**Тема: Проблемы защиты информации в**

**компьютерных сетях.**

**Содержание.**

Введение.

1. Проблемы защиты информации в компьютерных системах.

2. Обеспечение защиты информации в сетях.

3. Механизмы обеспечения безопасности:

3.1. Криптография.

3.2. Электронная подпись.

3.3. Аутентификация.

3.4. Защита сетей.

4. Требования к современным средствам защиты информации.

Заключение.

Литература.

**Введение.**

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надёжность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в неё изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех цивилизованных странах на страже безопасности граждан стоят законы, но в сфере вычислительной техники правоприменительная практика пока развита недостаточно, а законотворческий процесс не успевает за развитием компьютерных систем, во многом опирается на меры самозащиты.

Всегда существует проблема выбора между необходимым уровнем защиты и эффективностью работы в сети. В некоторых случаях пользователями или потребителями меры по обеспечению безопасности могут быть расценены как меры по ограничению доступа и эффективности. Однако такие средства, как, например, криптография, позволяют значительно усилить степень защиты, не ограничивая доступ пользователей к данным.

**1. Проблемы защиты информации в компьютерных системах.**

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жёстко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Известно очень большое число угроз информации, которые могут быть реализованы как со стороны внешних нарушителей, так и со стороны внутренних нарушителей.

Радикальное решение проблем защиты электронной информации может быть получено только на базе использования криптографических методов, которые позволяют решать важнейшие проблемы защищённой автоматизированной обработки и передачи данных. При этом современные скоростные методы криптографического преобразования позволяют сохранить исходную производительность автоматизированных систем. Криптографические преобразования данных являются наиболее эффективным средством обеспечения конфиденциальности данных, их целостности и подлинности. Только их использование в совокупности с необходимыми техническими и организационными мероприятиями могут обеспечить защиту от широкого спектра потенциальных угроз.

Проблемы, возникающие с безопасностью передачи информации при работе в компьютерных сетях, можно разделить на три основных типа:

**·** перехват информации – целостность информации сохраняется, но её конфиденциальность нарушена;

**·** модификация информации – исходное сообщение изменяется либо полностью подменяется другим и отсылается адресату;

**·** подмена авторства информации. Данная проблема может иметь серьёзные последствия. Например, кто-то может послать письмо от вашего имени (этот вид обмана принято называть спуфингом) или Web – сервер может притворяться электронным магазином, принимать заказы, номера кредитных карт, но не высылать никаких товаров.

Потребности современной практической информатики привели к возникновению нетрадиционных задач защиты электронной информации, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной цифровой подписи. Теоретической базой для решения этой проблемы явилось открытие двухключевой криптографии американскими исследователями Диффи и Хемиманом в середине 1970-х годов, которое явилось блестящим достижением многовекового эволюционного развития криптографии. Революционные идеи двухключевой криптографии привели к резкому росту числа открытых исследований в области криптографии и показали новые пути развития криптографии, новые её возможности и уникальное значение её методов в современных условиях массового применения электронных информационных технологий.

Технической основой перехода в информационное общество являются современные микроэлектронные технологии, которые обеспечивают непрерывный рост качества средств вычислительной техники и служат базой для сохранения основных тенденций её развития – миниатюризации, снижения электропотребления, увеличения объёма оперативной памяти (ОП) и ёмкости встроенных и съёмных накопителей, роста производительности и надёжности, расширение сфер и масштабов применения. Данные тенденции развития средств вычислительной техники привели к тому, что на современном этапе защита компьютерных систем от несанкционированного доступа характеризуется возрастанием роли программных и криптографических механизмов защиты по сравнению с аппаратными.

Возрастание роли программных и криптографических средств зашит проявляется в том, что возникающие новые проблемы в области защиты вычислительных систем от несанкционированного доступа, требуют использования механизмов и протоколов со сравнительно высокой вычислительной сложностью и могут быть эффективно решены путём использования ресурсов ЭВМ.

Одной из важных социально-этических проблем, порождённых всё более расширяющимся применением методов криптографической защиты информации, является противоречие между желанием пользователей защитить свою информацию и передачу сообщений и желанием специальных государственных служб иметь возможность доступа к информации некоторых других организаций и отдельных лиц с целью пресечения незаконной деятельности. В развитых странах наблюдается широкий спектр мнений о подходах к вопросу о регламентации использования алгоритмов шифрования. Высказываются предложения от полного запрета широкого применения криптографических методов до полной свободы их использования. Некоторые предложения относятся к разрешению использования только ослабленных алгоритмов или к установлению порядка обязательной регистрации ключей шифрования. Чрезвычайно трудно найти оптимальное решение этой проблемы. Как оценить соотношение потерь законопослушных граждан и организаций от незаконного использования их информации и убытков государства от невозможности получения доступа к зашифрованной информации отдельных групп, скрывающих свою незаконную деятельность? Как можно гарантированно не допустить незаконное использование криптоалгоритмов лицами, которые нарушают и другие законы? Кроме того, всегда существуют способы скрытого хранения и передачи информации. Эти вопросы ещё предстоит решать социологам, психологам, юристам и политикам.

Возникновение глобальных информационных сетей типа INTERNET является важным достижением компьютерных технологий, однако, с INTERNETсвязана масса компьютерных преступлений.

Результатом опыта применения сети INTERNET является выявленная слабость традиционных механизмов защиты информации и отставания в применении современных методов. Криптография предоставляет возможность обеспечить безопасность информации в INTERNET и сейчас активно ведутся работы по внедрению необходимых криптографических механизмов в эту сеть. Не отказ от прогресса в информатизации, а использование современных достижений криптографии – вот стратегически правильное решение. Возможность широкого использования глобальных информационных сетей и криптографии является достижением и признаком демократического общества.

Владение основами криптографии в информационном обществе объективно не может быть привилегией отдельных государственных служб, а является насущной необходимостью для самих широких слоёв научно-технических работников, применяющих компьютерную обработку данных или разрабатывающих информационные системы, сотрудников служб безопасности и руководящего состава организаций и предприятий. Только это может служить базой для эффективного внедрения и эксплуатации средств информационной безопасности.

Одна отдельно взятая организация не может обеспечить достаточно полный и эффективный контроль за информационными потоками в пределах всего государства и обеспечить надлежащую защиту национального информационного ресурса. Однако, отдельные государственные органы могут создать условия для формирования рынка качественных средств защиты, подготовки достаточного количества специалистов и овладения основами криптографии и защиты информации со стороны массовых пользователей.

В России и других странах СНГ в начале 1990-х годов отчётливо прослеживалась тенденция опережения расширения масштабов и областей применения информационных технологий над развитием систем защиты данных. Такая ситуация в определённой степени являлась и является типичной и для развитых капиталистических стран. Это закономерно: сначала должна возникнуть практическая проблема, а затем будут найдены решения. Начало перестройки в ситуации сильного отставания стран СНГ в области информатизации в конце 1980-х годов создало благодатную почву для резкого преодоления сложившегося разрыва.

Пример развитых стран, возможность приобретения системного программного обеспечения и компьютерной техники вдохновили отечественных пользователей. Включение массового потребителя, заинтересованного в оперативной обработке данных и других достоинствах современных информационно-вычислительных систем, в решении проблемы компьютеризации привело к очень высоким темпам развития этой области в России и других странах СНГ. Однако, естественное совместное развитие средств автоматизации обработки информации и средств защиты информации в значительной степени нарушилось, что стало причиной массовых компьютерных преступлений. Ни для кого не секрет, что компьютерные преступления в настоящее время составляют одну из очень актуальных проблем.

Использование систем защиты зарубежного производства не может выправить этот перекос, поскольку поступающие на рынок России продукты этого типа не соответствуют требованиям из-за существующих экспортных ограничений, принятых в США – основном производителе средств защиты информации. Другим аспектом, имеющим первостепенное значение, является то, что продукция такого типа должна пройти установленную процедуру сертифицирования в уполномоченных на проведение таких работ организациях.

Сертификаты иностранных фирм и организаций, никак не могут быть заменой отечественным. Сам факт использования зарубежного системного и прикладного программного обеспечения создаёт повышенную потенциальную угрозу информационным ресурсам. Применение иностранных средств защиты без должного анализа соответствия выполняемым функциям и уровня обеспечиваемой защиты может многократно осложнить ситуацию.

Форсирование процесса информатизации требует адекватного обеспечения потребителей средствами защиты. Отсутствие на внутреннем рынке достаточного количества средств защиты информации, циркулирующей в компьютерных системах, значительное время не позволяло в необходимых масштабах осуществлять мероприятия по защите данных. Ситуация усугублялась отсутствием достаточного количества специалистов в области защиты информации, поскольку последние, как правило, готовились только для специальных организаций. Реструктурирование последних, связанное с изменениями, протекающими в России, привело к образованию независимых организаций, специализирующихся в области защиты информации, поглотивших высвободившиеся кадры, и как следствие возникновению духа конкуренции, приведшей к появлению в настоящее время достаточно большого количества сертифицированных средств защиты отечественных разработчиков.

Одной из важных особенностей массового использования информационных технологий является то, что для эффективного решения проблемы защиты государственного информационного ресурса необходимо рассредоточение мероприятий по защите данных среди массовых пользователей. Информация должна быть защищена в первую очередь там, где она создаётся, собирается, перерабатывается и теми организациями, которые несут непосредственный урон при несанкционированном доступе к данным. Этот принцип рационален и эффективен: защита интересов отдельных организаций – это составляющая реализации защиты интересов государства в целом.

**2. Обеспечение защиты информации в сетях.**

В ВС сосредотачивается информация, исключительное право на пользование которой принадлежит определённым лицам или группам лиц, действующим в порядке личной инициативы или в соответствии с должностными обязанностями. Такая информация должна быть защищена от всех видов постороннего вмешательства: чтения лицами, не имеющими права доступа к информации, и преднамеренного изменения информации. К тому же в ВС должны приниматься меры по защите вычислительных ресурсов сети от их несанкционированного использования, т.е. должен быть исключён доступ к сети лиц, не имеющих на это права. Физическая защита системы и данных может осуществляться только в отношении рабочих ЭВМ и узлов связи и оказывается невозможной для средств передачи, имеющих большую протяжённость. По этой причине в ВС должны использоваться средства, исключающие несанкционированный доступ к данным и обеспечивающие их секретность.

Исследования практики функционирования систем обработки данных и вычислительных систем показали, что существует достаточно много возможных направлений утечки информации и путей несанкционированного доступа в системах и сетях. В их числе:

**·** чтение остаточной информации в памяти системы после выполнения санкционированных запросов;

**·** копирование носителей информации и файлов информации с преодолением мер защиты;

**·** маскировка под зарегистрированного пользователя;

**·** маскировка под запрос системы;

**·** использование программных ловушек;

**·** использование недостатков операционной системы;

**·** незаконное подключение к аппаратуре и линиям связи;

**·** злоумышленный вывод из строя механизмов защиты;

**·** внедрение и использование компьютерных вирусов.

Обеспечение безопасности информации в ВС и в автономно работающих ПЭВМ достигается комплексом организационных, организационно-технических, технических и программных мер.

**К организационным мерам защиты информации** относятся:

**·** ограничение доступа в помещения, в которых происходит подготовка и обработка информации;

**·** допуск к обработке и передаче конфиденциальной информации только проверенных должностных лиц;

**·** хранение магнитных носителей и регистрационных журналов в закрытых для доступа посторонних лиц сейфах;

**·** исключение просмотра посторонними лицами содержания обрабатываемых материалов через дисплей, принтер и т.д.;

**·** использование криптографических кодов при передаче по каналам связи ценной информации;

**·** уничтожение красящих лент, бумаги и иных материалов, содержащих фрагменты ценной информации.

**Организационно-технические меры защиты информации** включают:

**·** осуществление питания оборудования, обрабатывающего ценную информацию от независимого источника питания или через специальные сетевые фильтры;

**·** установку на дверях помещений кодовых замков;

**·** использование для отображения информации при вводе-выводе жидкокристаллических или плазменных дисплеев, а для получения твёрдых копий – струйных принтеров и термопринтеров, поскольку дисплей даёт такое высокочастотное электромагнитное излучение, что изображение с его экрана можно принимать на расстоянии нескольких сотен километров;

**·** уничтожение информации, хранящейся в ПЗУ и на НЖМД, при списании или отправке ПЭВМ в ремонт;

**·** установка клавиатуры и принтеров на мягкие прокладки с целью снижения возможности снятия информации акустическим способом;

**·** ограничение электромагнитного излучения путём экранирования помещений, где происходит обработка информации, листами из металла или из специальной пластмассы.

**Технические средства защиты информации** – это системы охраны территорий и помещений с помощью экранирования машинных залов и организации контрольно-пропускных систем. Защита информации в сетях и вычислительных средствах с помощью технических средств реализуется на основе организации доступа к памяти с помощью:

**·** контроля доступа к различным уровням памяти компьютеров;

**·** блокировки данных и ввода ключей;

**·** выделение контрольных битов для записей с целью идентификации и др.

**Архитектура программных средств защиты информации** включает:

**·** контроль безопасности, в том числе контроль регистрации вхождения в систему, фиксацию в системном журнале, контроль действий пользователя;

**·** реакцию (в том числе звуковую) на нарушение системы защиты контроля доступа к ресурсам сети;

**·** контроль мандатов доступа;

**·** формальный контроль защищённости операционных систем (базовой общесистемной и сетевой);

**·** контроль алгоритмов защиты;

**·** проверку и подтверждение правильности функционирования технического и программного обеспечения.

Для надёжной защиты информации и выявления случаев неправомочных действий проводится регистрация работы системы: создаются специальные дневники и протоколы, в которых фиксируются все действия, имеющие отношение к защите информации в системе. Фиксируются время поступления заявки, её тип, имя пользователя и терминала, с которого инициализируется заявка. При отборе событий, подлежащих регистрации, необходимо иметь в виду, что с ростом количества регистрируемых событий затрудняется просмотр дневника и обнаружение попыток преодоления защиты. В этом случае можно применять программный анализ и фиксировать сомнительные события. Используются также специальные программы для тестирования системы защиты. Периодически или в случайно выбранные моменты времени они проверяют работоспособность аппаратных и программных средств защиты.

К отдельной группе мер по обеспечению сохранности информации и выявлению несанкционированных запросов относятся программы обнаружения нарушений в режиме реального времени. Программы данной группы формируют специальный сигнал при регистрации действий, которые могут привести к неправомерным действиям по отношению к защищаемой информации. Сигнал может содержать информацию о характере нарушения, месте его возникновения и другие характеристики. Кроме того, программы могут запретить доступ к защищаемой информации или симулировать такой режим работы (например, моментальная загрузка устройств ввода-вывода), который позволит выявить нарушителя и задержать его соответствующей службой.

Один из распространённых способов защиты – явное указание секретности выводимой информации. В системах, поддерживающих несколько уровней секретности, вывод на экран терминала или печатающего устройства любой единицы информации (например, файла, записи и таблицы) сопровождается специальным грифом с указанием уровня секретности. Это требование реализуется с помощью соответствующих программных средств.

В отдельную группу выделены средства защиты от несанкционированного использования программного обеспечения. Они приобретают особое значение вследствие широкого распространения ПК.

**3. Механизмы обеспечения безопасности.**

**3.1. Криптография.**

Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа.

Системам шифрования столько же лет, сколько письменному обмену информацией.

“Криптография” в переводе с греческого языка означает “тайнопись”, что вполне отражает её первоначальное предназначение. Примитивные (с позиций сегодняшнего дня) криптографические методы известны с древнейших времён и очень длительное время они рассматривались скорее как некоторое ухищрение, чем строгая научная дисциплина. Классической задачей криптографии является обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, называемую шифртекстом или криптограммой. При этом шифр-пакет может содержать как новые, так и имеющиеся в открытом сообщении знаки. Количество знаков в криптограмме и в исходном тексте в общем случае может различаться. Непременным требованием является то, что, используя некоторые логические замены символов в шифртексте, можно однозначно и в полном объёме восстановить исходный текст. Надёжность сохранения информации в тайне определялось в далёкие времена тем, что в секрете держался сам метод преобразования.

Прошли многие века, в течении которых криптография являлась предметом избранных – жрецов, правителей, крупных военачальников и дипломатов. Несмотря на малую распространённость использование криптографических методов и способов преодоления шифров противника оказывало существенное воздействие на исход важных исторических событий. Известен не один пример того, как переоценка используемых шифров приводила к военным и дипломатическим поражениям. Несмотря на применение криптографических методов в важных областях, эпизодическое использование криптографии не могло даже близко подвести её к той роли и значению, которые она имеет в современном обществе. Своим превращением в научную дисциплину криптография обязана потребностям практики, порождённым электронной информационной технологией.

Пробуждение значительного интереса к криптографии и её развитие началось с XIX века, что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых стран стали относится к этой дисциплине как к обязательному инструменту своей деятельности.

В основе шифрования лежат два основных понятия: алгоритм и ключ. ***Алгоритм*** – это способ закодировать исходный текст, в результате чего получается зашифрованное послание. Зашифрованное послание может быть интерпретировано только с помощью ***ключа.***

Очевидно, чтобы зашифровать послание , достаточно алгоритма.

Голландский криптограф Керкхофф (1835 – 1903) впервые сформулировал правило: стойкость шифра, т.е. криптосистемы – набора процедур, управляемых некоторой секретной информацией небольшого объёма, должна быть обеспечена в том случае, когда криптоаналитику противника известен весь механизм шифрования за исключением секретного ключа – информации, управляющей процессом криптографических преобразований. Видимо, одной из задач этого требования было осознание необходимости испытания разрабатываемых криптосхем в условиях более жёстких по сравнению с условиями, в которых мог бы действовать потенциальный нарушитель. Это правило стимулировало появление более качественных шифрующих алгоритмов. Можно сказать, что в нём содержится первый элемент стандартизации в области криптографии, поскольку предполагается разработка открытых способов преобразований. В настоящее время это правило интерпретируется более широко: все долговременные элементы системы защиты должны предполагаться известными потенциальному злоумышленнику. В последнюю формулировку криптосистемы входят как частный случай систем защиты. В этой формулировке предполагается, что все элементы систем защиты подразделяются на две категории – долговременные и легко сменяемые. К долговременным элементам относятся те элементы, которые относятся к разработке систем защиты и для изменения требуют вмешательства специалистов или разработчиков. К легко сменяемым элементам относятся элементы системы, которые предназначены для произвольного модифицирования или модифицирования по заранее заданному правилу, исходя из случайно выбираемых начальных параметров. К легко сменяемым элементам относятся, например, ключ, пароль, идентификация и т.п. Рассматриваемое правило отражает тот факт, надлежащий уровень секретности может быть обеспечен только по отношению к легко сменяемым элементам.

Несмотря на то, что согласно современным требованиям к криптосистемам они должны выдерживать криптоанализ на основе известного алгоритма, большого объёма известного открытого текста и соответствующего ему шифртекста, шифры, используемые специальными службами, сохраняются в секрете. Это обусловлено необходимостью иметь дополнительный запас прочности, поскольку в настоящее время создание криптосистем с доказуемой стойкостью является предметом развивающейся теории и представляет собой достаточно сложную проблему. Чтобы избежать возможных слабостей, алгоритм шифрования может быть построен на основе хорошо изученных и апробированных принципах и механизмах преобразования. Ни один серьёзный современный пользователь не будет полагаться только на надёжность сохранения в секрете своего алгоритма, поскольку крайне сложно гарантировать низкую вероятность того, что информация об алгоритме станет известной злоумышленнику.

Секретность информации обеспечивается введением в алгоритмы специальных ключей (кодов). Использование ключа при шифровании предоставляет два существенных преимущества. Во-первых, можно использовать один алгоритм с разными ключами для отправки посланий разным адресатам. Во-вторых, если секретность ключа будет нарушена, его можно легко заменить, не меняя при этом алгоритм шифрования. Таким образом, безопасность систем шифрования зависит от секретности используемого ключа, а не от секретности алгоритма шифрования. Многие алгоритмы шифрования являются общедоступными.

Количество возможных ключей для данного алгоритма зависит от числа бит в ключе. Например, 8-битный ключ допускает 256 (28) комбинаций ключей. Чем больше возможных комбинаций ключей, тем труднее подобрать ключ, тем надёжнее зашифровано послание. Так, например, если использовать 128-битный ключ, то необходимо будет перебрать 2128 ключей, что в настоящее время не под силу даже самым мощным компьютерам. Важно отметить, что возрастающая производительность техники приводит к уменьшению времени, требующегося для вскрытия ключей, и системам обеспечения безопасности приходится использовать всё более длинные ключи, что, в свою очередь, ведёт к увеличению затрат на шифрование.

Поскольку столь важное место в системах шифрования уделяется секретности ключа, то основной проблемой подобных систем является генерация и передача ключа. Существуют две основные схемы шифрования: *симметричное шифрование* (его также иногда называют традиционным или шифрованием с секретным ключом) и *шифрование с открытым ключом* (иногда этот тип шифрования называют асимметричным).

При *симметричном шифровании* отправитель и получатель владеют одним и тем же ключом (секретным), с помощью которого они могут зашифровывать и расшифровывать данные.При симметричном шифровании используются ключи небольшой длины, поэтому можно быстро шифровать большие объёмы данных. Симметричное шифрование используется, например, некоторыми банками в сетях банкоматов. Однако симметричное шифрование обладает несколькими недостатками. Во-первых, очень сложно найти безопасный механизм, при помощи которого отправитель и получатель смогут тайно от других выбрать ключ. Возникает проблема безопасного распространения секретных ключей. Во-вторых, для каждого адресата необходимо хранить отдельный секретный ключ. В третьих, в схеме симметричного шифрования невозможно гарантировать личность отправителя, поскольку два пользователя владеют одним ключом.

В схеме *шифрования с открытым ключом* для шифрования послания используются два различных ключа. При помощи одного из них послание зашифровывается, а при помощи второго – расшифровывается. Таким образом, требуемой безопасности можно добиваться, сделав первый ключ общедоступным (открытым), а второй ключ хранить только у получателя (закрытый, личный ключ). В таком случае любой пользователь может зашифровать послание при помощи открытого ключа, но расшифровать послание способен только обладатель личного ключа. При этом нет необходимости заботиться о безопасности передачи открытого ключа, а для того чтобы пользователи могли обмениваться секретными сообщениями, достаточно наличия у них открытых ключей друг друга.

Недостатком асимметричного шифрования является необходимость использования более длинных, чем при симметричном шифровании, ключей для обеспечения эквивалентного уровня безопасности, что сказывается на вычислительных ресурсах, требуемых для организации процесса шифрования.

**3.2. Электронная подпись.**

Если послание, безопасность которого мы хотим обеспечить, должным образом зашифровано, всё равно остаётся возможность модификации исходного сообщения или подмены этого сообщения другим. Одним из путей решения этой проблемы является передача пользователем получателю краткого представления передаваемого сообщения. Подобное краткое представление называют контрольной суммой, или дайджестом сообщения.

Контрольные суммы используются при создании резюме фиксированной длины для представления длинных сообщений. Алгоритмы расчёта контрольных сумм разработаны так, чтобы они были по возможности уникальны для каждого сообщения. Таким образом, устраняется возможность подмены одного сообщения другим с сохранением того же самого значения контрольной суммы.

Однако при использовании контрольных сумм возникает проблема передачи их получателю. Одним из возможных путей её решения является включение контрольной суммы в так называемую ***электронную подпись.***

При помощи электронной подписи получатель может убедиться в том, что полученное им сообщение послано не сторонним лицом, а имеющим определённые права отправителем. Электронные подписи создаются шифрованием контрольной суммы и дополнительной информации при помощи личного ключа отправителя. Таким образом, кто угодно может расшифровать подпись, используя открытый ключ, но корректно создать подпись может только владелец личного ключа. Для защиты от перехвата и повторного использования подпись включает в себя уникальное число – порядковый номер.

**3.3. Аутентификация.**

**Аутентификация** является одним из самых важных компонентов организации защиты информации в сети. Прежде чем пользователю будет предоставлено право получить тот или иной ресурс, необходимо убедиться, что он действительно тот, за кого себя выдаёт.

При получении запроса на использование ресурса от имени какого-либо пользователя сервер, предоставляющий данный ресурс, передаёт управление серверу аутентификации. После получения положительного ответа сервера аутентификации пользователю предоставляется запрашиваемый ресурс.

При аутентификации используется, как правило, принцип, получивший название “что он знает”, - пользователь знает некоторое секретное слово, которое он посылает серверу аутентификации в ответ на его запрос. Одной из схем аутентификации является использование стандартных паролей. **Пароль** – совокупность символов, известных подключенному к сети абоненту, - вводится им в начале сеанса взаимодействия с сетью, а иногда и в конце сеанса (в особо ответственных случаях пароль нормального выхода из сети может отличаться от входного). Эта схема является наиболее уязвимой с точки зрения безопасности – пароль может быть перехвачен и использован другим лицом. Чаще всего используются схемы с применением одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего является крайне трудной задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Знание секретного слова необходимо пользователю для приведения этого устройства в действие.

Одной из наиболее простых систем, не требующих дополнительных затрат на оборудование, но в то же время обеспечивающих хороший уровень защиты, является S/Key, на примере которой можно продемонстрировать порядок представления одноразовых паролей.

В процессе аутентификации с использованием S/Key участвуют две стороны – клиент и сервер. При регистрации в системе, использующей схему аутентификации S/Key, сервер присылает на клиентскую машину приглашение, содержащее зерно, передаваемое по сети в открытом виде, текущее значение счётчика итераций и запрос на ввод одноразового пароля, который должен соответствовать текущему значению счётчика итерации. Получив ответ, сервер проверяет его и передаёт управление серверу требуемого пользователю сервиса.

**3.4. Защита сетей.**

В последнее время корпоративные сети всё чаще включаются в Интернет или даже используют его в качестве своей основы. Учитывая то, какой урон может принести незаконное вторжение в корпоративную сеть, необходимо выработать методы защиты. Для защиты корпоративных информационных сетей используются брандмауэры. **Брандмауэры -** этосистема или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Как правило, эта граница проводится между локальной сетью предприятия и INTERNETOM, хотя её можно провести и внутри. Однако защищать отдельные компьютеры невыгодно, поэтому обычно защищают всю сеть. Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение – пропускать его или отбросить. Для того чтобы брандмауэр мог принимать эти решения, для него определяется набор правил.

Брандмауэр может быть реализован как аппаратными средствами (то есть как отдельное физическое устройство), так и в виде специальной программы, запущенной на компьютере.

Как правило, в операционную систему, под управлением которой работает брандмауэр, вносятся изменения, цель которых – повышение защиты самого брандмауэра. Эти изменения затрагивают как ядро ОС, так и соответствующие файлы конфигурации. На самом брандмауэре не разрешается иметь разделов пользователей, а следовательно, и потенциальных дыр – только раздел администратора. Некоторые брандмауэры работают только в однопользовательском режиме, а многие имеют систему проверки целостности программных кодов.

Брандмауэр обычно состоит из нескольких различных компонентов, включая фильтры или экраны, которые блокируют передачу части трафика.

Все брандмауэры можно разделить на два типа:

**·** пакетные фильтры, которые осуществляют фильтрацию IP-пакетов средствами фильтрующих маршрутизаторов;

**·** серверы прикладного уровня, которые блокируют доступ к определённым сервисам в сети.

Таким образом, брандмауэр можно определить как набор компонентов или систему, которая располагается между двумя сетями и обладает следующими свойствами:

**·** весь трафик из внутренней сети во внешнюю и из внешней сети во внутреннюю должен пройти через эту систему;

**·** только трафик, определённый локальной стратегией защиты, может пройти через эту систему;

**·** система надёжно защищена от проникновения.

**4. Требования к современным средствам защиты информации.**

Согласно требованиям гостехкомиссии России средства защиты информации от несанкционированного доступа(СЗИ НСД), отвечающие высокому уровню защиты, должны обеспечивать:

**·** дискреционный и мандатный принцип контроля доступа;

**·** очистку памяти;

**·** изоляцию модулей;

**·** маркировку документов;

**·** защиту ввода и вывода на отчуждаемый физический носитель информации;

**·** сопоставление пользователя с устройством;

**·** идентификацию и аутентификацию;

**·** гарантии проектирования;

**·** регистрацию;

**·** взаимодействие пользователя с комплексом средств защиты;

**·** надёжное восстановление;

**·** целостность комплекса средств защиты;

**·** контроль модификации;

**·** контроль дистрибуции;

**·** гарантии архитектуры;

Комплексные СЗИ НСД должны сопровождаться пакетом следующих документов:

**·** руководство по СЗИ;

**·** руководство пользователя;

**·** тестовая документация;

**·** конструкторская (проектная) документация.

Таким образом, в соответствии с требованиями гостехкомиссии России комплексные СЗИ НСД должны включать базовый набор подсистем. Конкретные возможности этих подсистем по реализации функций защиты информации определяют уровень защищённости средств вычислительной техники. Реальная эффективность СЗИ НСД определяется функциональными возможностями не только базовых, но и дополнительных подсистем, а также качеством их реализации.

Компьютерные системы и сети подвержены широкому спектру потенциальных угроз информации, что обуславливает необходимость предусмотреть большой перечень функций и подсистем защиты. Целесообразно в первую очередь обеспечить защиту наиболее информативных каналов утечки информации, каковыми являются следующие:

**·** возможность копирования данных с машинных носителей;

**·** каналы передачи данных;

**·** хищение ЭВМ или встроенных накопителей.

Проблема перекрытия этих каналов усложняется тем, что процедуры защиты данных не должны приводить к заметному снижению производительности вычислительных систем. Эта задача может быть эффективно решена на основе технологии глобального шифрования информации, рассмотренной в предыдущем разделе.

Современная массовая система защиты должна быть эргономичной и обладать такими свойствами, благоприятствующими широкому её применению, как:

**·** комплексность – возможность установки разнообразных режимов защищённой обработки данных с учётом специфических требований различных пользователей и предусматривать широкий перечень возможных действий предполагаемого нарушителя;

**·** совместимость – система должна быть совместимой со всеми программами, написанными для данной операционной системы, и должна обеспечивать защищённый режим работы компьютера в вычислительной сети;

**·** переносимость – возможность установки системы на различные типы компьютерных систем, включая портативные;

**·** удобство в работе – система должна быть проста в эксплуатации и не должна менять привычную технологию работы пользователей;

**·** работа в масштабе реального времени – процессы преобразования информации, включая шифрование, должны выполняться с большой скоростью;

**·** высокий уровень защиты информации;

**·** минимальная стоимость системы.

**Заключение.**

Вслед за массовым применением современных информационных технологий криптография вторгается в жизнь современного человека. На криптографических методах основано применение электронных платежей, возможность передачи секретной информации по открытым сетям связи, а также решение большого числа других задач защиты информации в компьютерных системах и информационных сетях. Потребности практики привели к необходимости массового применения криптографических методов, а следовательно к необходимости расширения открытых исследований и разработок в этой области. Владение основами криптографии становится важным для учёных и инженеров, специализирующихся в области разработки современных средств защиты информации, а также в областях эксплуатации и проектирования информационных и телекоммуникационных систем.

Одной из актуальных проблем современной прикладной криптографии является разработка скоростных программных шифров блочного типа, а также скоростных устройств шифрования.

В настоящее время предложен ряд способов шифрования, защищённых патентами Российской Федерации и основанных на идеях использования:

**·** гибкого расписания выборки подключений;

**·** генерирования алгоритма шифрования по секретному ключу;

**·** подстановок, зависящих от преобразуемых данных.

**Литература.**

1. Острейковский В.А. Информатика: Учеб. пособие для студ. сред. проф. учеб. заведений. – М.: Высш. шк., 2001. – 319с.:ил.

2. Экономическая информатика / под ред. П.В. Конюховского и Д.Н. Колесова. – СПб.: Питер, 2000. – 560с.:ил.

3. Информатика: Базовый курс / С.В. Симонович и др. – СПб.: Питер, 2002. – 640с.:ил.

4. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Издательство “Лань”, 2001. – 224с.,ил. – (Учебники для вузов. Специальная литература).