МАТЕРИАЛЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ МДК 02.01 ТЕХНОЛОГИИ ПУБЛИКАЦИИ ЦИФРОВОЙ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ

НОРМАТИВНЫЕ ДОКУМЕНТЫ ПО УСТАНОВКЕ, ЭКСПЛУАТАЦИИ И ОХРАНЕ ТРУДА ПРИ РАБОТЕ С ПЕРСОНАЛЬНЫМ КОМПЬЮТЕРОМ, ПЕРИФЕРИЙНЫМ ОБОРУДОВАНИЕМ И КОМПЬЮТЕРНОЙ ОРГТЕХНИКОЙ

Нормативные документы России по эргономической безопасности при работе с компьютером

В 1996 г. утверждены:

– ГОСТ Р 50948-96. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности.

– ГОСТ Р 50949-96. Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности.

– ГОСТ Р 50923-96. Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения.

– Санитарные правила и нормы СанПиН 2.2.2.542-96. Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организация работы.

Многочисленными исследованиями российских и зарубежных специалистов доказано, что важнейшим условием безопасности человека перед экраном является правильный выбор визуальных параметров дисплея и светотехнических условий рабочего места.

В нормативных документах установлены требования к двум группам визуальных параметров:

первая – яркость, освещенность, угловой размер знака и угол наблюдения

вторая – неравномерность яркости, блики, мелькания, расстояние между знаками, словами, строками, геометрические и нелинейные искажения, дрожание изображения и т.д. (всего более 20 параметров).

Как показали исследования в России и за рубежом, значения технических характеристик дисплеев не дают гарантии комфортности и эффективности работы человека, объективные (технические) и субъективные (человеческие) оценки дисплеев чаще всего не совпадают, поскольку человек воспринимает изображение и делает вывод о его качестве по совокупности всех его параметров и условий наблюдения.

Отдельно в нормативных документах устанавливаются требования обеспечения эргономической безопасности по излучениям персональных компьютеров.

Основные положения некоторых нормативных документов

Санитарные нормы и правила содержат требования к проектированию, изготовлению отечественных и эксплуатации отечественных и импортных дисплеев и ПК, к проектированию, строительству и реконструкции помещений, предназначенных для эксплуатации всех типов ЭВМ и ПК, производственного оборудования и игровых комплексов на основе ПК.

Устанавливается, что визуальные эргономические параметры дисплеев и ПК являются параметрами безопасности, неправильный выбор которых приводит к ухудшению здоровья пользователей.

В СанПиН зафиксировано, что для обеспечения надежного считывания информации при соответствующей степени комфортности ее восприятия должны быть определены оптимальные и допустимые диапазоны визуальных эргономических параметров.

При проектировании и разработке дисплеев сочетания визуальных эргономических параметров и их значения, соответствующие оптимальным и допустимым диапазонам, полученным в результате испытаний в аккредитованных Госстандартом России лабораториях, должны вноситься в техническую документацию на дисплеи, без чего их эксплуатация не допускается.

Государственный стандарт ГОСТ Р 50948-96 распространяется на средства отображения информации индивидуального пользования на электронно-лучевых трубках и дискретных (матричных) экранах, являющиеся оконечными устройствами отображения средств информатизации и вычислительной техники. Стандарт устанавливает эргономические требования и требования безопасности к дисплеям, в том числе к визуальным эргономическим параметрам и излучениям дисплеев.

Стандарт обязателен для применения при проектировании, изготовлении, эксплуатации и сертификации.

Государственный стандарт, так же как и СанПиН, содержит требования к основным визуальным эргономическим параметрам, по которым устанавливаются в нормативных документах на дисплей значения оптимальных и предельно допустимых диапазонов. Это яркость знака (яркость фона), внешняя освещенность экрана, угловой размер знака, угол наблюдения.

Кроме того, в ГОСТах устанавливаются количественные требования к остальным визуальным эргономическим параметрам, таким, как контрастность деталей изображения и фона, неравномерность яркости элементов контура знака, элементов знаков дискретных экранов, рабочего поля экрана, относительная ширина линии контура знака, временная нестабильность изображения (мелькание), отношение яркости в зоне наблюдения (экран, лицевая панель, корпус дисплея, документы), формат матрицы знака, отношение ширины знака к его высоте для прописных букв, расстояние между знаками, между словами, между строками текста и др.

В стандарт и в СанПиН включены требования и нормы на параметры излучений дисплеев.

Электробезопасность - состояние защищённости работника от вредного и опасного воздействия электротока, электродуги, электромагнитного поля и статического электричества.

Пожарная безопасность – состояние защищённости личности, имущества, общества и государства от пожаров.

Термины охраны труда

Условия труда - совокупность факторов производственной среды и трудового процесса, оказывающих влияние на работоспособность и здоровье работника.

Вредный производственный фактор – производственный фактор, воздействие которого на работника может привести к его заболеванию.

Опасный производственный фактор – производственный фактор, воздействие которого на работника может привести к его травме.

Рабочее место – место, в котором работник должен находиться или в которое ему необходимо прибыть в связи с его работой и которое прямо или косвенно находится под контролем работодателя.

Средства индивидуальной и коллективной защиты работников – технические средства, используемые для предотвращения или уменьшения воздействия на работников вредных или опасных производственных факторов, а так же для защиты от загрязнения.

Производственная деятельность – совокупность действий людей с применением орудий труда, необходимых для превращения ресурсов в готовую продукцию, включающих в себя производство и переработку различных видов сырья, строительство, оказание различных услуг.

Информационная безопасность и право. Защита информации

Основной материал

Информационная безопасность

Информационная безопасность – это защищенность информационных ресурсов и систем от внешних и внутренних посягательств и угроз для граждан, организаций и государственных органов.

Для граждан информационная безопасность выражается в защищенности

- их персональных компьютеров,
- их личной информации в информационных системах и сетях ЭВМ,
- результатов их интеллектуальной деятельности.

Для организаций – защищенность

- от внешних посягательств служебной информации,
- корпоративных информационных систем и сети ЭВМ,
- принадлежащей им интеллектуальной собственности.

Для государства – защита

- от внешних и внутренних угроз национальных информационных ресурсов и государственных информационных систем,
- телекоммуникационной инфраструктуры, организаций и служб.

Работа на ЭВМ – это работа с программами, файлами, документами и базами данных, хранящимися в памяти ЭВМ. Неправильное обращение с ними или с компьютером может привести к их утрате или к неработоспособности ЭВМ.

Информация в ЭВМ – в личных или служебных компьютерах, на сетевых серверах приобретает все большую ценность и ее утрата или модификация может принести значимый материальный ущерб.

Для надежности хранения информация копируется на компакт-диски, либо жесткие диски сетевых серверов. Особо ценная информация копируется в двух экземплярах на разных носителях.

Для пакетов программ лучшим средством хранения и восстановления копий на персональных компьютерах служат компакт-диски, а в сети ЭВМ - архивные копии на общедоступных серверах.

Для ограничения доступа во всех операционных системах и сетевых информационных системах применяется регистрация пользователей с проверкой паролей доступа к тем или иным ресурсам ЭВМ.

Правовая охрана информации

Правовая охрана программ для ЭВМ и баз данных впервые в полном объеме введена в Российской Федерации Законом РФ «О правовой охране программ для электронных вычислительных машин и баз данных», который вступил в силу в 1992 году.

Предоставляемая настоящим законом правовая охрана распространяется на все виды программ для ЭВМ. Правовая охрана не распространяется на идеи и принципы, лежащие в основе программы для ЭВМ, в том числе на идеи и принципы организации интерфейса и алгоритма.

Авторское право

Информация на ЭВМ**,** а также программы и базы данных для ЭВМ согласно российским законам и международному праву является предметом авторского права и объектами интеллектуальной собственности.

На электронные книги, сайты, базы данных и программы для ЭВМ распространяются те же авторские права, что и на обычные литературные, научные и художественные произведения.

Для признания и осуществления авторского права на программы для ЭВМ не требуется ее регистрация в какой-либо организации. Авторское право на программы для ЭВМ возникает автоматически при их создании.

Автором считается лицо, творческим трудом которого создано произведение. Авторские права фиксируются знаком © (copyright – право копий) с указанием фамилии (псевдонима) и года создания.

Сайты в Интернет являются объектами авторского права. Т.к. всякий гипертекст – это программа для клиентских ЭВМ, а сами сайты – это базы данных, представляющие совокупность гипертекстов на сетевых серверах.

Автору программы принадлежит исключительное право осуществлять воспроизведение и распространение программы любыми способами, а также модификацию программы.

Организация или пользователь, правомерно владеющий экземпляром программы (купивший лицензию на ее использование), вправе без получения дополнительного разрешения разработчика осуществлять любые действия, связанные с функционированием программы, в том числе ее запись и хранение в памяти ЭВМ. Запись и хранение в памяти ЭВМ допускаются в отношении одной ЭВМ или одного пользователя в сети, если другое не предусмотрено договором с разработчиком.

В отношении организаций или пользователей, которые нарушают авторские права, разработчик может потребовать возмещения причиненных убытков и выплаты нарушителем компенсации в определяемой по усмотрению суда сумме от 5000-кратного до 50 000-кратного размера минимальной месячной оплаты труда.

Электронная подпись

В 2002 году был принят Закон РФ «Об электронно-цифровой подписи», который стал законодательной основой электронного документооборота в России. По этому закону электронная цифровая подпись в электронном документе признается юридически равнозначной подписи в документе на бумажном носителе.

При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа: секретный и открытый. Секретный ключ хранится на дискете или смарт-карте и должен быть известен только самому корреспонденту. Открытый ключ должен быть у всех потенциальных получателей документов и обычно рассылается по электронной почте.

Процесс электронного подписания документа состоит в обработке с помощью секретного ключа текста сообщения. Далее зашифрованное сообщение посылается по электронной почте абоненту. Для проверки подлинности сообщения и электронной подписи абонент использует открытый ключ.

Защита информации

Методы обеспечения информационной безопасности

1. Авторизация.

Этот метод позволяет создавать группы пользователей, наделять эти группы разными уровнями доступа к сетевым и информационным ресурсам и контролировать доступ пользователя к этим ресурсам.

2. Иденификация и аутентификация.

Идентификация позволяет определить субъект (терминал пользователя, процесс) по уникальному номеру, сетевому имени и другим признакам.

Аутентификация – проверка подлинности субъекта, например по паролю, PIN-коду, криптографическому ключу и т.д.

Методы аутентификации:

1. Биометрия.

Используется аутентификация по геометрии руки, радужной оболочки сетчатки глаза, клавиатурный почерк, отпечатки глаза и т.п.

2. SMART-карты (интеллектуальные карты).
3. e-Token (электронный ключ).

Аналог SMART-карты, выполненный в виде брелка, подключающегося через USB-порт.

4. Определение координат пользователя.

- GPS- глобальная система позиционирования,
- система GSM. (100-300м).

5. Криптография.
6. Протоколирование и аудит.
7. Экранирование.

Разделение информационных потоков между различными информационными системами.

8. Физическая защита.

Физические устройства защиты:

- Физические устройства доступности к сетевым узлам и линиям связи.
- Противопожарные меры
- Защита поддержки инфраструктуры (электропитание, кондиционирование)
- Защита мобильных и радио систем.
- Защита от перехвата данных.

9. Поддержка текущей работоспособности.

- Резервное копирование.
- Управление носителями.
- Регламентированные работы.

Дополнительный материал

Авторское право.

Информация на ЭВМ**,** а также программы и базы данных для ЭВМ согласно российским законам и международному праву является предметом авторского права и объектами интеллектуальной собственности.

На электронные книги, сайты, базы данных и программы для ЭВМ распространяются те же авторские права, что и на обычные литературные, научные и художественные произведения.

Автором считается лицо, творческим трудом которого создано произведение. Авторские права фиксируются знаком © (copyright – право копий) с указанием фамилии (псевдонима) и года создания. Примеры: **© ВАК, 1991** либо **© В.А.Каймин, 2004.**

Для оповещения о своих правах разработчик программы может, начиная с первого выпуска в свет программы, использовать знак охраны авторского права, состоящий из трех элементов:

- буквы С в окружности или круглых скобках ©;
- наименования (имени) правообладателя;
- года первого выпуска программы в свет.

Киберпреступность

Во всех развитых странах мира умышленный взлом компьютеров и распространение компьютерных вирусов приравнено к международным преступлениям, что влечет принудительную экстрадицию правонарушителей.

Ведущие страны Европы, Америки и Азии в 2001 году приняли Конвенцию о киберпреступности – трансграничной компьютерной преступности, которую на сегодняшний день ратифицировало более 40 государств мира.

Согласно Конвенции о киберпреступности страны-участники обязуются выявлять компьютерных правонарушителей по запросам международных организаций и передавать их стране, которой причинен ущерб.

Уголовно наказуемы в соответствии с Конвенцией:

- преступления против данных в ЭВМ,

- преступное использование ЭВМ,
- неправомерное содержание информации.

Преступления с данными в ЭВМ:

1) противозаконный доступ,

2) противозаконный перехват,

3) вмешательство в функционирование ЭВМ,

4) противозаконное использование компьютерных данных.

Преступное использование ЭВМ – подлог с использованием ЭВМ и мошенничество с использованием ЭВМ с намерениями неправомерного получения выгоды для себя или иного лица.

Неправомерное содержание:

- преступления, связанные с детской порнографией,
- правонарушения, связанные с нарушениями авторского права и смежных прав.

Детская порнография согласно Конвенции о киберпреступлениях является уголовным преступлением в США, Германии, Франции, Великобритании и во всех развитых странах Европы, Азии и Америки.

В Российской Федерации незаконное распространение порнографии наказывается по Уголовному Кодексу лишением свободы до 2 лет, а распространение детской порнографии – лишение свободы до 8 лет.

Особая осторожность необходима при установке на компьютерах новых пакетов программ или загрузке программ через Интернет. В любом случае при записи новых программ необходимо проверить отсутствие вирусов.

Компьютерные вирусы – это саморазмножающиеся программы, которые могут уничтожить или испортить все программы и файлы, хранящиеся в памяти ЭВМ или в компьютерной сети.

Особенно много компьютерных вирусов создано и распространяется через Интернет для операционной системы Windows. Известно несколько эпидемий компьютерных вирусов, поразивших через Интернет десятки тысяч компьютеров.

Заражение вирусами происходит при копировании файлов или при их перезаписи через Интернет. При обнаружении вирусов необходимо немедленно пролечить ЭВМ с помощью антивирусных программ.

Антивирусные программы - это средства защиты от вирусных атак должны быть обязательно установлены на ЭВМ.

При работе на чужих ЭВМ необходимо быть очень внимательными. Несанкционированный доступ и уничтожение информации на чужих машинах согласно российским законам и международному праву является серьезным правонарушениями.

Серьезными правонарушениями являются

1) нарушение правил эксплуатации ЭВМ, повлекшее существенный вред;

2) распространение вредоносных программ;

3) неправомерный доступ к информации, охраняемой законом.

Защита доступа к компьютеру

Для предотвращения несанкционированного доступа к данным, хранящимся на компьютере, используются пароли. Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может производиться регистрация всех попыток несанкционированного доступа.

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы авторизации и идентификации пользователей. Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными. К биометрическим системам защиты информации относятся системы распознавания речи, системы идентификации по отпечаткам пальцев, а также системы идентификации по радужной оболочке глаза.

Защита программ от нелегального копирования и использования

Компьютерные пираты, нелегально тиражируя программное обеспечение, обесценивают труд программистов, делают разработку программ экономически невыгодным бизнесом. Кроме того, компьютерные пираты нередко предлагают пользователям недоработанные программы, программы с ошибками или их демоверсии.

Для того чтобы программное обеспечение компьютера могло функционировать, оно должно быть установлено (инсталлировано). Программное обеспечение распространяется фирмами-производителями в форме дистрибутивов на CD-ROM. Каждый дистрибутив имеет свой серийный номер, что препятствует незаконному копированию и установке программ.

Для предотвращения нелегального копирования программ и данных, хранящихся на CD-ROM, может использоваться специальная защита. На CD-ROM может быть размещен закодированный программный ключ, который теряется при копировании и без которого программа не может быть установлена.

Защита от нелегального использования программ может быть реализована с помощью аппаратного ключа, который присоединяется обычно к параллельному порту компьютера. Защищаемая программа обращается к параллельному порту и запрашивает секретный код; если аппаратный ключ к компьютеру не присоединен, то защищаемая программа определяет ситуацию нарушения защиты и прекращает свое выполнение.

Защита данных на дисках

Каждый диск, папка и файл локального компьютера, а также компьютера, подключенного к локальной сети, может быть защищен от несанкционированного доступа. Для них могут быть установлены определенные права доступа (полный, только чтение, по паролю), причем права могут быть различными для различных пользователей.

Для обеспечения большей надежности хранения данных на жестких дисках используются RAID-массивы (Redantant Arrays of Independent Disks – избыточный массив независимых дисков). Несколько жестких дисков подключаются к специальному RAID-контроллеру, который рассматривает их как еди-

ный логический носитель информации. При записи информации она дублируется и сохраняется на нескольких дисках одновременно, поэтому при выходе из строя одного из дисков данные не теряются.

Защита информации в Интернете

Если компьютер подключен к Интернету, то любой пользователь, также подключенный к Интернету, может получить доступ к информационным ресурсам этого компьютера. Если сервер имеет соединение с Интернетом и одновременно служит сервером локальной сети (Интранет-сервером), то возможно несанкционированное проникновение из Интернета в локальную сеть.

Механизмы проникновения из Интернета на локальный компьютер и в локальную сеть могут быть разными:

– загружаемые в браузер Web-страницы могут содержать активные элементы ActiveX или Java-апплеты, способные выполнять деструктивные действия на локальном компьютере;

– некоторые Web-серверы размещают на локальном компьютере текстовые файлы cookie, используя которые можно получить конфиденциальную информацию о пользователе локального компьютера;

– с помощью специальных утилит можно получить доступ к дискам и файлам локального компьютера и др.

Для того чтобы этого не происходило, устанавливается программный или аппаратный барьер с помощью брандмауэра (firewall - межсетевой экран). Брандмауэр отслеживает передачу данных между сетями, осуществляет контроль текущих соединений, выявляет подозрительные действия и тем самым предотвращает несанкционированный доступ из Интернета в локальную сеть.

Основные виды угроз информационной безопасности. Уровни защиты

Основной материал

Уровни защиты

Защита информации в ЭВМ

Согласно законам любой владелец информации – гражданин, организация и государственное учреждение – имеют право на защиту принадлежащей ему по праву информации.

По Гражданскому Кодексу «к объектам гражданских прав относятся не только вещи, деньги, ценные бумаги и иное имущество», и «информация, результаты интеллектуальной деятельности (интеллектуальная собственность)».

Согласно УК РФ «Неправомерный доступ к компьютерной информации» подлежит гражданско-правовой или административной ответственности, вплоть до уголовной ответственности при нанесении крупного ущерба.

Защита информации в ЭВМ может быть создана на

– техническом,

– организационном

– правовом уровне.

Основными угрозами для личной информации, хранимой в ЭВМ и получаемой через Интернет, являются компьютерные эпидемии и спам.

Спам – это массовая несанкционированная анонимная рассылка рекламы по сети Интернет. Спам забивает ненужной информацией личные и служебные почтовые ящики и заставляет оплачивать ненужную Вам рекламу.

В национальном масштабе спам наносит существенный материальный ущерб всем гражданам и организациям, использующим Интернет, а также провайдерам электронной почты и доступа к Интернет.

Компьютерные эпидемии - это массовое распространение компьютерных вирусов по сети Интернет с разрушением информации на личных и служебных ЭВМ, и наносящее существенный материальный ущерб организациям.

Создание и распространение компьютерных вирусов, несанкционированный доступ к информации, нарушение правил эксплуатации ЭВМ карается по закону в Российской Федерации в уголовном порядке.

Компьютерные правонарушения квалифицируются как преступные деяния при наличии умысла и существенного материального ущерба, нанесенным гражданам, организациям или государству.

Защита доступа к компьютеру

Для предотвращения несанкционированного доступа к данным, хранящимся на компьютере, используются пароли. Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может производиться регистрация всех попыток несанкционированного доступа.

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы авторизации и идентификации пользователей. Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными. К биометрическим системам защиты информации относятся системы распознавания речи, системы идентификации по отпечаткам пальцев, а также системы идентификации по радужной оболочке глаза.

Защита программ от нелегального копирования и использования

Для того чтобы программное обеспечение компьютера могло функционировать, оно должно быть установлено (инсталлировано). Программное обеспечение распространяется фирмами-производителями в форме *дистрибутивов* на CD-ROM. Каждый дистрибутив имеет свой серийный номер, что препятствует незаконному копированию и установке программ.

Для предотвращения нелегального копирования программ и данных, хранящихся на CD-ROM, может использоваться специальная защита. На CD-ROM может быть размещен закодированный программный ключ, который теряется при копировании и без которого программа не может быть установлена.

Защита данных на дисках

Каждый диск, папка и файл локального компьютера, а также компьютера, подключенного к локальной сети, может быть защищен от несанкционированного доступа. Для них могут быть установлены определенные права доступа (полный, только чтение, по паролю), причем права могут быть различными для различных пользователей.

Защита информации в Интернете

Если компьютер подключен к Интернету, то любой пользователь, также подключенный к Интернету, может получить доступ к информационным ресурсам этого компьютера. Если сервер имеет соединение с Интернетом и одновременно служит сервером локальной сети (Интранет-сервером), то возможно несанкционированное проникновение из Интернета в локальную сеть.

Для того чтобы этого не происходило, устанавливается программный или аппаратный барьер с помощью брандмауэра (firewall – межсетевой экран). Брандмауэр отслеживает передачу данных между сетями, осуществляет контроль текущих соединений, выявляет подозрительные действия и тем самым предотвращает несанкционированный доступ из Интернета в локальную сеть.

Специализированное программное обеспечение для защиты программ и данных. Компьютерные вирусы и антивирусные программы

Основной материал

Специализированное программное обеспечение для защиты программ и данных

Для обеспечения безопасности информации при персональной работе применяют несколько видов программного обеспечения.

1. Антивирусные программы.

Средства выявления и устранения вредоносного программного обеспечения.

2. Брандмауэры.

Программы, определяющие политику взаимодействия с внешними сетями и контролирующие ее исполнение.

3. Средства разграничения доступа к информации на основе некоторых специальных данных (учетных записей пользователей, паролей на доступ к информации, ключей шифрования).

Компьютерные вирусы

Компьютерные вирусы – это программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на этом компьютере:

– создавать или удалять объекты,

– модифицировать файлы данных или программные файлы,

– осуществлять действия по собственному распространению по локальным вычислительным сетям или по сети Интернет.

Заражение – модификация программных файлов, файлов данных или загрузочных секторов дис-

ков таким образом, что последние сами становятся носителями вирусного кода и, в свою очередь, могут осуществлять вышеперечисленные операции.

Антивирусные программы

Программы-сканеры (полифаги)

Эти программы после запуска анализируют файлы на диске на предмет обнаружения программного кода вирусных программ. При их обнаружении полифаги принимают меры к удалению вредоносного кода, его блокированию или удалению всей вредоносной программы.

Программы-мониторы

Проверяют файлы, запускаемые, открываемые или модифицируемые во время работы системы.

Программы-фильтры

Эти программы проверяют поток данных, принимаемых системой по определенному протоколу (электронной почты, web-страниц и пр.) Позволяют защитить компьютер от получения вредоносных программ из сети.

Программы-детекторы нежелательного ПО

Со многими свободно распространяемыми программами или свободно доступными web-страницами связаны формально не вредоносные программы, которые, тем не менее, могут затруднять работу пользователя, использовать его компьютер для нежелательных операций или разглашать личные данные пользователей. Значительная часть таких программ выявляется антивирусами-полифагами, но иногда это не программы, а настройки уже имеющегося ПО. В таких ситуациях антивирусы бесполезны. Выявляют такие настройки и устраняют их программы-детекторы.

Все эти программы не могут полноценно противостоять распространяющимся с помощью уязвимостей в сетевом программном обеспечении **вирусам-червям.**

Для защиты от таких программ необходимо

– своевременно обновлять уже установленное ПО (обновлениями, выпущенными производителями),

– применять программы контроля работы с сетями – брандмауэры.

Брандмауэр

Брандмауэр (firewall), межсетевой экран – это средство, выполняющее фильтрацию входящей и исходящей информации на основе некоторой системы правил.

В современных персональных брандмауэрах (т. е. защищающих отдельную машину) предусматривается большой набор функций:

– контроль за тем, какие программы и компоненты пытаются осуществить доступ в Интернет,

– контроль за содержимым получаемых сообщений,

– фиксация попыток нанесения вреда путем некоторых широко известных атак,

– удаление рекламных сообщений и другие.

В случае фиксации какой-либо не предусмотренной в правилах попытки соединения брандмауэр может ее отклонить или предложить пользователю создать правило для последующей обработки.

Современные персональные брандмауэры имеют в своем составе также средства обнаружения атак – программные комплексы, выявляющие попытки найти или использовать какую-то уязвимость или реализовать угрозу. В этом случае брандмауэр может предпринять действия по предупреждению нанесения вреда.

Брандмауэры, защищающие индивидуальных пользователей и небольшие домашние сети, реализуются в двух видах:

– аппаратные средства, имеющие в своем составе средства защиты;

– программные брандмауэры, устанавливаемые на ПК.

При работе с сетью Интернет весьма вероятными считаются ***угрозы перехвата и несанкционированного изменения информации при передаче.***

Средством борьбы с этими угрозами является применение различных систем шифрования.

Существующие методы шифрования делятся на методы с закрытым ключом (симметричные) и с открытым ключом (асимметричные).

Первые системы применяются для передачи данных между двумя абонентами, обменявшимися некоторой секретной информацией – ключом. Тогда перехват сообщения не дает злоумышленнику возможности достаточно быстро проанализировать или изменить информацию, поскольку у него этого ключа нет.

В тех случаях, когда нет возможности обменяться ключами, или необходимо обеспечить неотрекаемость (т. е. свойство сообщения однозначно указывать на то, кто его сформировал), применяется шифрование с открытым ключом.

В этом случае для шифрования сообщения применяется пара ключей, один из которых известен всем участникам (открытый), а другой – только одному отправителю (закрытый).

Такое сообщение можно раскрыть с помощью одного ключа, что позволяет всем убедиться в том, кто отправитель сообщения, а при необходимости направить сообщение, которое сможет прочесть только тот, кому оно предназначено.

Это позволяет создать систему цифровых сертификатов – своеобразных «удостоверений», передаваемых вместе с сообщением. Сертификат включает в себя необходимую информацию об отправителе (название организации, имя, адрес узла и т. п.) и электронную подпись, т. е. контрольную сумму, зашифрованную общим удостоверяющим центром.

Расшифровать контрольную сумму могут все, а вот подготовить – только сам центр. Если узел-получатель доверяет удостоверяющему центру (удостоверений может быть целая цепочка), то сообщение (web-страница, например) считается заслуживающей доверия.

Такая система позволяет организовать зашифрованный канал обмена информацией двум «незнакомым» абонентам, удостоверив их и организовав обмен ключами для симметричного шифрования.

Дополнительный материал

Макровирусы

Макровирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

Макровирусы активны не только в момент открытия/закрытия файла, но до тех пор, пока активен сам редактор.

Word/Excel-вирусы

При работе с документом текстовый редактор Word (либо Excel) выполняет различные действия – открывает документ, сохраняет, печатает, закрывает и т.д.

Характерными проявлениями вирусов семейства Macro.Word являются следующие:

1. Невозможность конвертирования зараженного документа Word в другой формат.

2. Невозможность записи документа командой «Save As».

3. Зараженные файлы имеют формат Template. При заражении вирусы WinWord конвертируют файлы из формата Word Document в Template.

Java-вирусы

Написаны на языке программирования Java и являются стандартными Java-программами. Заражают приложения Java (Java applications). Размножаются, если зараженный файл запустить как дисковую Java-программу при помощи Java-машины.

Обычно эти вирусы не способны размножаться при запуске под известными броузерами (при стандартных настройках). Встроенные в браузеры системы защиты не позволяют вирусу получить доступ к файлам.

Скрипт-вирусы

Скрипт-вирусы являются скрипт-программами на PHP. Они заражают файлы с расширением .php (иногда и .htm). Записываются в начало или в конец файлов (иногда записывают только ссылку на свой код).

Файловые черви

Файловые черви (worms) являются, разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и прочие). Некоторые вирусы записывают команду запуска зараженного файла в BAT-файлы.

Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.

Вирусы – «черви» (worms), или Сетевые вирусы

Вирусы, которые распространяются в компьютерной сети и не изменяют файлы или секторы дисков. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других

компьютеров и рассылают по этим адресам свои копии. Такие вирусы могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Обстановку в современной сети Интернет иначе как «криминогенной» назвать нельзя. Постоянные вирусные и троянские атаки терроризируют практически всех пользователей интернета – домашних пользователей, небольшие и средние компании, глобальные корпорации и государственные структуры. Причина подобной криминализации сети – это корыстный интерес. Извлечение нелегальной прибыли путем создания и распространения вредоносных программ – это:

– воровство частной и корпоративной банковской информации (получение доступа к банковским счетам персональных пользователей и организаций);

– воровство номеров кредитных карт;

– распределенные сетевые атаки (DDoS-атаки) с последующим требованием денежного выкупа за прекращение атаки (современный компьютерный вариант обычного рэкета);

– создание сетей троянских прокси-серверов для рассылки спама (и коммерческое использование этих сетей);

– создание зомби-сетей для многофункционального использования;

– создание программ, скачивающих и устанавливающих системы показа нежелательной рекламы;

– внедрение в компьютеры троянских программ, постоянно звонящих на платные (и весьма дорогие) телефонные номера.