Лекция №9

С.А. Краснов

Организация антивирусной защиты

# Организация антивирусной защиты

Лекция №9.

Тема №3: Методы и средства и антивирусной защиты.

Тема лекции: Организация антивирусной защиты.

**Изучаемые вопросы:**

1. Уровни защиты от компьютерных вирусов.
2. Политика безопасности компьютерной системы. Характеристика антивирусных программ.

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

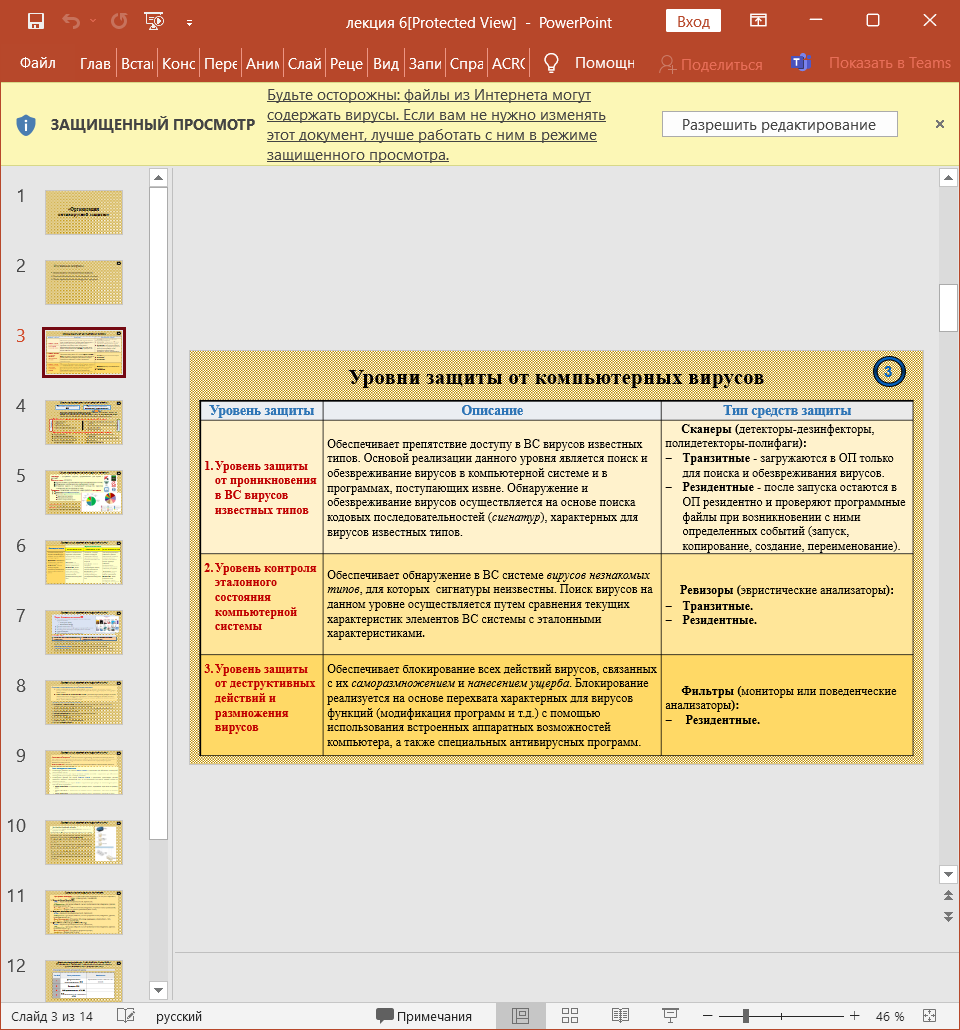


Рисунок 1

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 (кодовых последовательностей - сигнатур). Для непосредственной защиты от проникновения вирусов известных типов используют - *сканеры*. 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*.

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

**Второй уровень защиты** - обеспечивает обнаружение в ВС системе вирусов, которым удалось обойти 1 уровень защиты. Это в основном касается вирусов незнакомых типов, для которых неизвестны характерные им кодовые последовательности (сигнатуры). Поиск вирусов осуществляется путем сравнения текущих характеристик элементов ВС системы с эталонными характеристиками, соответствующими их незараженному состоянию.

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.

*Наибольшая результативность* *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. *Фильтры* являются **резидентными** программами и после своего запуска постоянно находятся в ОП, перехватывая все попытки выполнения контролируемых ими действий. Перехват попыток выполнения контролируемых действий реализуется фильтром за счет перехвата соответствующих прерываний процессора. К действиям, 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.

Политика безопасности компьютерной системы в отношении защиты от вредоносного ПО базируется на *двух основных принципах*:

* Должно инсталлироваться только то ПО, которое необходимо пользователям для выполнения служебных обязанностей. Остальные компоненты должны удаляться. Предпочтительней использовать нестандартное ПО, уязвимости которого изучены не так сильно.
* Пользователю предоставляются полномочия, минимально необходимые для выполнения служебных обязанностей. Каждый пользователь должен иметь свою учетную запись без прав администратора, особенно при выходе в интернет. В основе этого принципа лежит концепция **изолированной программной среды**.

В отличие от дискреционной модели доступа, в изолированной программной среде возможность доступа к объекту определяется не для тройки **пользователь-объект-право**, а для четверки **пользователь-объект-право-субъект**. *Пример:* доступ на запись к файлам *\*.exe* разрешен только компиляторам и запрещен другим программам. Кроме того, список программ, которые могут запускать пользователи, задается администратором для каждого из них и не может быть расширен самим пользователем.

Поддержание адекватной политики безопасности в изолированной программной среде требует от администратора безопасности значительно больших усилий, чем в условиях избирательно разграничения доступа. Ни одна из современных многопользовательских ОС не поддерживает систему правил *изолированной программной среды*. Таким образом, для предотвращения атак, необходимы дополнительные СЗИ. Сформулируем требования к таким СЗИ **(рисунок 2)**. Можно разделить на **типовые** требования к ПО и **специфичные** требования для данного типа ПО.

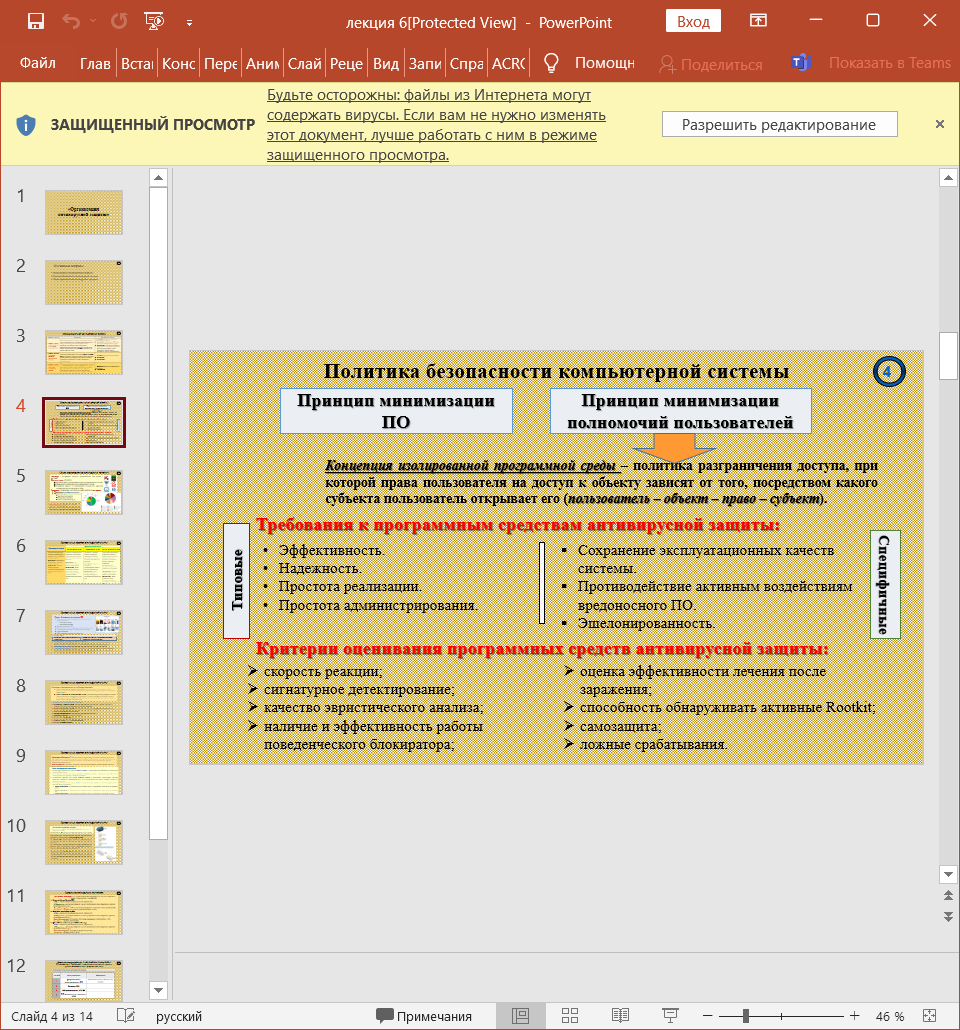


Рисунок 2

В настоящее время для борьбы с вредоносным ПО используют АВС. Технологии, применяемые в антивирусах, можно разбить на две группы:

* Технологии сигнатурного анализа.
* Технологии вероятностного анализа.

**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*, которая нуждается в периодическом обновлении.

Наличие сигнатур вирусов предполагает возможность лечения инфицированных файлов. 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. Большинство вирусов использует более-менее стандартные алгоритмы, что позволяет антивирусным сканерам использовать для построения сигнатур около *100 принципиально различных схем*. Для выявления специфичных вирусов используют сигнатуры, имеющие *особый формат* (или фрагмент кода), уникальный для данного вируса.

При **эвристическом анализе** – проверяется структура файла с целью обнаружения следов применения, специфичных для вирусописателей, приемов программирования (алгоритм вероятностный, поэтому грешит ошибками первого и второго рода).

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.

**Поведенческий анализ** - весьма узко применим на практике, так как большинство действий, характерных для вирусов, могут выполнять и обычные приложения. 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, 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.

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 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.

*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 ОС, когда количество вирусов было относительно небольшим, файлов было немного и менялись они редко. Сегодня ревизоры изменений 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.

На основании описанных технологий, в антивирусных средствах реализованы и успешно используются описанные методы.

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. Сегодня, для борьбы с вредоносным ПО используются следующие **методы обнаружения**:

Сканирование может быть *тотальным* – сканирование дисков через определенные промежутки времени или «*на лету*» - файл проверяется перед запуском.

*Контроль целостности ПО* – для каждого программного модуля в системе заранее подсчитываются длина и контрольная сумма. Эта информация хранится в файле, зашифрованном имитостойким шифром и подписанным ЭЦП. Периодически осуществляется проверка модулей с эталоном, либо тотальным сканированием, либо перед загрузкой модуля.

*Контроль целостности конфигурации защищаемой системы* – для всех элементов конфигурации создаются эталонные копии. Во многих ОС организуется с помощью стандартных средств аудита (для Widows – ключи реестра).

*Антивирусный мониторинг* – включает в себя технологию поведенческого анализа, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций:

* информационные потоки, связанные с паролями пользователей;
* информационные потоки, связанные с обращениями к файловым системам;
* информационные потоки, связанные с обращениями к сетевым ресурсам.

*Пример*: программа аутентификации пользователей работает только с файлами, содержащими эталоны паролей и настройки конфигурации самой программы. Если зафиксировано обращение к другому файлу, то в системе присутствует перехватчик паролей.

*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 ОС и устанавливать соответствующие заплаты безопасности.

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.

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 так же необходимы.

**Критерии качества антивирусных программ**:

* **Надежность** и **удобство работы** — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
* **Качество обнаружения вирусов** всех распространенных типов, **сканирование внутри** файлов-документов/таблиц (Word, Excel), упакованных и архивированных файлов.
* **Отсутствие «ложных срабатываний»**.
* **Многоплатформенность** антивирусного программного обеспечения.
* **Возможность лечения** зараженных объектов.
* Периодичность **обновления**.
* Существование **серверных версий** с возможностью проверки сетевых дисков.
* **Скорость работы** и другие **полезные функции**.

Различные **режимы защиты**.

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 – Состоит из средств непрерывной работы и предназначенных для периодического запуска, а также средств обновления антивирусных баз.

2. Антивирусный комплекс для защиты файловых серверов - Указание на файловый сервер в названии является скорее данью истории, корректней будет звучать термин «сетевой». Определение того, насколько нуждается в антивирусной защите сервер, осуществляется не только исходя из его назначения (является сервер файловым, почтовым, либо выполняет другую функцию), а и из используемой на нем платформы.

3. Антивирусный комплекс для защиты почтовых систем - Как уже указывалось ранее, сегодня одним из главных средств доставки вирусов в локальную сеть является именно электронная почта. Поэтому, при наличии в локальной сети специализированного узла, обрабатывающего входящую и исходящую из сети почтовую корреспонденцию (почтового сервера), логично будет использовать средство централизованной проверки всего почтового потока на наличие вирусов. При этом под *почтовым трафиком* понимается SMTP-поток*.* Антивирусные комплексы для защиты почтовых систем не проверяют данные, передаваемые по *протоколам IMAP и POP* при обращении пользователей к своим персональным внешним по отношению к организации ящикам, поскольку это - задача антивирусного комплекса для защиты рабочих станций*.*

4. Антивирусный комплекс для защиты шлюзов - предназначен для проверки на наличие вирусов данных, через этот шлюз передаваемых.

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 установить АВК после него или возложить на МЭ также и функции антивирусной защиты.

*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).

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.

*Сравнивать антивирусы* - сложнейшее и не благодарнейшее 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.

**Три лучших антивируса** ( по тестам независимых лабораторий AV-Test, AV-Comparatives, Dennis Technology Labs, Virus Bulletin):

1. **Kaspersky Internet 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* – 100% во всех тестах (обнаружение, отсутствие ложных срабатываний);

*Virus Bulletin* – пройдено, без ложных срабатываний (RAP 75-90%).

1. **Bitdefender Internet 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* – 92% защита, 98% точные срабатывания, общий рейтинг – 90%;

*Virus Bulletin* – пройдено (RAP 90-96%).

1. **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%).

Требования ФСТЭК к средствам антивирусной зашиты. Требования к средствам антивирусной защиты (САЗ) включают общие требования к средствам антивирусной защиты и требования к функциям безопасности средств антивирусной защиты.

Выделяются следующие **типы средств** антивирусной защиты:

1. *тип «А»* – средства антивирусной защиты (компоненты САЗ), предназначенные для централизованного администрирования средствами антивирусной защиты, установленными на компонентах информационных систем (серверах, АРМ);
2. *тип «Б»* – средства антивирусной защиты (компоненты САЗ), предназначенные для применения на серверах информационных систем;
3. *тип «В»* – средства антивирусной защиты (компоненты САЗ), предназначенные для применения на АРМ информационных систем;
4. *тип «Г»* – средства антивирусной защиты (компоненты САЗ), предназначенные для применения на автономных АРМ.

Для дифференциации требований к функциям безопасности средств антивирусной защиты установлено шесть **классов защиты** САЗ, с точки зрения защищаемой информации. Самый низкий класс – шестой, самый высокий – первый.

**Информационное сообщение № 240/24/3095 от 30 июля 2012 г. Об утверждении Требований к средствам антивирусной защиты (приказ ФСТЭК № 9 от 9 февраля 2016 года)**

Определяют классы классов защиты средств антивирусной защиты:

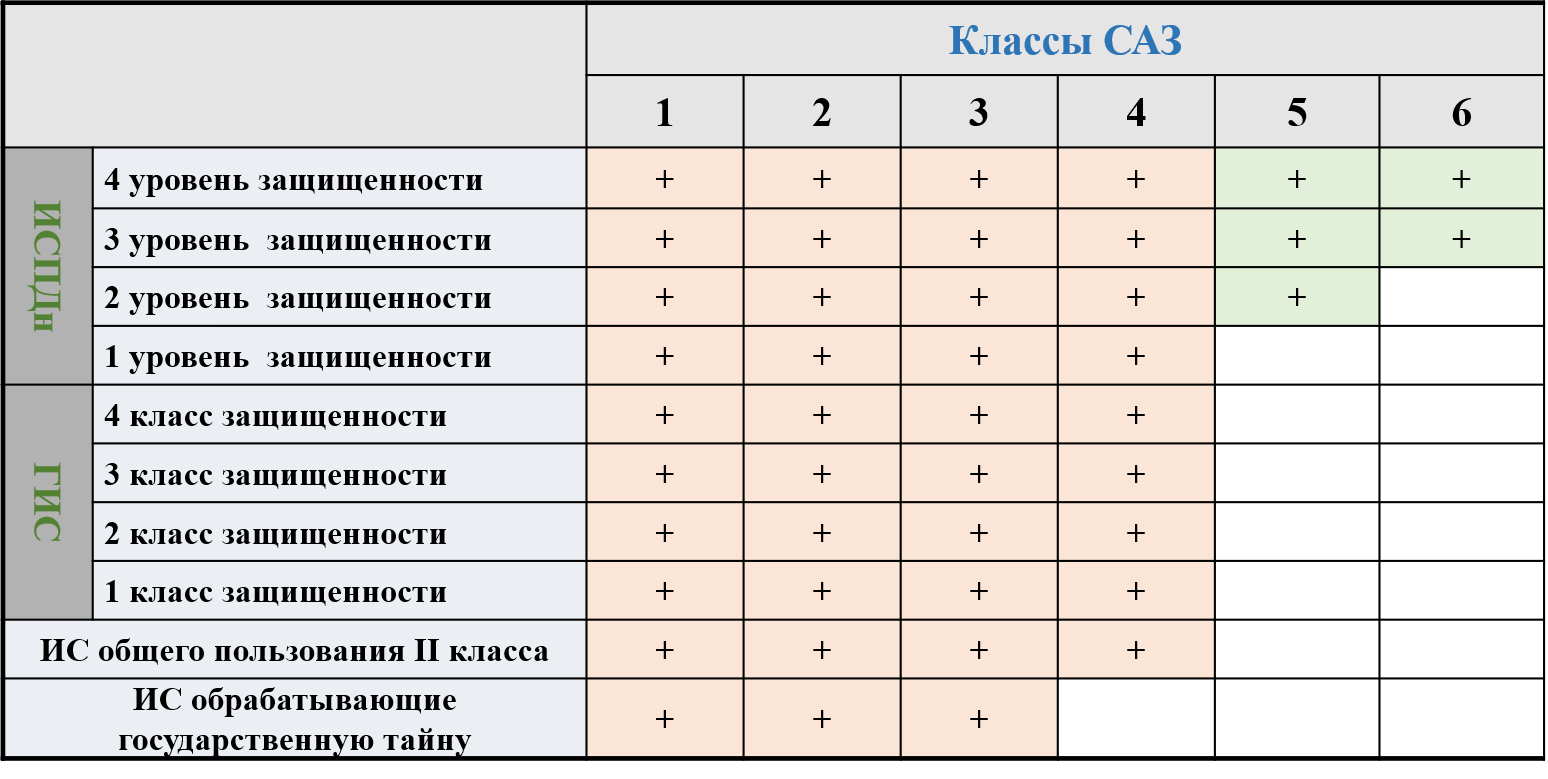


Рисунок 3

Вопросы:

1. Понятие компьютерного вируса. Основные особенности компьютерных вирусов.
2. Классическая классификация компьютерных вирусов.
3. Типы вредоносных программ по версиям ведущих антивирусных компаний («Dr.Web», «Лаборатория Касперского» и др.)
4. Краткая характеристика вредоносного ПО типа «логическая бомба», «люк», «троян».
5. Краткая характеристика вредоносного ПО типа «червь», «бактерия», «вирус».
6. Классификация программных закладок по способу несанкционированных действий.
7. Жизненный цикл вирусного ПО.
8. Перечислите уровни защиты от компьютерных вирусов?

Вопросы?