ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 201_ г.

Автор: преподаватель 27 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 15

Тема: «ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
протокол № __ «____» _____ 201_ г.

Санкт-Петербург
201_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Уровни защиты от компьютерных вирусов – 40 мин.
2. Общая характеристика сертифицированных антивирусных средств – 40 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания о вредоносно ПО.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на используемых в ВС РФ сертифицированных антивирусных средствах.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите уровни защиты от компьютерных вирусов?
2. Охарактеризуйте жизненный цикл вируса?
3. Перечислите используемые в ВС РФ антивирусные средства?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 13

Тема 15. Организация антивирусной защиты.

В.1. Уровни защиты от компьютерных вирусов.

Подсистема защиты от компьютерных вирусов является одним из основных компонентов системы защиты информации и процесса ее обработки в вычислительных системах.

Для высокой эффективности подсистема антивирусной защиты должна иметь многоуровневую структуру. При этом можно выделить следующие уровни защиты от компьютерных вирусов:

1) уровень защиты от проникновения в ВС вирусов известных типов;
2) уровень контроля эталонного состояния компьютерной системы;
3) уровень защиты от деструктивных действий и размножения вирусов.

Каждый из данных уровней реализуется путем комплексного использования организационных и программно-аппаратных средств.

Первый уровень защиты обеспечивает препятствие доступу в ВС вирусов известных типов. Основой реализации данного уровня является поиск и обезвреживание вирусов в компьютерной системе, а также во всех программах, поступающих в компьютерную систему извне. Обнаружение и обезвреживание вирусов осуществляется на основе поиска кодовых последовательностей (сигнатур), характерных для вирусов известных типов.

для непосредственной защиты от проникновения вирусов известных типов используют антивирусные программные средства, называемые **сканерами**. Их синонимы - детекторы-дезинфекторы, полидетекторы-полифаги. Они ориентированы на обнаружение фиксированного набора вирусов, количество которых повышается при переходе к более новым версиям этих антивирусных программ. Кроме того, сканеры позволяют восстанавливать зараженные файлы и загрузчики, а при невозможности восстановления файлов обеспечивают их уничтожение.

Существуют следующие **виды программ-сканеров**:

- транзитные, которые загружаются в оперативную память только для поиска и обезвреживания вирусов;
- резидентные, которые после запуска остаются в оперативной памяти резидентно и проверяют программные файлы при возникновении с ними определенных событий (запуск, копирование, создание, переименование).

Наибольшая результативность достигается при совместном использовании транзитного и резидентного сканеров, когда обеспечивается не только периодический поиск и обезвреживание вирусов на дисковом пространстве и в оперативной памяти, но и контроль на наличие вирусов в программах, к которым происходит обращение.

Второй уровень защиты обеспечивает обнаружение в ВС системе вирусов, которым удалось обойти первый уровень защиты. Это в основном касается вирусов незнакомых типов, для которых неизвестны характерные им кодовые последовательности (сигнатуры). Поиск вирусов на данном уровне осуществляется путем сравнения текущих характеристик элементов ВС системы с эталонными характеристиками, соответствующими их незараженному состоянию.

Для этого используют антивирусные программные средства, называемые ревизорами (эвристическими анализаторами). В зависимости от возможностей ревизора могут использоваться следующие виды периодических проверок:

- периодическая разовая (например, ежедневная или еженедельная), при которой после запуска ревизора проверяются все элементы компьютера, для которых созданы эталонные характеристики;
- в режиме реального времени, при которой осуществляется проверка контролируемых элементов только при попытке их использования, например, при попытке запуска программ.

Как и сканеры, ревизоры можно ***разделить на следующие виды***:

- транзитные, которые загружаются в оперативную память только для поиска и

обезвреживания вирусов;

• резидентные, которые после запуска остаются в оперативной памяти резидентно и проверяют контролируемые элементы компьютера при возникновении с ними определенных событий (запуск и модификация программ, копирование, создание, переименование программных файлов);

Наибольшая результативность антивирусной защиты *достигается* при ***совместном использовании*** транзитного и резидентного ревизоров, когда осуществляется не только периодический разовый поиск неизвестных вирусов, но и динамический контроль на наличие неизвестных вирусов в программах, к которым происходит обращение.

Третий уровень защиты обеспечивает защиту от деструктивных действий и размножения вирусов, которым удалось преодолеть первые два уровня. На данном уровне должно быть обеспечено блокирование всех действий вирусов, связанных с их саморазмножением и нанесением ущерба. Такое блокирование реализуется на основе перехвата характерных для вирусов функций (модификация программ и т.д.) с помощью использования встроенных аппаратных возможностей компьютера, а также специальных антивирусных программ, называемых фильтрами (мониторами или поведенческими анализаторами).

Фильтры являются резидентными программами и после своего запуска постоянно находятся в оперативной памяти компьютера, перехватывая все попытки выполнения контролируемых ими действий. Перехват попыток выполнения контролируемых действий реализуется фильтром за счет перехвата соответствующих прерываний процессора. К **действия**м, которые могут контролировать большинство **фильтров**, относятся следующие:

• модификация загрузочных секторов винчестера;
• модификация загрузочных секторов гибких дисков;
• изменение файлового атрибута «только чтение»;
• модификация программных файлов;
• оставление в оперативной памяти резидентной программы.

В. 2. Общая характеристика сертифицированных антивирусных программ.

Антивирус - программное средство, предназначенное для борьбы с вирусами.

Как следует из определения, основными задачами антивируса является:

- Препятствование проникновению вирусов в компьютерную систему
- Обнаружение наличия вирусов в компьютерной системе
- Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы
- Минимизация ущерба от действий вирусов

Технологии обнаружения вирусов

Технологии, применяемые в антивирусах, можно разбить на две группы -

- Технологии сигнатурного анализа
- Технологии вероятностного анализа

Сигнатурный анализ - метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур вирусов.

Сигнатурный анализ является наиболее известным методом обнаружения вирусов и используется практически во всех современных антивирусах. Для проведения проверки антивирусу необходим набор вирусных сигнатур, который хранится в антивирусной базе.

Антивирусная база - база данных, в которой хранятся сигнатуры вирусов.

Ввиду того, что сигнатурный анализ предполагает проверку файлов на наличие сигнатур вирусов, антивирусная база нуждается в периодическом обновлении для поддержания актуальности антивируса. Сам принцип работы сигнатурного анализа также определяет границы его функциональности - возможность обнаруживать лишь уже известные вирусы - против новых вирусов сигнатурный сканер бессилен.

С другой стороны, наличие сигнатур вирусов предполагает возможность лечения инфицированных файлов, обнаруженных при помощи сигнатурного анализа. Однако, лечение

допустимо не для всех вирусов - трояны и большинство червей не поддаются лечению по своим конструктивным особенностям, поскольку являются цельными модулями, созданными для нанесения ущерба.

Грамотная реализация вирусной сигнатуры позволяет обнаруживать известные вирусы со стопроцентной вероятностью.

Технологии вероятностного анализа в свою очередь подразделяются на три категории:

- Эвристический анализ
- Поведенческий анализ
- Анализ контрольных сумм

Эвристический анализ - технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов.

В процессе эвристического анализа проверяется структура файла, его соответствие вирусным шаблонам. Наиболее популярной эвристической технологией является проверка содержимого файла на предмет наличия модификаций уже известных сигнатур вирусов и их комбинаций. Это помогает определять гибриды и новые версии ранее известных вирусов без дополнительного обновления антивирусной базы.

Эвристический анализ применяется для обнаружения неизвестных вирусов, и, как следствие, не предполагает лечения.

Данная технология не способна на 100% определить вирус перед ней или нет, и как любой вероятностный алгоритм грешит ложными срабатываниями.

Поведенческий анализ - технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций.

Поведенческий анализ весьма узко применим на практике, так как большинство действий, характерных для вирусов, могут выполняться и обычными приложениями. Наибольшую известность получили поведенческие анализаторы скриптов и макросов, поскольку соответствующие вирусы практически всегда выполняют ряд однотипных действий. Например, для внедрения в систему, почти каждый макровирус использует один и тот же алгоритм: в какой-нибудь стандартный макрос, автоматически запускаемый средой Microsoft Office при выполнении стандартных команд (например, "Save", "Save As", "Open", и т.д.), записывается код, заражающий основной файл шаблонов normal.dot и каждый вновь открываемый документ.

Средства защиты, вшиваемые в BIOS, также можно отнести к поведенческим анализаторам. При попытке внести изменения в MBR компьютера, анализатор блокирует действие и выводит соответствующее уведомление пользователю.

Помимо этого поведенческие анализаторы могут отслеживать попытки прямого доступа к файлам, внесение изменений в загрузочную запись дискет, форматирование жестких дисков и т. д.

Поведенческие анализаторы не используют для работы дополнительных объектов, подобных вирусным базам и, как следствие, неспособны различать известные и неизвестные вирусы - все подозрительные программы априори считаются неизвестными вирусами. Аналогично, особенности работы средств, реализующих технологии поведенческого анализа, не предполагают лечения.

Как и в предыдущем случае, возможно выделение действий, однозначно трактующихся как неправомерные - форматирование жестких дисков без запроса, удаление всех данных с логического диска, изменение загрузочной записи дискеты без соответствующих уведомлений и пр. Тем не менее, наличие действий неоднозначных - например, макрокоманда создания каталога на жестком диске, заставляет также задумываться о ложных срабатываниях и, зачастую, о тонкой ручной настройке поведенческого блокиратора.

Анализ контрольных сумм - это способ отслеживания изменений в объектах компьютерной системы. На основании анализа характера изменений - одновременность, массовость, идентичные изменения длин файлов - можно делать вывод о заражении системы.

Анализаторы контрольных сумм (также используется название "*ревизоры изменений*") как и поведенческие анализаторы не используют в работе дополнительные объекты и выдают вердикт о наличии вируса в системе исключительно методом экспертной оценки. Большая популярность

анализа контрольных сумм связана с воспоминаниями об однозадачных операционных системах, когда количество вирусов было относительно небольшим, файлов было немного и менялись они редко. Сегодня ревизоры изменений утратили свои позиции и используются в антивирусах достаточно редко. Чаще подобные технологии применяются в сканерах при доступе - при первой проверке с файла снимается контрольная сумма и помещается в кэше, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

Подводя итоги обзора технологий, применяемых в антивирусах, отметим, что сегодня практически каждый антивирус использует несколько из перечисленных выше технологий, при этом использование сигнатурного и эвристического анализа для проверки файлов и именно в этом порядке является повсеместным. В дальнейшем средства, реализующие комбинацию сигнатурного и эвристического анализа, мы будем называть антивирусными сканерами.

Вторая группа технологий более разнородна, поскольку ни один из применяемых подходов не дает гарантии обнаружения неизвестных вирусов. Очевидно, что и совместное использование всех этих технологий не дает такой гарантии.

ВЫВОД: На сегодняшний день лучшим способом борьбы с новыми угрозами является максимально быстрое реагирование разработчиков на появление новых экземпляров вирусов выпуском соответствующих сигнатур. Также, учитывая наличие активных вредоносных программ, необходимо не менее быстро реагировать на обнаружение новых уязвимостей в операционных системах и устанавливать соответствующие заплаты безопасности.

Режимы работы антивирусов

Помимо используемых технологий, антивирусы отличаются друг от друга условиями эксплуатации. Уже из анализа задач можно сделать вывод о том, что препятствование проникновению вредоносного кода должно осуществляться непрерывно, тогда как обнаружение вредоносного кода в существующей системе - скорее разовое мероприятие. Следовательно, средства, решающие эти две задачи должны функционировать по-разному.

Таким образом, антивирусы можно разделить на две большие категории:

- **Предназначенные для непрерывной работы** - к этой категории относятся средства проверки при доступе, почтовые фильтры, системы сканирования проходящего трафика Интернет, другие средства, сканирующие потоки данных
- **Предназначенные для периодического запуска** - различного рода средства проверки по запросу, предназначенные для однократного сканирования определенных объектов. К таким средствам можно отнести сканер по требованию файловой системы в антивирусном комплексе для рабочей станции, сканер по требованию почтовых ящиков и общих папок в антивирусном комплексе для почтовой системы (в частности, для Microsoft Exchange)

Как показывает практика, предотвратить возникновение проблемы гораздо проще, чем пытаться впоследствии ее решить. Именно поэтому современные антивирусные комплексы в большинстве своем подразумевают непрерывный режим эксплуатации. Тем не менее, средства периодической проверки гораздо эффективнее при борьбе с последствиями заражения и поэтому не менее необходимы.

Антивирусный комплекс

Антивирусное ядро - реализация механизма сигнатурного сканирования и эвристического анализа на основе имеющихся сигнатур вирусов.

Антивирусный комплекс - набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

Помимо этого антивирусный комплекс дополнительно может включать в себя поведенческие анализаторы и ревизоры изменений, которые вовсе не используют антивирусное ядро.

В качестве вспомогательной утилиты антивирусный комплекс может содержать (и на практике обычно содержит) планировщик заданий.

Исходя из текущей необходимости в средствах защиты выделяют следующие **типы**

антивирусных комплексов:

1. Антивирусный комплекс для защиты рабочих станций
2. Антивирусный комплекс для защиты файловых серверов
3. Антивирусный комплекс для защиты почтовых систем
4. Антивирусный комплекс для защиты шлюзов

Имеют сертификат ФСТЭК России следующие антивирусные средства:

1. Dr. Web Enterprise Security Suite версии 10;
2. ESET NOD32 Secure Enterprise Pack 5.0;
3. Kaspersky Security Center 10.

Наиболее надежная защита от компьютерных вирусов может быть обеспечена только в том случае, если проверка на их наличие производится во всех точках доступа в сеть предприятия. Поскольку МЭ с точки зрения прохождения сетевого трафика обеспечивает единую точку входа (выхода) в сеть, то целесообразно возложить на него также и функции антивирусной защиты [13].

Межсетевой экран, поддерживающий протокол перенаправления содержания CVP, выступает как клиент сервера CVP. На сервере CVP осуществляется обработка информационных потоков (в данном случае – обнаружение вирусов), поступающих от клиента.

При обнаружении вируса антивирусный сервер производит его удаление либо осуществляет другие необходимые действия. Результат обработки возвращается обратно МЭ.

Например, организации необходимо обеспечить проверку всех вложений электронной почты на наличие компьютерных вирусов. Это легко обеспечить, проводя проверку почты проходящей через шлюз с FireWall-1. В этом случае FireWall-1 перехватит все потоки данных, отвечающие соответствующим правилам политики безопасности и, используя протокол перенаправления содержания (CVP), перенаправит их на сервер антивирусной проверки. Прежде, чем вернуть полученные данные, сервер антивирусной проверки выполнит необходимые действия по сканированию вложений почты на наличие в них вирусов и лечению зараженных данных. Получив данные обратно, FireWall-1 отправляет их получателю. Таким образом, ни одно соединение не будет организованно напрямую без соответствующей проверки.

Антивирусный сервер для повышения производительности может быть расположен как на отдельно выделенном компьютере, так и на компьютере с МЭ. Благодаря такому подходу, администратор информационной безопасности предприятия может легко реализовать оптимальную схему борьбы с компьютерными вирусами, быстро развернуть ее и администрировать весь комплекс из общего центра управления.

Вместо настройки двух совершенно независимых программных продуктов, администратор безопасности определяет правила разграничения доступа и правила проверки информационных потоков в общей политике безопасности, посредством ее редактора (FireWall-1 Security Policy Editor).

По умолчанию для сервера CVP выделяется транспортный порт TCP 18181. Протокол CVP поддерживают такие хорошо зарекомендовавшие себя антивирусные программы, как AVP for Fire Wall (лаборатория Касперского), Norton AntiVirus for Fire Wall (Symantec).

Некоторые производители МЭ ранее включали в состав своих продуктов антивирусные средства. Однако из-за сложности поддержки антивирусных баз самими производителями МЭ такие решения быстро «умирали». Следует обратить внимание на совместимость МЭ и CVP-сервера.

Сравнение антивирусных комплексов

Сравнивать антивирусы - сложнейшее и неблагодарнейшее дело. Уйма подобных материалов публиковалась в одной только "Компьютерре-Онлайн", не говоря уж о других изданиях, и каждый раз выходит, что автор что-то упустил, что-то интерпретировал неверно и вызвал гнев читателей или даже работников антивирусных компаний. В конце концов, некоторые аспекты работы антивирусных программ просто невозможно оценить без дополнительных средств.

В тестах проведённых ведущими независимыми антивирусными лабораториями (AV-Test, AV-Comparatives, Dennis Technology Labs, Virus Bulletin) было выявлено три лучших антивируса:

1. Kaspersky Internet Security 2015
   - AV-Test – Защита 6/6, Производительность 6/6, Удобство 6/6;
   - AV-Comparatives – три звезды (Advanced +) во всех пройденных тестах

(обнаружение, удаление, проактивная защита и др.);
- Dennis Technology Labs – 100% во всех тестах (обнаружение, отсутствие ложных срабатываний);
- Virus Bulletin – пройдено, без ложных срабатываний (RAP 75-90%).

2. Bitdefender Internet Security 2015
   - AV-Test – Защита 6/6, Производительность 6/6, Удобство 6/6;
   - AV-Comparatives - три звезды (Advanced +) во всех пройденных тестах (обнаружение, удаление, проактивная защита и др.);
   - Dennis Technology Labs – 92% защита, 98% точные срабатывания, общий рейтинг – 90%;
   - Virus Bulletin – пройдено (RAP 90-96%).
3. Qihoo 360 Internet Security (или 360 Total Security)
   - AV-Test – Защита 6/6, Производительность 6/6, Удобство 6/6;
   - AV-Comparatives - три звезды (Advanced +) во всех пройденных тестах (обнаружение, удаление, проактивная защита и др.);
   - Dennis Technology Labs – тест данного продукта отсутствует;
   - Virus Bulletin – пройдено (RAP 87-96%).

В. 3. Основные положения приказа № 40 Командующего КВ от 2004 г. по противодействию компьютерным вирусам на объектах ВТ КВ.

1. **Выполнение мероприятий по антивирусной защите** объектов вычислительной техники (ВТ) является неотъемлемой частью обеспечения безопасности информации (ОБИ) от несанкционированного доступа (НСД) и **имеет своей целью**:

а) предотвращение поражения объекта ВТ компьютерными вирусами;

б) выявление, локализацию компьютерных вирусов и их уничтожение;

в) оперативное и максимально полное восстановление работоспособности объекта ВТ и информации в случае деструктивного воздействия компьютерных вирусов;

г) анализ и локализацию возможных последствий воздействия компьютерных вирусов на объекты ВТ.

2. **Защита объектов ВТ** от поражения компьютерными вирусами **достигается:**

а) планированием и выполнением комплекса мероприятий по защите информации в соответствии с требованиями приказов Министра обороны Российской Федерации, директив и указаний Генерального штаба Вооруженных Сил Российской Федерации, командующего и штаба Космических войск, настоящей Инструкции;

б) применением средств защиты от поражения компьютерными вирусами, сертифицированных в Системе сертификации Министерства обороны Российской Федерации по требованиям безопасности информации, и их периодическим обновлением;

в) строгим соблюдением правил приема, ввода в эксплуатацию и эксплуатации на объекте ВТ общего и специального программного обеспечения, средств защиты информации от несанкционированного доступа;

г) подготовкой должностных лиц по вопросам применения средств антивирусной защиты;

д) своевременной ликвидацией последствий поражения компьютерными вирусами;

е) контролем соблюдения должностными лицами требований по защите информации от поражения компьютерными вирусами, своевременным устранением выявленных недостатков;

ж) проведением анализа эффективности применяемых мер и средств защиты от поражения компьютерными вирусами.

3. **Поставка сертифицированных средств** антивирусной защиты для объектов вычислительной техники (ВТ) Космических войск в соответствии с директивой Генерального

штаба Вооруженных Сил Российской Федерации 1997 года № ДГШ-06 **осуществляется Восьмым управлением** Генерального штаба.

5. Ипользование на объектах вычислительной техники Космических войск других (**несертифицированных**) антивирусных средств **запрещается***.

10. **Начальник объекта вычислительной техники** (объекта ВТ) несет непосредственную ответственность за организацию антивирусной защиты на подчиненном объекте ВТ.

Он **обязан**:

а) организовывать выполнение указаний необъектового органа ОБИ (службы ЗГТ) воинской части по вопросам обеспечения антивирусной защиты объекта;

б) знать и строго соблюдать установленные правила применения средств антивирусной защиты при организации работы на средствах вычислительной техники.

в) организовывать своевременное получение и установку обновленных версий антивирусных средств, а также докладывать о выполнении указанных мероприятий в необъектовый орган ОБИ (службу ЗГТ) воинской части.

г) требовать от подчиненных (пользователей средств ВТ) выполнения ими своих обязанностей в части применения средств антивирусной защиты.

12. **Объектовые органы ОБИ** (нештатные ответственные за ОБИ объекта ВТ), в соответствии с должностными обязанностями, инструкциями и документацией на антивирусные средства **осуществляют** получение, учет, заказ, хранение, инсталляцию, настройку и применение средств антивирусной защиты на объекте ВТ.

На них возлагается:

а) анализ защищенности объекта ВТ и информации от компьютерных вирусов, достаточности проводимых на объекте ВТ мероприятий по антивирусной защите информации, выработка предложений по их совершенствованию;

б) разработка проектов инструкций по защите информации от компьютерных вирусов на объекте вычислительной техники;

в) участие в проведении испытаний автоматизированных систем, средств вычислительной техники в части защиты информации от компьютерных вирусов;

г) применение антивирусных средств для предупреждения заражения, обнаружения и локализации распространения компьютерных вирусов на объекте ВТ;

д) участие в проведении расследований и экспертиз по фактам воздействия компьютерных вирусов на средства ВТ, создавшим предпосылки или приведшим к искажению, уничтожению информации, сбою в работе средств ВТ.

13. **Непосредственная ответственность за защиту средств ВТ** и информации от воздействия компьютерных вирусов **возлагается на** назначенных приказом командира воинской части **лиц, ответственных за эксплуатацию средств вычислительной техники** и программного обеспечения.

15. **Пользователи и должностные лица объекта ВТ обязаны** докладывать по команде обо всех фактах вывода из строя средств ВТ и уничтожения информации компьютерными вирусами.

16. До личного состава, связанного с применением и эксплуатацией вычислительной техники, **ежегодно** доводятся **под роспись статьи 272-274 УК РФ** об ответственности за преступления в сфере компьютерной информации.

21. Полученные на объект ВТ **средства антивирусной защиты устанавливаются** на средства ВТ **в срок не более пяти дней** со дня их получения. Установка средств антивирусной защиты производится на всех эксплуатируемых в воинской части объектах ВТ, на которых антивирусная защита может быть осуществлена с использованием поставляемых средств, независимо от их категории и степени секретности обрабатываемой на них информации.*

24. **На** программные **средства защиты от компьютерных вирусов** на каждом объекте ВТ **ведется паспорт** в порядке, установленном в Руководстве по ОБИ от НСД на объектах ВТ, введенном в действие приказом министра обороны 1990 года № 0215. В паспортах производится запись о каждой переустановке средств антивирусной защиты на объекте ВТ.

Порядок проверки носителей информации и программного обеспечения на наличие компьютерных вирусов:

- ответственным за ОБИ объекта ВТ (объектовым органом ОБИ) – **еженедельно**, а также при вводе в эксплуатацию (инсталляции) новых программных средств;
- пользователями ПЭВМ (АРМ ЛВС) – **ежедневно** перед началом работы и после ее окончания, **а также перед операциями копирования** (перемещения) **информации** (данных), связанными с использованием гибких магнитных, оптических, магнитооптических дисков и других машинных носителей информации.

28. Все поступающие в воинские части машинные носители информации с записанной информацией (программными средствами общего и специального назначения, информационными массивами) подлежат обязательной проверке на наличие компьютерных вирусов. О произведенной проверке и ее результатах делается отметка на сопроводительном письме пользователем, производившим проверку.

При обнаружении на поступивших в воинские части машинных носителях информации компьютерных вирусов пользователи докладывают об этом в объектовый орган ОБИ (нештатному ответственному за ОБИ объекта ВТ) и принимают меры по восстановлению работоспособности программных средств и данных.

30. **По выявлению фактов заражения компьютерными вирусами осуществляются следующие мероприятия:**

а) прекращаются все работы, проводимые на объекте ВТ;

б) производится отключение ПЭВМ от вычислительной сети в случае ее функционирования в качестве рабочей станции;

в) принимаются меры по удалению компьютерных вирусов с помощью имеющихся средств антивирусной защиты;

г) проводится учет выявленных компьютерных вирусов с описанием последствий и примененных средств ликвидации последствий их действия;

д) проводится восстановление работоспособности программных средств и данных в случае их повреждения компьютерными вирусами.

32. По фактам обнаружения компьютерных вирусов, **ликвидацию которых** имеющимися средствами антивирусной защиты **осуществить невозможно**, докладывается по команде в службу ЗГТ Космических войск. Зараженные файлы или же носители информации представляются в Центр обеспечения ЗГТ Космических войск для последующего анализа.

33. **Отключать** установленные на объектах ВТ **средства антивирусной защиты запрещается.**

39. Контроль обеспечения антивирусной защиты на объектах ВТ Космических войск проводится:

службой ЗГТ воинской части – в ходе проведения проверок состояния режима секретности и обеспечения безопасности информации, но не реже 1 раза в учебный период (полугодие);

начальником объекта ВТ – ежемесячно;

ответственным за ОБИ (объектовым органом ОБИ) – еженедельно.