2. Гринченко Т.А. Гипертекст – новая информационная технология // Кибернетика и системный анализ, 1992,–5. – С.116–136.

3. Курковский С. Гипертексты с практической точки зрения // Монитор, 1993, – 4 – С 10–14.

4 Михеева Т.И. Обучение алгоритмизации на основе использования информационных процессов рекурсивного типа / Информационные технологии в непрерывном образовании // Тезисы докладов международной конф –выставки. – Петрозаводск – 1995. – С. 130 –131.

5. Михеева Т.И., Курилкин С.Ю. Инструментальная среда для создания компьютерных учебников "АРГУС" / Математика. Компьютер. Образование // Тезисы докладов второй международной конф. –Пущино: МГУ,- 1995. – С. 188.

ЗАЩИТА ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ И СЕТЯХ

А.С. Овсянников, В.В. Камышников, Ю.М. Казаченко

Новые информационные технологии, активно развивающиеся в последние годы, позволили осуществить своеобразную революцию в проблеме обработки и передачи информации. В частности, технология электронных коммуникаций на базе ПЭВМ и модемов позволила решить многие задачи повышения эффективности процессов обработки и передачи информации практически во всех сферах жизнедеятельности человека. Однако современные достижения в области телекоммуникаций, с другой стороны, существенно обострили проблему информационной безопасности. Этому способствовало массовое использование ПЭВМ, открытых компьютерных сетей и общедоступных каналов связи.

В общем виде можно выделить следующие типовые пути несанкционированного получения информации - перехват электронных излучений; применение подслушивающих средств (закладок), дистанционное фотографирование; принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей; перехват акустических излучений и восстановление текста принтера; хищение носителей информации, считывание данных в массивах других пользователей; чтение остаточной информации в памяти си-

стемы после выполнения санкционированных запросов; копирование носителей с преодолением мер защиты; маскировка под зарегистрированного пользователя; мистификация (маскировка под запросы системы); использование недостатков языков и операционных систем; незаконное подключение к аппаратуре или линиям связи; вывод из строя механизмов защиты; внедрение и использование компьютерных вирусов.

В практической деятельности по применению мер и средств защиты информации следует выделить следующие направления:

- защита информации от несанкционированного доступа (НСД);
- защита информации в системах связи;
- защита юридической значимости электронных документов;
- защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);
- защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ.
- защита от несанкционированного копирования, распространения программ и ценной компьютерной информации;
- организационные средства защиты информации.

Проведем краткий анализ основных видов защиты информации.

1. Центральной в проблеме защиты от НСД является задача разграничения функциональных полномочий и доступа к информации, направленная на предотвращение возможности потенциального нарушителя модифицировать ее штатными и нештатными средствами. Требования по защите от НСД всегда направлены на достижение трех основных свойств защищаемой информации

- конфиденциальность (засекреченная информация должна быть доступна только тому, кому она предназначена);
- целостность (информация, на основе которой принимаются важные решения, должна быть достоверной, точной и защищенной от возможных непреднамеренных и злоумышленных искажений);
- готовность (информация и соответствующие автоматизированные службы должны быть доступны, готовы к обслуживанию всегда, когда в них возникает необходимость)

На практике существует весьма широкий спектр различных подходов и методов реализации программных и аппаратных средств разграничения доступа (СРД). Однако общими для всех СРД являются диспетчер доступа, модель защиты и блок аутентификации. Реализуемый в виде совокупности программно-аппаратных механизмов, диспетчер доступа обеспечивает необходимую дисциплину разграничения доступа субъектов (активных элементов вычислительного процесса пользователей, процессов, процедур и т.п.) к объектам (пассивным информационным элементам - контейнерам данных: файлам, томам данных, устройствам, программам и т.п), описываемую посредством математически строгой модели защиты. На основании полномочий субъекта и свойств объекта данных, записанных в базе полномочий, и характеристик доступа, диспетчер принимает решение разрешить доступ, либо отказать в нем.

Блок аутентификации ответственен за достоверность опознания или подтверждение подлинности пользователя. В большинстве практических случаев вполне приемлемым может считаться способ аутентификации, основанный на проверке предъявляемого пользователем секретного пароля. Достоверность процедуры автоматического опознания личности может быть усилена за счет применения дополнительных устройств - электронных и механических ключей различного вида. Модель защиты является той математической абстракцией, которая отображает взаимоотношения между пользователем и информацией в вычислительной системе. Применяются два типа моделей защиты - матричная и многоуровневая.

В терминах матричной модели состояние системы защиты описывается тройкой: (S,O,M), где S - множество субъектов доступа, O - множество объектов доступа; M - матрица доступов, в которой строки соответствуют субъектам, а столбцы - объектам, значение элемента матрица M[S,O] определяет права доступа субъекта S к объекту O. С помощью матрицы доступа может быть описано состояние любой, сколь угодно сложной системы защиты в произвольный момент ее существования.

Многоуровневые модели переносят в операционную среду ЭВМ общепринятые и хорошо отработанные принципы обращения с бумажными секретными, особоважными, конфиденциальными документами, в течение многих лет применяемые на практике. При этом активные элементы вычислительного процесса

(пользователи, задачи и т.п.) при многоуровневой защите наделяются определенными правами доступа, надежно зафиксированными в мандате субъекта. Пассивные элементы вычислительного процесса - разнообразные контейнеры данных наделяются определенными признаками конфиденциальности, зависящими от уровня содержащейся в этих контейнерах информации.

Признаки конфиденциальности надежно фиксируются в метке объекта.

Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности. Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений, например, конфиденциально, секретно, только для узкого круга, несекретно и т.п..

С помощью многоуровневых моделей удается проследить направление потоков информации, предупреждая возможность преднамеренного или случайного снижения уровня секретности защищаемой информации за счет ее утечки из объектов с высоким уровнем конфиденциальности и узким набором категорий доступа в объекты с меньшим уровнем конфиденциальности и более широким набором категорий доступа

Практика показывает, что многоуровневые модели защиты находятся гораздо ближе к реальной жизни, нежели матричные модели, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа.

2. Наиболее эффективным средством защиты информации в общедоступных каналах связи является применение криптографии и специальных связных протоколов. В большинстве криптографических систем секретность способа шифрования базируется на двух элементах:

• алгоритме шифрования данных, представляющем собой набор математических правил, определяющих последовательность выполнения элементарных действий над данными, в совокупности обеспечивающих их шифрование и расшифровку;

• криптографическом ключе, однозначно определяющем конкретный вариант преобразования открытого текста в шифртекст (и наоборот) из многообразия всех возможных вариантов, обусловленных алгоритмом шифрования.

Алгоритмы шифрования, ориентированные на применение в информационно-вычислительных сетях (ИВС) общего пользования должны отвечать следующим основным требованиям:

• криптограмма (шифртекст) дешифруется только при наличии ключа;

• знание алгоритма шифрования не должно упрощать процедуры криптоанализа, выполняемого с целью вскрытия ключей и дешифрования криптограмм;

• структура алгоритма должна быть постоянной;

• в процессе шифрования должен быть предусмотрен контроль за шифруемым открытым текстом и ключом;

• длина криптограммы должна быть равна длине открытого текста;

• изменение длины ключа не должно ухудшать характеристики алгоритма шифрования;

• криптограмма должна быть структурно однородной, т.е. не делиться на открытые и зашифрованные части;

• сложность вскрытия ключа не должна зависеть от количества имеющихся в наличии криптограмм и открытого текста;

• множество всех возможных ключей должно быть однородным, т.е. не содержать "слабых" ключей, применительно к которым процедуры криптоанализа относительно более просты и эффективны;

• алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

Алгоритм шифрования, удовлетворяющий перечисленным требованиям, считается криптостойким и пригодным для применения в ИВС общего пользования.

В настоящее время используются два вида криптографических алгоритмов - симметричные, основанные на использовании секретных ключей, и асимметричные, использующие ключи двух типов - секретные и открытые.

В классических симметричных криптосистемах применяются простые и давно известные методы шифрования - подстановка, перестановка и гаммирование. Как показывает практика, ни один из таких методов шифрования в отдельности не отвечает сформулированным выше требованиям. В связи с этим для достижения потребного уровня криптостойкости реальные алгоритмы шифрования включают

многократно повторяемые шаги перестановок, гаммирование и нелинейные подстановки.

В современных асимметричных криптосистемах предусмотрены два ключа (один для шифрования, другой для дешифрования), каждый из которых практически невозможно вычислить из другого, хотя один ключ уникальным образом связан с другим. В таких системах, если ключ шифрования (КШ) является общедоступным, то любой пользователь может зашифровать сообщение с его помощью но расшифровать такие сообщения могут только пользователи, имеющие соответствующий ключ дешифрования (КД). И наоборот, пользователь может сохранять КШ в секрете, а КД сделать общедоступным. В этом случае любое лицо, имеющее КД, может не только расшифровать сообщение, но и будет знать, что сообщение не было изменено, поскольку только пользователь, имеющий КШ, может быть источником данного шифртекста. Это свойство позволяет пользователю, обладающему секретным КШ, посылать "подписанные" сообщения, т.е. сообщения, содержащие аутентификационную информацию.

Основным недостатком асимметричных алгоритмов криптографии выступает относительно невысокая скорость работы. Поэтому на практике используются криптосистемы гибридного типа, когда асимметричные алгоритмы обеспечивают обмен секретными ключами, необходимыми для реализации механизмов симметричного шифрования.

Проблема аутентификации пользователей может эффективно решаться с помощью криптографических методов. Однако, в сетях построенных на базе коммутируемых каналов связи, можно использовать более простые, некриптографические способы, связанные с применением модемов, обеспечивающих функцию обратного вызова. При этом в процессе аутентификации, помимо традиционной проверки секретного пароля, автоматически инициируется обратный телефонный вызов (с предшествующим принудительным разрывом соединения) к абоненту, претендующему на доступ к информации.

3. Защита юридической значимости электронных документов оказывается необходимой при использовании вычислительных систем и сетей для обработки, хранения и передачи информационных объектов (сообщений, файлов, баз данных), содержащих распорядительное, договорное, финансовое и нотариальные документы. Их общая особенность заключается в том, что в случае возникнове-

ния споров должна быть обеспечена возможность доказательства того факта, что автор действительно фиксировал свое волеизъявление в данном электронном документе. В общем случае, незащищенные вычислительные системы не обладают свойством подтверждения подлинности и фиксации авторства электронных документов, хранящихся в памяти ПЭВМ или циркулирующих по каналам ИВС. Для решения данной проблемы могут использоваться разнообразные криптографические методы, на практике же вопросы юридической значимости электронных документов решаются совместно с вопросами защиты систем связи.

4. В проблеме защиты информации от утечки за счет ПЭМИН в зависимости от способа попадания сигналов в среду распространения можно выделить четыре возможных канала утечки обрабатываемой информации:

• канал электромагнитного излучения, образующийся за счет непосредственного перехвата электромагнитных полей, порождаемых компонентами средств вычислительной техники (СВТ);

• канал случайных антенн, образующийся за счет перехвата наведенных по эфиру сигналов в проводах, кабелях или иных токопроводящих коммуникациях с оконечным оборудованием (телефонные, телеграфные аппараты и т.п.),либо без таковых, но проходящих вблизи работающих СВТ, однако не связанных с ними гальванически и имеющих выход за пределы охраняемой территории;

• канал отходящих проводов и кабелей, гальванически связанных с обрабатывающими информацию СВТ, образующийся за счет перехвата наведенных по эфиру и внутренним паразитным связям сигналов. Перехват осуществляется (как и в предыдущем случае) путем подключения к указанным проводникам специальной приемной аппаратуры с использованием согласующих устройств;

• канал неравномерного потребления тока из сети электропитания, образующийся за счет амплитудной модуляции, вызванной срабатыванием элементов СВТ при прохождении через них сигналов информации.

Имеется потенциальная опасность существования еще одного класса искусственно создаваемых каналов утечки за счет скрытой установки специальных, так называемых "закладных" устройств.

Защита информации от утечки за счет ПЭМИН для действующих СВТ на практике достигается применением активных и пассивных методов. Так как пассивные методы защиты отдельных ПЭВМ и особенно всей сети (экранирование,

установка фильтров, использование электропитания по схеме "электродвигатель-генератор" и т.п.) практически затруднительно, на практике обычно используются активные методы. Активные методы защиты заключаются в создании маскирующих помех в каналах ПЭМИН, затрудняющих выделение информационных сигналов. В качестве маскирующих помех наиболее эффективны "прицельные" помехи, представляющие собой случайную последовательность помеховых сигналов, идентичных информационным сигналам. Применяется также метод пространственного зашумления, что обеспечивает защиту не только мониторов, но и системных блоков, клавиатур и принтеров СВТ.

5. Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ приобрела за последнее время особую актуальность. Масштабы реальных проявлений "вирусных эпидемий" оцениваются сотнями тысяч случаев "заражения" ПЭВМ. Особо опасны вирусы для компьютеров, входящих в состав однородных вычислительных сетей.

Некоторые особенности современных вычислительных систем создают благоприятные условия для распространения вирусов. К ним, в частности, относятся: необходимость совместного использования программ, ненадежность существующих механизмов защиты и разграничения доступа к информации в отношении противодействия вирусу. Как правило, рассматриваются два направления в методах защиты от вируса :

- применение "иммуностойких" программных средств, защищенных от возможности несанкционированной модификации;
- применение специальных программ анализаторов, осуществляющих постоянный контроль возникновения "аномалий" в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности, а также "входной" контроль новых программ перед их использованием.

Имеющийся в настоящее время арсенал средств противодействия компьютерным вирусам достаточен для того, чтобы предотвратить серьезный ущерб от их воздействия. В общем случае, существуют следующие основные виды программ автоматического поиска вирусов: детекторы, вакцины и фаги.

Программы-детекторы - это специальные программы, предназначенные для просмотра всех возможных мест нахождения вирусов (файлы ОС, основная па-

мять, возможно даже пустое в данный момент пространство диска) и сигнализировать об их наличии или отсутствии.

Программы вакцины - это программы, "вшиваемые" в тело защищаемой программы (дописывающиеся к ее коду), либо резидентно оставляемые в оперативной памяти с целью обнаружения присутствия вируса по признакам аномального поведения (попытки записи в определенные области памяти и т.п.) и, возможно обезвредить его.

Программы-фаги - это детекторы, дополненные специальными функциями по обезвреживанию данного вируса (удаление его из файлов ОС, оперативной памяти и т.д). Большинство антивирусных программ просты в использовании. Минимальный их комплект должен находиться в каждом компьютере.

6. Технические методы защиты от несанкционированного копирования программ (НСК) для ПЭВМ тесно увязаны с вопросами защиты информации от НСД. Хотя НСД не всегда направлен на копирование информации, большинство методов защиты от НСД можно применять и для защиты от НСК. Однако в проблеме защиты от НСК имеются свои специфические методы, включающие специальные программные средства, которые подвергают защищаемые программы предварительной обработке - вставка парольной защиты, проверка по обращению к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабочей ПЭВМ по ее уникальным характеристикам и т.п. Такая обработка приводит исполняемый код защищенной программы в состояние препятствующее выполнению ее на "чужих" ПЭВМ.

В других случаях для повышения защищенности применяются дополнительные аппаратные средства, подключаемые к разъему принтера или к системной шине ПЭВМ и обеспечивающие шифрование файлов, содержащих исполняемый код программы.

Общим свойством средств защиты от НСК является ограниченная стойкость такой защиты, т.к. в конечном счете исполняемый код программы поступает на выполнение в центральный процессор ПЭВМ в открытом виде и может быть прослежен с помощью аппаратных отладчиков

7. Организационные средства защиты информации представляют из себя организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации информационно-

вычислительных сетей для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы сетей на всех этапах их жизненного цикла (строительство помещений, проектирование сети, монтаж и наладка оборудования, испытания и эксплуатация). Подобные мероприятия хорошо известны, достаточно многочисленны. Обсуждение данного вопроса выходит за рамки статьи.

Подводя итог проведенному обзору, следует отметить, что защита информации может решаться разными методами, но наибольшего эффекта и требуемой надежности можно достигнуть только реализацией ряда комплексных мероприятий.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А.С. Овсянников, В.В. Камышников, Ю.М. Казаченко, Н.Н. Мошак

Необходимой, а точнее, центральной составной частью мероприятий по защите информации в вычислительных системах и сетях являются внутренние эффективные системы защиты отдельных ПЭВМ от несанкционированного доступа (НСД). Основными направлениями защиты от НСД являются:

- идентификация и аутентификация пользователей средств вычислительной техники (СВТ) и АС (автоматизированных систем);
- реализация правил разграничения доступа;
- регистрация действий пользователей и их процессов;
- предоставление возможностей по изменению конфигурации системы защиты: введение новых пользователей, изменение их полномочий, и т.д.;
- реакция на попытки НСД;
- очистка оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователей с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как системы разграничения доступа, так и обеспечивающих ее средств.

Сравнение систем защиты проводилось с учетом следующих факторов: