Лекция 10

Аппаратные методы, способы и средства защиты информации.

Содержание проблемы защиты информации специалистами интерпретируются следующим образом. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость. Основными факторами, способствующими повышению этой уязвимости, являются:

-Резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации;

-Сосредоточение в единых базах данных информации различного назначения и различных принадлежностей;

-Резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней данных;

-Усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение многопрограммного режима, а также режимов разделения времени и реального времени;

-Автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

В этих условиях возникает уязвимость двух видов: с одной стороны, возможность уничтожения или искажения информации (т.е. нарушение ее физической целостности), а с другой - возможность несанкционированного использования информации (т.е. опасность утечки информации ограниченного пользования). Второй вид уязвимости вызывает особую озабоченность пользователей ЭВМ.

Основными потенциально возможными каналами утечки информации являются:

-Прямое хищение носителей и документов;

-Запоминание или копирование информации;

-Несанкционированное подключение к аппаратуре и линиям связи или незаконное использование "законной" (т.е. зарегистрированной) аппаратуры

системы (чаще всего терминалов пользователей).

Аппаратные средства – это технические средства, используемые для обработки данных. Сюда относятся: Персональный компьютер (комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач).

Периферийное оборудование (комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора).

Физические носители машинной информации.

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

-специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

-генераторы кодов, предназначенные для автоматического генерирования идентифицирующего кода устройства;

-устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

-специальные биты секретности, значение которых определяет уровень секретности информации, хранимой в ЗУ, которой принадлежат данные биты;

-схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных. Особую и получающую наибольшее распространение группу аппаратных средств защиты составляют устройства для шифрования информации (криптографические методы).

Аппаратные средства - основа построения систем защиты от несанкционированного доступа к информации

Разработке и производству современных средств защиты от несанкционированного доступа (НСД) к информации в ОКБ САПР

предшествовало выполнение научно-исследовательских и опытно-конструкторских работ в этой области. Большинство разработчиков на первоначальном этапе были сосредоточены на создании только программного обеспечения, реализующего функции защиты в автоматизированных системах, что не может гарантировать надежной защищённости автоматизированных систем от НСД к информации. К примеру, проверка целостности программной среды, осуществляемая какой-либо другой программой, находящейся на одном носителе с проверяемыми объектами, не может гарантировать правильности проводимых процедур. Необходимо обеспечить достоверность самой программы проверки целостности, а только затем выполнение ее контрольных процедур. Таким образом, это привело к осознанию необходимости использования в системах защиты информации от НСД аппаратных средств со встроенными процедурами контроля целостности программ и данных, идентификации и аутентификации, регистрации и учета.

В 90-е годы сотрудниками ОКБ САПР была разработана методология применения аппаратной защиты, признанная необходимой основой построения систем защиты от НСД к информации. Основные идеи этого подхода состоят в следующем:

-комплексный подход к решению вопросов защиты информации в автоматизированных системах (АС) от НСД. Признание мультипликативной парадигмы защиты, и, как следствие, равное внимание надежности реализации контрольных процедур на всех этапах работы АС ;

-«материалистическое» решение «основного вопроса» информационной безопасности: «что первично — hard или soft?»;

-последовательный отказ от программных методов контроля как очевидно ненадежных и перенос наиболее критичных контрольных процедур на аппаратный уровень;

-максимально возможное разделение условно-постоянных и условно-переменных элементов контрольных операций;

-построение средств защиты информации от несанкционированного доступа (СЗИ НСД), максимально независимых от операционных и файловых систем, применяемых в АС. Это выполнение процедур идентификации / аутентификации, контроля целостности аппаратных и программных средств АС до загрузки операционной системы, администрирования и т. д.

Вышеперечисленные принципы аппаратной защиты были реализованы в программно-аппаратном комплексе средств защиты информации от несанкционированного доступа — аппаратном модуле доверенной загрузки — **«Аккорд-АМДЗ»**. Этот комплекс обеспечивает режим доверенной загрузки в различных операционных средах: MS DOS, Windows 3.x, Windows 9.x, Windows NT/2000/XP, OS/2, Unix, Linux .

Основным принципом работы «Аккорд-АМДЗ» является выполнение процедур, реализующих основные функции системы защиты информации до загрузки операционной системы. Процедуры идентификации / аутентификации пользователя, контроля целостности аппаратных и программных средств, администрирование, блокировка загрузки операционной системы с внешних носителей информации размещены во внутренней памяти микроконтроллера платы «Аккорд». Таким образом, пользователь не имеет возможности изменения процедур, которые влияют на функциональность системы защиты информации. В энергонезависимой памяти контроллера «Аккорд» хранится информация о персональных данных пользователей, данные для контроля целостности программных и аппаратных средств, журнал регистрации и учета системных событий и действий пользователя. Эти данные могут быть изменены только авторизованным администратором безопасности информации, так как доступ к энергонезависимой памяти полностью определяется логикой работы программного обеспечения, размещенного в микроконтроллере платы.

СЗИ НСД семейства «Аккорд» реализованы на базе контроллера «Аккорд-4.5» (для ПЭВМ с шинным интерфейсом ISA) и его функционального аналога для шинного интерфейса PCI — «Аккорд-5».

PCI-устройства ОКБ САПР являются легальными и имеют свой идентификатор, предоставленный ассоциацией разработчиков данных устройств: Vendor ID 1795.

Для организаций, использующих промышленные компьютеры с шинным интерфейсом PC/104, может представлять интерес программно-аппаратный комплекс СЗИ НСД «Аккорд-PC104». Данный комплекс прошел испытания в жестких условиях эксплуатации (повышенная вибрация, широкий диапазон температур, высокая влажность и т. д.). Он может применяться в специализированных компьютерах, используемых в бортовой аппаратуре (наземные, воздушные, морские и промышленные системы), в измерительной аппаратуре, в устройствах связи, в мобильных системах, в том числе и военного назначения.

Наиболее наукоёмкой разработкой ОКБ САПР является сопроцессор безопасности «Аккорд-СБ», в котором интегрированы все необходимые средства для реализации комплексной защиты информации от НСД. Контроллер сопроцессора безопасности «Аккорд-СБ/2» имеет высокопроизводительный микропроцессор и аппаратный ускоритель математических функций. Доступ к функциям этого процессора определяется встроенным программным обеспечением контроллера.

Используя библиотеку программирования (SDK) контроллера сопроцессора безопасности «Аккорд-СБ/2», разработчик может применять данный комплекс как многофункциональное устройство. В частности, кроме задач по защите информации от несанкционированного доступа, он может быть использован для передачи конфиденциальной информации по открытым каналам связи в зашифрованном виде с высокой скоростью обработки и передачи данных, шифрования дисков, формирования и проверки ЭЦП, защиты электронных документов с использованием

защитных кодов аутентификации (ЗКА), а также в качестве межсетевого экрана.

Требования к аппаратным СЗИ и принципы аппаратной защиты, реализованные в СЗИ НСД семейства «Аккорд», уже стали фактическим стандартом и применяются всеми крупными разработчиками средств защиты, действующими на российском рынке СЗИ.

Применение сильной аппаратной поддержки в комплексах СЗИ НСД семейства «Аккорд» позволило выйти на новый уровень в развитии средств защиты информации. Как известно, для построения автоматизированных систем по классам защищённости 1Д–1А требуется установка правил разграничения доступа к ее информационным ресурсам. Для реализации функций разграничения доступа пользователей к информационным ресурсам и создания изолированной программной среды (ИПС) программистами ОКБ САПР разработано специальное программное обеспечение, поддерживающее все типы контроллеров «Аккорд», включая работу с датчиком случайных чисел. Это такие комплексы СЗИ НСД, как «Аккорд-1.95» (MS DOS, Windows 9x), «Аккорд-1.95-00» (Windows 9x), «Аккорд-NT/2000» (Windows NT/2000/XP).

Особенностью комплексов «Аккорд-1.95-00» и «Аккорд-NT/2000» является то, что в данных версиях, кроме дискреционного, реализован мандатный принцип доступа субъектов к информационным ресурсам. Специальное программное обеспечение, реализующее функции разграничения доступа, позволяет администратору безопасности информации описать любую не противоречивую политику безопасности на основе наиболее полного набора атрибутов (более 15 атрибутов по доступу к файлам и каталогам) и меток конфиденциальности объектов (файлов) и процессов (программ), с помощью которых осуществляется их обработка.

Следующим этапом стала разработка основ защиты локальных вычислительных сетей с применением программно-аппаратных средств

защиты от НСД к информации. Для полноценной защиты локальной вычислительной сети ОКБ САПР предлагает комплексную технологию:

-установку на рабочих станциях СЗИ «Аккорд АМДЗ» с ПО «Аккорд-1.95», «Аккорд-1.95-00», «Аккорд-NT/2000»;

-установку подсистемы контроля целостности на каждом файл-сервере;

-установку подсистемы распределенного аудита и управления;

-установку подсистемы усиленной аутентификации.

Управление вышеперечисленными подсистемами в локальных вычислительных сетях обеспечивается с помощью автоматизированного рабочего места администратора безопасности (АРМ АБИ). Данная технология позволяет администратору безопасности информации однозначно опознавать авторизованных пользователей и зарегистрированные рабочие станции в сети; в режиме реального времени контролировать задачи, выполняемые пользователями; в случае несанкционированных действий блокировать рабочие станции, с которых такие действия осуществлялись; удаленно вести администрирование. Особый интерес представляет подсистема усиленной аутентификации, суть которой заключается в дополнительном механизме проверки подлинности рабочих станций. Процедура проверки подлинности выполняется не только в момент подключения станции, но и с установленной администратором периодичностью. Подсистема предотвращает как подмену локальной станции или сервера, так и подключение в ЛВС нелегальных станций / серверов. Усиленная аутентификация в ЛВС основана на применении математических методов, позволяющих однозначно опознать участников диалога.

Как известно, невозможно решить все вопросы обработки информации в АС только средствами защиты от НСД к защищаемой информации. Поэтому необходимо также обеспечить юридическую доказательность подлинности электронных документов. Специалистами ОКБ САПР предложен и реализован новый путь — разработка контролируемой

технологии обработки электронных документов в вычислительных системах — технология защиты электронных документов с использованием защитных кодов аутентификации (ЗКА). Данная технология уже используется в банковских платежных системах с целью предотвращения попыток злоумышленников ввести фиктивные или модифицировать обрабатываемые электронные банковские документы, а также с целью организации сквозного контроля при прохождении электронных документов всех предписанных этапов их существования (создание, обработка, передача, хранение, окончательный зачет). Это обеспечивается установкой на документ ЗКА. В результате электронный документ на каждом этапе обработки имеет два ЗКА, первый из которых позволяет авторизовать и проконтролировать его целостность на предыдущем этапе обработки, а второй является его индивидуальным признаком на текущем.

Технологическая защита электронного документооборота реализуется всеми типами контроллеров семейства «Аккорд». Кроме того, для реализации данной технологии при использовании других СЗИ НСД в ОКБ САПР разработаны эффективные устройства: блок установки кодов аутентификации (БУКА), изделие **«ШИПКА»** (Шифрование, Аутентификация, Подпись, Коды Аутентификации).

“ШИПКА” содержит микропроцессор с встроенным программным обеспечением, аппаратный датчик случайных чисел, подключается через имеющийся интерфейс — шину USB — и может выполнять операции:

-шифрование по ГОСТ 28147-89;

-хеширование по ГОСТ Р 34.11-94;

-формирование и проверка электронной цифровой подписи по ГОСТ Р 34.10-94;

-выработка и проверка защитных кодов аутентификации.

В последней модификации изделия имеется защищенный электронный диск объемом 16 Мбайт, 32, 64 или 128 Мбайт http://www.pcmore.ru/security/naa/okbsapr-hwnaa.html?print - 9 для записи пользовательской информации.

Любая система защиты информации — это комплекс организационно-технических мероприятий, который включает в себя совокупность правовых норм, организационных мер и программно-технических средств защиты, направленных на противодействие угрозам объекту информатизации с целью сведения до минимума возможного ущерба пользователям и владельцам системы. Без организационных мер, наличия четкой организационно-распорядительной системы на объекте информатизации эффективность любых технических СЗИ снижается.

Поэтому ОКБ САПР большое внимание уделяет вопросам разработки нормативно-технической и методической документации, комплектов организационно-распорядительных документов по политике защиты объектов информатизации в соответствии с действующим законодательством РФ. Совместно с Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации» (ВНИИПВТИ) активно участвует в научных работах в области защиты информации, прежде всего в разработке:

-концептуальных и теоретических основ защиты электронных документов;

-теории применения программно-технических средств защиты от НСД к информации;

-управления защитой информации в локальных и корпоративных вычислительных сетях различного назначения.

В настоящее время ОКБ САПР является признанным разработчиком и производителем программно-аппаратных средств защиты информации от несанкционированного доступа, передовых методов управления защитой информации и технологий защищенного электронного документооборота на их основе.

ОКБ САПР является лицензиатом ФСБ, Гостехкомиссии России и ФАПСИ, имеет аттестованное Гостехкомиссией России производство

средств защиты информации от несанкционированного доступа и широкую дилерскую сеть в большинстве субъектов Российской Федерации, ведет активную работу по подготовке специалистов в области защиты информации.

Оптимизация аппаратных средств криптографической защиты нформации (АСКЗИ).

В последнее время возрос интерес к современным аппаратным средствам криптографической защиты информации (АСКЗИ). Это обусловлено, прежде всего, простотой оперативностью их внедрения. Для этого достаточно у абонентов на передающей и приемной сторонах иметь аппаратуру АСКЗИ и комплект ключевых документов, чтобы гарантировать конфиденциальность циркулирующей в автоматизированных системах управления (АСУ) информации.

Современные АСКЗИ строятся на модульном принципе, что дает возможность комплектовать структуру АСКЗИ по выбору заказчика.

Задачи аппаратного обеспечения защиты информации.

Под аппаратным обеспечением средств защиты операционной системы традиционно понимается совокупность средств и методов, используемых для решения следующих задач:

-управление оперативной и виртуальной памятью компьютера;

-распределение процессорного времени между задачами в многозадачной операционной системе;

-синхронизация выполнения параллельных задач в многозадачной операционной системе;

-обеспечение совместного доступа задач к ресурсам операционной системы.

Перечисленные задачи в значительной степени решаются с помощью аппаратно реализованных функций процессоров и других узлов компьютера. Однако, как правило, для решения этих задач принимаются и программные средства, и по этому термины “аппаратное обеспечение защиты ” и

“аппаратная защита” не вполне корректны. Тем не менее, поскольку эти термины фактически общеприняты, мы будем их использовать.

Дополнительные аппаратные средства обеспечивающий повышенный уровень защиты.

Отсутствие штатных средств защиты в первых операционных системах для защиты персональных компьютеров (ПК) породило проблему создания дополнительных средств. Актуальность этой проблемы не уменьшилась с появлением более мощных ОС с развитыми подсистемами защиты. Дело в том, что большинство систем до сих пор не способны защитить данные, “вышедшие за ее пределы”, например в случае использования сетевого информационного обмена или при попытке доступа к дисковым накопителям путем загрузки альтернативной незащищенной ОС.

Основные выводы о способах использования средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.

2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.

3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.