и, наконец, выразить свое мнение в виде анкеты, по которой будут приняты соответствующие меры.

Конечно, невозможно описать всю технологию создания мультимедийной энциклопедии в рамках одной статьи. Мы привели здесь только общую схему организации работ и перечислили основные проблемы, с которыми приходится сталкиваться разработчику. В каждом конкретном случае эта схема, естественно, будет претерпевать какие-то изменения, но принципы ее построения и сама идея остаются неизменными.

Библиографический список

1. Долинер Л.И., Нечкин Д.Б. Психолого-педагогические основы использования ИКТ в обучении. // Л.И. Долинер, Д.Б. Нечкин. Екатеринбург, 2003.

2. Информационно-энциклопедический проект компании «Русс портал» [Электронный ресурс]. Режим доступа: http:// www.rubricon.com/

3. Электронный словарь [Электронный ресурс]. Режим доступа: http:// slovari.yandex.ru/.

4. Создание мультимедийной энциклопедии в лицах [Электронный ресурс]. Режим доступа: http:// www.pcworld/index.html

Л.О. Овечкин, РГППУ
студент группы КТ-306
Руководитель: ст. преп. кафедры СИС
Н.В. Меньшикова

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И СПОСОБЫ ЗАЩИТЫ

Информация правит миром. Кто владеет информацией – правит всем. Это не пафосные лозунги, а реалия жизни. Информация бывает очень ценной. Именно поэтому актуальным вопросом является защита персональных данных. Основным направлением противодействия утечке информации является обеспечение физической (технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность дости-

гается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий [2].

Под защитой информации в настоящее время понимается область науки и техники, которая включает совокупность средств, методов и способов человеческой деятельности, направленных на обеспечение защиты всех видов информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

Информация, которая подлежит защите, может быть представлена на любых носителях, может храниться, обрабатываться и передаваться различными способами и средствами. Эти же носители могут служить каналом утечки информации. Необходимо как можно качественнее их защитить, т.е. провести анализ возможных способов похищения данных.

Комплекс проблем, связанных с информационной безопасностью, включает в себя не только технические, программные и технологические аспекты защиты информации, но и вопросы защиты прав на нее. Таким образом, информация может рассматриваться как объект права собственности. С этой точки зрения можно выделить следующие особенности информационной собственности [44]:

- информация не является материальным объектом;
- информация копируется с помощью материального носителя, т.е. является перемещаемой;
- информация является отчуждаемой от собственника.

В зависимости от способа перехвата, от физической природы возникновения сигналов, а также среды их распространения технические каналы утечки информации можно разделить на следующие [66]:

1) электромагнитные каналы;
2) электрические каналы;
3) параметрические каналы (воздушные технические каналы; вибрационные каналы; электроакустические каналы; оптико-электронный канал; параметрический канал)
4) другие каналы.

Особый интерес представляет перехват информации при ее передаче по каналам связи. Единственным гарантированным методом защиты информации в этом случае является криптографическая защита.

Видовая информация, получаемая техническими средствами в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и копирования документов.

Методы съема компьютерной информации обеспечиваются компьютерными вирусами, «троянскими конями» и прочим вредоносным программным обеспечением (ПО).

Внутренние каналы утечки связаны, как правило, с администрацией и обслуживающим персоналом, с качеством организации режима работы. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, съем информации с ленты принтера и плохо стертых дискет, использование производственных и технологических отходов, визуальный съем информации с дисплея и принтера, несанкционированного копирования и т.п. [4].

Утечка информации может происходить так же путем несанкционированного доступа к ресурсам компьютерной системы.

Часто для получения доступа к конфиденциальным данным используют уязвимости компьютерной системы, под которой понимается некоторая слабость системы безопасности, которая может послужить причиной нанесения компьютерной системе ущерба.

Другим методом получения информации может послужить социальная инженерия. Социальная инженерия – это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным [55].

Для предотвращения утечки важных данных используются средства защиты информации - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации [2].

Интегральная защита это монолитная непроницаемая защита, основной смысл которой состоит в необходимости обеспечить такое состояние условий функционирования человека, объектов и информации, при котором они надежно защищены от всех реальных видов угроз в ходе непрерывного производственного процесса и жизнедеятельности [1].

Одним из основных требований интегральной защиты является системный подход, поэтому при выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное оборудование технических средств обработки информации (ТСОИ), соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления и т.п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной о пожарной сигнализации, радиофикации, электробытовые приборы и другие.

В качестве каналов утечки большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещение, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Для обнаружения утечек по этим каналам, используют различные сложные технические устройства, называемые анализаторами и обнаружителями [33].

В заключение, хотелось бы отметить, что отличительной особенностью хищения информации стала скрытность этого процесса, в результате чего жертва может не догадываться о происшедшем. Помните, что защитить информацию может только сам пользователь или владелец. Для этого нужно правильно организовать работу и ограничить доступ к ценной информации. И принять все меры для предотвращения ее утечки. Например, для надежной защиты своих конфиденциальных данных вы можете хра-

нить логины и пароли в проверенном месте или шифровать их. Выходя в сеть Интернет, и посещая различные ресурсы и форумы, меньше выкладывать информацию личного характера. Использовать софт только из надежных источников и не устанавливать на компьютер неизвестное вам ПО.

Число уязвимостей и использующих их атак растет с каждым годом. Злоумышленники постоянно ищут новые способы проникновения в информационные системы, и пользователи должны понимать, что недооценка способностей хакеров может привести к очень печальным последствиям.

Библиографический список

1. Lundes Каналы утечки информации / Lundes // Хакер. – 200. - №60. – С. 50-53.

2. Аппаратура защиты информации от утечки по техническим каналам [Электронный ресурс] // сайт компании «Специальная техника и технологии» – Режим доступа: http://www.detektor.ru/index.php? option=com_catalogue&section=3. Дата обращения: 31.03.2011.

3. Барсуков В.С. Интегральная защита информации [Электронный ресурс] /В.С. Барсуков // сайт журнала «Специальная техника» – Режим доступа: http://ess.ru/publications/5_2002/ barsukov/barsukov.htm. Дата обращения: 31.03.2011.

4. Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков – М.: Кудиц-Образ, 2001. - 496с.

5. Социальная инженерия [Электронный ресурс] // электронная энциклопедия «Википедия» – Режим доступа: http://ru.wikipedia.org/wiki/ Социальная_инженерия. Дата обращения: 25.03.2011.

6. Хорев А.А., Классификация и характеристика технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи [Электронный ресурс] / А.А. Хореев // сайт журнала «Специальная техника» – Режим доступа: http://ess.ru/publications/articles/tspi/ tspi.htm. Дата обращения: 28.03.2011.