АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

СОДЕРЖАНИЕ

1. АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

1.1. Виды возможных угроз

1. Атаки (Фишинг, DDOS и т.п.);
2. Фальсификация (Подделка документов, внедрение в персонал, шпионаж и т.п.);
3. Взлом (обход системы защиты ИС.);
4. Вандализм (повреждение компьютерных ресурсов, включая оборудование, данные и программное обеспечение).

1.2. Характер происхождения угроз

Характер происхождения угроз можно разделить на 2 составляющие:

1)Случайные или природные факторы.

Несчастные случаи и стихийные бедствия. Они могут уничтожить всю информацию, которая хранится на твердых или/и электронных носителях.

2)Умышленные факторы.

Ошибки в процессе обработки информации. Они могут привести к искажению достоверной информации.

К умышленным факторам относятся:

- Несанкционированный доступ;
- Копирование данных.

1.3. Источники появления угроз

1 источник - люди:

- Посторонние лица;
- Пользователи;
- Персонал.

Пользователи и персонал - это люди, которые имеют прямой или косвенный доступ к информации, которая хранится на носителях. При внедрении злоумышленника в рабочую сферу, может произойти несанкционированное хищение информации, ее модификация или уничтожение.

2 источник - технические устройства:

К ним можно отнести устройства передачи, хранения и переработки информации о тоталитарных сектах. При перехвате сообщений с данных технических устройств, также может произойти модификация, хищение и уничтожение информации.

3 источник - модели, алгоритмы, программы:

Данный источник угроз характерен для электронных носителей, при несанкционированном внедрении программ злоумышленника.

4 источник - технологические схемы обработки:

Может привести к модификации или удалению поступающей информации (ручные для твердых носителей и сетевые для электронных носителей).

1.4. Потенциально возможные злоумышленные действия

- Использование служебного положения, т.е. незапланированного просмотра(ревизии) документов без разрешения разработчиков ИС;
- Подкуп или шантаж разработчиков или отдельных пользователей, имеющих определенные полномочия;
- Внедрение агентов в число персонала системы (в том числе, возможно, и в группу, ответственную за безопасность);
- Перехват информации о разработке, планах, и дальнейших действиях проекта (ИС) ;

- Хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.).

1.5. Рекомендации повышения защищенности ИС

- Выделение больших временных и денежных ресурсов на обеспечение безопасности ИС (Найм профессионалов по защите информации, покупка и установка более совершенного ПО для поддержания полного и более безопасного функционирования ИС и т.п.);
- Повышение общей квалификации(знаний) персонала о возможных атаках со стороны злоумышленников, проведение конференций по обучению персонала навыкам защиты информации в ИТ;
- Изучение общих “повадок” и умений потенциальных взломщиков ИС изнутри, понимание всех действий хакеров, направленных на получение информации незаконным путём;
- Соблюдение базовой грамотности безопасности в интернете и повседневных делах(на работе, при общении с незнакомыми людьми и т.п.).