УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (ПО)

Работу выполнила студентка 3-го курса

гр. ПСА - 336

Анисимова Ангелина Максимовна

Программное обеспечение (ПО) - это совокупность всех программ и соответствующей документации, обеспечивающая использование ЭВМ в интересах каждого ее пользователя.

Различают системное и прикладное ПО. Схематически программное обеспечение можно представить так:

Системное ПО – это совокупность программ для обеспечения работы компьютера. Системное ПО подразделяется на базовое и сервисное. Системные программы предназначены для управления работой вычислительной системы, выполняют различные вспомогательные функции (копирования, выдачи справок, тестирова

Базовое ПО включает в себя:

- операционные системы;
- оболочки;
- сетевые операционные системы.

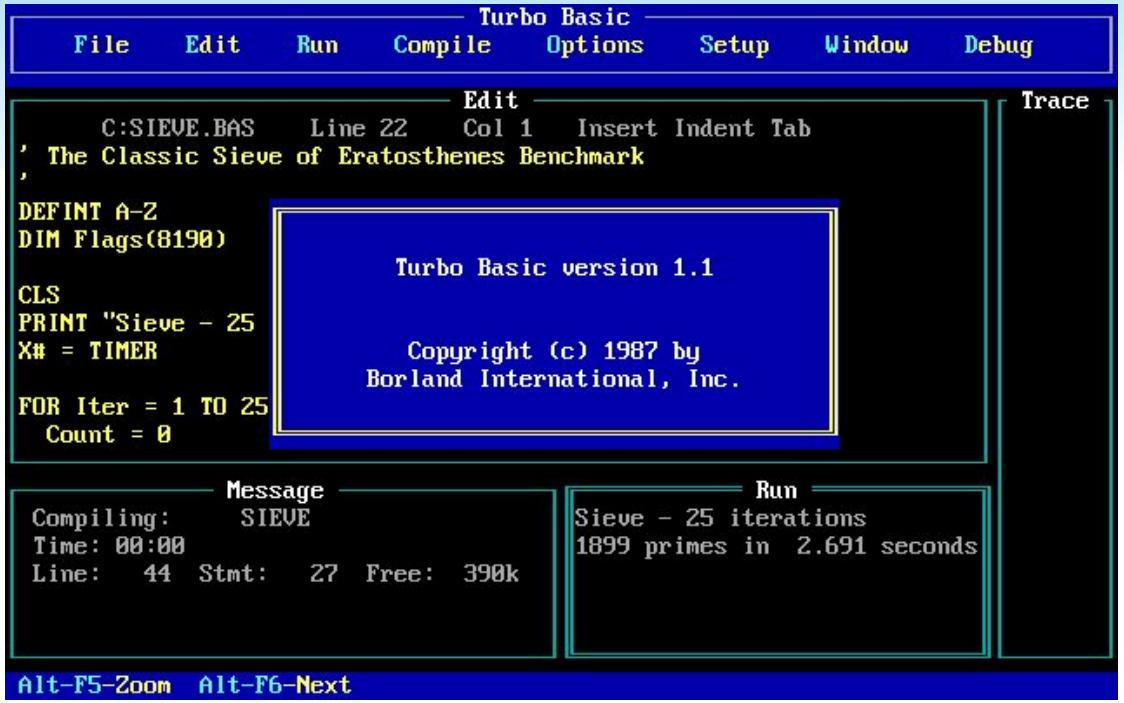
Сервисное ПО включает в себя программы (утилиты):

- диагностики;
- антивирусные;
- обслуживания носителей;
- архивирования;
- обслуживания сети.

Прикладное ПО – это комплекс программ для решения задач определённого класса конкретной предметной области. Прикладное ПО работает только при наличии системного ПО.

Прикладные программы называют приложениями. Они включает в себя:

- текстовые процессоры;
- табличные процессоры;
- базы данных;
- интегрированные пакеты;
- системы иллюстративной и деловой графики (графические процессоры
- экспертные системы;
- обучающие программы;
- программы математических расчетов, моделирования и анализа;
- игры;
- коммуникационные программы.



Особую группу составляют системы программирования (инструментальные системы), которые являются частью системного ПО, но носят прикладной характер. Системы программирования – это совокупность программ для разработки, отладки и внедрения новых программных продуктов. Системы программирования обычно содержат:

- трансляторы;
- среду разработки программ;
- библиотеки справочных программ (функций, процедур);
- отладчики;
- редакторы связей и др.

Программное обеспечение (англ. software) – это совокупность программ, обеспечивающих функционирование компьютеров и решение с их помощью задач предметных областей. Программное обеспечение (ПО) представляет собой неотъемлемую часть компьютерной системы, является логическим продолжением технических средств и определяет сферу применения компьютера.

ПО современных компьютеров включает множество разнообразных программ, которое можно условно разделить на три группы (рис. 3.1):

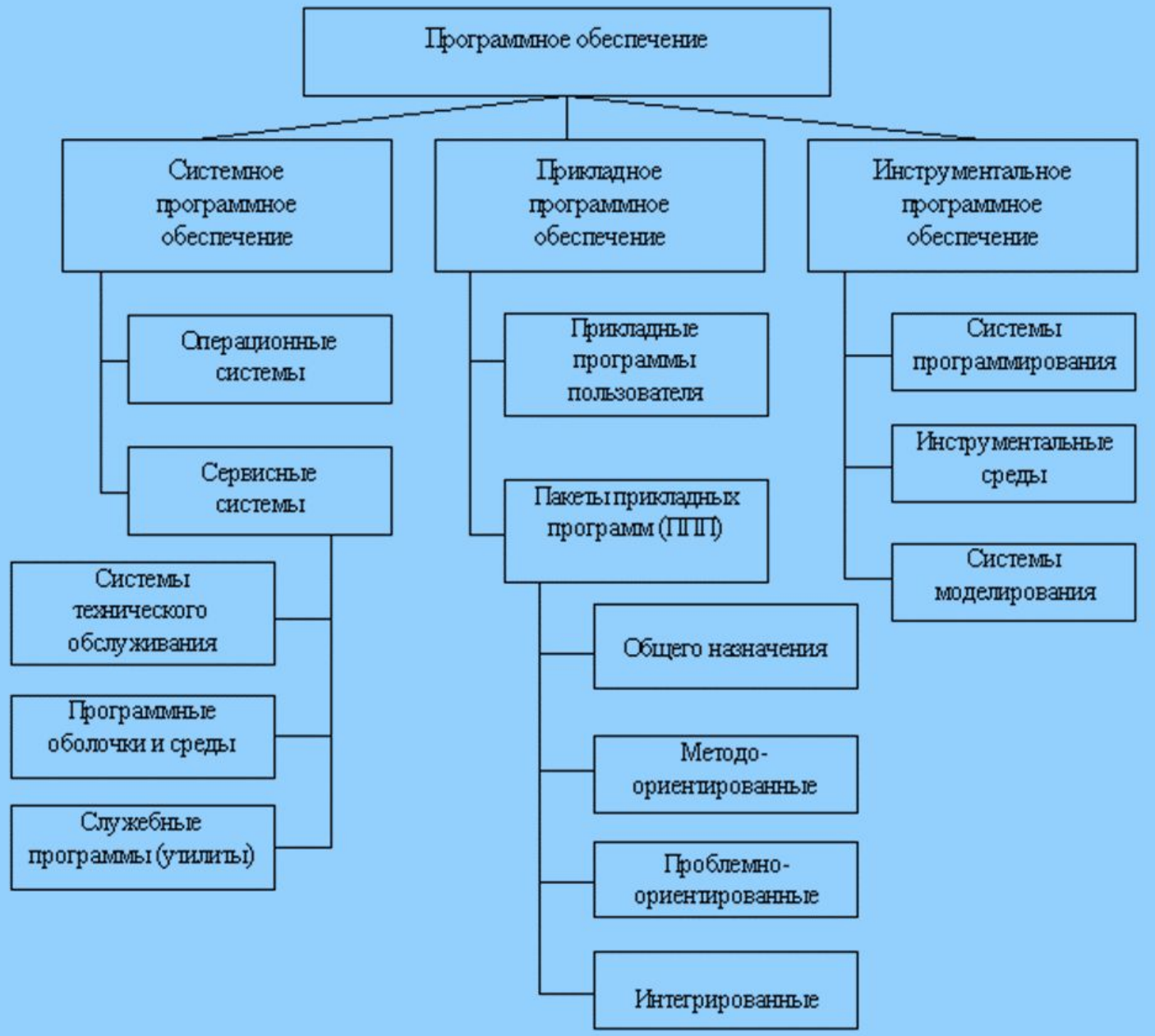
1. Системное программное обеспечение (системные программы);
2. Прикладное программное обеспечение (прикладные программы);
3. Инструментальное обеспечение (инструментальные системы).

Системное программное обеспечение (СПО) – это программы, управляющие работой компьютера и выполняющие различные вспомогательные функции, например, управление ресурсами компьютера, создание копий информации, проверка работоспособности устройств компьютера, выдача справочной информации о компьютере и др. Они предназначены для всех категорий пользователей, используются для эффективной работы компьютера и пользователя, а также эффективного выполнения прикладных программ.

Центральное место среди системных программ занимают операционные системы (англ. operating systems). Операционная система (ОС) – это комплекс программ, предназначенных для управления загрузкой, запуском и выполнением других пользовательских программ, а также для планирования и управления вычислительными ресурсами ЭВМ, т.е. управления работой ПЭВМ с момента включения до момента выключения питания. Она загружается автоматически при включении компьютера, ведет диалог с пользователем, осуществляет управление компьютером, его ресурсами (оперативной памятью, дисковым пространством и т.д.), запускает другие программы на выполнение и обеспечивает пользователю и программам удобный способ общения – интерфейс – с устройствами компьютера. Другими словами, операционная система обеспечивает функционирование и взаимосвязь всех компонентов компьютера, а также предоставляет пользователю доступ к его аппаратным возможностям.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Сервисные системы расширяю возможности ОС по обслуживани системы, обеспечивают удобств работы пользователя. К это категории относят систем технического обслуживани программные оболочки и среды О а также служебные программы.



Системы технического обслуживания – это совокупность программно-аппаратных средств ПК, которые выполняют контроль, тестирование и диагностику и используются для проверки функционирования устройств компьютера и обнаружения неисправностей в процессе работы компьютера. Они являются инструментом специалистов по эксплуатации и ремонту технических средств компьютера.

Для организации более удобного и наглядного интерфейса пользователя с компьютером используются программные оболочки операционных систем – программы, которые позволяют пользователю отличными от предоставляемых ОС средствами (более понятными и эффективными) осуществлять действия по управлению ресурсами компьютера. К числу наиболее популярных оболочек относятся пакеты Norton Commander (Symantec), FAR (File and Archive manageR) (Е.Рошаль).

Служебные программы (утилиты, лат. utilitas – польза) – это вспомогательные программы, предоставляющие пользователю ряд дополнительных услуг по реализации часто выполняемых работ или же повышающие удобство и комфортность работы. К ним относятся:

- программы-упаковщики (архиваторы), которые позволяют более плотно записывать информацию на дисках, а также объединять копии нескольких файлов в один, так называемый, архивный файл (архив);
- антивирусные программы, предназначенные для предотвращения заражения компьютерными вирусами и ликвидации последствий заражения;
- программы оптимизации и контроля качества дискового пространства;
- программы восстановления информации, форматирования, защиты данных;
- программы для записи компакт-дисков;
- драйверы – программы, расширяющие возможности операционной системы по управлению устройствами ввода/вывода, оперативной памятью и т.д. При подключении к компьютеру новых устройств необходимо установить соответствующие драйверы;
- коммуникационные программы, организующие обмен информацией между компьютерами и др.

Прикладное программное обеспечение (ППО) предназначено для решения задач пользователя. В его состав входят прикладные программы пользователей и пакеты прикладных программ (ППП) различного назначения.

Прикладная программа пользователя – это любая программа, способствующая решению какой-либо задачи в пределах данной проблемной области. Прикладные программы могут использоваться либо автономно, либо в составе программных комплексов или пакетов.

Пакеты прикладных программ (ППП) – это специальным образом организованные программные комплексы, рассчитанные на общее применение в определенной проблемной области и дополненные соответствующей технической документацией. Различают следующие типы ППП:

- ППП общего назначения – универсальные программные продукты, предназначенные для автоматизации широкого класса задач пользователя.
- методо-ориентированные ППП, в основе которых лежит реализация математических методов решения задач. К ним относятся, например, системы математической обработки данных (Mathematica, MathCad, Maple), системы статистической обработки данных (Statistica, Stat).;
- проблемно-ориентированные ППП предназначены для решения определенной задачи в конкретной предметной области. Например, информационно-правовые системы ЮрЭксперт, ЮрИнформ; пакеты бухгалтерского учета и контроля 1С: Бухгалтерия, Галактика, Анжелика; в области маркетинга –Касатка, Marketing Expert; банковская система СТБанк;
- интегрированные ППП представляют собой набор нескольких программных продуктов, объединенных в единый инструмент. Наиболее развитые из них включают в себя текстовый редактор, персональный менеджер (органайзер), электронную таблицу, систему управления базами данных, средства поддержки электронной почты, программу создания презентационной графики. Результаты, полученные отдельными подпрограммами, могут быть объединены в окончательный документ, содержащий табличный, графический и текстовый материал. К ним относят, например, MS Works. Интегрированные пакеты, как правило, содержат некоторое ядро, обеспечивающее возможность тесного взаимодействия между составляющими.

Обычно пакеты прикладных программ имеют средства настройки, что позволяет при эксплуатации адаптировать их к специфике предметной области.

К инструментальному программному обеспечению относят: системы программирования – для разработки новых программ, например, Паскаль, Бейсик. Обычно они включают: редактор текстов, обеспечивающий создание и редактирование программ на исходном языке программирования (исходных программ), транслятор, а также библиотеки подпрограмм; инструментальные среды для разработки приложений, например, C++, Delphi, Visual Basic, Java, которые включают средства визуального программирования; системы моделирования, например, система имитационного моделирования MatLab, системы моделирования бизнес-процессов BpWin и баз данных ErWin и другие.

Транслятор (англ. translator – переводчик) – это программа-переводчик, которая преобразует программу с языка высокого уровня в программу, состоящую из машинных команд. Трансляторы реализуются в виде компиляторов или интерпретаторов, которые существенно различаются по принципам работы.

Компилятор (англ. compiler – составитель, собиратель) читает всю программу целиком, делает ее перевод и создает законченный вариант программы на машинном языке, который затем и выполняется. После компилирования получается исполняемая программа, при выполнении которой не нужна ни исходная программа, ни компилятор.

Интерпретатор (англ. interpreter – истолкователь, устный переводчик) переводит и выполняет программу строка за строкой. Программа, обрабатываемая интерпретатором, должна заново переводиться на машинный язык при каждом очередном ее запуске.

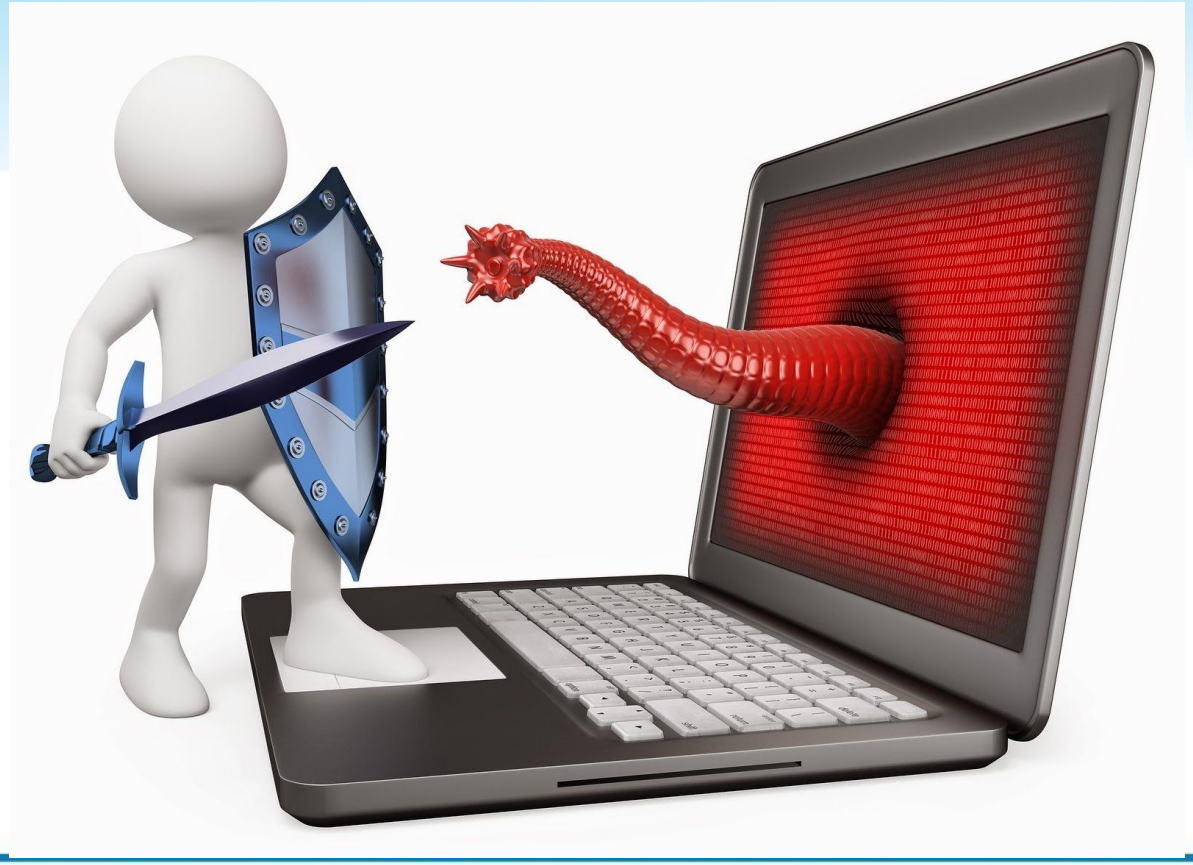
Откомпилированные программы работают быстрее, но интерпретируемые проще исправлять и изменять.

Компьютерный вирус это специальная программа, как правило, очень маленького размера, способная внедряться в тело другой программы, перехватывать управление этой программой, саморазмножаться (распространяться) и внедряться в другие программы с задачей дестабилизации работы компьютера и порче информации.

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус.

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.



Классификация вирусов:

1. По среде обитания: - сетевые вирусы (они распространяются по разным компьютерным сетям); - файловые вирусы (заражают исполняемые файлы программ — com, exe, bat); - загрузочные вирусы (заражают загрузочный сектор диска (boot-sector) или сектор, содержащий программу загрузки системного диска Master Boot Records); - файлово-загрузочные (действуют так же как и загрузочные вирусы).

2. По способу заражения: - резидентные (такой вирус при инфицировании ПК оставляет в оперативке свою резидентную часть), которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК); – нерезидентные (не заражают оперативную память и могут быть активными ограниченное время).

3. По результату воздействия: - неопасные (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости — проигрывать заложенную в них мелодию или показывать картинку); - опасные (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.); - очень опасные (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)

4. По алгоритму работы: - паразитические (меняют содержимое файлов и секторов диска). Такие вирусы легко вычисляются и удаляются; - мутанты (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования; каждая следующая копия размножающегося вируса не будет похожа на предыдущую); - репликаторы (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их); - троянский конь (один из самых опасных вирусов, так как Трояны не размножаются, а воруют ценную (порой очень дорогую) информацию пароли, банковские счета, электронные деньги и т.д.); - невидимки (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

Методы обнаружения вирусов Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

- Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах
- Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Метод соответствия определению вирусов в словаре Обнаружение, основанное на сигнатурах. Это метод, когда антивирусная программа, просматривая файл, обращается к антивирусным базам, которые составлены производителем программы-антивируса. В случае соответствия, какого либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базах, программа антивирус может по запросу выполнить одно из следующих действий:

1. Удалить инфицированный файл.

2. Заблокировать доступ к инфицированному файлу.

3. Отправить файл в карантин (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).

4. Попытаться восстановить файл, удалив сам вирус из тела файла.

5. В случае невозможности лечения/удаления. выполнить эту процедуру при перезагрузке.

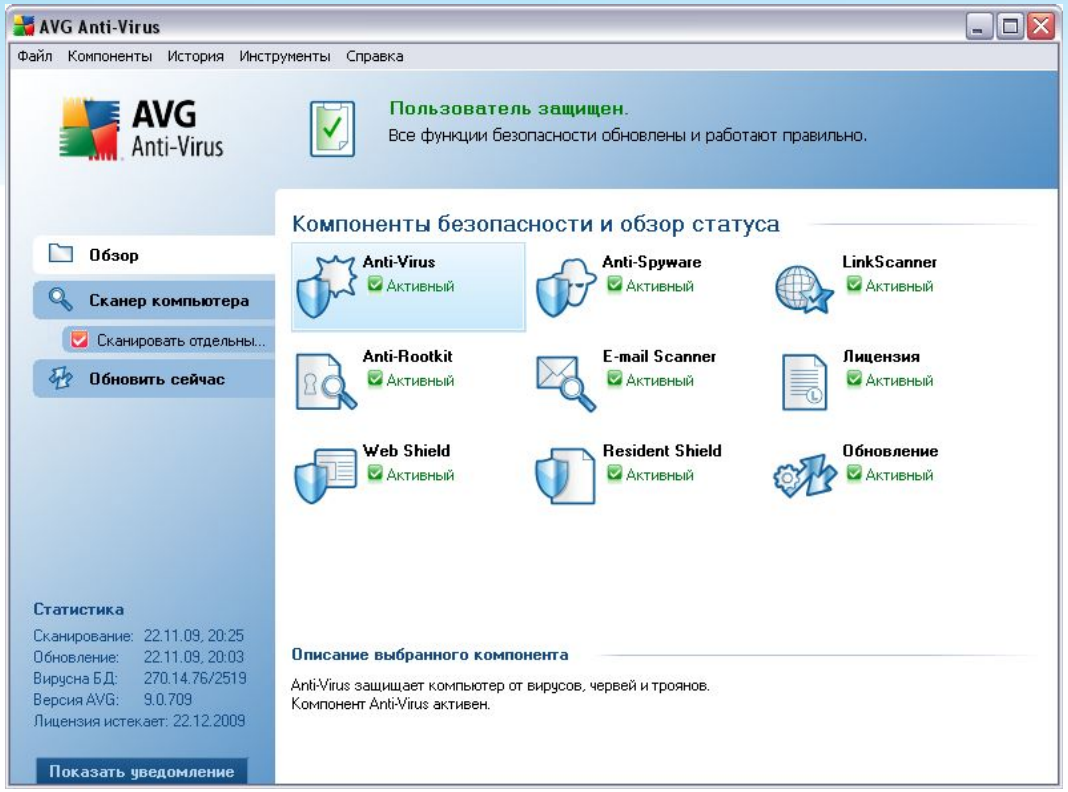
УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Метод обнаружения странного поведения программ Обнаружение аномалий Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (exe-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить что следует сделать. В настоящее время, подобные превентивные методы обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта.

Метод обнаружения при помощи эмуляции Обнаружение, основанное на эмуляции Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (то есть немедленно начинает искать другие exe-файлы например), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

Метод «Белого списка» Общая технология по борьбе с вредоносными программами — это «белый список». Вместо того, чтобы искать только известные вредоносные программы, это технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные. Выбрав этот параметр отказа по умолчанию, можно избежать ограничений, характерных для обновления сигнатур вирусов. К тому же, те приложения на компьютере, которые системный администратор не хочет устанавливать, не выполняются, так как их нет в «белом списке».

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ



Эвристическое сканирование – метод работы антивирусной программы, основанный на сигнатурах и эвристике, призван улучшить способность сканеров применять сигнатуры и распознавать модифицированные версии вирусов в тех случаях, когда сигнатура совпадает с телом неизвестной программы не на 100 %, но в подозрительной программе налицо более общие признаки вируса. Данная технология, однако, применяется в современных программах очень осторожно, так как может повысить количество ложных срабатываний. Практически все современные антивирусные средства применяют технологию эвристического анализа программного кода. Эвристический анализ нередко используется совместно с сигнатурным сканированием для поиска сложных шифрующихся и полиморфных вирусов. Методика эвристического анализа позволяет обнаруживать ранее неизвестные инфекции, однако, лечение в таких случаях практически всегда оказывается невозможным. В таком случае, как правило, требуется дополнительное обновление антивирусных баз для получения последних сигнатур и алгоритмов лечения, которые, возможно, содержат информацию о ранее неизвестном вирусе. В противном случае, файл передается для исследования антивирусным аналитикам или авторам антивирусных программ.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Классификация антивирусов

Касперский использовал следующую классификацию антивирусов в зависимости от их принципа действия (определяющего функциональность): Сканеры (устаревший вариант «полифаги»). Определяют наличие вируса по БД, хранящей сигнатуры (или их контрольные суммы) вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического анализатора Ревизоры. Запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений. (Класс близкий к Юз). Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, и другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелсвирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная и России программа Kaspersky Monitor.

Сторожа (мониторы или фильтры). Отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции. При попытке какой- либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К недостаткам программ-сторожей можно отнести их «назойливостью (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением. Вакцины. Изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым. В современных условиях, когда количество возможных вирусов измеряется десятками тысяч, этот подход неприменим.

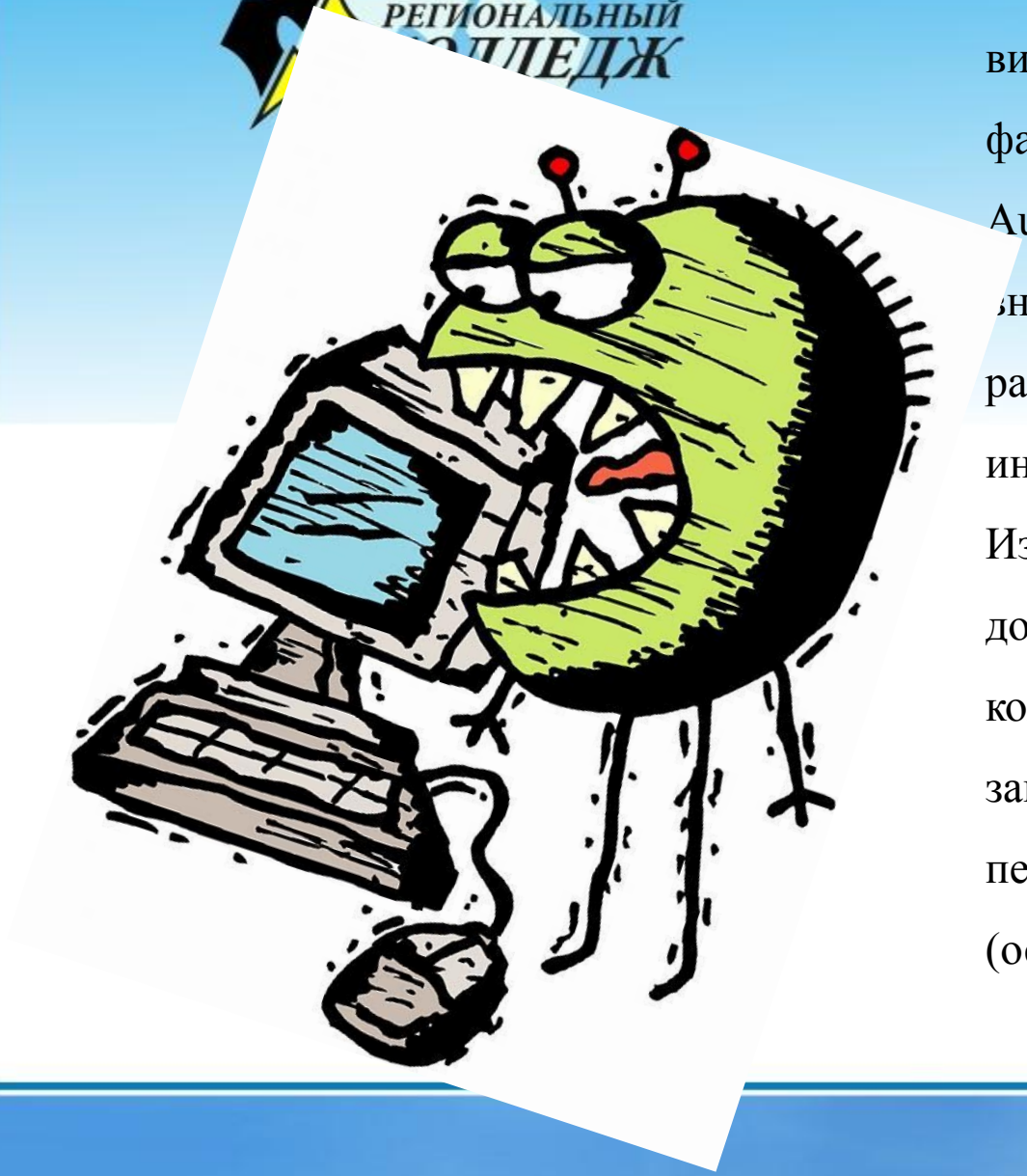
УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Наиболее распространенные современные вирусы и вредоносные программы Internet-черви Самым распространённым типом вирусов в последние два года являются Интернет – черви. Именно они представляют главную угрозу для всех пользователей глобальной сети. Почти все Интернет черви - это почтовые черви, и лишь малая доля - это не почтовые черви, применяющие уязвимости программного обеспечения (как правило, серверного). Примеры не почтовых Интернет – червей: IIS-Worm, CodeRed, , CodeBlue и др. Почтовые черви можно делить на подклассы по-разному, но для конечного пользователя они делятся на два основных класса: 1. Черви, которые запускаются сами (без ведома пользователя); 2. Черви, которые активизируются, только если пользователь сохранит присоединённый к письму файл и запустит его. К первому типу относятся черви, которые используют уязвимости (ошибки) почтовых клиентов. Чаще всего такие ошибки находятся в почтовом клиенте Outlook, а вернее даже не в нём, а в Интернет браузере Internet Explorer. Дело в том, что Outlook создаёт письмо в виде HTML страницы и при отображении этих страниц он использует функции браузера Internet Explorer. Наиболее распространённая уязвимость, применяемая червями, ошибка IFRAME.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Почтовые черви второго типа рассчитаны на то, что пользователь, по каким то соображениям сам запустит программу, присоединённую к письму. Для того чтобы подтолкнуть пользователя к запуску инфицированного файла авторами червей применяются различные психологические ходы. Самый распространённый приём - выдать зараженный файл, за какой то важный документ, картинку или полезную программку создаёт ответы на письма, содержащиеся в почтовой базе. Практически всегда червями применяются “двойные расширения”. Данный принцип рассчитан на то, что почтовые клиенты не отображают полное имя файла (если оно слишком длинное), и пользователь не увидит второго расширения, которое и является “реальным”. То есть пользователь думает, что файл является документом или картинкой, а тот на самом деле является исполняемым файлом с расширением вроде: EXE, COM, PIF, SCR, BAT, CMD и т.п.

Если такой файл “открыть”, то тело червя активизируется. Кроме основной функции, размножения, черви почти всегда несут в себе и боевую нагрузку. Действительно, зачем писать червя и выпускать его “в свет”, предварительно не заложив бомбу. Вложенные функции чрезвычайно разнообразны. Так, например, очень часто почтовые черви призваны для того, чтобы установить на зараженный компьютер троянскую программу или утилиту скрытого администрирования и сообщить адрес компьютера творцу червя. Не редко просто уничтожают информацию или просто делают невозможной дальнейшую работу на компьютере. Так червь I–Worm.Magistr выполнял те же действия, что и печально-известный WinCIH - стирал содержимое FLASH BIOS и затирал мусорными данными информацию на жёстком диске. В любом случае, независимо от наличия или отсутствия вредоносных функций и их “опасности” почтовые черви вредны уже только потому, что они существуют. Это связано с тем, что при размножении они загружают каналы связи и нередко настолько, что полностью парализуют работу человека или целой организации.

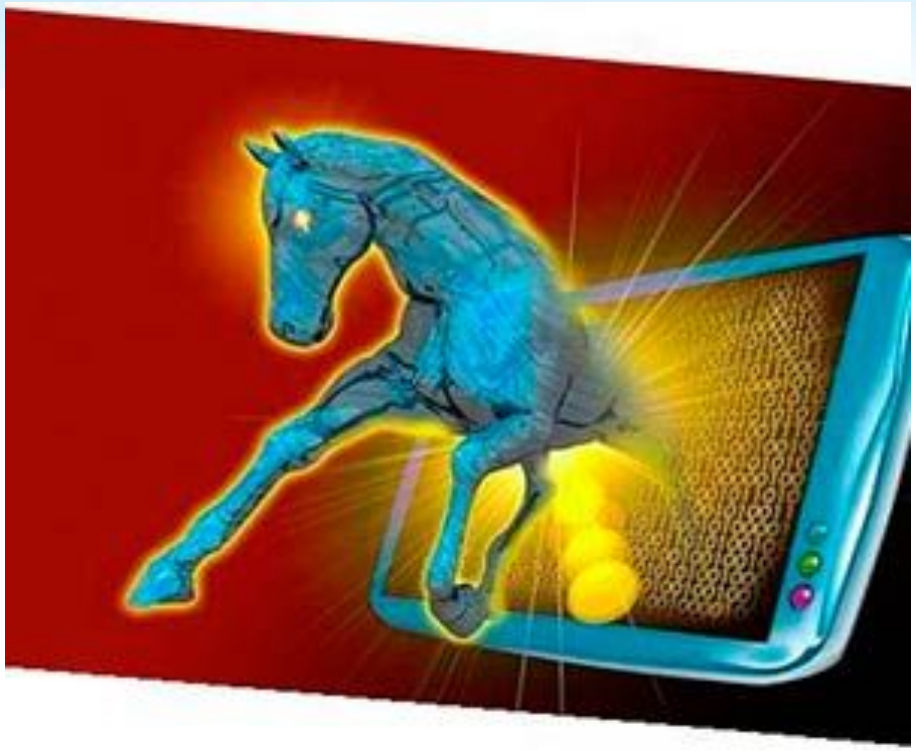


Макро-Вирусы

Вторыми по распространённости в диком виде являются макро-вирусы. Данные вирусы являются макросами, хранящимися во внешних файлах программного обеспечения (документах Microsoft Office, AutoCAD, CorelDRAW и пр.) и при открытии документа исполняются внутренними интерпретаторами данных программ. Широкое распространение они получили благодаря огромным возможностям интерпретатора языка Visual Basic, интегрированного в Microsoft Office. Излюбленным местом обитания этих вирусов являются офисы с большим документооборотом. В таких организациях людям, работающим за компьютерами (секретари, бухгалтеры, операторы ЭВМ) некогда заниматься такими мелочами как компьютерные вирусы. Документы лихо переносятся с компьютера на компьютер, без какого либо контроля (особенно при наличии локальной сети).

К сожалению, людям свойственно не воспринимать всерьёз макровирусы, а напрасно. На самом деле макрос, написанный на языке VBA и интегрированный в документ того же Word или Excel, обладает всеми теми же возможностями, что и обычное приложение. Он может отформатировать Ваш винчестер или просто удалить информацию, украсть какие то файлы или пароли и отправить их по электронной почте. Фактически вирусы этого класса способны парализовать работу целого офиса, а то даже и не одного. Опасность макровирусов заключается ещё и в том, что распространяется вирус целиком в исходном тексте. Если человек, к которому попал вирус, более-менее умеет писать на Visual Basic, то он без труда сможет модифицировать вирус, вложить в него свои функции и сделать его невидимым для антивирусов. Не забывайте, что авторы вирусов пользуются теми же антивирусными программами и модифицируют свои вирусы до тех пор, пока те не перестают детектироваться антивирусами. Фактически, таким образом, рождаются новые модификации уже известных вирусов, но для того, чтобы данный вирус обнаруживался антивирусом, он сначала должен попасть в антивирусную лабораторию и только после этого будут добавлены функции детектирования и обезвреживания новой модификации.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ



Троинские программы и утилиты скрытого администрирования. Следующими по распространённости являются Troian и Backdoor программы. Отличие этих двух типов программ заключается в том, что троянская программа выполняет активные действия (уничтожение данных, сбор данных и отправка через Internet, выполнение каких либо действий в определённое время), в то время как Backdoor программы открывают удалённый доступ к компьютеру и ожидают команды злоумышленника. Для простоты будем называть оба этих класса троянскими программами. Главное отличие “троянов” от всех перечисленных выше творений человеческого разума является то, что троянские программы не размножаются сами. Они единоразово устанавливаются на компьютер и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы, по какой либо причине) выполняет свои функции. При этом троянский конь не может самостоятельно переместиться с одного компьютера в локальной сети на другой.

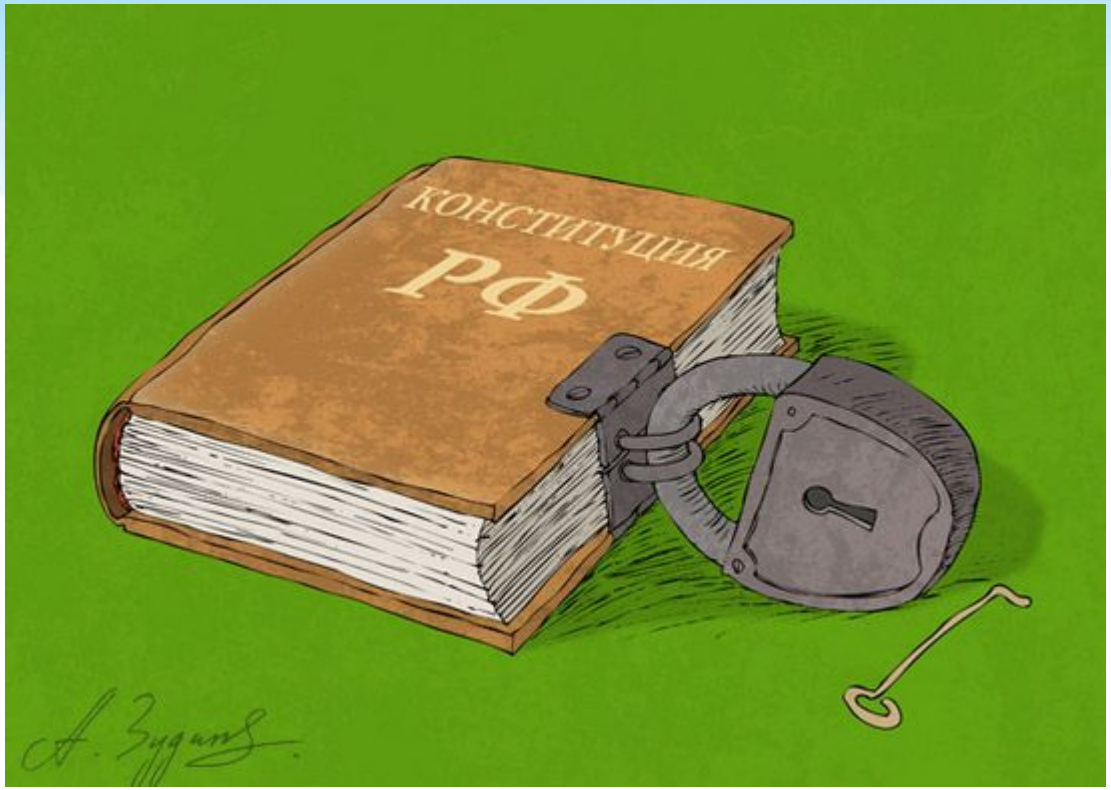
Все троянекие программы можно разделить на три основных класса по выполняемым действиям: 1. Логические (временные) бомбы - программы, различными методами удаляющие/модифицирующие информацию в определённое время, либо по какому то условию. 2. Шпионы - собирающие информацию (имена, пароли, нажатия на клавиши) и складирующие её определённым образом, а нередко и отправляющие собранные данные по электронной почте или другим методом. 3. Собственно backdoor программы - удалённое управление компьютером или получение команд от злоумышленника (через локальную/глобальную сеть, по электронной почте, в файлах, от других приложений, например тех же червей или вирусов). Одинаково опасны все три типа программ. Каждый из них способен либо уничтожить данные, либо украсть ценную информацию (хотя бы те же имена и пароли доступа к различным ресурсам). Стоит отметить, что многие троянские программы постоянно обновляются, выходят всё новые и новые модификации.

Учитывая то, что троянская программа не может попасть к вам случайно, злоумышленник старательно выбирает: какой бы Троян вам установить. Очень велика вероятность того, что он пойдёт в Интернет и выкачает что-то свеженькое. Именно поэтому необходимо регулярно обновлять базы антивирусного продукта. Так обновления для системы антивирусной защиты “Украинский Национальный Антивирус” (УНА) выходят каждый день, и если вы активно пользуетесь Интернетом, рекомендуем обновлять антивирус минимум раз в неделю (хотя конечно идеально было бы обновляться каждый день). В завершение хотелось бы сказать: процесс развития вирусов и антивирусов - это постоянная война технологий. Регулярно в вирусах реализовываются оригинальные идеи, что требует адекватных действий от разработчиков антивирусного ПО. Поэтому рядовому пользователю рекомендуется следить за новостями на сайтах антивирусных компаний и прислушиваться к советам специалистов по информационной безопасности о необходимости обновления программного обеспечения (не только антивирусного) или выполнении специфических действий по улучшению защищённости ПК.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Защита информации

Проникая во все сферы деятельности общества и государства, информация приобретает конкретные политические, материальные и стоимостные выражения. С учетом усиления роли информации на современном этапе, правовое регулирование общественных отношений, возникающих в информационной сфере, является приоритетным направлением процесса нормотворчества в Российской Федерации (РФ), целью которого является обеспечение информационной безопасности государства.



Конституция РФ является основным источником права в области обеспечения информационной безопасности в России.

Согласно Конституции РФ:

- каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);
- сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);
- каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);
- каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;
- необходимый уровень безопасности информации, подлежащей защите;
- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи информации).

Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации включают:

- Законы Российской Федерации
- Указы Президента Российской Федерации и утверждаемые этими указами нормативные документы
- Постановления Правительства Российской Федерации и утверждаемые этими постановлениями нормативные документы (Положения, Перечни …)
- Государственные и отраслевые стандарты
- Положения, Порядки. Руководящие документы и другие нормативные и методические документы уполномоченных государственных органов (Гостехкомиссии России, ФАПСИ, ФСБ).

Федеральные законы и другие нормативные акты предусматривают:

• разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется на:

отнесенную к государственной тайне

отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн)

и другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

• правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:

• в отношении сведений, отнесенных к государственной тайне, -уполномоченными государственными органами на основании Закона Российской Федерации "О государственной тайне" (от 21.07.93 г. N 5485-1);

• в отношении конфиденциальной документированной информации -собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации "Об информации, информатизации и защите информации" (от 20.02.95 г. N 24-ФЗ);

• в отношении персональных данных - отдельным федеральным законом;

• лицензирование деятельности предприятий, учреждений и организаций в области защиты информации;

• аттестование автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);

• сертификацию средств защиты информации и средств контроля эффективности защиты, используемых в АС;

• возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;

• создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;

• определение прав и обязанностей субъектов в области защиты информации.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

Государственная система защиты информации

Структура и основные функции государственной системы защиты информации от ее утечки по техническим каналам и организация работ по защите информации определены в "Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам", утвержденном Постановлением Правительства от 15 сентября 1993 г. № 912-51.

Этим Положением предусматривается, что мероприятия по защите информации, обрабатываемой техническими средствами, являются составной частью управленческой, научной и производственной деятельности учреждений и предприятий и осуществляются во взаимосвязи с другими мерами по обеспечению установленного федеральными законами "Об информации, информатизации и защите информации" и "О государственной тайне" комплекса мер по защите сведений, составляющих государственную и служебную тайну.

В то же время эти мероприятия являются составной частью работ по созданию и эксплуатации систем информатизации учреждений и предприятий, располагающих такой информацией, и должны осуществляться в установленном нормативными документами » порядке в виде системы защиты секретной информации.

Основные задачи государственной системы защиты информации:

• проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

• исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных специальных программно-технических воздействий на информацию с целью ее разрушения, уничтожения, искажения или блокирования в процессе обработки, передачи и хранения;

• принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;

• общая организация сил, создание средств защиты информации и средств контроля эффективности ее защиты;

• контроль за проведением работ по защите информации в органах государственного управления, объединениях, на предприятиях, в организациях и учреждениях (независимо от форм собственности).

Лицензирование

Законодательство Российской Федерации предусматривает установление Правительством РФ порядка ведения лицензионной деятельности, перечня видов деятельности, на осуществление которых требуется лицензия, и органов, уполномоченных на ведение лицензионной деятельности.

Деятельность в области защиты информации регулируются совместным решением Гостехкомиссии России и ФАПСИ от 27 апреля 1994 № 10, которым утверждено и введено в действие с 1 июня 1994 г. "Положение о государственном лицензировании деятельности в области защиты информации", а также закреплены за ними конкретные виды деятельности и области защиты

ие 1 к данному Положению).

Сертификация средств защиты

Сертификация — это комплекс действий, проводимых с целью подтверждения соответствия определенным нормам ГОСТ и других нормативных документов.

Конкретные средства и меры защиты информации должны разрабатываться и применяться в зависимости от уровня конфиденциальности и ценности информации, а также от уровня возможного ущерба в случае ее утечки, уничтожения, модификации или блокирования.

В настоящее время в Госстандарте России зарегистрированы три системы сертификации средств защиты:

• (Гостехкомиссия России) система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU . ООО 1. О 1БИ ОО ;

• (ФАПСИ) система сертификации средств криптографической защиты информации (система сертификации СКЗИ) №РОСС RU .0001.030001;

• (ФСБ) система обязательной сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ - ГТ) №РОСС RU .0001.

УРАЛЬСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ

СПАСИБО ЗА ВНИМАНИЕ!