**Задание на 04.02.2022**

МДК 03.02 Программно-аппаратные средства защиты информации

1. **Сделать конспект лекции**
2. **Сделать практическую работу №13 Работа с антивирусной программой «NOD 32»**
3. **Сделать практическую работу №14 Управление доступом в операционных системах**
4. **Отчет отправить на почту svebalch@mail.ru**

**Лекция 13**

**Основные подходы к защите данных от НСД. Защита ПЭВМ от несанкционированного доступа**

Как показывает практика, несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленного за­владения защищаемой информацией в современных АСОД. Как ни по­кажется странным, но для ПЭВМ опасность данной угрозы по сравнению с большими ЭВМ повышается, чему способствуют следующие объектив­но существующие обстоятельства:

1) подавляющая часть ПЭВМ располагается непосредственно в ра­бочих комнатах специалистов, что создаст благоприятные условия для доступа к ним посторонних лиц;

2) многие ПЭВМ служат коллективным средством обработки ин­формации, что обезличивает ответственность, в том числе и за защиту информации;

3) современные ПЭВМ оснащены несъемными накопителями на ЖМД очень большой емкости, причем информация на них сохраняется даже в обесточенном состоянии;

4) накопители па ГМД производятся в таком массовом количестве, что уже используются для распространения информации так же, как и бумажные носи гели;

5) первоначально ПЭВМ создавались именно как персональное средство автоматизации обработки информации, а потому и по оснаща­лись специально средствами защиты от НСД.

В силу сказанного те пользователи, которые желают сохранить конфиденциальность своей информации, должны особенно позаботиться об оснащении используемой ПЭВМ высокоэффективными средствами защиты от НСД.

Основные механиз­мы защиты ПЭВМ от НСД могут быть представлены следующим переч­нем:

**1) физическая защита ПЭВМ и носителей информации;**

**2) опознавание (аутентификация) пользователей и используемых компонентов обработки информации;**

**3) разграничение доступа к элементам защищаемой информации;**

**4) криптографическое закрытие защищаемой информации, храни­мой на носителях (архивация данных);**

**5) криптографическое закрытие защищаемой информации в процес­се непосредственной ее обработки;**

**6) регистрация всех обращений к защищаемой информации.**

**1**. **Физическая защита ПЭВМ и носителей информации***.* Содержание физической защиты общеизвестно потому детально обсуждать ее здесь нет необходимости. Заметим только, что ПЭВМ лучше размещать в на­дежно запираемом помещении, причем в рабочее время помещение долж­но быть закрыто или ПЭВМ должна быть под наблюдением законного пользователя. При обработке же закрытой информации в помещении мо­гут находиться только лица, допущенные к обрабатываемой информа­ции. В целях повышения надежности физической защиты в нерабочее время 1 ГЭВМ следует хранить в опечатанном сейфе.

**2.****Опознавание (аутентификация) пользователей и используемых компонентов обработки информации***.* В концептуальном плане решение данной задачи принципиально не отличается от аналогичной задачи, ре­шаемой в любой ЛС'ОД: система защиты должна надежно определять за­конность каждого обращения к ресурсам, а законный пользователь дол­жен иметь возможность убедиться, что ему предоставляются именно те компоненты (аппаратура, программы, массивы данных), которые ему не­обходимы.

Для опознавания пользователей к настоящему времени разработа­ны и нашли практическое применение следующие способы:

1) с использованием простого пароля;

2) в диалоговом режиме с использованием нескольких паролей и/или персональной информации пользователей;

3) по индивидуальным особенностям и физиологическим характе­ристикам человека (отпечатки пальцев, геометрия руки, голос, персо­нальная роспись, структура сетчатки глаза, фотография и некоторые дру­гие);

4) с использованием радиокодовых устройств;

5) с использованием электронных карточек.

Рассмотрим коротко перечисленные способы.

*Распознавание по простому паролю* заключается в том, что каждому зарегистрированному пользователю выдается персональный пароль, который oн должен держать в тайне и вводить в ЗУ ЭВМ при каждом об­ращении к ней . Специальная программа сравнивает введенный пароль с эталоном, хранящимся в ЗУ ЭВМ, и при совпадении паролей запрос пользователя принимаем си к исполнению. Простота способа очевидна, но очевидны неявные недостатки: пароль можем быть утерян или подобран перебором возможных комбинаций, а искусный злоумышленник можем проникнуть в ту область ЗУ, в которой хранятся эталонные пароли. По­пытки преодолеть указанные недостатки, естественно, ведут к усложне­нию способа.

*Опознавание в диалоговом режиме* может быть осуществлено но сле­дующей схеме. В файлах механизмов защиты заблаговременно создаются записи, содержащие персонифицирующие пользователи данные (цата рождения, рост, вес, имена и даты рождения родных и близких и т.п.) или достаточно большой и упорядоченный набор паролей. При обращении пользователи программа механизма защиты предлагает пользователю назвать некоторые данные из имеющейся записи, которые сравниваются с .хранящимися в файле. По результатам сравнения принимается решение о допуске. Для повышения надежности опознавания запрашиваемые у пользователя данные могут выбираться каждый раз разные. Достоинства и недостатки данного способа очевидны.

*Опознавание по индивидуальным особенностям и физиологическим ха­рактеристикам* может быть весьма надежным, но для его реализации не­обходима специальная аппаратура для съема и ввода соответствующих параметров и достаточно сложные программы их обработки и сравнении с эталоном. Все это в настоящее время вполне разрешимо, однако сопря­жено с удорожанием и усложнением аппаратуры и программ ПЭВМ. В силу сказанного данный способ применительно к ПЭВМ пока не получил сколько-нибудь значительного распространения, Заманчивым но срав­нительной простите и доступности может оказаться опознавание пользо­вателя по параметрам его работы с клавиатурой ПЭВМ (скорость набора текста, интервалы между нажатием клавиш и др.), которые тоже носят сугубо индивидуальный характер.

*Опознавание по радиокодовым устройствам,* как но следует из са­мого названия, заключаемся в том, что изготавливают специальные устройства, каждое из которых может генерировать радиосигналы, имеющие индивидуальные характеристики. ПЭВМ оснащается про­граммно-аппаратными средствами приема (например, при приближении к экрану дисплея), регистрации и обработки сигналов. Каждому зарегистрированному пользователю выдается такое устройство, а его параметры заносятся в ЗУ механизмов защиты. Надеж­ность опознавания по данному способу может быть высокой, однако та­кие устройства персонифицируют владельца, а не персону, полому по­хищение устройства дает злоумышленнику реальные шансы несанкцио­нированного доступа.

*Опознавание по специальным идентификационным карточкам* заключается в том, что изготавливаются специальные карточки, на которые наносятся данные, персонифицирующие пользователя: персональный идентификационный номер, специальный шифр или код и т.п. Эти дан­ные на карточку заносятся в зашифрованном виде, причем ключ шифро­вания может быть дополнительным идентифицирующим параметром, поскольку он может быть известен только пользователю, вводится им каждый раз при обращении к системе и уничтожается сразу же после ис­пользования. Опознавание по карточкам может быть очень надежным, однако для его реализации необходимы предприятия - изготовители кар­точек, а ПЭВМ должна быть оснащена устройством считывания данных с карточки. Поскольку все это сопряжено со значительными дополнитель­ными расходами, то данный способ опознавания оказывается эффек­тивным при его использовании в больших территориально распределен­ных сетях, где он в последнее время находит все большее применение, причем особенно в автоматизированных банковских системах. Более де­тально он будет рассмотрен в § 8.7.

Для опознавания компонентов обработки данных, т.е. ЭВМ, ОС, программ функциональной обработки, массивов данных (такое опозна­вание особенно актуально при работе в сети ЭВМ) используются сле­дующие средства:

1) специальные аппаратные блоки-приставки 0с"я опознавания ЭВМ, терминалов, внешних устройств);

2) специальные программы, реализующие процедуру "запрос-ответ";

3) контрольные суммы (для опознавания щкмрамм и массивов дан­ных).

*Опознавание с помощью блоков-приставок* заключается в том, что технические средства оснащаются специальными устройствами, генери­рующими индивидуальные сигналы. В целях предупреждения перехвата этих сигналов и последующего их злоумышленного использования они могут передаваться в зашифрованном виде, причем периодически может меняться не только ключ шифрования, но и используемый способ (алгоритм) криптографического преобразования.

*Программное опознавание по процедуре "запрос-ответ"* заключается в ТОМ, что в ЗУ опознающего и опознаваемого объектов заблаговременно вносится достаточно развитые массивы идентифицируемых данных. Тог­да опознающий объект в диалоговом режиме запрашивает те или иные данные из массива опознаваемого объекта и сравнивает их с соответ­ствующими данными своего массива. Опять-таки в целях предупреждения перехвата и злоумышленного использования передаваемых идентифици­рующих данных может осуществляться их кришографическос закрытие. *Опознавание по контрольной сумме* заключается в том, что для про-|рамм и массивов данных заблаговременно вычисляются их контрольные суммы (или другие величины, зависящие от содержания опознаваемых объектов). Дальнейшая процедура опознавания очевидна.

**3. Разграничение доступа к злеменпшм защищаемой информации***.* Сущность указанного разграничения заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспре­пятственного доступа к информации в пределах его полномочий, и ис­ключить возможности превышения своих полномочий. И лих целях раз­работаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, к программам обработки информации, к нолям (областям ЗУ) и к массивам (базам) данных. Само разграничение можег осуществляться несколькими способами, а именно:

1) но уровням (кольцам) секретности;

2) по специальным спискам;

3) гго так называемым матрицам полномочий;

4) по специальным мандатам. .

Приведем краткую характеристику перечисленных способов.

*Разграничение доступа по уровням (кольцам) секретности* заключа­ется в том, что защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались дан­ные одного уровня секретности (например, только с грифом "конфи­денциально", или только "секретно", или только "совершенно секретно", или каким-либо другим). Каждому зарегистрированному пользователю предоставляется вполне определенный уровень допуска (например, "сек­ретно", "совершенно секретно" и т.н.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня массивам (базам) низших уров­ней, и запрещается доступ к массивам (базам) более высоких уровней.

*Разграничение доступа по специальным спискам* заключается в том, что дня каждого элемента защищаемых данных (файла, базы) составляется список всех тех пользователей, которым предоставлено

право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

*Разграничение доступа по матрицам полномочий* предполагает фор­мирование двумерной матрицы, по строкам которой содержатся иденти­фикаторы зарегистрированных пользователей, а по столбцам - иденти­фикаторы защищаемых элементов данных. Элементы матрицы содержат информацию об уровне полномочий соответствующего пользователя от­носительно соответствующего элемента. Например, при размерах элемен­тов матрицы в два бита их содержание может быть следующим: 00 - до­ступ запрещен, 01 - разрешено только чтение, 10 - разрешена только за­пись, 11 - разрешены и чтение и запись.

*Разграничение доступа по мандатам* есть способ разового разреше­ния на допуск к защищаемому элементу данных. Заключается он в том, что каждому защищаемому элементу присваивается персональная уни­кальная метка, после чего доступ к этому элементу будет разрешен только тому пользователю, который в своем запросе предъявит метку элемента (мандат), которую ему может выдать администратор защиты или владе­лец элемента.

**4. Криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных).**Данный механизм, как следует из са­мого названия, предназначается для обеспечения защиты информации, которая подлежит продолжительному хранению на машинных носителях. Но при разработке методов его реализации имелась в виду и еще одна весьма важная цель - уменьшение объемов ЗУ, занимаемых хранимой ин­формацией. Указанные цели и выступают в качестве основных критериев при поиске оптимальных вариантов решения задачи архивации данных.

Для предупреждения несанкционированного доступа к хранимой информации могут и должны использоваться все три рассмотренных вы­ше механизма. Но особенно эффективными оказались методы крипто­графического преобразования информации, поэтому они составляют основу практически всех известных механизмов архивации. Уменьшение объемов ЗУ достигается применением так называемых методов сжатия данных, сущность которых заключается в использовании таких систем кодирования архивируемых данных, которые при сохранении содержа­ния информации требуют меньшего объема носителя. Но тогда есте­ственной представляется идея выбора такого способа кодирования, кото­рый удовлетворял бы обоим требованиям: обеспечивал бы уменьшение объема ЗУ и обладал бы требуемой надежностью криптографической защиты.

Классическим примером такого способа кодирования может слу­жить достаточно известный код Хоффмана, суть которого заключается в том, что для кодирования часто встречающихся символов (букв) исполь­зуются более короткие кодовые комбинации, чем для кодирования редко встречающихся. Нетрудно видеть, что если таблицу кодирования держать а секрете, то кодированный таким образом текст будет не только коро­че исходного, но и недоступен для чтения посторонними лицами.

**5. Криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки***.* Назначение указанного закрытия оче­видно, а целесообразность применения определяется возможностями не­санкционированного доступа к защищаемой информации в процессе не­посредственной обработки. Если же обработка информации осуществля­ется в сетевой среде, то без применения криптографических средств на­дежное предотвращение несанкционированного доступа к ней практиче­ски не может быть обеспечено. Этим и обусловлено то достаточно боль­шое внимание, которое уделяется разработке криптографических средств, ориентированных на применение в ПЭВМ

Рассмотрим краткое описание одной из серий криптографических устройств, получившей название "КРИПТОН".

КРИПТОН - это ряд выполненных в виде одноплатных устройств программно-аппаратных комплексов, обеспечивающих шифрование и дешифрование информации в ЭВМ и в информационно-вычислительных сетях. Устройства содержат датчики случайных чисел для генерации клю­чей и узлы шифрования, реализованные аппаратно в специализирован­ных однокристальных микроЭВМ. Открытый интерфейс позволяет внед­рять устройства КРИПТОН в любые системы и дополнять программным обеспечением специального назначения.

Устройства КРИПТОН позволяют осуществлять:

1) шифрование и дешифрование файлов, групп файлов и разделов дисков;

2) разграничение и контроль доступа к компьютеру;

3) защиту информации, передаваемой но открытым каналам связи и сетям межмашинного обмена;

4) электронную подпись документов;

5) прозрачное шифрование жестких и гибких дисков.

Для криптографического преобразования защищаемых данных ис­пользован алгоритм отечественного стандарта ГОСТ 28147-89. Длина ключа - 256 бит, причем предусмотрено 7 типов ключевых систем, любую из которых пользователь может выбрать по своему усмотрению. Кон­кретные ключи в пределах выбранного типа ключевой системы пользова­тель может изготовить самостоятельно или заказать в специализирован­ном центре.

КРИПTOH работает в среде MS DOS версии 3.0 и выше.

На базе устройств КРИПТОН разработана и серийно выпускается система КРИПТОН-ИК, обеспечивающая дополнительно к перечислен­ным выше функциям также чтение, запись и защиту данных, хранящихся на так называемых интеллектуальных идентификационных карточках, получающих в последнее время широкое применение как в виде дебетно-кредитных карточек при безналичных расчетах, так и в виде средства хранения прав доступа, ключей шифрования и другой конфиденциальной информации.

**6. Регистрация всех обращений к защищаемой информации***.* Реги­страция обращений к защищаемой информации позволяет решать ряд важных задач, способствующих существенному повышению эффектив­ности защиты, поэтому оно непременно присутствует во всех системах защиты информации.

Основные задачи, при решении которых заметную роль играет ре­гистрация обращений, могут быть представлены следующим перечнем:

1) контроль использования защищаемой информации;

2) выявление попыток несанкционированного доступа к защищае­мой информации;

3) накопление статистических данных о функционировании систем защиты.

Вообще говоря, регистрация обращений может быть осуществлена серийными средствами операционных систем ПЭВМ. Однако учитывая специфичность и избирательность необходимой регистрации в системах защиты, разработчики этих систем предпочитают создавать свои версии программ регистрации.

Таким образом, даже такое беглое рассмотрение вопросов пред­упреждения несанкционированного доступа достаточно убедительно по­казывает, что они, во-первых, составляют основу систем защиты инфорнации в ПЭВМ, а во-вторых, что их реализация сопряжена с решением широкою спектра разноплановых задач. Теоретические исследования и практический опыт показали, что наиболее эффективным способом их решения является создание комплексных систем защиты ПЭВМ от не­санкционированного доступа.

**Лекция 14**

**Программно-аппаратные средства шифрования. Защита алгоритма шифрования. Необходимые и достаточные функции аппаратного средства криптозащиты. Построение аппаратных компонент криптозащиты данных**

**1. Полностью контролируемые компьютерные системы.**

Любая компьютерная система (КС) использует стандартное и специализированное оборудование и программное обеспечение, выполняющее определенный набор функций: аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись и др.

Целостность и ограничение доступа к информации обеспечиваются специализированными компонентами системы, использующими криптографические методы защиты. Для того чтобы компьютерной системе можно было полностью доверять, ее необходимо аттестовать, а именно:

* 1. определить множество выполняемых функций;
  2. доказать конечность этого множества;
  3. определить свойства всех функций.

Отметим, что в процессе функционирования системы невозможно появление в ней новой функции, в том числе и в результате выполнения любой комбинации функций, заданных при разработке. Здесь мы не будем останавливаться на конкретном составе функций, поскольку они перечислены в соответствующих руководящих документах Федерального агентства правительственной связи и информации (ФАПСИ ) и Государственной технической комиссии (ГТК) России.

При использовании системы ее функциональность не должна нарушаться, иными словами, необходимо обеспечить целостность системы в момент ее запуска и в процессе функционирования.

Надежность защиты информации в компьютерной системе определяется:

* 1. конкретным перечнем и свойствами функций КС;
  2. используемыми в функциях КС методами;

1. способом реализации функций КС.

Перечень используемых функций соответствует классу защищенности, присвоенному КС в процессе сертификации, и в принципе одинаков для систем одного класса. Поэтому при рассмотрении конкретной КС следует обратить внимание на используемые методы и способ реализации наиболее важных функций: аутентификацию и проверку целостности системы. Здесь следует отдать предпочтение криптографическим методам: шифрования (ГОСТ 28147-89), электронной цифровой подписи (ГОСТР 34.10-94) и функции хэширования (ГОСТР 34.11-94), надежность которых подтверждена соответствующими государственными организациями.

**Программная реализация функций КС.**

Большинство функций современных КС реализованы в виде программ, поддержание целостности которых при запуске системы и особенно в процессе функционирования является трудной задачей.

Значительное число пользователей в той или иной степени обладают познаниями в программировании, осведомлены об ошибках в построении операционных систем. Поэтому существует достаточно высокая вероятность применения ими имеющихся знаний для "атак" на программное обеспечение.

Проверка целостности одних программ при помощи других не является надежной. Необходимо четко представлять, каким образом обеспечивается целостность собственно программы проверки целостности. Если обе программы находятся на одних и тех же носителях, доверять результатам такой проверки нельзя. В связи с этим к программным системам защиты от несанкционированного доступа (НСД) следует относиться с особой осторожностью.

**Аппаратная реализация функций КС.**

Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, для внесения изменений в ПО необходимо получить доступ к соответствующей плате и заменить микросхему.

В случае использования универсального процессора реализация подобных действий потребует применения специального оборудования, что еще более затруднит проведение атаки. Использование специализированного процессора с реализацией алгоритма работы в виде интегральной микросхемы полностью снимает проблему нарушения целостности этого алгоритма.

На практике для повышения класса защищенности КС функции аутентификации пользователя, проверки целостности (платы Таблица 7.1 Аппаратные устройства криптографической защиты данных серии КРИПТОН , КРИПТОН -НСД, АККОРД и др.), криптографические функции (платы КРИПТОН -4, КРИПТОН -4К/8, КРИПТОН -4К/16, КРИПТОН -4/PCI, КРИПТОН -7/PCI, КРИПТОН -8/PCI), образующие ядро системы безопасности, реализуются аппаратно (табл. 7.1), все остальные функции - программно.

Для построения надежной системы защиты КС ее разработчик должен владеть возможно более полными знаниями о конкретной операционной системе (ОС), под управлением которой будет работать система. В настоящее время отечественные разработчики располагают относительно полной информацией только об одной операционной системе-DOS. Таким образом, к целиком контролируемым можно отнести КС, работающие в операционной системе DOS, или КС собственной разработки.

Таблица 7.1

|  |  |
| --- | --- |
| Наименование | Описание |
| КРИПТОН -4 | Шифрование по ГОСТ28147-89 (специализированным  шифропроцессором "Блюминг-1"). Генерация случайных чисел. Хранение 3 ключей и 1 узла замены в шифраторе.  Загрузка ключей в устройство до загрузки ОС с дискеты  или со смарт-карты, минуя оперативную память ПК. Защита от НСД. Скорость шифрования до 350 Кбайт/с. Интерфейс шины ISA-8 |
| КРИПТОН -4К/8 | Функции устройства КРИПТОН -4. Более современная, чем в КРИПТОН -4, отечественная элементная база (шифропроцессор "Блюминг-1К'). Аппаратный журнал работы с устройством. Загрузка ключей с Touch-Memory.  Скорость шифрования до 610 Кбайт/с.  Интерфейс шины ISA-8 |  |
| КРИПТОН -4К/16 | Функции устройства КРИПТОН -4К/8. Функции электронного замка персонального компьютера  разграничение доступа, проверка целостности ОС.  Скорость шифрования до 950 Кбайт/с.  Интерфейс шины ISA-16 |  |
| КРИПТОН -4/PCI | Функции устройства КРИПТОН -4К/16.  Скорость шифрования до 1100 Кбайт/с.  Интерфейс шины PCI Target.  Возможность параллельной работы нескольких плат |  |
| КРИПТОН -7/PCI | Функции устройства КРИПТОН -4/PCI.  Хранение до 1000 ключей (таблиц сетевых ключей) в  защищенном ОЗУ. Управление доступом к ключам.  Скорость шифрования до 1300 Кбайт/с.  Интерфейс шины PCI Master/Target.  Возможность параллельной работы нескольких плат |  |
| КРИПТОН -8/PCI | Функции устройства КРИПТОН -7/PCI. Хранение 32  ключей и 2 узлов замены в шифраторе, до 4000 ключей в  защищенном ОЗУ. Аппаратная реализация быстрой смены ключей. Скорость шифрования до 8800 Кбайт/с. Интерфейс шины PCI Master/Target. Возможность параллельной работы нескольких плат |  |
| КРИПТОН -НСД | Шифрование по ГОСТ28147-89 (программой из ПЗУ ).  Генерация случайных чисел. Защита от НСД.  Загрузка ключей с дискет, смарт-карт и Touch-Memory |
| Специализирован-  ная сетевая плата | Размещение коммуникационных модулей внутри платы  для исключения их обхода (стадия разработки) |

**2. Частично контролируемые компьютерные системы.**

Именно к таким системам можно отнести современные КС, использующие ОС Windows 95/98, Windows NT, различные версии UNIX, поскольку аттестовать их программное обеспечение полностью не представляется возможным. Сегодня вряд ли кто-нибудь возьмется достоверно утверждать, что в нем отсутствуют ошибки, программные закладки недобросовестных разработчиков или соответствующих служб.

Безопасность в таких КС может быть обеспечена:

1. использованием специальных аттестованных (полностью контролируемых) аппаратно-программных средств, выполняющих ряд защищенных операций и играющих роль специализированных модулей безопасности;
2. изоляцией от злоумышленника ненадежной компьютерной среды,

отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.

В частично контролируемых КС использование каких-либо программно реализованных функций, отвечающих за шифрование, электронную цифровую подпись, доступ к информации, доступ к сети и т.д., становится показателем наивности администратора безопасности. Основную опасность представляет при этом возможность перехвата ключей пользователя, используемых при шифровании и предоставлении полномочий доступа к информации.

Одним из наиболее известных и надежных аппаратных модулей безопасности являются платы серии КРИПТОН , обеспечивающие как защиту ключей шифрования и электронной цифровой подписи (ЭЦП ), так и неизменность их алгоритмов. Все используемые в системе ключи могут шифроваться на мастер-ключе (загружаемом в плату минуя шину компьютера) и храниться на внешнем носителе в зашифрованном виде. Они расшифровываются только внутри платы, в которой применяются специальные методы фильтрации и зашумления для предотвращения возможности считывания ключей с помощью специальной аппаратуры. В качестве ключевых носителей используются дискеты, микропроцессорные электронные карточки (смарт-карты) и "таблетки" Touch-Memory.

В современных аппаратно-программных средствах защиты от НСД для частично контролируемых КС можно серьезно рассматривать только функции доступа к ПК , выполняемые до загрузки операционной системы, и аппаратные функции блокировки портов ПК . Таким образом, существуют широкие возможности для разработки модулей безопасности для защиты выбранных процессов в частично контролируемых системах.

Основная проблема защиты отечественных корпоративных и ведомственных сетей состоит в том, что их программное и аппаратное обеспечение в значительной степени является заимствованным, приспособленным к ведомственным нуждам и производится за рубежом. Сертификация и аттестация компонентов этих сетей очень трудоемкий процесс. За время аттестации одной системы в продажу поступает, как правило, не одна, а несколько новых версий системы или отдельных ее элементов.

Для построения защищенной сети необходимо прежде всего обеспечить защиту ее компонентов. К основным компонентам сети относятся:

1. абонентские места, персональные компьютеры или терминалы клиента;
2. центры коммутации пакетов, маршрутизаторы, шлюзы и сетевые экраны;
3. корпоративный сервер, локальные серверы и серверы приложений;
4. отдельные сегменты сетей.

Защита каждого из компонентов (как правило, компьютера) складывается из:

1. исключения несанкционированного доступа к компьютеру со сто

роны консоли;

1. разграничения доступа к ресурсам компьютера со стороны консоли;
2. исключения несанкционированного доступа к компьютеру со стороны сети;
3. разграничения доступа к ресурсам компьютера со стороны сети;
4. обеспечения секретности используемых для защиты криптографических ключей.

Кроме того, необходимо также защитить сеть целиком от проникновения извне и каналы обмена с другими сетями.

**Основные элементы и средства защиты**

**от несанкционированного доступа.**

**"Снег-2.0"**

Приведем краткое описание одной из наиболее рас­пространенных систем защиты информации, разработанной в ЦНИИ Атоминформ и получившей название **"Снег-2.0".** Система состоит из под­систем управления доступом, peгистрации и учета, и криптографической.

***Подсистема управления доступом***осуществляет следующие функ­ции:

1) идентификацию и проверку подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия ДЛИНОЙ до восьми буквенно-цифровых символов;

2) идентификацию внешних устройств ПЭВМ по физическим адре­сам (номерам);

3) идентификацию программ, томов, каталогов, файлов по именам;

4) контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;

5) управление потоками информации с помощью меток конфиден­циальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них инфор­мации.

***Подсистема регистрации и учета***осуществляет следующие функции.

а) Регистрацию входа субъектов доступа в систему, причем в параметрах регистрации указываются:

1) время и дата входа субъекта доступа в систему;

2) результат попытки входа: успешная или неуспешная - несанкционированная;

3) идентификатор (код или фамилия субъекта), предъявленный при попытке доступа.

б) Регистрацию выдачи печатных графических документов на "твердую" копию, причем выдача сопровождается автоматической мар­кировкой каждою листа (страницы) документа порядковым номером и учетными реквизитами С указанием на последнем листе документа об­щего количества листов (страниц), и автоматическим оформлением учетной карточки документа с указанием даты выдачи, учетных реквизитов, краткого содержания (наименования, вида, шифра, кода) и уровня кон­фиденциальности, фамилии лица, выдавшего документ, количества стра­ниц и копий документа.

В параметрах регистрации указываются:

1) время и дата выдачи (обращения к подсистеме вывода);

2) идентификатор субъекта доступа, запросившего выдачу;

3) краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;

4)объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем) или неуспеш­ный.

в) Регистрацию запуска всех программ и процессов (заданий, задач), причем в параметрах регистрации указываются:

1) дата и время запуска;

2) имя (идентификатор) программы (процесса, задания);

3) идентификатор субъекта доступа, запросившего программу (про­цесс, задание);

4)результат запуска: успешный или неуспешный-несанкционирован­ный.

г) Регистрацию попыток доступа программных средств (программ, процессов, заданий, задач) к защищаемым файлам, причем в параметрах регистрации указываются:

1) дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная или неуспешная-несанкционированная;

2) идентификатор субъекта доступа;

3) спецификация защищаемого файла;

4) имя программы (процесса, задания, задачи), осуществляющей до­ступ к файлу;

5) вид запрашиваемой операции (чтение, запись, удаление, выпол­нение, расширение и т.н.).

д) Регистрацию попыток доступа программных средств к следую­щим дополнительным защищаемым объектам доступа: внешним уст­ройствам ПЭВМ, программам, томам, каталогам, файлам, причем в па­раметрах регистрации указываются:

1) дата и время попытки доступа к защищаемому объекту с указа­нием ее результата: успешная или неуспешная-несанкционированная;

2) идентификатор субъекта доступа;

3) спецификация защищаемого объекта (логическое имя/номер);

4) имя программы (процесса, задания, задачи), осуществляющей до-ciyn к защищаемому объекту;

5) вид запрашиваемой операции (чтение, запись, монтирование, за­хват и т.п.).

е) Автоматический учет создаваемых защищаемых файлов, ини­циируемых защищаемых томов, каталогов, выделяемых дня обработки защищаемых файлов, внешних устройств ПЭВМ.

ж) Очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ПЭВМ.

з) Сигнализацию ПОПЫТОК нарушения защиты.

***Криптографическая система обеспечивает****:*

а) шифрование всей конфиденциальной информации, записы­ваемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, с выполнением автоматической очистки областей внешней памяти, содержащих ранее не зашифрованную инфор­мацию;

6) возможность использования разных криптографических ключей для шифрования информации, принадлежащей различным субъектам до­ступа (группе субъектов).

Владельцем ПЭВМ должна осуществляться периодическая замена всех криптографических ключей, используемых для шифрования инфор­мации (перешифрования).

Используемые средства криптографической зашиты должны быть сертифицированы специальными сертификационными центрами, имею­щими лицензию на проведение сертификации криптографических средств защиты.

В системе "Снег 2.0" предусмотрены средства обеспечения целост­ности программных средств защиты и неизменности программной среды, а именно:

а) целостность программных средств системы "Снег 2.0" проверяет­ся по контрольным суммам всех компонентов СЗИ НСД;

б) целостность программной среды должна обеспечиваться пользо­вателем (владельцем) ПЭВМ, качеством программных средств, предназ­наченных для применения в ПЭВМ при обработке защищенных файлой.

***Общие положения по применению системы "Снег 2.0"***

Система защиты информации от несанкционированного доступа "Снег 2.0" (ВП А.07106-01) предназначена для применения в ПЭВМ типа IBM PC/AT с операционной системой MS DOS версии 5.0 или выше с вы­полнением требований но защите от НСД.

Система "Снег 2.0" обеспечивает конфиденциальность и защиту от НСД к информации в ПЭВМ до уровня "Сов. секретно ".Документацией на систему "Снег 2.0" предусмотрены меры организационной поддержки класса защищенности информации от НСД. В частности, предприятие (фирма, владелец ПЭВМ) обязано обеспечить реализацию следующих ор­ганизационно-распорядительных защитных мер:

1) введение и организация работы службы безопасности информа­ции (службы БИ);

2) ведение журнала учета работы ПЭВМ;

3) организация учета носителей информации;

4) обеспечение физической сохранности оборудования;

5) исключение возможности загрузки ОС с дискет пользователя при помощи применения специальной платы КРИПТОН-3, опечатывание корпуса ПЭВМ и контроль сохранности печатей;

6) запрещение доступа пользователям к программам-отладчикам, имеющим непосредственный доступ к оперативной или дисковой памяти, а также к средствам построения и запуска задач пользователя;

7) обеспечение уникальности ключевых дискет (по группам пользо­вателей, пользователям, ценности информации, принадлежности инфор­мации и т.д.);

8) ведение журнала учета работы ПЭВМ (гак называемого "ручного журнала") при обработке секретной информации.

Рекомендуется хранение и использование главного ключа шифро­вания и узла замены на одной дискете, применяемой администратором, а рабочих ключей пользователей на других дискетах, устанавливаемых на дисковод при запросах программ шифрования.