциальные угрозы НСД к информации АС делятся на преднамеренные и случайные. Аналогично делятся на преднамеренные и случайные все потенциальные каналы несанкционированного доступа или влияния на информацию, которая подлежит защите. Таким образом, потенциальные угрозы и соответствующие потенциальные каналы несанкционированного доступа (ПКНСД) и потенциальные каналы несанкционированного влияния (ПКНСВ) тесно связаны между собой и дополняют друг друга.

Если абстрактную АС рассматривать как объект защиты от угроз НСД, то в этом случае ее типичными потенциальными каналами угроз НСД могут быть следующие элементы:

- серверы банков данных, серверы доступа и пр.;
- рабочие места компьютерной сети, сетевых станций, мобильных станций и др.;
- элементы телекоммуникационного оборудования (маршрутизаторы, коммутаторы, концентраторы, репитеры, коммутированные каналы связи, конечные устройства);
- бесперебойные блоки питания АС;
- системы записи языковой информации;
- копировально-множительные средства АС;
- системы защиты информации АС;
- терминалы пользователей АС;
- терминалы администраторов АС;
- терминалы операторов АС;
- средства отображения информации АС;
- средства документирования информации АС;
- средства загрузки программного обеспечения АС;
- физические и виртуальные носители информации (ПЗУ, ОЗУ, бумажные, магнитные, лазерные, магнитооптические и прочие носители информации);
- внутренние каналы связи АС;
- внешние каналы связи АС.

Потенциальными объектами атак нарушителя ТЗИ в АС могут быть:

1. Все вышеперечисленные штатные аппаратные средства АС при использовании их санкционированными пользователями не по назначению и за пределами своих полномочий.

2. Все вышеперечисленные штатные аппаратные средства при использовании их посторонними лицами.

3. Технологические пульты управления.

4. Внутренний монтаж аппаратуры.

5. Линии связи (коммуникаций) между аппаратными средствами АС.

6. Побочные электромагнитные излучения и наводки аппаратных и телекоммуникационных средств обработки и передачи информации АС, побочные наводки информации в сети электропитания и заземления аппаратуры АС, побочные наводки информации по цепям вспомогательных инженерных и других посторонних коммуникаций в отдельных помещениях и на территории АС.

7. Отходы обработки информации в виде бумажных, магнитных и других носителей в мусорной корзине.

8. Программное обеспечение АС.

9. Другие возможные потенциальные каналы несанкционированного доступа и несанкционированного влияния.

Угрозы информации при разработке модели угроз удобно рассматривать с точки зрения их любого нежелательного действия и возможного нарушения свойств защищенности информации, указанных в начале раздела. С этой точки зрения в информационных системах различают следующие классы угроз информации:

- нарушение конфиденциальности;
- нарушение целостности;
- нарушение доступности или отказ в обслуживании;
- нарушение наблюдаемости или управляемости.

ЗАКЛЮЧЕНИЕ

Таким образом, угроза – это потенциально возможное неблагоприятное воздействие на информацию, которое приводит к нарушениям хотя бы одного из приведенных свойств. Модель угроз – абстрактное формализованное или неформализованное описание методов и средств осуществления угроз.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС – автоматизированная система;

ИС – информационная система;

НД – нормативный документ;

НСД – несанкционированный доступ;

ОЗУ – оперативное запоминающее устройство;

ОС – операционная система;

ПЗУ – постоянное запоминающее устройство;

ПКНСВ – потенциальный канал несанкционированного влияния;

ПКНСД – потенциальный канал несанкционированного доступа;

ПО – программное обеспечение;

СЗИ – система защиты информации;

СУБД – система управления базами данных;

ТЗИ – техническая защита информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конеев И.Р., Беляев А.В., Информационная безопасность предприятия., 2003.

2. Вертузаев М.С., Юрченко О.М., Защита информации в компьютерных системах от несанкционированного доступа.

3. Петраков А.В. Основы практической защиты информации. Учебное пособие для вузов., Радио и связь. 2001.

4. Лукацкий А. Обнаружение атак.–СПб.:, 2001.– 624с.

5. Хатч Б., Ли Д., Курц Д. Секреты хакеров. Безопасность Linux – готовые решения.: Пер. с англ. – М.: ИД "Вильямс", 2002. – 544 с.

6. Домарев В.В. Модель и программа оценки систем защиты // www.security.ukrnet.net

7. Домарев В.В. Защита информации и безопасность компьютерных систем. – Киев: "DiaSoft", 1999.