В.С. Подсеваткин, А.М. Самойлов

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ПРИ РАБОТЕ НА КОМПЬЮТЕРЕ И ВОЗМОЖНЫЕ СРЕДСТВА ЗАЩИТЫ

ФГБОУ ВО «Саратовская государственная юридическая академия»

Научный руководитель: к. п. н., доцент Т.Н. Романченко

С каждым днём в современном мире роль персональных электронно-вычислительных машин, или персональных компьютеров (ПК) растёт с каждым днём всё больше и больше. Чаще всего мы используем ПК для передачи, обмена или хранения личной информации. В связи с этим появляются новые каналы утечки информации.

В современном мире роль персональных компьютеров при обработке, передаче и хранении информации неуклонно растет. Это связанно и с новым взглядом на информацию, которая приобретает новый статус - экономический, в обществе развивается информационное право, информация переходит в категорию защищаемых и охраняемых объектов. В связи с этим важным моментом при работе с информацией на персональных компьютерах, является знание и исследование возможных каналов утечки информации.

Рассмотрим понятия, связанные с утечкой информации. Хранение информации представляет собой поддержание исходной информации в виде, обеспечивающем выдачу данных по запросам пользователей в необходимые или установленные сроки. Утечка информации на уровне принятой терминологии представляет собой несанкционированный доступ.

Несанкционированный доступ – доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к данной информации. Несанкционированным доступом в отдельных случаях называют также получение лицом, имеющим право на доступ к информации в

объёме, превышающем необходимый для выполнения служебных обязанностей.

Развитие компьютерной техники и информационных технологий позволяет работать на компьютерах как независимо друг от друга, так и взаимодействуя с другими компьютерами по компьютерным сетям, причем последние могут быть локальными и глобальными. С учетом названного перечень участков, где могут находиться подлежащие защите данные, может быть представлен следующими элементами:

- оперативная и постоянная память ПК;
- съемные магнитные, магнитооптические, лазерные и другие носители информации;
- внешние устройства хранения информации коллективного доступа (RAID-массивы, файловые серверы и т.п.);
- экраны устройств отображения (дисплеи, мониторы, консоли);
- память устройств ввода/вывода (принтеров, графопостроителей, сканеров);
- память управляющих устройств и линии связи, образующие каналы сопряжения компьютерных сетей.

Существует несколько причин и каналов утечки важной информации, в сановном это:

- ошибки конфигурации (прав доступа, файерволов, ограничений на массовость запросов к базам данных),
- слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников),
- электромагнитные каналы
- сетевая разведка
- оптические каналы (утечка изображения)
- инсайдерские каналы утечки информации

- злоупотребление служебными полномочиями (воровство резервных копий, копирование информации на внешние носители при праве доступа к информации),
- использование клавиатурных шпионов, вирусов и троянов на компьютерах сотрудников для их персонализации.

Раскроем каждый и названных каналов подробнее.

1. Наиболее популярной причиной утечки информации среди ошибок конфигурации на данный момент является именно ограничение на массовость запросов к базам данных (DoS – атака):

DoS - хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Отказ «вражеской» системы может быть и шагом к овладению системой. Целью большинства атак является либо несанкционированый доступ в систему, либо получение прав администратора, либо другие неправомерные действия пользователя, такие как подмена документов и кража конфиденциальной информации. Вариантов проведения такой атаки множество. Самыми популярными являются наводнение (flood) сети пакетами различных протоколов (например, ICMP, UDP или TCP), в результате которого почти все вычислительные и сетевые ресурсы уходят на создание бесполезных ICMP-ответов или TCP-сессий. В настоящее время DoS и DDoS-атаки позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик.

2. Если у пользователя стоит лёгкий пароль, то украсть его для хакеров очень просто. В современном мире существует большое множество программ для подбора паролей к учётным записям (PasswordCracker, PasswareKitEnterprise, MultiPasswordRecovery). Злоумышленнику будет достаточно знать только ваш логин. Чаще всего такому взлому подвергаются учётные записи на различных сайтах, в которых может хранится личная информация. Иногда злоумышленнику даже не нужно подбирать пароль,т.к.

владелец ПК, например в офисе, может оставить свой компьютер включённым и отойти от рабочего места, что даёт другому человеку сесть за стол и воспользоваться компьютером в полной мере.

3.Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки. Данный канал утечки наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым средствам связи и при общении с другими людьми с помощью ПК. Для перехвата побочных электромагнитных излучений ТСПИ (Технические средства передачи информации) “противником” могут использоваться как обычные средства радио-, радиотехнической разведки, так и специальные средства разведки, которые называются техническими средствами разведки побочных электромагнитных излучений и наводок (ТСР ПЭМИН). Как правило, полагается, что ТСР ПЭМИН располагаются за пределами контролируемой зоны объекта. Для перехвата информации, обрабатываемой ТСПИ, также возможно использование электронных устройств перехвата информации (закладных устройств), скрытно внедряемых в технические средства и системы. Они представляют собой миниатюрные передатчики, излучение задающих генераторов которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается в специальное запоминающее устройство, а уже затем по команде управления передается по радиоканалу. Наиболее вероятна установка закладных устройств в ТСПИ иностранного производства.

4.Под сетевой разведкой подразумевается сбор информации о сети с помощью общедоступных данных и приложений. При подготовки атаки против какой либо сети злоумышленник, как правило, пытается получить о ней как можно больше информации. Сетевая разведка проводится в форме запросов доменных сетевых имён – DNS, эхо-тестирования и сканирования портов.

Запросы DNS помогают понять, кто владеет тем или иным доменом и какие адреса этому домену присвоены.

Эхо-тестирование (pingsweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, хакер использует средства сканирования портов, чтобы составить полный список услуг, поддерживаемых этими хостами. Далее,он получает доступ к файлам, которые находятся на ПК.

5. В оптическом канале получение информации возможно путем:визуального наблюдения ,фото-видеосъемки,использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

Наиболее опасным каналом утечки является дисплей, так как с точки зрения защиты информации он является самым слабым звеном в компьютерной системе. Это обусловлено принципами работы видеоадаптера, состоящего из специализированных схем для генерирования электрических сигналов управления оборудования, которое обеспечивает генерацию изображения. Кроме того, в существующих программах удаленного доступа имеется функция записи экрана дисплея по расписанию в отдельный файл.

6. Инсайдер – член какой-либо группы людей, имеющей доступ к информации, недоступной широкой общественности. Термин используется в контексте, связанном с секретной, скрытой или какой-либо другой закрытой информацией или знаниями: инсайдер – это член группы, обладающий информацией, имеющейся только у этой группы.

7.Сознательные действия сотрудников, обусловленные инициативным сотрудничеством с другой фирмой; продажей информации за взятку, под угрозой шантажа, в виде мести; переход на другую фирму на более высокую оплату

8.Компьютерный вирус – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ,

системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера ит.п. Вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы. Они могут распространятся через интернет (в случае скачивания файла, в нём может находится вирус), через локальные сети, через съёмные носители. Существует разновидность вирусов, которая называется «Программа-шпион». Она собирает информацию о действиях и поведении пользователя. В основном их интересует информация (адреса, пароли). Поэтому, злоумышленники получают полный контроль над личной информацией человека

Каналами распространения вирусов могут быть: дискеты, флеш-накопители, электронная почта, системы обмена мгновенными сообщениями, веб-страницы, интернет и др. При использовании флеш-накопителей и дискет опасность представлял размещаемый на них с целью заражения файл autorun.inf. Но, начиная с Windows 7 возможность автозапуска файлов с переносных носителей отключена. Вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу для рассылки самого себя дальше. В системах мгновенного обмена сообщениями распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами. Заражение через страницы Интернета реализуется посредством размещенных на них скриптов и ActiveX-компонентов . Сетевое заражение могут осуществлять черви, они используют так называемые уязвимости в программном обеспечении операционных систем, чтобы проникнуть на

компьютер. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Если на компьютере стоит слабая защита,то данные пользователя могут подвергнуться взлому, результатом которого могут быть следующие последствия: утечкаперсональных данных,коммерческой тайны, служебной переписки,государственной тайны,полное либо частичное лишение работоспособности системы безопасности компании.

Чтобы компьютер не подвергся атаке со стороны злоумышленников, данные на компьютере нужно держать в защите. Существуют различные способы, которые помогут сделать это: шифрование данных, использование надёжных паролей, защита Wi-Fi доступа, установка антивирусных программ

Шифрование данных можно произвести всего один раз,например с помощью программы TrueCrypt. Шифрование нужно делать для того, чтобы никто не смог смотреть ваши файлы, войти в систему, кроме вас самих.

Использование надежных паролей затрудняет доступ к информации. Надежные пароли представляют собой сложную комбинацию цифр, букв, символов, длиной не менее 8 символов, причем с использованием прописных и строчных символов различных алфавитов (русского и английского). Желательно записывать свои пароли на отдельный лист и хранить в надёжном месте. Не следует хранить пароли в блокноте на компьютере, т.к. существует множество вирусов, которые могут просматривать файлы на вашем ПК. Никому не сообщайте свой пароль.

Попадание вируса на компьютер чревато неприятными последствиями. Лучше сразу поставить надёжный антивирус и держать его постоянно включённым. При работе в сети Интернет постоянное включение антивируса является необходимостью.

У хакеров имеется множество средств и способов, чтобы обойти защищенные сети и шифрование. Они ежедневно крадут номера кредитных карт, банковские счета и сведения о персональных данных. Поэтому при работе

на ПК необходимо предпринимать всевозможные меры защиты информации, как программно-аппаратные, так и организационные.

В РФ в целях защиты информации от неправомерного доступа введены и действуют и законодательные меры защиты. В УК РФ предусмотрены статьи в целях предотвращения неправомерного доступа к информации, это статья 137 «Нарушение неприкосновенности частной жизни», статья 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», статья 272 «Неправомерный доступ к компьютерной информации», статья 273 «Создание, использование и распространение вредоносных компьютерных программ», статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Список источников и использованной литературы

1. Загинайлов Ю. Н «Теория информационной безопасности и методология защиты информации» http://window.edu.ru/resource/984/71984 (дата обращения 18.03.2016).

2. А.А. Хорев «Технические каналы утечки информации» http://www.analitika.info/kanalutechki.php (дата обращения 18.03.2016).

3. В. А. Артамонов, Е.В. Артамонова «Каналы утечки информации» http://media.professionaly.ru/processor/topics/original/2013/09/24/utechki-kanal.pdf (дата обращения 18.03.2016)

4. http://ftemk.mpei.ac.ru/ip/IPTextBook/05/5-4/5-4.htm (дата обращения 18.03.2016).