Лекция 2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Важно уметь не только работать на компьютере, но и защитить ваши документы от чужих глаз.

Абсолютной защиты быть не может. Бытует такое мнение: установил защиту и можно ни о чем не беспокоиться. Полностью защищенный компьютер — это тот, который стоит под замком в бронированной комнате в сейфе, не подключен ни к какой сети (даже электрической) и выключен. Такой компьютер имеет абсолютную защиту, однако использовать его нельзя.

Первой угрозой безопасности информации можно считать некомпетентность пользователей. Если мы говорим об информации, хранящейся в компьютере на рабочем месте, то также серьезную угрозу представляют сотрудники, которые чем-либо не довольны, например зарплатой.

В 1996г. Федеральное бюро расследований совместно с Институтом компьютерной безопасности США провело исследование, результаты которого свидетельствуют о том, что почти в половине всех известных случаев попытки проникновения к информации в организации предпринимались внутри самой организации.

Одна из проблем подобного рода — это так называемые слабые пароли. Пользователи для лучшего запоминания выбирают легко угадываемые пароли. Причем проконтролировать сложность пароля невозможно. Другая проблема — пренебрежение требованиями безопасности. Например, опасно использовать непроверенное или пиратски изготовленное программное обеспечение. Обычно пользователь сам «приглашает» в систему вирусы и «троянских коней».

Чем шире развивается Интернет, тем больше возможностей для нарушения безопасности наших компьютеров, даже если мы и не храним в них сведения, содержащие государственную или коммерческую тайну. Нам угрожают хулиганствующие хакеры, рассылающие вирусы, чтобы просто позабавиться; бесконечные любители пожить за чужой счет; нам угрожают наша беспечность (ну что стоит раз в день запустить антивирус!) и беспринципность (как же отказаться от дешевого пиратского ПО, возможно, зараженного вирусами?).

За последнее время в Интернете резко увеличилось число вирусных атак, а также «шпионских» программ типа «троянского коня» и просто краж паролей нечистоплотными пользователями.

Безопасность в информационной среде

Любая технология на каком-то этапе своего развития приходит к тому, что соблюдение норм безопасности становится одним из важнейших требований. И лучшая защита от нападения — не допускать нападения. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

С точки зрения компьютерной безопасности каждое предприятие обладает своим собственным корпоративным богатством — информационным. Его нельзя спрятать, оно должно активно работать. Средства информационной безопасности должны обеспечивать содержание информации в состоянии, которое описывается тремя категориями требований: доступность, целостность и конфиденциальность. Основные составляющие информационной безопасности сформулированы в Европейских критериях, принятых ведущими странами Европы:

— доступность информации — обеспечение готовности системы к обслуживанию поступающих к ней запросов;
— целостность информации — обеспечение существования информации в неискаженном виде;
— конфиденциальность информации — обеспечение доступа к информации только авторизованному кругу субъектов.

Классификация средств защиты

Классификацию мер защиты можно представить в виде трех уровней

Законодательный уровень.

В Уголовном кодексе РФ имеется глава 28. Преступления в сфере компьютерной информации. Она содержит три следующих статьи:

статья 272. Неправомерный доступ к компьютерной информации;

статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;

статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Административный и процедурный уровни.

На административном и процедурном уровнях формируются политика безопасности и комплекс процедур, определяющих действия персонала в штатных и критических ситуациях. Этот уровень зафиксирован в руководящих документах, выпущенных Гостехкомиссией РФ и ФАПСИ.

Программно-технический уровень.

К этому уровню относятся программные и аппаратные средства, которые составляют технику информационной безопасности. К ним относятся и идентификация пользователей, и управление доступом, и криптография, и экранирование, и многое другое.

И если законодательный и административный уровни защиты не зависят от конкретного пользователя компьютерной техники, то программно-технический уровень защиты информации каждый пользователь может и должен организовать на своем компьютере.

Обычный пользователь, такой как мы с вами, как правило, не является профессиональным шифровальщиком или программистом, поэтому нас интересуют «подручные» средства защиты информации. Рассмотрим средства защиты информации и попробуем оценить их надежность. Ведь знание слабых мест защиты может уберечь нас от многих неприятностей.

Первое, что обычно делает пользователь персонального компьютера — ставит два пароля: один пароль в настройках BIOS и другой — на заставку экрана. Защита на уровне BIOS будет требовать ввод пароля при загрузке компьютера, а зашита на заставке экрана перекроет доступ к информации при прошествии определенного, вами заданного, времени бездействия компьютера.

Установка пароля на уровне BIOS — достаточно тонкий процесс, требующий определенных навыков работы с настройками компьютера, поэтому желательно его устанавливать с коллегой, имеющим достаточный опыт такой деятельности. Пароль на заставку экрана поставить не так сложно, и его может поставить сам пользователь.

Для задания пароля на заставку необходимо выполнить следующие действия: нажмите кнопку Пуск, выберите команды

Настройка и Панель управления, дважды щелкните по значку Экран и в открывшемся окне Свойства экрана выберите вкладку Заставка. Задайте вид заставки, установите временной интервал (предположим, 1 мин), установите флажок Пароль и нажмите на кнопку Изменить.

В открывшемся окне Изменение пароля введите пароль на заставку экрана, затем повторно его наберите для подтверждения и нажмите на кнопку ОК.

Если вы решили сами снять пароль на заставку, то проделайте все вышеизложенные процедуры, только в окне Изменение пароля не следует ничего набирать, а просто нажмите на кнопку ОК. Пароль будет снят.

После установки паролей можно считать, что первый уровень защиты вы сделали, и информационная защита обеспечена. Однако не обольщайтесь: существует, как минимум три способа разрушить эту защиту.

Первый способ — воспользоваться одной из лазеек, часто предусмотренных производителями системной платы, так называемым «универсальным паролем для забывчивых людей». Обычный пользователь, каковыми мы и являемся, как правило, его не знает.

Можно использовать второй способ взлома секретности: снимите кожух компьютера, выньте примерно на 20...30 мин литиевую батарейку на системной плате, после чего вставьте ее обратно. После этой операции BIOS на 99 % забудет все пароли и пользовательские настройки. Кстати, если вы сами забыли пароль, что достаточно часто случается на практике, то можно воспользоваться именно этим способом.

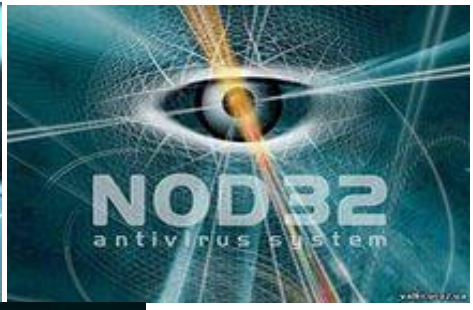
Третий способ узнать постороннему лицу нашу защищенную информацию — вынуть из компьютера жесткий диск и подключить его к другому компьютеру в качестве второго устройства. А дальше без проблем можно читать и копировать чужие секреты. При определенном навыке эта процедура занимает 15...20 мин.

Так что постарайтесь при вашем длительном отсутствии просто не допускать посторонних лиц в помещение, где находится компьютер.

Антивирусы

Антивирус NOD 32

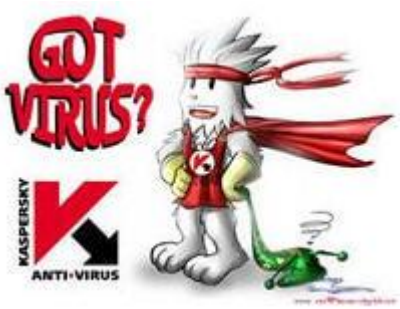
NOD 32является один из самых популярных антивирусов, построенный на эвристическом методе поиска новых вирусов. Антивирусный пакет NOD 32 защищает ваш компьютер от проникновения червей, троянов, макровирусов и вирусов-шпионов. Программное обеспечение NOD 32 постоянно обновляется, поэтому необходимо не только приобрести лицензию на установку, но и подключить обновление версий. NOD 32 включает в себя несколько методов сканирования, которые могут происходить как по запросу пользователя, так и в автоматическом режиме. По мнению большинства экспертов, NOD 32 не влияет на скорость работы компьютера, поэтому является одним из лидеров рынка антивирусных программ.



Антивирусы лаборатории Касперского

Лаборатория Касперского выпускает широкий спектр антивирусов, которые могут использоваться как на домашнем компьютере, так и для защиты корпоративных сетей. По мнению аналитиков, антивирусы Касперского являются одним из самых надежных средств защиты информации, кроме того, многие продукты лаборатории Касперского отмечены заслуженными наградами на выставках и компьютерных форумах. Кроме стандартного набора защиты от вирусов, лаборатория Касперского предлагает дополнительные решения, например, разблокировка компьютера без

отсылки СМС вымогателям или защита, хранение и автоматизированный ввод паролей на страницах интернет-сайтов. Антивирусы Касперского активно используются различными государственными органами, в том числе, и для защиты персональных данных пользователей.



Антивирусы McAfee

McAfee предлагает набор антивирусных программ, которые не только защищают ваш компьютер от вирусов, но и позволяют определить сайты, которые могут нанести вред вашему компьютеру, или создать резервную копию вашей системы. По мнению экспертов, антивирусы McAfeeработают намного быстрее остальных конкурентов и обеспечивают очень надежную защиту, благодаря постоянному анализу вредоносных программ, которые появляются в сети интернет.

Защита жесткого диска (винчестера)

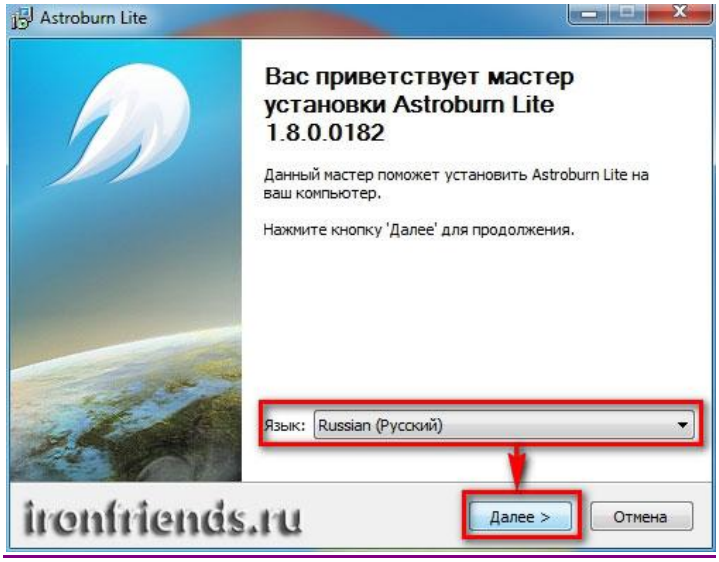
Любую часть компьютерной системы можно заменить на новую, но утратив данные, записанные на жестком диске, вы будете вынуждены воссоздать их заново. На это могут уйти месяцы, а то и годы. Гораздо проще заранее организовать защиту содержимого жесткого диска.

Начинать следует с создания загрузочного диска. Он очень пригодится, если по какой-то причине не удастся загрузить операционную систему с жесткого диска.

Создание загрузочного диска

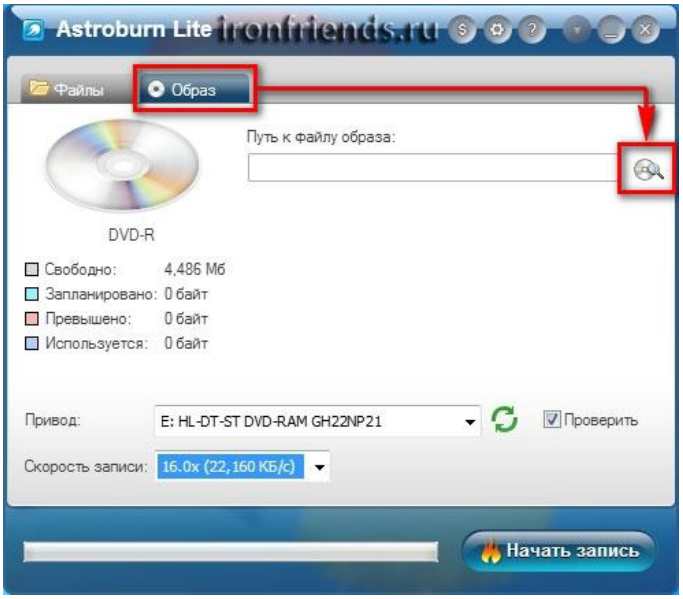
Установка Astroburn

Установить программу довольно просто. Запустите установочный файл и несколько раз нажмите «Далее».

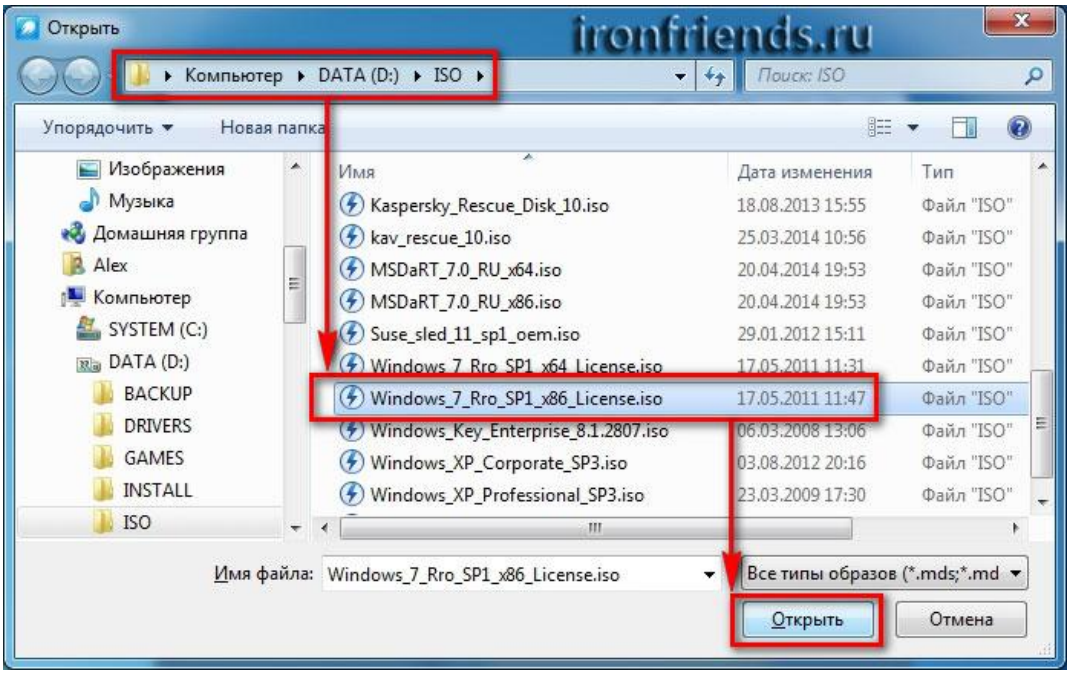


Запись диска в Astroburn

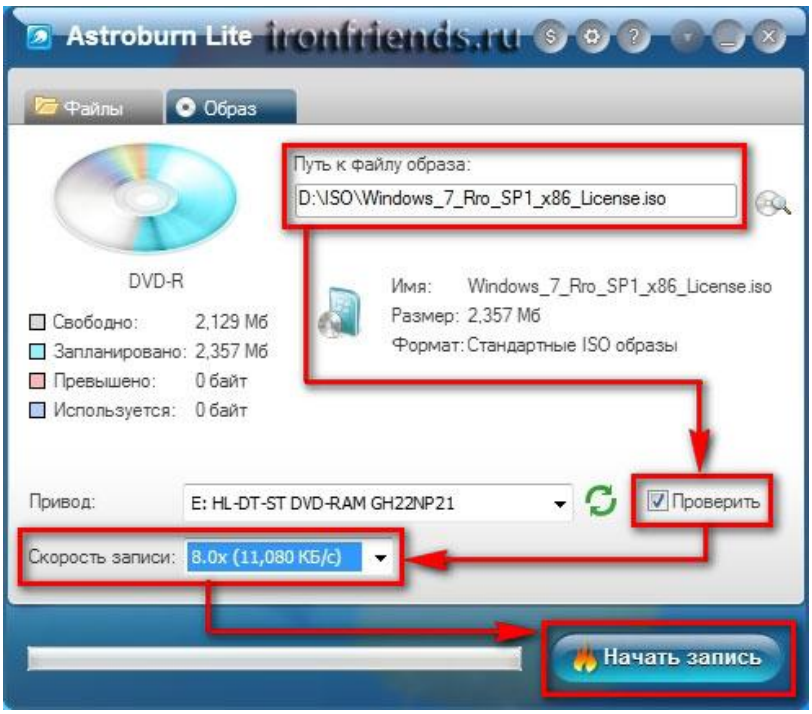
Вставьте чистый диск в DVD-привод и закройте окно автозапуска, если оно появится. Найдите ярлык «Astroburn Lite» на рабочем столе или в меню «ПУСК» и запустите программу. Переключитесь на вкладку «Образ» и нажмите на значок справа от поля «Путь к файлу образу».



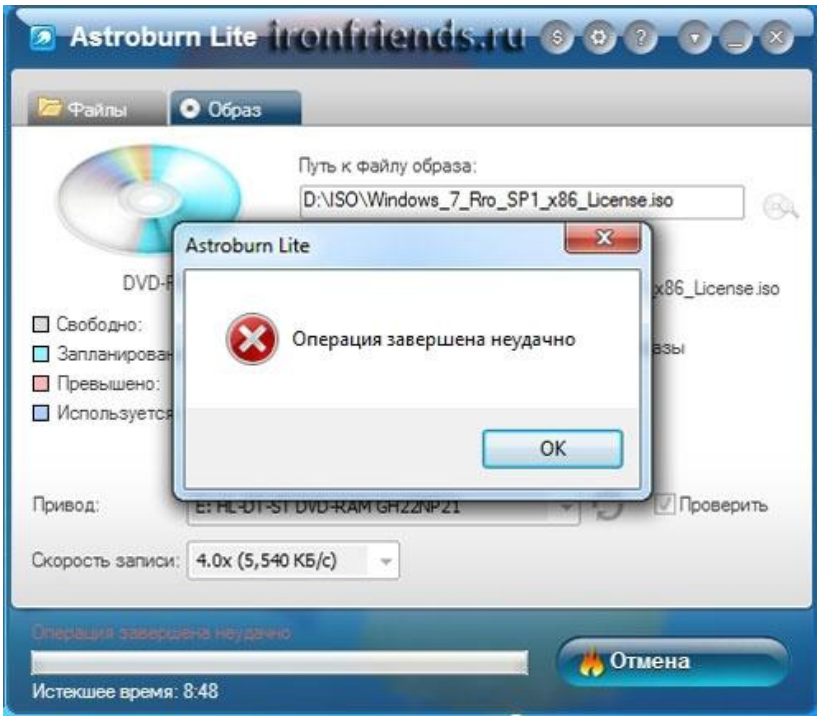
Найдите где у вас на диске находится файл-образ Windows, выделите его левой кнопкой мышки и нажмите «Открыть». Например, у меня все образы дисков находятся на диске «D» в папке «ISO».



Еще раз проверьте, что вы выбрали правильный файл и установлена галочка «Проверить» возле названия DVD-привода. Это позволит убедиться в том, что диск записан без ошибок и процесс установки Windows неожиданно не прервется. Также рекомендую выставить скорость записи 8.0x, это оптимально для дисков DVD-R 16x. Нажмите «Начать запись».



Процесс записи диска вместе с проверкой занимает до 10 минут. По завершении записи закройте программу. Если появилось сообщение с ошибкой или процесс завис на месте, значит либо вам попался плохой диск, либо изношен DVD-привод.



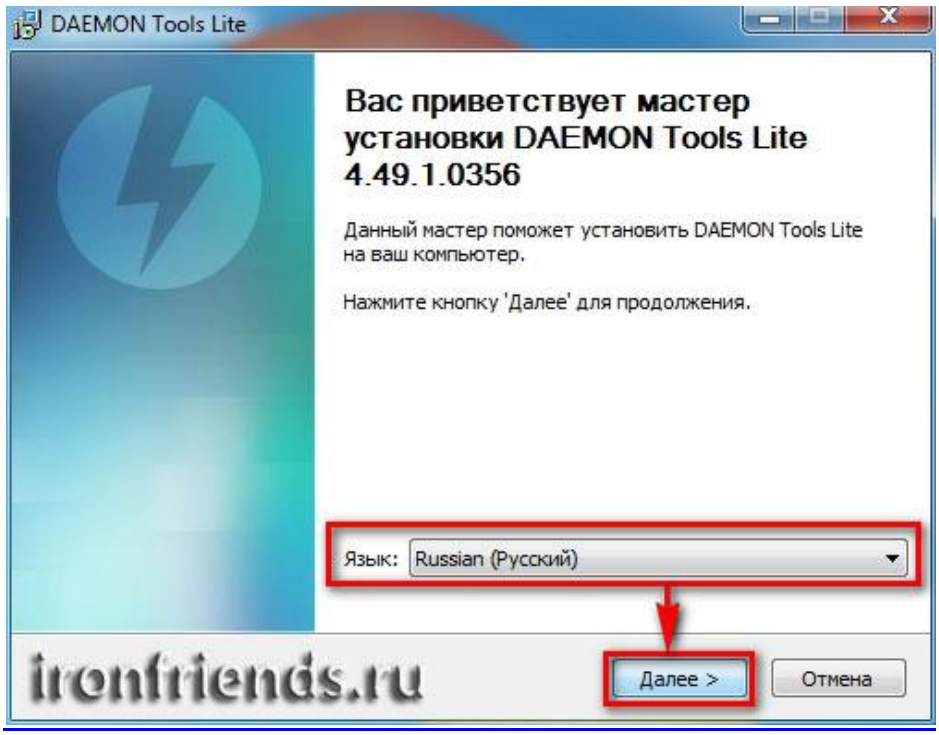
Попробуйте записать еще раз на новый диск, если не получиться, то используйте другой компьютер.

Создание образа диска

Мы используем программу Daemon Tools для создания файла-образа из установочного диска Windows, который в дальнейшем понадобится для создания загрузочной флешки.

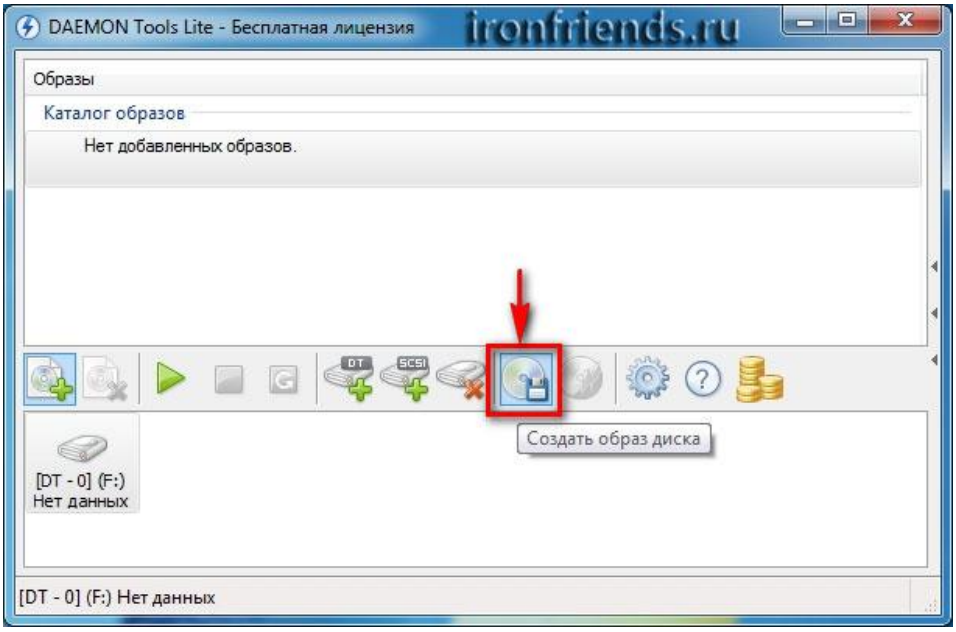
Установка Daemon Tools

Установить программу довольно просто. Запустите установочный файл и несколько раз нажмите «Далее».

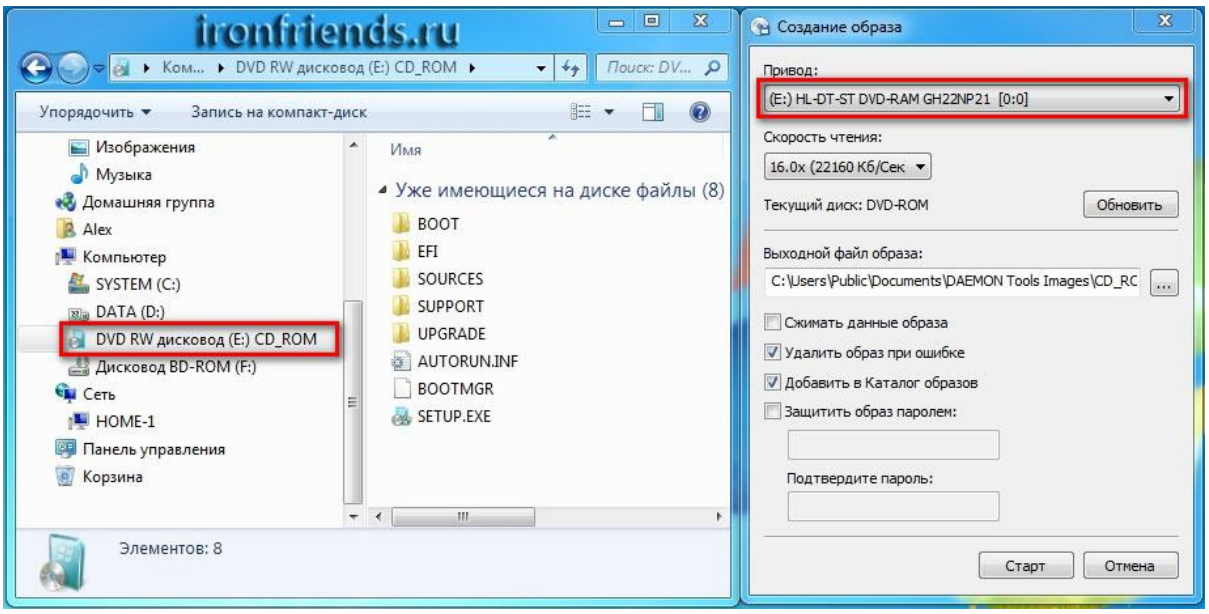


Создание образа в Daemon Tools

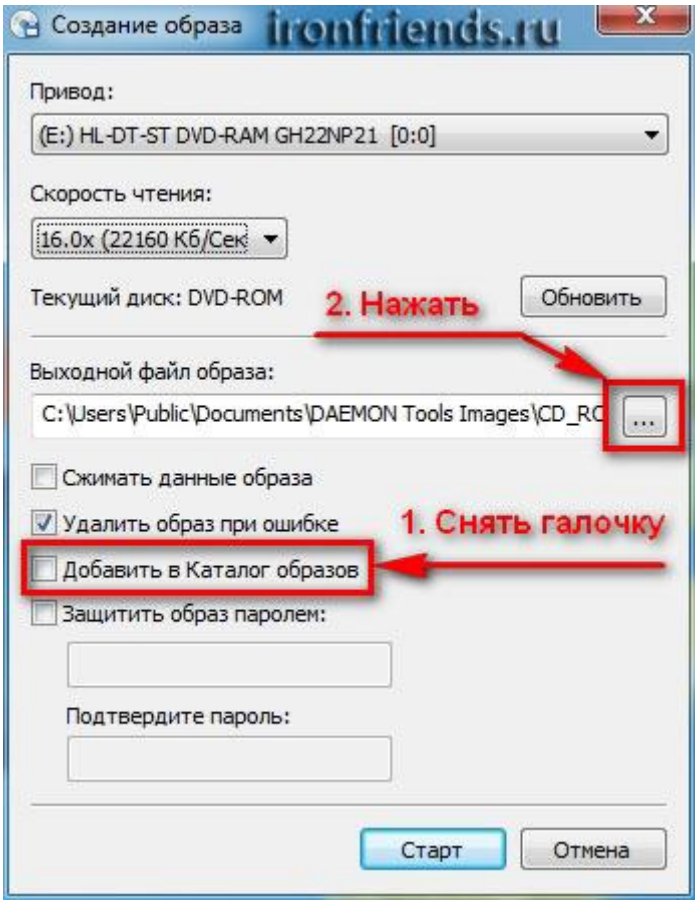
Вставьте установочный диск Windows в DVD-привод и закройте окно автозапуска, если оно появится. Найдите ярлык «DAEMON Tools Lite» на рабочем столе или в меню «ПУСК» и запустите программу. Нажмите на значок диска с дискетой «Создать образ диска».



Проверьте, что выбран именно тот привод, в который вы вставили установочный диск Windows. Буква диска в проводнике Windows и в окне программы должны совпадать.

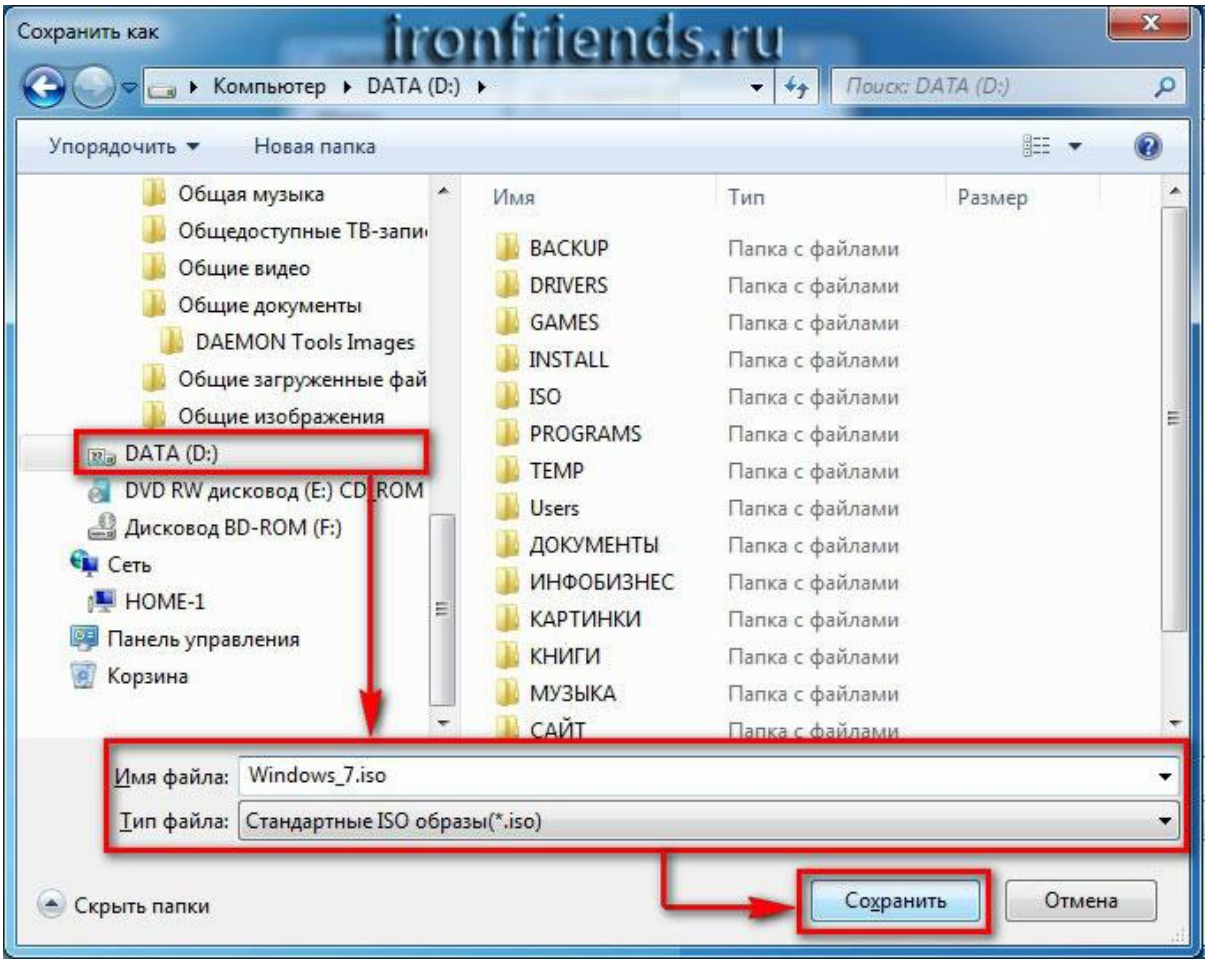


Снимите галочку с пункта «Добавить в Каталог образов» и нажмите на кнопочку с тремя точками «…» для выбора папки для сохранения файла-образа. Учтите, что он может занять до 3.5 Гб.

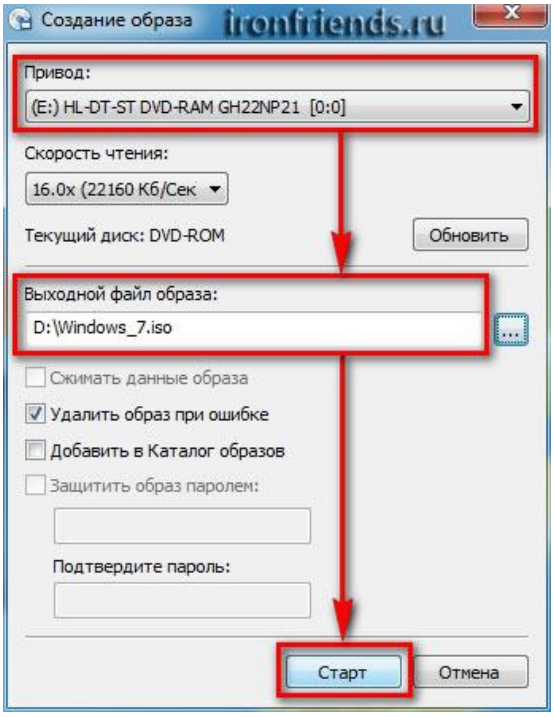


Рекомендую сохранять файл-образ на отдельном разделе диска (например, «D»). В графе «Имя файла» введите, например, «Windows_7», чтобы вы потом могли понять, что это за файл. В названии рекомендую не использовать русские буквы и пробелы. В

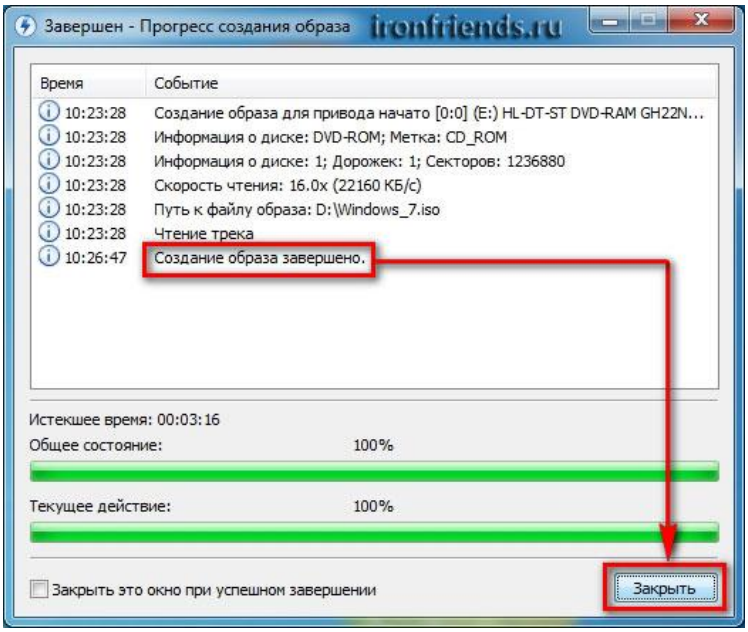
графе «Тип файла» обязательно выберите «Стандартные ISO образы (*.iso)» и нажмите «Сохранить».



Проверьте, что все указано правильно и нажмите «Старт».



Процесс создания образа занимает всего 3-5 минут. В конце должно появиться сообщение «Создание образа завершено». Нажмите кнопку «Закрыть» и завершите работу основной программы, нажав на крестик.



Если появилось сообщение с ошибкой или процесс завис на месте, значит либо установочный диск, либо DVD-привод повреждены. Попробуйте протереть диск сухой мягкой тканью и повторите все заново или используйте другой компьютер.

Резервное копирование данных

Другой враг нашей информации — сбои самого компьютера. Даже при самом строгом соблюдении мер профилактики нельзя быть абсолютно застрахованным от потери данных, хранящихся на жестком диске. Рано или поздно что-нибудь случается, и восстановить все в прежнем виде можно будет только в том случае, если у вас имеется копия содержимого жесткого диска.

Логика здесь очень простая: если одни и те же данные хранятся в двух разных местах, вероятность лишиться их значительно уменьшается. Поэтому всегда следует хранить данные в двух экземплярах: один на жестком диске, другой на сменных носителях, используемых для резервного копирования. Чтобы определиться со стратегией создания резервных копий, необходимо решить, каким носителем вы будете пользоваться и какие данные нужно продублировать.

Информацию можно хранить на различных съемных носителях: флэшках,DVD-дисках и дисках CD ROM, в облаке.

Устройства со сменным диском, например более универсальны, поскольку их можно использовать как для резервного копирования, так и в качестве обычных накопителей. Они просты и удобны в использовании, однако из-за высокой цены они мало применяются.

Следует не забывать, что наша конфиденциальная информация интересна не только взломщику, но и нам самим, и потерять ее не хочется. В этом смысле самый надежный способ хранения — диски CDROM.

Однако для записи информации на CD-диск в компьютере должно быть установлено специальное аппаратное и программное обеспечение — записывающий CDROM и программы типа DirectCD или InCD. Да и диск должен быть специального перезаписывающего типа —CDRW. Записывающие CDROM сегодня стоят значительно дороже, чем обычные, но наблюдается тенденция к снижению цены.

При резервировании информации на записывающем CD-диске можно говорить о сравнительно надежном и одновременно безопасном хранении важной информации.

Основные понятия информационной безопасности автоматизированных систем обработки информации

Безопасность автоматизированной системы обработки информации (АСОИ) - свойство защищенности системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов.

Природа воздействий на АСОИ может быть самой разнообразной. Это и стихийные бедствия (землетрясение, ураган, пожар), и выход из строя составных элементов АСОИ, и ошибки персонала, и попытка проникновения злоумышленника.

Безопасность АСОИ достигается принятием мер по обеспечению конфиденциальности и целостности обрабатываемой ею информации, а также доступности и целостности компонентов и ресурсов системы.

Под доступом к информации понимается ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Различают следующие виды доступа к информации:

санкционированный доступ - доступ к информации, не нарушающий установленные правила разграничения доступа;

Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Правила разграничения доступа служат для регламентации права доступа субъектов доступа к объектам доступа.

Конфиденциальность данных - это статус, предоставленный данным и определяющий требуемую степень их защиты. По существу - это свойство информации быть известной только допущенным и прошедшим проверку (авторизированным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Субъект - это активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.

Объект - пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.

Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении отданных в исходных документах, т.е. если не произошло их случайного или преднамеренного искажения или разрушения.

Целостность компонента или ресурса системы это свойство компонента или ресурса быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

Доступность компонента или ресурса системы - это свойство компонента или ресурса быть доступным для авторизованных законных субъектов системы.

Под угрозой безопасности АСОИ понимаются возможные воздействия на АСОИ, которые прямо или косвенно могут нанести ущерб ее безопасности.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в АСОИ. С понятием угрозы безопасности тесно связано понятие уязвимости АСОИ.

Уязвимость АСОИ - это некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.

Атака на компьютерную систему это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака — это одна из реализаций угрозы безопасности.

Противодействие угрозам безопасности является целью защиты систем обработки информации.

Безопасная или защищенная система - это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплекс средств защиты - программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности АСОИ. Комплекс создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.

Политика безопасности - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

Основные угрозы безопасности систем обработки информации

По цели воздействия различают три основных типа угроз безопасности АСОИ:

угрозы нарушения конфиденциальности информации;

угрозы нарушения целостности информации;

угрозы нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

Угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации - компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция некоторой базы данных).

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСОИ, либо блокируют доступ к некоторым ее ресурсам.Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными.

АСОИ состоит из следующих компонент:

— ЭВМ и их составные части (процессоры, мониторы, терминалы, периферийные устройства-дисководы, принтеры, контроллеры, кабели, линии связи) и т.д.;

обеспечение — приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные

программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

данные — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;

персонал — обслуживающий персонал и пользователи.

Практически каждый компонент может подвергнуться внешнему

воздействию или выйти из строя.

Опасные воздействия на АСОИ можно подразделить на:

случайные;

преднамеренные.

Случайные воздействия. Анализ опыта проектирований, изготовления и эксплуатации АСОИ показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования АСОИ.

Причинами случайных воздействий при эксплуатации АСОИ могут быть:

аварийные ситуации из-за стихийных бедствий и отключений электропитания;

отказы и сбои аппаратуры;

ошибки в программном обеспечении;

ошибки в работе обслуживающего персонала и пользователей;

помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные угрозы связаны с целенаправленными действиями

нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т. п.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить гипотетическую модель потенциального нарушителя:

квалификация нарушителя может быть на уровне разработчика данной системы;

нарушителем может быть как постороннее лицо, так и законный пользователь системы;

нарушителю известна информация о принципах работы системы;

нарушитель выберет наиболее слабое звено в защите.

В частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:

несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;

ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;

несанкционированное копирование программ и данных;

кража магнитных носителей, содержащих конфиденциальную информацию;

кража распечатанных банковских документов;

умышленное уничтожение информации;

несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;

фальсификация сообщений, передаваемых по каналам связи;

отказ от авторства сообщения, переданного по каналам связи;

10.отказ от факта получения информации;

навязывание ранее переданного сообщения;

разрушение информации, вызванное вирусными воздействиями;

разрушение архивной банковской информации, хранящейся на магнитных носителях;

кража оборудования.

В таблице 2.1 показаны основные пути реализации угроз безопасности АСОИ при воздействии на ее компоненты. Конечно, таблица 2.1 дает самую общую картину того, что может произойти с системой. Конкретные обстоятельства и особенности должны рассматриваться отдельно.

Таблица 2.1 - Основные пути реализации угроз безопасности АСОИ при

воздействии на ее компоненты

Объекты воздействия	**Нарушение конфиденциальности информации**	**Нарушение целостности информации**	**Нарушение работоспособности системы**
Аппаратные средства	НСД-подключение; использование ресурсов; хищение носителей.	НСД-подключение; использование ресурсов; модификация, изменение режимов	НСД-изменение режимов; вывод из строя; разрушение
Программное обеспечение	НСД-копирование; хищение; перехват.	НСД, внедрение «троянского коня», «вирусов», «червей»	НСД-искажение; удаление; подмена
Данные	НСД-копирование; хищение; перехват	НСД-искажение; модификация	НСД - искажение; удаление: подмена
Персонал	Разглашение: передача сведений о защите; халатность.	«Маскарад»; вербовка; подкуп персонала	Уход с рабочего места; физическое устранение

Термин «вирус» в применении к компьютерам был предложен Фредом Коэном из Университета Южной Калифорнии. Исторически первое определение, которое дал Ф. Коэн: «Компьютерный вирус - это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению». Ключевыми понятиями в определении компьютерного вируса являются способность вируса к саморазмножению и способность к модификации вычислительного процесса. Указанные свойства компьютерного вируса аналогичны па - разитиоованию в живой природе биологического вируса.

Компьютерный вирус пытается тайно записать себя на компьютерные диски. Способ функционирования большинства вирусов заключается в таком изменении системных файлов компьютера, чтобы вирус начинал свою деятельность при каждой загрузке. Например, вирусы, поражающие загрузочный сектор, пытаются инфицировать часть дискеты или жесткого диска, зарезервированную, только для операционной системы и хранения файлов запуска. Эти вирусы особенно коварны, так как они загружаются в память при каждом включении компьютера. Такие вирусы обладают наибольшей способностью к размножению и могут постоянно распространяться на новые диски.

Сетевой «червь» представляет собой разновидность программы-вируса, которая распространяется по глобальной сети и не оставляет своей копии на магнитном носителе. Термин «червь» пришел из научно- фантастического романа Джона Бриннера «По бурным волнам». Этот термин используется для именования программ, которые подобно ленточным червям перемещаются по компьютерной сети от одной системы к другой.

Первоначально «черви» были разработаны для поиска в сети других компьютеров со свободными ресурсами, чтобы получить возможность выполнить распределенные вычисления. При правильном использовании технология «червей» может быть весьма полезной. Например, «червь» World Wide Web Worm формирует индекс поиска участков Web. Однако «червь» легко превращается во вредоносную программу. «Червь» использует механизмы поддержки сети для определения узла, который может быть поражен. Затем с помощью этих же механизмов передает свое тело в этот узел и либо активизируется, либо ждет походящих условий для активизации.

Понятие несанкционированного доступа

Несанкционированный доступ (НСД) состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД является наиболее распространенным и многообразным видом компьютерных нарушений. НСД использует любую ошибку в системе зашиты и возможен при нерациональном выборе средств зашиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АСОИ. так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам АСОИ и осуществить хищение, модификацию и/или разрушение информации:

все штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;

технологические пульты управления;

линии связи между аппаратными средствами АСОИ;

побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Из всего разнообразия способов и приемов несанкционированного доступа наиболее распространенными нарушениями являются:

перехват паролей;

«маскарад»;

незаконное использование привилегий.

Перехват паролей осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы- перехватчика, после чего на экран выводится сообщение

об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

«Маскарад» - это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями. Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий или привилегий другого пользователя.

Примерами реализации «маскарада» являются:

вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);

передача сообщений в сети от имени другого пользователя.

Незаконное использование привилегий. Большинство систем защиты

устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный. Несанкционированный захват привилегий, например посредством «маскарада», приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий

Угрозы, компьютерных сетей.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами (объектами) сети осуществляется физически с помощью сетевых линий связи и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между объектами сети, передаются в виде пакетов обмена.

При вторжении в компьютерную сеть злоумышленник может использовать как пассивные, так и активные методы вторжения

Пассивное вторжение (перехват информации) - нарушитель только наблюдает за прохождением информации по каналу связи, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации. Как правило, злоумышленник может определить пункты назначения и идентификаторы либо только факт прохождения сообщения, его длину и частоту обмена, если содержимое сообщения не распознаваемо, т.е. выполнить анализ трафика (потока сообщений) в данном канале.

Активное вторжение - нарушитель стремится подменить информацию, передаваемую в сообщении. Он может выборочно модифицировать, изменить или добавить правильное или ложное сообщение, удалить, задержать или изменить порядок следования сообщений. Злоумышленник может также аннулировать и задержать все сообщения, передаваемые по каналу. Подобные действия можно квалифицировать как отказ в передаче сообщений.

Полезные советы. Как защитить данные?

Установите пароли на BIOS и на экранную заставку.

Исключите доступ посторонних лиц к вашему компьютеру,

Создайте загрузочный дискет.

Систематически делайте резервное копирование данных.

Регулярно очищайте Корзину с удаленными файлами.

Устанавливайте пароли на файлы с важной информацией.

При установке пароля не используйте ваше имя, фамилию, телефон.

Проводите архивацию файлов.

После удаления большого количества файлов, но не реже одного раза в месяц, производите дефрагментацию жесткого диска.

Говоря о безопасности информации, я сознательно глубоко не затрагивала проблему компьютерных вирусов, и могло сложиться мнение, что такая проблема не актуальна. Ничего подобного! Борьба с

вирусами — это несомненно часть информационной безопасности, просто мимоходом говорить о такой важной проблеме неправильно. Борьба с вирусами — это тема отдельного разговора.