*СОДЕРЖАНИЕ*

|  |  |
| --- | --- |
| Введение | 3 |
| Угрозы данным | 5 |
| Безопасность в Интернет | 8 |
| Проблема защиты радиоэлектронных средств передачи информации | 11 |
| Проблемы защиты информации в компьютерной технике. Криптография. Стеганография | 13 |
| Заключение | 15 |
| Список литературы | 16 |

*ВВЕДЕНИЕ*

Вхождение Украины в мировое информационное пространство через информационные сети общего пользования, каковой является сеть Интернет, создало проблему обеспечения безопасности различных информационных систем и создаваемых информационных ресурсов, а также организации управления информационными ресурсами и их содержанием. А в связи с интенсивным развитием глобальных систем передачи данных и Internet ориентированных информационных систем и электронных библиотек, проблема защиты информации приобретает особую важность.

Темпы роста украинского сегмента Internet в последние 2-3 года не уступают и даже превосходят среднеевропейские. В то же время используемые "средства защиты информации" не удовлетворяют сегодняшним потребностям в первую очередь по чисто организационно-технологическим причинам.

Определяющим фактором интеграции в единое информационное пространство различных информационных систем и ресурсов является обеспечение должного уровня информационной безопасности, которая включает следующий комплекс мероприятий и технических решений по защите информации:

от нарушения функционирования сети путем воздействия на информационные каналы, каналы сигнализации, управление и удаленную загрузку баз данных, коммуникационное оборудование, системное и прикладное программное обеспечение;

от несанкционированного доступа к информации путем обнаружения и ликвидации попыток использования ресурсов сети, приводящих к нарушению целостности сети и информации, изменению функционирования подсистем распределения информации;

от разрушения встраиваемых средств защиты с возможностью доказательства неправомочности действий пользователей и обслуживающего персонала сети;

от внедрения программных "вирусов" и "закладок" в программные продукты и технические средства.

Построение системы безопасности компьютерной сети имеет своей целью предотвращение или снижение возможного ущерба, который может быть нанесен в результате атаки на сеть. Ценные файлы или информация могут быть уничтожены, серверы или иное оборудование могут быть приведены в нерабочее состояние так, что на их полное восстановление может потребоваться несколько дней. Кроме того, защита сети имеет целью защиту репутации организации от ущерба вследствие, например, несанкционированного изменения содержимого страниц ее WWW-сервера третьими лицами, публикации информации третьими лицами под чужим авторством или появление в публичном доступе информации, нежелательной для широкого распространения (или секретной).

Защита информации в глобальной сети имеет свою специфику, отличающую ее от проблемы защиты информации в локальных сетях.

Важнейшей отличительной особенностью задачи защиты информации в глобальной сети является тот факт, что защита информации возлагается полностью на программно-аппаратные средства, и не может быть решена путем физического ограничения доступа пользователей к компьютерам или к оборудованию, как это может быть сделано для ограничения доступа к информации в рамках отдельной организации. В глобальной сети потенциальную возможность доступа к ресурсам имеет любой пользователь сети, находящийся в любой точке Земного шара, и момент доступа к той или иной информации не может быть предсказан заранее.

*УГРОЗЫ ДАННЫМ*

В принципе есть лишь два вида угрозы: раскрытие и видоизменение данных. Раскрытие данных предполагает, что кому-то случайно или после целенаправленных действий стал известен смысл информации. Этот вид нарушения встречается наиболее часто. Последствия могут быть самые разные. Если похищен текст книги справочника, на которую потрачены месяцы работы десятков людей, то для коллектива авторов это катастрофа и потери могут выражаться в тысячах долларов. Однако если книга уже издана, то достаточно лишь слегка пожурить похитителя и рассказать о случившемся в отделе новостей газеты или TV, похититель может сделать книге великолепную рекламу. Очень важную информацию, тщательно оберегаемую от раскрытия, представляют сведения о людях: истории болезни, письма, состояния счетов в банках. Однако, по мнению большого числа специалистов, угрозы личности с введением компьютеров остались на том же уровне и в том же состоянии, что и до обширного использования ЭВМ.

Рассмотрим виды потерь, возникающие от раскрытия информации. Обычно данные о людях наиболее важны для них самих, но, как бы это не описывали в шпионских фильмах, мало что значат для похитителей. Иногда личные данные могут использоваться для компрометации не только отдельных людей, но целых организаций, например, если выяснится скрываемая прежняя судимость за растрату директора коммерческого банка. Но тот, кто компрометирует, не имея твердой моральной основы для этого, в большинстве случаев теряет больше самого компрометируемого. Лишь малая кучка профессиональных негодяев из адвокатов и журналистов, которым уже нет дела до своего морального облика, наживается, занимаясь компрометацией. Тем не менее информация о людях ценна сама по себе, основной убыток от ее разглашения - личное несчастье человека. Другое дело - раскрытие стратегической управляющей информации. Если вскрыт долгосрочный план развития производства или анализ конъюнктуры на рынке, то потери для держателя этой информации будут невелики, но для конкурентов такие сведения очень важны. Думается, что хотя несанкционированное чтение данных бывает довольно часто, но редко когда приносит существенный вред, так как часто делается без злого умысла - случайно или из любопытства.

Искажения информации представляют существенно большую опасность. Во многих организациях жизненно важные данные хранятся в файлах: инвентарные описи, графики работ, списки заказов. Если такие данные будут искажены или стерты, то работа надолго парализуется. Самое опасное в этом то, что в примитивных криптографических системах необходимые для этого искажения могут быть сделаны и без знания ключа. Поэтому серьезные шифры должны гарантировать не только устойчивость их раскрытия, но и невозможность незаметной модификации одиночного бита. Владение ключом открывает полный доступ к данным - тогда можно скомпрометировать бухгалтерскую или конструкторскую систему, чуть исказив десяток-другой чисел, или удалить сведения о реальном движении товара, чтобы счет за него не был выставлен. Похоже, что наиболее уязвима для искажения информация экономического характера, где потери могут быть чрезвычайно велики. Самое первое компьютерное преступление в нашей стране было именно этого типа и принесло прямые убытки в десятки тысяч рублей, когда в конце семидесятых, один из прибалтийских банков обнаружил у себя недостачу наличных денег. Руководителям крупных научных и программных проектов следует помнить, что большую опасность для их данных представляют не конкуренты, а собственные сотрудники. По различнейшим причинам они могут уничтожить или исказить окончательный проект. Совсем неожиданный случай произошел в фирме IBM, которая привезла в Австралию заказанную ей программную систему. После предварительного успешного опробования состоялась демонстрация, на которой система оказалась неработоспособной. Расследование выяснило, что один программист во время опробования нашел в своей программе ошибку и тайно внес исправления в тщательно охраняемую копию системы. Он не знал, что ошибка уже корректировалась другими программами и получившаяся во время демонстрации двойная коррекция чуть не обошлась IBM в миллион долларов. Таким образом, критические данные обязательно должны храниться в шифрованном виде или хотя бы подтверждаться имитоприставкой иди цифровой подписью, чтобы исключить искажения.

*БЕЗОПАСНОСТЬ В INTERNET*

Internet не был бы Internet`ом, если бы в его недрах не родилось решение, отвечающее выставляемым жизнью проблемам. Причем, технические идеи предлагаемых решений обладает общностью, позволяющей говорить о том, что Internet после их внедрения по степени безопасности может превзойти даже специализированные закрытые корпоративные сети.

Информационная безопасность Internet определяется особенностями базовых коммуникационной (TCP/IP) и операционной платформ (UNIX). TCP/IP обладает высокой совместимостью как с различными по физической природе и скоростным характеристикам каналами, так и с широким кругом аппаратных платформ; кроме того, этот протокол в равной мере эффективно работает как в локальных сетях, так и в региональных и глобальных сетях; совокупность этих характеристик делает Internet технологии уникальным средством для создания и интеграции больших распределенных гетерогенных информационных систем.

В Internet информационных системах по сравнению с классическими системами архитектуры "клиент-сервер" вопросы информационной безопасности решаются намного проще. Это связано прежде всего со следующими особенностями:

гораздо большая часть информационных ресурсов централизована - их предоставляет сервер, а централизованными ресурсами не только легче управлять, но их и легче защищать;

для обмена информацией между рабочими станциями и сервером используется протокол TCP/IP, для которого разработана система защитных средств, включая криптографические;

на рабочих станциях выполняется только WWW просмотрщик и программы интерпретации Web-документов сервера, которые загружаются непосредственно с сервера.

***Принципы безопасности.*** Решение проблемы защиты информации состоит в использовании организационно-технологических (административных), технических и программных мер, а так же в профилактической работе среди пользователей для уменьшения возможностей для несанкционированного доступа к информации.

В целом система защиты информации строится на:

конверсии технологий информационной безопасности и защиты информации и информационных систем, телекоммуникационной среды от несанкционированного использования и воздействий;

обеспечении защиты ресурсов за счет параллельного доступа к управляющим базам данных и проверки полномочий при обращении к ресурсам сети;

реконфигурации сетей, узлов и каналов связи;

организации замкнутых подсетей и адресных групп;

развития специализированных защищенных компьютеров, локальных вычислительных сетей и корпоративных сетевых сегментов (что особенно важно для разработчиков информационных систем);

обеспечении защиты технических средств и помещений от утечки информации по побочным каналам и от возможного внедрения в них электронных устройств съема информации;

развитии и использовании технологий подтверждения подлинности объектов данных, пользователей и источников сообщений;

использовании протоколов шифрования IP пакетов, систем шифрования учетных данных и прав доступа к информации, передача информации с использованием секретных ключей;

применении технологий обнаружения целостности объектов данных.

Таким образом, реализация системы защиты информации и информационных ресурсов распадается на три независимые задачи:

обеспечение системы целостности информации и информационных систем;

организация авторизованного доступа к информации;

недопустимости появления в открытом доступе информации, составляющей государственную тайну или имеющую конфиденциальный характер.

*ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ ТЕХНИКЕ. КРИПТОГРАФИЯ. СТЕГАНОГРАФИЯ.*

Отличительной чертой второй половины XX века является бурное развитие радиоэлектронных средств связи. Одновременно развиваются и средства электронного шпионажа, что делает проблему защиты информации все более и более актуальной. Основное количество информации перехватывается сегодня с помощью технических средств. Агентство национальной безопасности США, например, поставляет до 80 % информации разведывательного характера благодаря радиоэлектронным методам, остальное поступает по агентурным каналам. Объясняется это довольно просто: большинство информации сейчас хранится, обрабатывается и передается электронными методами, которые позволяют вести наблюдение и регистрацию перехватываемых данных со стороны с помощью специальной аппаратуры, не вмешиваясь непосредственно в работу технических систем.

Каналы утечки информации достаточно многочисленны. Они могут быть как естественными, так и искусственными, т.е. созданными с помощью технических средств. Ниже рассматриваются некоторые характеристики и особенности применения основных средств радиоэлектронного шпионажа.

***Таблица 1. Характеристики и особенности применения основных средств радиоэлектронного шпионажа.***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Контролируемое устройство*** | ***Приемник информации*** | ***Место установки*** | ***Стоимость аппаратуры*** | ***Вероятность применения*** | ***Качество перехвата*** |
| Телефон | индуктивный или контактный датчик | Телефонная линия от аппарата до районной АТС | Низкая | Высокая | Хорошее |
| Телефон, использование микрофонного эффекта | контактный датчик | Телефонная линия от аппарата до районной АТС | Низкая | Низкая | Плохое |
| Телефон или любое устройство с питанием от сети | Радио микрофон с передачей по телефонной сети или по сети 220В | Тел. аппарат, тел. розетка, любое устройство с питанием | Низкая | Высокая | Хорошее |
| Любое место в помещении | Различные автономные радио микрофоны, направленные микрофоны, в т.ч. лазерные | Любое место в помещении | Высокая | Средняя | Хорошее |
| Радиотелефон, радиостанция | Панорамный радиоприемник | Прием с эфира | Средняя | Высокая | Хорошее |
| Сотовый телефон | Устройство прослушивания сотовой сети | Прием с эфира | Высокая | Высокая | Хорошее |
| Монитор ПК | Широкополосная антенна | Прием с эфира | Очень высокая | Низкая | Посредственное |
| Монитор ПК | Широкополосный контактный датчик | Питающая электросеть | Очень высокая | Низкая | Посредственное |
| Магистраль компьютерной сети | индуктивный или контактный датчик | кабель магистрали | Высокая | Высокая, если кабель проходит по неохраняемой территории | Хорошее |

Перекрытие всех возможных каналов несанкционированного съема информации требует значительных затрат, и, поэтому, в полном объеме сделать это удается далеко не всегда. Следовательно, в первую очередь необходимо обратить внимание на те из них, которыми с наибольшей вероятностью могут воспользоваться недобросовестные конкуренты.  
  
Как видно из приведенной выше таблицы, наибольшую привлекательность для злоумышленников представляют акустические каналы утечки информации, в особенности телефонная сеть, ввиду ее общедоступности и невысокой стоимости подслушивающей аппаратуры.

*ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ ТЕХНИКЕ. КРИПТОГРАФИЯ. СТЕГАНОГРАФИЯ.*

Все больше информации на персональных компьютерах, все чаще возникает необходимость защиты своей информации от попытки прочтения.

Неэффективность стандартных средств удаления (на примере популярных оболочек)

 ДОС - восстановление, чтение поврежденных файлов. Защита - затирание данных специальными программами. Требует определенной дисциплины, т.к. усложняет жизнь пользователя. На практике с течением времени все реже пользователем используются специальные программы.

 Windows - восстановление информации непосредственно с жесткого диска. Ведет файлы истории, логи, своп (временный файл непостоянного размера на жестком диске, используемый операционной системой для промежуточной записи данных с целью ускорения работы). Причем запускаемые приложения ведут свои лог - файлы, используют кэш - файлы и т.д. Защита та же, но большие трудности с поиском записываемой на винчестер информации. В своп - файле Windows хранит массу информации. Файл постоянно меняет размер, однако, при использовании программы - просмотрщика (16-теричной с неограниченным размером файла, типа Hiew) и DiskEdit для просмотра стертой части, из него можно получить вполне читаемую информацию. Учитывая размер файла, желательно при этом знать, что искать. Откровенно слабо хранятся пароли и данные о пользователях, что очень легко используется при получении доступа к компьютеру.

Криптография. Выбор алгоритма. Слабые алгоритмы шифрования в архиваторах, продуктах фирмы Микрософт. Грубые ошибки в выборе паролей, причем иногда опытными людьми, своеобразный синдром привычки. Даже при использовании тяжелой криптографии (на примере PGP) не применяется ограничение доступа к КТ (чревато копированием ключа) и используются элементарные ключевые фразы. Вообще, использование сложных паролей, вводимых с клавиатуры, - вопрос дисциплины, а не опыта. Удобство в работе с системами прозрачного шифрования, виртуальными зашифрованными дисками. Однако все это достаточно слабо помогает, если к проблемам защиты информации не подходить комплексно. Клавиатурные шпионы, программы, отслеживающие информацию в портах, разветвления кабелей периферии, позволяют рассекречивать информацию без непосредственной атаки средств тяжелой криптографии. Осуществлять комплекс защитных мер сложно технически, морально и т.д. Необходимость такой работы определяется ценностью информации. Но, в принципе, расшифрована может быть любая информация, к тому же, у определенного круга людей любая зашифрованная информация вызывает желание ее узнать.

Стеганография. "Искусство скрытого письма". На мой взгляд, значительно повышает секретность информации ее скрытость. В КТ - от использования стертых файлов, утилит типа Diskhide, до записи информации в графические или музыкальные файлы или в любые другие, имеющие более - менее сложный формат. Существуют утилиты, позволяющие переносить текстовый файл в графический. Учитывая, что в полноцветном файле, имеющем разрешение 800x600 точек/дюйм и глубину цвета 30 бит имеется огромное количество "ячеек" для записи данных, его изменение, вызванное заменой части информации практически не воспринимается визуально. Обнаружить постороннюю информацию может только человек, досконально знающий формат данного графического файла. В принципе, изучив даже формат файлов распространенных баз данных, можно обнаружить достаточно возможностей для записи в служебные поля своей информации, не доступной в дальнейшем стандартными средствами просмотра. Кроме того, при поиске информации на жестком диске размером даже 20-40 Gb, достаточно сложно обнаружить просто зашифрованную информацию. Необходимость поиска скрытой информации в различных вариантах - от стертых файлов до анализа графических и музыкальных файлов, потребует многократного увеличения потраченного времени, и результат в значительно большей степени будет зависеть от квалификации эксперта. А ведь найденная информация может оказаться и зашифрованной средствами тяжелой криптографии.

Таким образом, сочетание стеганографии с криптографией, во многих случаях даст значительное повышение эффективности защиты информации на компьютерной технике, а экспертам, проводящим подобные исследования, необходимо брать в расчет возможность сокрытия информации самыми различными средствами.

*ЗАКЛЮЧЕНИЕ*

С конца 80-ых начала 90-ых годов проблемы связанные с защитой информации беспокоят как специалистов в области компьютерной безопасности так и многочисленных рядовых пользователей персональных компьютеров. Это связано с глубокими изменениями вносимыми компьютерной технологией в нашу жизнь. Изменился сам подход к понятию “информация”. Этот термин сейчас больше используется для обозначения специального товара который можно купить, продать, обменять на что-то другое и т.д. При этом стоимость подобного товара зачастую превосходит в десятки, а то и в сотни раз стоимость самой вычислительной техники, в рамках которой он функционирует.

Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий. Однако, большая часть пользователей не осознает, что постоянно рискует своей безопасностью и личными тайнами. И лишь немногие хоть каким либо образом защищают свои данные. Пользователи компьютеров регулярно оставляют полностью незащищенными даже такие данные как налоговая и банковская информация, деловая переписка и электронные таблицы. Проблемы значительно усложняются, когда вы начинаете работать или играть в сети так как хакеру намного легче в это время заполучить или уничтожить информацию, находящуюся на вашем компьютере.

*СПИСОК ЛИТЕРАТУРЫ*

1. Агеев А. С. Организация работ по комплексной защите информации.-К., 2003.
2. Андрианов В. И Шпионские штучки и устройства для защиты объектов и информации.-СПб., 2001.
3. Киселев А. Е. Коммерческая безопасность – М., 2001.
4. Ковалев А. Н. Защита информации: правила и механизм лицензирования.-К.,2000.
5. Лихарев С. Б., Фомин Г. А. Обзор средств криптографической защиты информации в персональных компьютерах.-М., 2004.
6. Лысов А.В., Остапенко А.Н.. Энциклопедия промышленного шпионажа.-СПб., 2003.
7. Максимов Ю. Н. Защита информации в системах и средствах информатизации и связи. - СПб., 2005.
8. Мельников В. В. Защита информации в компьютерных системах. – М., 2002
9. Халяпин Д. Б., Ярочкин В. И. Основы защиты промышленной и коммерческой.-К.,2001.  
   Ярочкин В. И. Технические каналы утечки информации.- М., 2005