ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Защита информации в персональных компьютерах

Федоров Дмитрий Николаевич
dnf@dnf.su

XI

РАЗДЕЛЫ ТЕМЫ

- Особенности защиты информации в персональных ЭВМ
- Угрозы информации в персональных ЭВМ
- Обеспечение целостности информации в ПК
- Защита ПК от несанкционированного доступа
- Защита информации от копирования
- Защита от несанкционированного доступа к компьютеру без завершения сеанса работы
- Защита ПК от вредоносных закладок

Раздел 1

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ПЕРСОНАЛЬНЫХ ЭВМ

СВОЙСТВА РС С ТОЧКИ ЗРЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

- малые габариты и вес, что делает их не просто транспортабельными, а легко переносимыми;
- наличие встроенного внутреннего ЗУ большого объема, сохраняющего записанные данные после выключения питания;
- наличие сменного ЗУ большого объема и малых габаритов;
- наличие устройств сопряжения с каналами связи;
- оснащенность программным обеспечением с широкими функциональными возможностями;
- массовость производства и распространения;
- относительно низкая стоимость.

РАЗЛИЧИЕ ПОДХОДОВ К ЗАЩИТЕ У АСОД И РС

- В АСОД с большими ЭВМ основные вопросы защиты решаются специализированными профессиональными подразделениями.
- Для персональных ЭВМ превалирующую роль играет внутренняя защита :
  - вопросы общей организации защиты могут быть решены физической изоляцией (например, размещением ПК в отдельной комнате, закрываемой на замок);
  - в большинстве случаев заботу о защите информации должны проявлять сами пользователи, которые как правило не являются профессионалами в области защиты информации.

ФАКТОРЫ, ВЛИЯЮЩИЕ НА ВЫБОР ПОДХОДА К ЗАЩИТЕ ИНФОРМАЦИИ НА PC

- цели защиты;
  - обеспечение физической целостности / логической целостности (в меньшей степени);
  - предупреждение несанкционированного получения;
  - предупреждение несанкционированной модификации;
  - предупреждение несанкционированного копирования.
- потенциально возможные (доступные) способы защиты;
- имеющиеся средства защиты.

1. ОБЕСПЕЧЕНИЕ ФИЗИЧЕСКОЙ ЦЕЛОСТНОСТИ

- Физическая целостность информации в ПК зависит от целостности самого ПК, целостности дисков и дискет, целостности информации на дисках, дискетах и полях оперативной памяти.
- В широком спектре угроз целостности, информации в ПК следует обратить особое внимание на угрозы, связанные с недостаточно высокой квалификацией большого числа владельцев ПК. В этом плане особо опасной представляется возможность уничтожения или искажения данных на жестком диске (винчестере), на котором могут накапливаться очень большие объемы данных, самим пользователем.

2. ПРЕДУПРЕЖДЕНИЕ НЕСАНКЦИОНИРОВАННОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ В ПК

- Данная цель защиты приобретает особую актуальность в тех случаях, когда хранимая или обрабатываемая информация содержит тайну того или иного характера (государственную, коммерческую и т. п.).
- Возможности несанкционированного получения информации в современных ПК очень широки и разнообразны, поэтому данный вид защиты требует серьезного внимания.

3. ПРЕДУПРЕЖДЕНИЕ НЕСАНКЦИОНИРОВАННОЙ МОДИФИКАЦИИ

- Весьма опасной разновидностью несанкционированной модификации информации в ПК является действие вредоносных программ (компьютерных вирусов), которые могут разрушать или уничтожать программы или массивы данных.
- Данная опасность приобретает актуальность в связи с тем, что среди владельцев ПК общепринятой становится практика обмена носителями. В получаемой дискете (диске, флешке) может содержаться весьма неприятный «сюрприз».

4. ПРЕДУПРЕЖДЕНИЕ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ ИНФОРМАЦИИ

- Актуальность данной разновидности защиты определяется следующими тремя обстоятельствами:
  - накопленные массивы информации все больше становятся товаром;
  - все более широкое распространение получает торговля компьютерными программами;
  - внешние накопители (оптические дисководы) создают весьма благоприятные условия для широкомасштабного копирования информации ПК.

Раздел 2

УГРОЗЫ ИНФОРМАЦИИ В ПЕРСОНАЛЬНЫХ ЭВМ

КЛАССИФИКАЦИЯ КАНАЛОВ УТЕЧКИ

- Принята система классификации по типу средств, которые используются в целях несанкционированного получения по ним информации: человек, аппаратура, программа.
- Группа каналов «человек»
  - хищение носителей информации (магнитных дисков и дискет, распечаток и т. д.);
  - чтение или фотографирование информации с экрана;
  - чтение или фотографирование информации с распечаток.
- Группа каналов «аппаратура»
  - подключение к устройствам ПК специальной аппаратуры, с помощью которой можно уничтожать или регистрировать защищаемую информацию;
  - регистрацию с помощью специальных средств электромагнитных излучений устройств ПК в процессе обработки" защищаемой информации

КЛАССИФИКАЦИЯ КАНАЛОВ УТЕЧКИ - 2

- Группа каналов «программа»
  - программный несанкционированный доступ к информации;
  - уничтожение (искажение) или регистрация защищаемой информации с помощью программных закладок или ловушек;
  - чтение остаточной информации из ОЗУ;
  - программное копирование информации с магнитных носителей.

ПОЛНЫЙ БАЗОВЫЙ ПЕРЕЧЕНЬ МЕСТ, В КОТОРЫХ МОГУТ НАХОДИТЬСЯ ЗАЩИЩАЕМЫЕ ДАННЫЕ

- Системные платы ПК
- Внешние накопители
- ВЗУ типа «Винчестер»
- Дисплей
- Печатающее устройство
- Каналы сопряжения

Носители информации могут быть персонального, группового и общего использования.

ЧТО НЕОБХОДИМО ЗНАТЬ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ

Для разработки мероприятий защиты информации необходимы следующие исходные характеристики элементов защиты:

- возможные объемы находящейся в них информации;
- возможная продолжительность пребывания информации;
- возможные угрозы информации;
- возможные средства защиты.

В соответствии с изложенным каждый пользователь ПК может применительно к своим условиям составить перечень потенциально возможных угроз его информации и на этой основе целенаправленно решать вопросы надежной ее защиты.

Раздел 3

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ПК

СЛУЧАЙНЫЕ УГРОЗЫ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

- Угрозы целостности информации в ПК, как и в любой другой автоматизированной системе, могут быть случайными и преднамеренными.
- Основными разновидностями случайных угроз являются:
  - отказы, сбои, ошибки, стихийные бедствия и побочные явления,
- Конкретными источниками их проявления являются:
  - технические средства, программы и пользователи.
- К наиболее реальным угрозам целостности информации случайного характера следует отнести ошибки пользователей. Основными из этих ошибок являются неправильные обращения к компонентам программного обеспечения.

ПРЕДНАМЕРЕННЫЕ УГРОЗЫ ЦЕЛОСТНОСТИ

- Гораздо большую опасность целостности информации в ПК представляют преднамеренные угрозы, создаваемые людьми в злоумышленных целях.
- Такая угроза может быть:
  - непосредственной, если злоумышленник получает доступ к ПК,
  - опосредованной, когда угроза создается с помощью промежуточного носителя, чаще всего с помощью дискеты.
- Из преднамеренных угроз наибольшее распространение получили так называемые разрушающие программные средства (РПС): электронные вирусы, черви, троянские кони и др. Они же представляют и наибольшую опасность целостности информации в ПК.

Раздел 4

ЗАЩИТА ПК ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ОБЩАЯ ИНФОРМАЦИЯ

- Несанкционированный доступ (НСД) представляет одну из наиболее серьезных угроз для злоумышленного завладения защищаемой информацией в современных АСОД.
- Для ПК опасность данной угрозы по сравнению с большими ЭВМ повышается, чему способствуют следующие объективно существующие обстоятельства:
  - подавляющая часть ПК располагается непосредственно в рабочих комнатах специалистов, что создает благоприятные условия для доступа к ним посторонних лиц;
  - многие ПК служат коллективным средством обработки информации, что обезличивает ответственность, в том числе и за **защиту информации**;
  - современные ПК оснащены несъемными накопителями очень большой емкости, причем информация на них сохраняется даже в обесточенном состоянии;
  - внешние накопители производятся в таком массовом количестве, что уже используются для распространения информации так же, как и бумажные носители;
  - первоначально ПК создавались именно как персональное средство автоматизации обработки информации, а потому и не оснащались специально средствами защиты от НСД.

ОСНОВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ОТ НСД

1. физическая защита ПК 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.

Рассмотрим общее содержание и способы использования данных механизмов.

1. ФИЗИЧЕСКАЯ ЗАЩИТА ПК И НОСИТЕЛЕЙ ИНФОРМАЦИИ

- ПК лучше размещать в надежно запираемом помещении, причем, в рабочее время помещение должно быть закрыто или ПК должен быть под наблюдением законного пользователя.
- При обработке закрытой информации в помещении могут находиться только лица, допущенные к обрабатываемой информации.
- В целях повышения надежности физической защиты в нерабочее время ПК следует хранить в опечатанном сейфе.

2. ОПОЗНАВАНИЕ (АУТЕНТИФИКАЦИЯ) ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИИ

Задача: 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 эти способы подробнее ->

2.1. РАСПОЗНАВАНИЕ ПО ПРОСТОМУ ПАРОЛЮ

- Каждому зарегистрированному пользователю выдается персональный пароль, который он 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 принимается к исполнению.
- Простота способа очевидна, но очевидны и явные недостатки: пароль может быть утерян или подобран перебором возможных комбинаций, а искусный злоумышленник может проникнуть в ту область ЗУ, в которой хранятся эталонные пароли.

2.2. ОПОЗНАВАНИЕ В ДИАЛОГОВОМ РЕЖИМЕ

- В файлах механизмов защиты заблаговременно создаются записи, содержащие персонифицирующие данные пользователя (дата рождения, рост, имена и даты рождения родных и близких и т. п.) или достаточно большой и упорядоченный набор паролей.
- При обращении пользователя программа механизма защиты предлагает пользователю назвать некоторые данные из имеющейся записи, которые сравниваются с данными, хранящимися в файле.
- По результатам сравнения принимается решение о допуске.
- Для повышения надежности опознавания каждый раз запрашиваемые у пользователя данные могут выбираться разные.

2.3. 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 сравнения с эталоном.
- Это сопряжено с удорожанием и усложнением аппаратуры и программ ПК.
- Поэтому способ применительно к ПК пока не получил значительного распространения.
- Заманчивым по сравнительной простоте и доступности может оказаться опознавание пользователя по параметрам его работы с клавиатурой ПК (скорость набора текста, интервалы между нажатием клавиш и др.), которые тоже носят сугубо индивидуальный характер.

2.4. ОПОЗНАВАНИЕ ПО РАДИОКОДОВЫМ УСТРОЙСТВАМ

- Изготавливаются специальные устройства, каждое из которых может генерировать радиосигналы, имеющие индивидуальные характеристики.
- ПК оснащается программно-аппаратными средствами приема (например, при приближении устройства к экрану дисплея), регистрации и обработки генерируемых 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, поэтому похищение устройства дает злоумышленнику реальные шансы несанкционированного доступа.

2.5. ОПОЗНАВАНИЕ ПО СПЕЦИАЛЬНЫМ ИДЕНТИФИКАЦИОННЫМ КАРТОЧКАМ

- 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 изготовители карточек (оборудование), а ПК должна быть оснащена устройством считывания данных с карточки.
- Используется в больших компаниях, банковских структурах.

2. ОПОЗНАВАНИЕ (ИСПОЛЬЗУЕМЫХ КОМПОНЕНТОВ ОБРАБОТКИ ИНФОРМАЦИИ) (ПРОДОЛЖЕНИЕ)

- Для опознавания компонентов обработки данных, т. е. (ЭВМ, ОС, программ функциональной обработки, массивов данных, используются следующие средства:

1. специальные аппаратные блоки-приставки (для опознавания ЭВМ, терминалов, внешних устройств);
2. специальные программы, реализующие процедуру «запрос-ответ»;
3. контрольные суммы (для опознавания программ и массивов данных).

Рассмотрим эти средства подробнее ->

2.1. ОПОЗНАВАНИЕ С ПОМОЩЬЮ БЛОКОВ-ПРИСТАВОК

- 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.

2.2. ПРОГРАММНОЕ ОПОЗНАВАНИЕ ПО ПРОЦЕДУРЕ «ЗАПРОС-ОТВЕТ»

- В ЗУ опознающего и опознаваемого объектов заблаговременно вносятся достаточно развитые массивы идентифицируемых данных.
- Опознающий объект в диалоговом режиме запрашивает те или иные данные из массива опознаваемого объекта и сравнивает их с соответствующими данными своего массива.
- В целях предупреждения перехвата и злоумышленного использования передаваемых идентифицирующих данных может осуществляться их криптографическое закрытие.

2.3. ОПОЗНАВАНИЕ ПО КОНТРОЛЬНОЙ СУММЕ

- Для программ и массивов данных заблаговременно вычисляются их контрольные суммы (или другие величины, зависящие от содержания опознаваемых объектов).
- Дальнейшая процедура стандартная.

СПРАВОЧНО: ТЕРМИНОЛОГИЯ

- **Контро́льная су́мма** — некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Также контрольные суммы могут использоваться для быстрого сравнения двух наборов данных на неэквивалентность: с большой вероятностью различные наборы данных будут иметь неравные контрольные суммы.
  - С точки зрения математики контрольная сумма является хеш-функцией, используемой для вычисления контрольного кода — небольшого количества бит внутри большого блока данных, например, сетевого пакета или блока компьютерного файла, применяемого для обнаружения ошибок при передаче или хранении информации. Значение контрольной суммы добавляется в конец блока данных непосредственно перед началом передачи или записи данных на какой-либо носитель информации. Впоследствии оно проверяется для подтверждения целостности данных.
- **Хеширование** - преобразование по определённому алгоритму входного массива данных *произвольной* длины в выходную битовую строку *фиксированной* длины.

3. РАЗГРАНИЧЕНИЕ ДОСТУПА К ЭЛЕМЕНТАМ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

- Каждому зарегистрированному пользователю предоставляется возможность беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий.
- В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, к программам обработки информации, к полям (областям ЗУ) и к массивам (базам) данных.
- Само разграничение может осуществляться несколькими способами, а именно:

1. по уровням (кольцам) секретности;
2. по специальным спискам;
3. по матрицам полномочий;
4. по специальным мандатам.

Рассмотрим эти способы подробнее ->

3.1. РАЗГРАНИЧЕНИЕ ДОСТУПА ПО УРОВНЯМ (КОЛЬЦАМ) СЕКРЕТНОСТИ

- 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. п.). Тогда пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней и запрещается доступ к массивам (базам) более высоких уровней.

3.2. РАЗГРАНИЧЕНИЕ ДОСТУПА ПО СПЕЦИАЛЬНЫМ СПИСКАМ

- Для каждого элемента защищаемых данных (файла, базы, программы) 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.

3.3. 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: 00 — доступ запрещен, 01 — разрешено только чтение, 10 — разрешена только заспись, 11 — разрешены и чтение и запись.
- Недостаток метода - с увеличением масштаба ВС данная матрица может оказаться слишком громоздкой. Преодолеть данный недостаток можно путем применения следующих рекомендаций по сжатию матрицы установления полномочий:
  - объединение пользователей, имеющих идентичные полномочия, в группы;
  - объединение ресурсов, полномочия на доступ к которым совпадают;
  - комбинирование метода разграничения доступа на основе матрицы полномочий с методом разграничения по уровням секретности.

	Каталог D:\WORK	Каталог D:\BOOK	Каталог D:\TEST
Пользователь YM07	10	01	10
Пользователь YK16	10	10	00
Пользователь ZN21	00	10	01
.....	.....	.....	.....
Пользователь HУ12	10	00	00

3.4. РАЗГРАНИЧЕНИЕ ДОСТУПА ПО МАНДАТАМ

- Это способ разового разрешения на допуск к защищаемому элементу данных.
- Заключается 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

- Данный механизм предназначается для обеспечения защиты информации, которая подлежит продолжительному хранению на машинных носителях.
- 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.

АРХИВАЦИЯ И СЖАТИЕ

- Методы криптографического преобразования информации являются основой 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 памяти носителя.

КОД ХАФФМЕНА

Классическим примером такого способа кодирования может служить достаточно известный код Хаффмена, суть которого заключается в том, что:

- Для кодирования часто встречающихся символов (букв) используются более короткие кодовые комбинации, чем для кодирования редко встречающихся.
- Видно, что если таблицу кодирования держать в секрете, то закодированный 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 метода очевидно, а целесообразность применения определяется возможностями (степенью вероятности угрозы)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 ПК.

6. РЕГИСТРАЦИЯ ВСЕХ ОБРАЩЕНИЙ К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

- Способ 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:
  - контроль использования защищаемой информации;
  - выявление попыток несанкционированного доступа к защищаемой информации;
  - накопление статистических данных о функционировании систем защиты.
- Вообще говоря, регистрация обращений может быть осуществлена серийными средствами операционных систем ПК.
- Однако, учитывая специфичность и избирательность необходимой регистрации в системах защиты, многие разработчики этих систем предпочитают создавать свои версии программ регистрации.

ВЫВОД ПО РАЗДЕЛУ

- Проведенное рассмотрение вопросов предупреждения несанкционированного доступа достаточно убедительно показывает, что они,
- Во-первых, составляют основу систем защиты информации в ПК.
- Во-вторых, что их реализация сопряжена с решением широкого спектра разноплановых задач.
- Теоретические исследования и практический опыт показали, что наиболее эффективным способом их решения является создание комплексных систем защиты ПК от несанкционированного доступа (система может состоять из подсистем управления доступом, регистрации и учета, и криптографической).

Раздел 5

ЗАЩИТА ИНФОРМАЦИИ ОТ КОПИРОВАНИЯ

АКТУАЛЬНОСТЬ ТИПА ЗАЩИТЫ

- Защита от копирования заключается в предупреждении возможностей несанкционированного снятия копии с информации, находящейся в ОЗУ ЭВМ или на МД (гибком или жестком), в целях злоумышленного ее использования.
- Нетрудно видеть, что данная защита может быть представлена составной частью защиты от несанкционированного получения информации.
- Выделение же ее в самостоятельный вид защиты обусловлено, главным образом, стремлением защитить авторские и коммерческие интересы разработчиков и собственников программ для ПК.
- Как известно, программы для ЭВМ законодательно признаны интеллектуальной собственностью, и уже вполне сформировался рынок их распространения на коммерческой основе. В условиях рыночных отношений это с неизбежностью привело к так называемому программному пиратству, т. е. к злоумышленному присвоению чужих программ, причем, как в целях присвоения авторства, так и в целях наживы.

ЧТО И КАК ЗАЩИЩАЕМ

- Защищаемые программы для ПК могут находиться в ОЗУ, на носителях (внутренних HDD и внешних) .
- Защита программ, находящихся в ОЗУ и на HDD, ничем не отличается от рассмотренной выше защиты от НСД.
- Поэтому здесь основное внимание сосредоточено на защите от копирования данных внешних носителей, поскольку эта разновидность пиратства получила достаточно широкое распространение, а защита от него носит сугубо специфический характер.
- Под системой защиты программы от копирования понимается система, которая обеспечивает выполнение ею своих функций только при опознании некоторого уникального не поддающегося копированию элемента, называемого ключевым.
- В качестве ключевого элемента могут выступать дискета (диск, флешка), определенная часть аппаратуры ПК или специальное устройство, подключаемое к ПК.

ОСНОВНЫЕ ФУНКЦИИ СИСТЕМЫ ЗАЩИТЫ ОТ КОПИРОВАНИЯ

1. идентификация (т. е. присвоение индивидуального трудноподделываемого отличительного признака) той среды (дискеты или ПК), из которой будет запускаться защищаемая программа;
2. аутентификация (опознавание) той среды, из которой поступает запрос на копирование защищаемой программы;
3. регистрация санкционированного копирования;
4. реагирование на попытки несанкционированного копирования;
5. противодействие изучению алгоритмов работы системы защиты.

1. ИДЕНТИФИКАЦИЯ НОСИТЕЛЯ

Наибольшее распространение получили два способа:

- нанесение повреждения на часть поверхности
  - создание так называемой лазерной дыры, заключающееся в прожигании дискеты в некотором месте лазерным лучом. Доказано, что создание в дискете-копии такой же метки и в том же самом месте, что и на дискете-оригинале, весьма сложно.
- нестандартное (некопируемого) форматирование носителя
  - Способ достаточно надежный, однако задача нахождения некопируемого формата носит эмпирический характер, и ее решение возможно лишь при детальном знании всех тонкостей процессов функционирования контроллера.
  - К настоящему времени разработан ряд методов реализации данного способа идентификации: нарушение последовательности секторов на дорожке дискеты, изменение межсекторной дистанции, форматирование с кодом длины 0 или 1, контроль длины дорожки, прерывание операции и выключение мотора и др.

4. РЕАГИРОВАНИЕ НА ПОПЫТКИ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Варианты реагирования:

- отказ в исполнении запроса,
- предупреждение злоумышленника о более серьезных санкциях,
- уничтожение защищаемой программы (после первой попытки или после нескольких попыток и т. п.).

5.1. ПРОТИВОДЕЙСТВИЕ ИЗУЧЕНИЮ АЛГОРИТМОВ РАБОТЫ СИСТЕМЫ ЗАЩИТЫ

- Функция предусмотрена для того, чтобы воспрепятствовать злоумышленнику в изучении структуры и содержания реализованной на дискете (носителей) системы защиты в целях ее преодоления (нейтрализации).
- Важность данной функции определяется тем, что квалифицированный системный программист, в общем случае, может определить (восстановить) логику работы любого модуля всей системы защиты и найти способы ее преодоления.

5.2. ИЗУЧЕНИЕ ЛОГИКИ РАБОТЫ

- Изучение логики работы программы может осуществляться двумя способами:
  - дисассемблированием (преобразованием выполняемого программного модуля в листинг исходного текста)
  - трассировкой программы (выполнением ее в такой среде, которая позволяет осуществлять доступ к регистрам и областям памяти, останов исполнения программы по некоторым адресам и т. п.).
- Отсюда следует, что основное содержание рассматриваемой функции должно заключаться в создании надежных препятствий на пути дизассемблирования и трассировки программных модулей системы защиты.

ПРОГРАММНЫЕ СИСТЕМЫ ЗАЩИТЫ НОСИТЕЛЕЙ ОТ КОПИРОВАНИЯ

- К настоящему времени разработано значительное число программных систем защиты носителей от копирования.
- Для защиты от несанкционированного входа в персональную компьютерную систему могут использоваться как общесистемные, так и специализированные программные средства защиты.
- К общесистемным средствам относится утилита Setup, входящая в состав BIOS и предназначенная для настроек аппаратных параметров компьютера.

УТИЛИТА SETUP BIOS

Для реализации рассматриваемого вида защиты необходимо с помощью данной утилиты установить следующие параметры загрузки компьютера:

- порядок загрузки операционной системы (ОС), задающий первичную загрузку с жесткого диска (устройство C:)/
- запрос пароля перед загрузкой операционной системы.

Установка первичной загрузки с жесткого диска необходима для предотвращения возможности загрузки ОС с дискеты или компакт-диска, так как некоторые устаревшие версии BIOS позволяют осуществить загрузку с дискеты без запроса пароля. Если используемая версия BIOS при установленном пароле загрузки обеспечивает запрос пароля и при загрузке с дискеты, что, как правило, реализовано во всех современных версиях базовой системы ввода-вывода, то изменять порядок загрузки для защиты от несанкционированного входа в компьютерную систему нет необходимости.

МЕТОДИКА НАСТРОЙКИ УТИЛИТЫ

- Запуск утилиты Setup выполняется, как правило, нажатиями клавиши Del после активизации процесса загрузки операционной системы.
- После запуска утилиты необходимо войти в пункт меню «BIOS Features Setup» («Advanced CMOS Setup») и с помощью клавиш PgUp и PgDn установить следующие переключатели:
  - «Boot Sequence» («System Boot Up Sequence») — в положение «C, A» или «C, CDROM, A»;
  - «Security Option» («Password Checking Options») — а положение «System».
- Далее следует задать пароль входа в систему с помощью пункта меню «Password Setting» («Change Password»), а потом сохранить сделанные изменения и выйти из утилиты с помощью пункта меню «Save & Exit Setup».
- После указанных действий загрузка компьютера будет выполняться только после ввода правильного пароля.
- При необходимости изменения пароля следует активизировать утилиту Setup, изменить пароль с помощью пункта меню «Password Setting» («Change Password»), а потом сохранить сделанные изменения и выйти из утилиты с помощью пункта меню «Save & Exit Setup».

НЕДОСТАТОК «SETUP BIOS»

- Недостатком реализации защиты от несанкционированной загрузки компьютера с помощью утилиты BIOS Setup является то, что установленная с помощью данной утилиты защита может быть преодолена путем принудительного обнуления содержимого энергонезависимой памяти компьютера (CMOS-памяти) после вскрытия его корпуса.

СПЕЦИАЛИЗИРОВАННЫЕ ПРОГРАММНЫЕ СИСТЕМЫ

- Для эффективной защиты необходимо использование специализированных программных систем, которые для каждого пользователя позволяют реализовать один из следующих уровней подтверждения подлинности:
  - ввод пароля с клавиатуры;
  - ввод пароля с носителя;
  - вход в систему при условии раздельного ввода независимыми субъектами двух разных паролей.

ОПИСАНИЕ УРОВНЕЙ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ

- Каждый последующий уровень из перечисленных является мощнее предыдущего.
- При вводе пароля с клавиатуры его длина может достигать 64 символа, набор которых возможен на трех регистрах, переключаемых с помощью клавиш Fl, F2 и F3 (по умолчанию — F1).
- Для высокой надежности аутентификации пароли должны быть длинными и нетривиальными. Но чем длиннее и нетривиальнее пароль, тем сложнее его запомнить. Поэтому при формировании труднозапоминаемого пароля большой длины отдельные системы позволяют записать его на дискету и в дальнейшем использовать эту дискету в качестве электронного аутентификатора для подтверждения подлинности.
- Кроме возможности использования электронного аутентификатора системы позволяют создать ключевую дискету, без которой загрузка операционной системы на компьютере станет невозможной. В этом случае появляется возможность организации входа в компьютерную систему только при условии раздельного ввода двух разных паролей — пароля, хранящегося на ключевой дискете, и пароля, используемого для подтверждения подлинности.

Раздел 6

ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРУ БЕЗ ЗАВЕРШЕНИЯ СЕАНСА РАБОТЫ

ОПИСАНИЕ

- В ряде случаев в процессе работы пользователя за компьютером может возникнуть необходимость кратковременно оставить компьютер без присмотра, не завершая при этом сеанс работы (не выключая компьютер).
- При отсутствии пользователя ничто не мешает осуществлению несанкционированного доступа к компьютерной системе, так как процесс подтверждения подлинности уже выполнен санкционированным пользователем, оставившим компьютер.
- Для предотвращения такой ситуации перед оставлением компьютера необходимо либо завершить сеанс работы, либо заблокировать клавиатуру, мышь и экран до активизации процесса подтверждения подлинности.
- Кроме того, должна быть предусмотрена возможность автоматического блокирования клавиатуры, мыши и экрана по истечении заданного времени бездействия пользователя. Это обеспечит защиту, если при оставлении компьютера пользователь забудет завершить сеанс работы или принудительно заблокировать клавиатуру, мышь и экран.

БЛОКИРОВКИ

- Особенности реализации уровня защиты от несанкционированного доступа к компьютеру при его оставлении без завершения сеанса работы для сред MS-DOS, Windows отличаются друг от друга.
- При использовании общесистемных средств защиты в среде MS-DOS блокировка клавиатуры, экрана и мыши, по тайм-ауту при отсутствии признаков активности пользователя не обеспечивается.
- Недостатком хранителей экрана для защиты от несанкционированного доступа в средах Windows является отсутствие возможности принудительной блокировки клавиатуры, экрана и мыши без завершения сеанса работы.

Раздел 7

ЗАЩИТА ПК ОТ ВРЕДОНОСНЫХ ЗАКЛАДОК

ОБЩИЕ ПОНЯТИЯ ЗАЩИТЫ ОТ ЗАКЛАДОК

- К основным разновидностям вредоносного воздействия относятся воздействие на информацию (уничтожение, искажение, модификация) и воздействие на систему (вывод из строя, ложное инициирование действия, модификация содержания выполняемых функций, создание помех в работе).
- Поэтому важным аспектом работы по защите ПК является борьба с закладками (определение дальше).
- Данный вид защиты для ПК имеет особое значение по ряду причин, а именно:
  - он актуален для всех без исключения пользователей-ПК независимо от того, конфиденциальная или открытая информация ими обрабатывается;
  - заражение разрушающими программными средствами (РПС) представляет угрозу повышенной опасности для ПК, чему особенно способствует высокий динамизм обмена информацией как по каналам связи (в сетях ЭВМ), так и посредством гибких дисков;
  - защита ПК от РПС требует особого профессионализма, поскольку многие из них носят специфический индивидуальный характер, а их нейтрализация и устранение сопряжены с программными манипуляциями нередко весьма сложного и даже искусного характера.

АППАРАТНЫЕ ЗАКЛАДКИ

- Аппаратные закладки могут быть осуществлены в процессе изготовления ПК, ее ремонта или проведения профилактических работ.
- Реальная угроза таких закладок создается массовым и практически неконтролируемым распространением ПК.
- Особая опасность аппаратных закладок заключается в том, что они могут длительное время не проявлять своих вредоносных воздействий, а затем начать их осуществление или по истечении определенного времени, или при наступлении некоторого состояния ПК (например, при заполнении данными жесткого магнитного диска до заданного уровня), или по специальной, подаваемой дистанционно команде.
- Заблаговременное обнаружение аппаратных закладок возможно только в условиях проверок с использованием специальных методов и средств.

ПРОГРАММНЫЕ ЗАКЛАДКИ

- Программные закладки (РПС) с точки зрения массового пользователя представляются особо опасными в силу сравнительной (относительно аппаратных) простоты их осуществления, высокой динамичности их распространения и повышенной трудности защиты от них.
- Если в итоге специальных проверок аппаратные закладки не были обнаружены или они были ликвидированы (нейтрализована возможность их действия), то с высокой степенью можно быть уверенными в их отсутствии в соответствующей ПК.
- Программные же закладки могут появиться в любое время, чему особенно способствуют следующие обстоятельства;
  - массовый обмен информацией на гибких МД, принявший к настоящему времени характер броуновского движения;
  - широкое распространение копий программ, приобретенных незаконным путем;
  - возможности дистанционного воздействия на ПК, подключенные к сети;
  - широкий и непрерывно растущий диапазон разновидностей закладок, что усложняет процессы их обнаружения и нейтрализации.

ДЕТАЛИЗАЦИЯ

В силу изложенных причин защиту от программных закладок рассмотрим несколько детальней, выделив при этом следующие вопросы:

1. Классификация закладок и их характеристики.
2. Принципиальные подходы и общая схема зашиты от закладок.
3. Методы и средства защиты.
4. Рекомендации пользователям ПК по защите от программных закладок.

КЛАССИФИКАЦИЯ ЗАКЛАДОК И ИХ ОБЩИЕ ХАРАКТЕРИСТИКИ

- К сожалению, научно обоснованная классификация закладок до настоящего времени пока не разработана, что объясняется отчасти недостаточным объемом статистических данных, а отчасти тем, что работы по защите от закладок различных разновидностей ведутся изолированно. Системные исследования и разработки еще только предстоит выполнить. Поэтому излагаемое ниже должно рассматриваться лишь в качестве первого приближения.
- Всякая классификация осуществляется по вполне определенному и существенно значимому критерию или по их совокупности. Исходя из целей защиты от вредоносного воздействия закладок, их целесообразно классифицировать по следующей совокупности критериев:
  - По характеру вредоносного воздействия на АСОД;
  - По способу реализации;
  - По способу проникновения в АСОД;
  - По способность к саморазмножению.

ЗНАЧЕНИЯ 1-ГО КРИТЕРИЯ (ХАРАКТЕР ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА АСОД)

Основные значения первого критерия могут быть представлены в следующем виде:

- 1) уничтожение или искажение программ и/или массивов данных;
- 2) формирование каналов несанкционированного получения информации;
- 3) вывод АСОД из числа действующих, т. е. приведение ее в такое состояние, при котором она не может осуществлять свои основные функции;
- 4) инициирование выполнения предусмотренных в АСОД функций (например, ложная подача команды на остановку производства в автоматизированных системах управления технологическими процессами);
- 5) создание препятствий в выполнении функций АСОД (например, блокировка отображения информации на экране дисплея, выдачи на печать и др.).

ЗНАЧЕНИЯ ВТОРОГО КРИТЕРИЯ (ПО СПОСОБУ РЕАЛИЗАЦИИ)

Возможные значения второго критерия (способ реализации) могут быть представлены следующим перечнем:

- аппаратный;
- программный;
- организационный.

ОРГАНИЗАЦИОННЫЕ ЗАКЛАДКИ

- Первые два способа реализации (аппаратный, программный) рассмотрены выше, и являются основными.
- Однако в общем случае можно предположить возможность создания также организационных закладок.
- Например, в инструкций об уничтожении информации, находящейся в ЭВМ, в злоумышленных целях можно предусмотреть преждевременное ее уничтожение или, наоборот, сохранение той информации, которую надлежало бы уничтожить.
- В инструкции по использованию криптографических средств злоумышленно можно внести такие положения, выполнение которых может дать криптоаналитику дополнительную информацию, облегчающую криптоанализ шифртекста.

ЗНАЧЕНИЯ 3-ГО КРИТЕРИЯ (ПО СПОСОБУ ПРОНИКНОВЕНИЯ)

По способу проникновения в АСОД (третий критерий классификации) закладки могут быть разделены на следующие группы:

- злоумышленно создаваемые в процессе производства аппаратуры ЭВТ и компонентов ее программного обеспечения;
- бессознательно вносимые персоналом или пользователями АСОД в процессе ее функционирования;
- злоумышленно вносимые в процессе функционирования АСОД;
- злоумышленно создаваемые в процессе ремонта аппаратуры или модификации АСОД.

ЗНАЧЕНИЯ 4-ГО КРИТЕРИЯ (ПО СПОСОБНОСТИ РАЗМНОЖАТЬСЯ)

По способности к размножению (четвертый критерий классификации) закладки естественным образом делятся на две разновидности:

1) саморазмножающиеся;

2) несаморазмножаюшиеся.

ПРИМЕРЫ ЗАКЛАДОК

- Известно значительное количество закладок, получивших такие условные наименования: троянский конь, бомба, ловушка, люк, вирус, червь.
- **Троянский конь** — несаморазмножающееся РПС, способное осуществлять несанкционированное считывание данных, их уничтожение и другие деструктивные функции.
- **Бомба** — несаморазмножающееся РПС одноразового использования, приводящееся в действие в определенных условиях (в заданное время, в заданном состоянии ЭВМ, по команде извне) и осуществляющее крупномасштабное уничтожение информации.
- **Ловушка** — несаморазмножающаяся программа, осуществляющая несанкционированный перехват информации и запись ее в соответствующее поле ЗУ или выдачу в канал связи.
- **Люк** — несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного Доступа к защищаемой информации.
- **Вирус** — саморазмножающееся РПС, способное уничтожать или изменять данные и/или программы, находящиеся в ЭВМ.
- **Червь** — саморазмножающееся РПС, способное уничтожать элементы данных или программ.

ПРИНЦИПИАЛЬНЫЕ ПОДХОДЫ И ОБЩАЯ СХЕМА ЗАЩИТЫ ОТ ЗАКЛАДОК

Основу защиты составляют следующие функции:

1. создание таких условий, при которых дестабилизирующие факторы (ДФ) не могут появляться;
2. предупреждение появления ДФ, даже если для этого имеются условия;
3. обнаружение появления ДФ;
4. предупреждение воздействия на информацию появившихся
5. ДФ;
6. обнаружение негативного воздействия ДФ на информацию;
7. локализация негативного воздействия ДФ на информацию;
8. ликвидация последствий воздействия ДФ.

МЕТОДЫ И СРЕДСТВА БОРЬБЫ С ЗАКЛАДКАМИ

- Для защиты от закладок должны использоваться методы анализа, синтеза и управления, организационно-правовые, аппаратные и программные средства.
- Средства борьбы с вирусами и другими вредоносными закладками можно разделить на:
  - Юридические
  - Организационно-административные
  - Аппаратные
  - Программные.

ЮРИДИЧЕСКИЕ СРЕДСТВА БОРЬБЫ

- Юридические средства сводятся к установлению ответственности за умышленное создание и распространение вирусов и других закладок в целях нанесения ущерба, хотя доказать авторство и умышленность создания таких программ довольно трудно.
- На Западе соответствующие правовые нормы разработаны гораздо лучше, чем в России.
- В Российской Федерации в последнее время также предпринимаются серьезные усилия по созданию юридической основы борьбы с рассматриваемыми угрозами.

ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНЫЕ СРЕДСТВА

- Данные средства заключаются в выработке и неукоснительном осуществлении организационных и организационно-технических мероприятий, направленных на предупреждение заражения компьютеров этими программами, обнаружение заражения, нейтрализацию негативного их воздействия и ликвидацию последствий.
- Названные мероприятия должны осуществляться как в организациях — разработчиках программных средств, так и в организациях, эксплуатирующих эти программы.

В ОРГАНИЗАЦИЯХ-РАЗРАБОТЧИКАХ

В организациях-разработчиках весьма целесообразно из состава высококвалифицированных программистов создавать специальные группы для выполнения следующих функций:

- определения потенциально возможных источников вредоносных программ и выработка рекомендаций по их обходу;
- выявления и изучения всех нештатных ситуаций, возникающих при разработке программного обеспечения, документального оформления результатов анализа и оповещение всех заинтересованных при выявлении опасностей;
- регулярного контроля состояния программного обеспечения и средств борьбы с вредоносными программами;
- возможно более быстрой ликвидации последствий произошедшей атаки вредоносных программ и изготовления соответствующих средств защиты;
- оказания методической помощи своим абонентам в организации необходимой защиты от вредоносных программ.

ОРГАНИЗАЦИИ, ИСПОЛЬЗУЮЩИЕ ПРОГРАММЫ

Основными мероприятиями по защите программ и данных в организациях, использующих программы, представляются следующие:

- приобретение только законным путем необходимых технических средств и программ, сертифицированных на отсутствие вредоносных закладок;
- создание эталонных копий основных программ и резервирование баз данных;
- организация автоматизированной обработки данных с соблюдением всех приемов и правил;
- периодическая тщательная проверка состояния программного обеспечения и баз данных;
- проверка психологических особенностей сотрудников При приеме на работу;
- создание и поддержание в коллективах здорового морально-психологического климата.

АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ

Из аппаратных средств защиты рекомендуются следующие:

- форматирование диска (для винчестера — полное стирание и переразметка), перезагрузка операционной системы и восстановление программ с незараженных копий;
- заклеивание (закрывание) отверстия защиты записи дискеты;
- физическая блокировка ключом клавиатуры ЭВМ;
- запрет и регистрация попыток записи в файлы операционной системы в области памяти, занятые системной информацией.

ПРОГРАММНЫЕ СРЕДСТВА

Важнейшим компонентом среди средств защиты от вредоносных программ выступают специальные программы, получившие название антивирусных. Известные к настоящему времени антивирусные программы по функциональному признаку делятся на 4 класса:

- — класс А — предупреждение заражения;
- — класс Б — выявление последствий заражения;
- — класс В — минимизация причиненного ущерба;
- — класс Г — общего характера.

ГРУППЫ ПРОГРАММ КЛАССА А

- Al — фильтры, следящие за операциями других исполняемых программ и реагирующие на подозрительные действия;
- А2 — резидентные детекторы и фаги, следящие за появлением в оперативной памяти конкретных вирусов и подающие при их появлении специальные сигналы оператору;
- А3 — иммунизаторы, изменяющие файлы и области оперативной памяти таким образом, что вирус их после этого не заражает;
- А4 — разграничители доступа, ограничивающие распространение вирусов путем разграничения доступа к ресурсам ЭВМ, программам и массивам данных со стороны других программ и пользователей;
- А5 — преобразователи параметров операционной среды, реализующие изменение соглашений, принятых в операционной системе (форматы записей, команды, расположение системной информации и др.), недоступные разработчикам вирусов и тем самым препятствующие заражению ЭВМ.

ГРУППЫ ПРОГРАММ КЛАССА Б

- Б1 — нерезидентные детекторы и фаги, осуществляющие просмотр запоминающих устройств, определяющие зараженность файлов и дисков и организующие их лечение;
- Б2 — программы проверки подозрительных характеристик, осуществляющие просмотр запоминающих устройств и выявление таких характеристик, которые могут говорить о наличии вируса в системе. К таким характеристикам относятся недопустимые значения отдельных полей в заголовке файла, подозрительные переходы, странные изменения в программах и т. п.;
- Б3 — программы, осуществляющие просмотр файлов и носителей, определение различных их характеристик (контрольные суммы, криптографические суммы, длины, даты и времени создания и др.) и сравнение этих величин с эталонами в целях определения возможного заражения;
- Б4 — программы, осуществляющие слежение и регистрацию в системном журнале операций, осуществляемых на ЭВМ. При заражении анализ журнала помогает выявить источник заражения, характер поведения вируса;
- Б5 — программы-ловушки (дрозофилы, уловители), специально выделяемые для заражения, которые, заражаясь, сигнализируют о наличии вируса;
- Б6 — программы автономной защиты файла, защищающие файлы от вирусов путем дописывания своей копии к защищаемым модулям.

ГРУППЫ ПРОГРАММ КЛАССА В

Программы класса В (минимизирующие ущерб, причиненный заражением РПС) делятся на следующие 3 группы:

- BI — программы полного копирования, предназначенные для создания резервных копий программного обеспечения;
- B2 — программы частичного копирования, предназначенные для копирования и восстановления наиболее уязвимых частей диска (Boot-сектор, FAT, корневое оглавление);
- B3 — программы, прерывающие вычислительный процесс, т. е. осуществляющие принудительное прерывание вычислительного процесса в целях локализации распространения вируса.

ГРУППЫ ПРОГРАММ КЛАССА Г

Программы класса Г (общего назначения) предназначены не для прямой борьбы с вирусами, а для оказания помощи в этой борьбе. Эти программы делятся на 5 групп следующего назначения:

- Г1 — программы просмотра диска, позволяющие отображать значения каждого сектора, копировать одну физическую область в другую.
- Применяются для определения целостности отдельных частей диска, наличия вируса в файлах и внесения небольших изменений;
- Г2 — программы, позволяющие искать на диске контекст определенного содержания. С их помощью можно найти участки кодов вирусов и пораженные ими сектора;
- Г3 — программы, позволяющие восстанавливать отдельные части диска;
- Г4 — программы, реализующие просмотр состояния оперативной памяти, состав и характеристики находящихся там модулей;
- Г5 — программы, позволяющие упорядочить информацию на диске на физическом уровне по заранее заданному закону.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru