Лекция №8

С.А. Краснов

Вредоносное ПО. Программно-математическое воздействие

# Вредоносное ПО. Программно-математическое воздействие

Лекция №8.

Тема №3: Методы и средства и антивирусной защиты.

Тема лекции: Вредоносное ПО. Программно-математическое воздействие.

**Изучаемые вопросы:**

1. Понятие программно-математического воздействия и вредоносной программы.
2. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации.

Каждая программа обязательно несет в себе некоторую *смысловую нагрузку* - точно в соответствии с задумками программиста или же вследствие каких-либо причин немного видоизмененную. Все программы должны вести себя четко в соответствии с их описанием и приложенной документацией, при этом пользователь должен полностью контролировать установку и удаление программы на свой компьютер. Однако на деле это не всегда так.

Существует класс программ, которые были изначально написаны с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов и т. п., или же приобрели такие свойства вследствие каких-либо причин. Такие программы несут вредоносную нагрузку и соответственно называются *вредоносными*.

## Понятие программно-математического воздействия и вредоносной программы

**Среда существования вредоносного ПО**

Причиной появления подобных программ в конкретной ОС или приложении является одновременное выполнение следующих **условий**:

* популярность, широкое распространение данной системы;
* документированность — наличие разнообразной и достаточно полной документации по системе;
* незащищенность системы или существование известных уязвимостей в её безопасности и приложениях.

**Способы проникновения в систему:**

Достигается эта цель различными способами, которые делятся на 2-е основные категории:

* социальная инженерия (также употребляется термин «социальный инжиниринг» — калька с английского «social engineering»);
* технические приёмы внедрения вредоносного кода в заражаемую систему без ведома пользователя.

В тоже время компьютерные вирусы, черви, троянские программы существуют для десятков ОС и приложений. В то же время имеется огромное количество других ОС и приложений, для которых вредоносные программы пока не обнаружены. Что является *причиной существования* вредных программ в одних системах и *отсутствия* их в других?

**Вредоносная программа (буквальный перевод англоязычного термина Malware, malicious — *злонамеренный* и software — *программное обеспечение*) — злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями.**

**Вирус – ПО, обладающее способностью к размножению.**

**Особенности вирусного ПО:**

* + **понятие вируса связано с его окружением;**
  + **для любого кода можно создать среду, где он будет вредоносным;**
  + **любая последовательность символов является вирусом для какой то ЭВМ;**
  + **нет универсального антивирусного средства, т.к. нет универсального алгоритма обнаружения.**

**Вирус — программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам (*ГОСТ Р 51188-98*).**

Необходимая задача - *внедрение* вируса, червя или троянской программы в компьютер-жертву. Часто эти способы проникновения используются одновременно.

При этом так же часто используются специальные меры по противодействию антивирусным программам.

**Вирус** – ПО, обладающее способностью к размножению (саморепликации). Копии вируса не обязательно точно совпадают друг с другом побайтно, однако функционально все копии одного вируса всегда идентичны друг другу.

Компьютерный вирус относится к вредоносным программам (*ГОСТ Р 51188-98*).

*Особенности вирусного ПО*: Свойство **саморазмножения вирусов** само по себе представляет одну из его опасностей и может привести к снижению, вплоть до нуля, производительности вычислительной системы. Это происходит за счет повышения количества ресурсов ВС, расходуемых на выполнение программ-вирусов:

* увеличивается время процессора;
* увеличивается задействованное пространство ОП зараженного компьютера, которое занимают копии вируса;
* увеличиваются объемы ресурсов внешних устройств, задействованных в процессе саморазмножения.

**История появления** вирусов**.** На начальном этапе это *была теория*.

По материалам этой статьи Ф.Шталь запрограммировал на машинном языке IBM 560 имитационную модель, в которой «киберсущества» «двигались» и «питались» определенными последовательностями байт из памяти ПК. «Съев» некое количество байт существо размножалось, при этом дочерние существа могли отличаться от родителей – *мутировать*. Если «киберсущество» двигалось заданное время без питания, то оно «погибало».

В 1961 г. В.Высотский, Х.Макилрой, Р.Моррис придумали игру «Дарвин», в которой программы специального вида (организмы) загружались в память. Организмы каждого игрока (одного вида) должны были уничтожать других и захватывать жизненное пространство. Цель захват всей памяти или набор наибольшего количества очков.

Все перечисленные вирусы могли существовать только в **специальных эмуляторах**.

«На свободе» вирусы появились намного позже (начиная с 80-х гг.) – *2 этап* (**Слайд 5**)

Проблема вирусов стала по-настоящему серьезной с середины *1980-х гг*., во времена ОС MS-DOS, т.к. в ее архитектуре полностью отсутствует подсистема безопасности. Поскольку исполняемые файлы, системные объекты в ОП, boot-сектора логических дисков не защищены. Не требуется знаний архитектуры ОС, достаточно базовых знаний ассемблера.

С появлением Windows 95 и NT большинство вирусов устарело, т.к. изменилась архитектура ОС, появился новый формат 32-разрядных исполняемых файлов и появилась виртуальная машина DOS. Это привело к появлению специализированных вирусов под windows. Но из-за встроенной подсистемы безопасности значительно снижается их эффективность.

Новый скачок в развитии вирусов связан с появлением макросов в Microsoft Office и популяризации сети Интернет – макровирусы. Типичная работа макровируса – при открытии документа происходит заражение стандартного файла шаблонов normal.dot, а также все файлы, открываемые после этого (защита – предложение отключить макросы при открытии документа).

Признаки *вирусной активности*. И действия при наличии таковых признаков. Явные проявления обычно **заражений через Браузер** выражаются в неожиданно появляющихся рекламных сообщениях и баннерах (обычно это следствие проникновения *рекламной утилиты*). Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также явные проявления могут вызывать ряд *троянских программ*, *например,* утилиты несанкционированного дозвона к платным сервисам. Они вынуждены быть явными, поскольку используемые ими приложения сложно использовать незаметно от пользователя. Либо невозможности закрытия окна.

**Подозрительные процессы**. Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов (в ОС Windows вызывается через *CTRL+ALT+DEL*) подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих только скрытые или косвенные проявления.

Неожиданно возросшая **сетевая активность** может служить ярким свидетельством работы на компьютере подозрительный программы. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, *например,* для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

**Элементы автозапуска**. Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили. Оптимальным с точки зрения вируса вариантом служит запуск одновременно с ОС - в этом случае запуск практически гарантирован.

Вредоносная программа может вносить изменения в системные файлы *win.ini* и *system.ini*. В файле **system.ini** кроме секции *[boot]* вредоносные программы могут использовать секцию *[Drivers]*. Диагностика элементов автозапуска возможно путем изучения *секций*: SYSTEM.INI; WIN.INI; «Автозапуск» и «Службы», в утилите конфигурирования **msconfig**. Удаление запускаемого вируса из автозагрузки возможно путем использования утилиты **regedit**.

**Другие признаки**:

* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* неожиданное открытие и закрытие лотка CD/DVD дисковода;
* произвольный запуск на компьютере каких-либо программ;
* частые зависания и сбои в работе компьютера;
* медленная работа компьютера при запуске программ;
* исчезновение или изменение файлов и папок;
* частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
* зависание или неожиданное поведение браузера.
* Признаки поражения сетевым вирусом через электронную почту:
* знакомые говорят о полученных от вас сообщениях, которые вы не отправляли;
* в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

*Подходы к классификация вирусного ПО*

Необходимость создания классификации детектируемых объектов возникла одновременно с появлением первой антивирусной программы. Несмотря на то, что вирусов в то время было мало, их необходимо было как-то отличать друг от друга по названиям.

Пионеры антивирусной индустрии, как правило, использовали самую простую классификацию, состоящую из *уникального имени* вируса и *размера* детектируемого файла. Однако из-за того, что один и тот же вирус в разных антивирусных программах мог именоваться по-разному, началась путаница. *Первая попытка* упорядочить процесс классификации - в начале 90-х годов прошлого века, в рамках альянса антивирусных специалистов **CARO** (Computer AntiVirus Researcher's Organization). Альянсом был создан документ «CARO malware naming scheme», который на какой-то период стал стандартом для индустрии.

Но со временем стремительное развитие вредоносных программ, *появление новых платформ*, рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться.

Ещё более важной причиной отказа от неё стали существенные *отличия в технологиях детектирования* каждой антивирусной компании и, как следствие, невозможность унификации результатов проверки разными антивирусными программами.

Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов, однако они, по большей части, остаются безуспешными.

Последним значительным проектом - было создание организации **CME**

## Классификация ВПО (классическая), рисунок 1.

Говоря о вредоносном ПО, следует говорить о целой *технологии разработки,* а именно:

* утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
* программные библиотеки, разработанные для создания вредоносного ПО;
* хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);

**Программные закладки** включают в себя элементы (характерные особенности) присущие всем классам перечисленного вредоносного ПО.

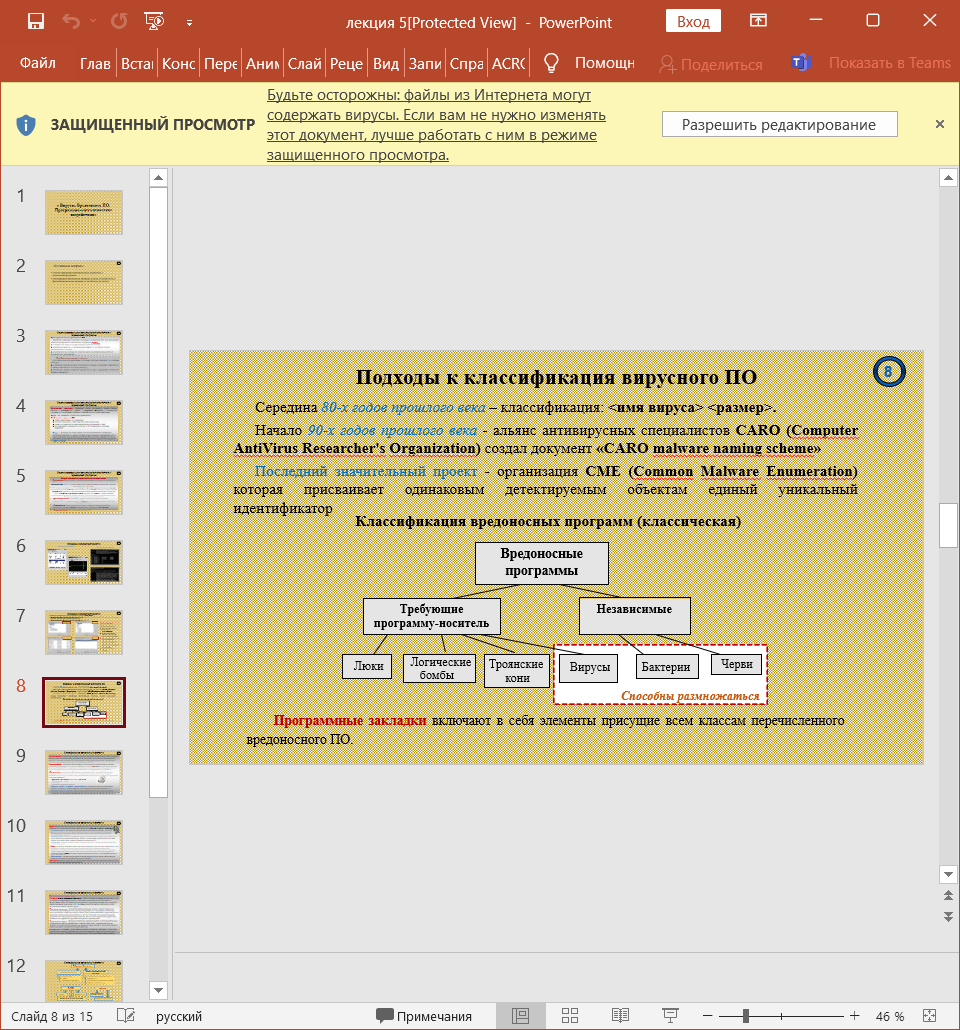


Рисунок 1

***Люк, или лазейка****.* Люки используются в программистской практике для ускорения отладки и тестирования программ. Эта возможность обычно применяется программистом при создании приложе­ния, в состав которого входит процедура аутентификации или слишком долгая программа установки, требующая от пользователя ввода множества различных параметров для запуска программы.

Реализовать выявление возможных лазеек стандартными средствами ОС очень трудно. Меры защиты в данном случае должны быть сфокусированы на осуществлении контроля процесса разработки ПО и его обновления.

***Логические бомбы.*** Одним из самых старых типов вредоносных программ, возникших еще до появления вирусов и «червей», является логическая бомба.

***«Троянские кони»*** Трояны отличаются отсутствием механизма создания собственных копий. *Примером* «троянского коня», является ком­пилятор, модифицированный с целью внедрения дополнительного кода в про­граммы определенного вида во время их компиляции. Соответствующий код *создает в модуле регистрации люк*, позволяющий автору кода войти в систему с помощью специального паро­ля. Обнаружить такого «троянского коня» по исходному коду программы входа в систему будет просто невозможно.

Вторым побудительным мотивом создания «троянских коней» является *раз­рушение данных*. В этом случае программа, выполняющая какие-то полезные функции (*например*, программа-калькулятор), может без каких бы то ни было внешних проявлений удалить все файлы пользователя.

***Вирусы.*** Внесенный в компь­ютерную систему, типичный вирус временно захватывает управление дисковой ОС компьютера. Затем при каждом контакте зараженного компьютера с незараженным ПО очередная копия виру­са помещается в новую программу. Таким образом инфекция может передавать­ся от компьютера к компьютеру ничего не подозревающими пользователями, обменивающимися содержимым флэш-накопителей или пересылающими про­граммы по сети.

**Загрузочные** - их принцип действия основан на алгоритмах запуска ОС при включении или перезагрузке компьютера.

Практически все **загрузочные** и **файловые вирусы** резидентные (стирают данные на дисках, изменяют названия и другие атрибуты файлов и т. д.). Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к ОС или программной оболочке, для которой он был написан.

***«Черви»*** К сожалению, определение червя отсутствует в ГОСТ и РД.Во время работы на отдельном компьютере сетевой «червь» может вести себя как компьютерный вирус или «бактерия», внедрять «троянских коней», или же выполнять какие-то другие разрушительные или подрывные действия. Сетевой «червь» во многом *подобен* компьютерному вирусу — у него тоже есть инкубационный период, фаза распространения, фаза активизации и фаза выполнения.

На этапе *проникновения* в систему черви делятся преимущественно по типам используемых протоколов. Многие сетевые черви используют *более одного способа распространения* своих копий по компьютерам локальных и глобальных сетей.

Перед тем как копировать себя в другую систему, сетевой «червь» может также пытаться проверить, не была ли система уже инфицирована ранее. В многозадачной среде он может скрывать свое присутствие с помощью назначения себе другого имени (системного процесса и др.)

*Уязвимыми* для червей являются ОС с заложенными возможностями удаленного управления или запуска программ.

***«Бактерии»*** Скорость размножения «бактерий» растет экспоненциально, что в конце концов приводит к быстрому захвату всех ресурсов процессора, памяти или дискового пространства, а результатом является отказ пользователям в дос­тупе к этим ресурсам.

Кроме вирусов, червей и троянов существует еще множество других вредоносных программ, для которых нельзя привести общий критерий. Однако среди них можно выделить небольшие группы.

**Условно опасные программы:**

***Riskware* (*опасное программное обеспечение*) - вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. Это обычные утилиты удаленного управления, которыми часто пользуются администраторы распределенных сетей, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и другие.**

***Рекламные* *утилиты* - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров. После официальной оплаты и регистрации обычно показ рекламы заканчивается. Проблема кроется в механизмах загрузки рекламы на компьютер т.к. для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме.**

***Хакерские* *утилиты* - программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют для скрытного взятия под контроль взломанной системы (RootKit) и др.**

***Злые* *шутки* - программы, которые намеренно вводят пользователя в заблуждение путем показа уведомлений о, например, форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит. Текст таких сообщений целиком и полностью отражает фантазию автора.**

Тем не менее современные антивирусные компании используют свою классификацию. Связанно это с тем, что сегодня под *вирусом* чаще всего понимается не "традиционный" вирус, а практически *любая вредоносная программа*. Первые широко известные вредоносные программы были именно вирусами, и в течение следующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ вместе взятых. Однако в последнее время наметились тенденции к появлению новых, невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем, числе инцидентов с вредоносными программами за последние годы значительно сократилась. На сегодняшний день вредоносные программы - это уже большей частью именно не вирусы, хотя такие термины как "заражение вирусом", "вирусный инцидент" применяются по отношению ко всем вредоносным программам повсеместно. Поэтому термином "*компьютерный вирус*" часто называют любую *вредоносную программу*.

В настоящее время *классификация «Лаборатории Касперского»* включает в себя весь объём детектируемых Антивирусом Касперского вредоносных или потенциально нежелательных объектов, и основана на *разделении* объектов по типу совершаемых ими на компьютере пользователей действий.

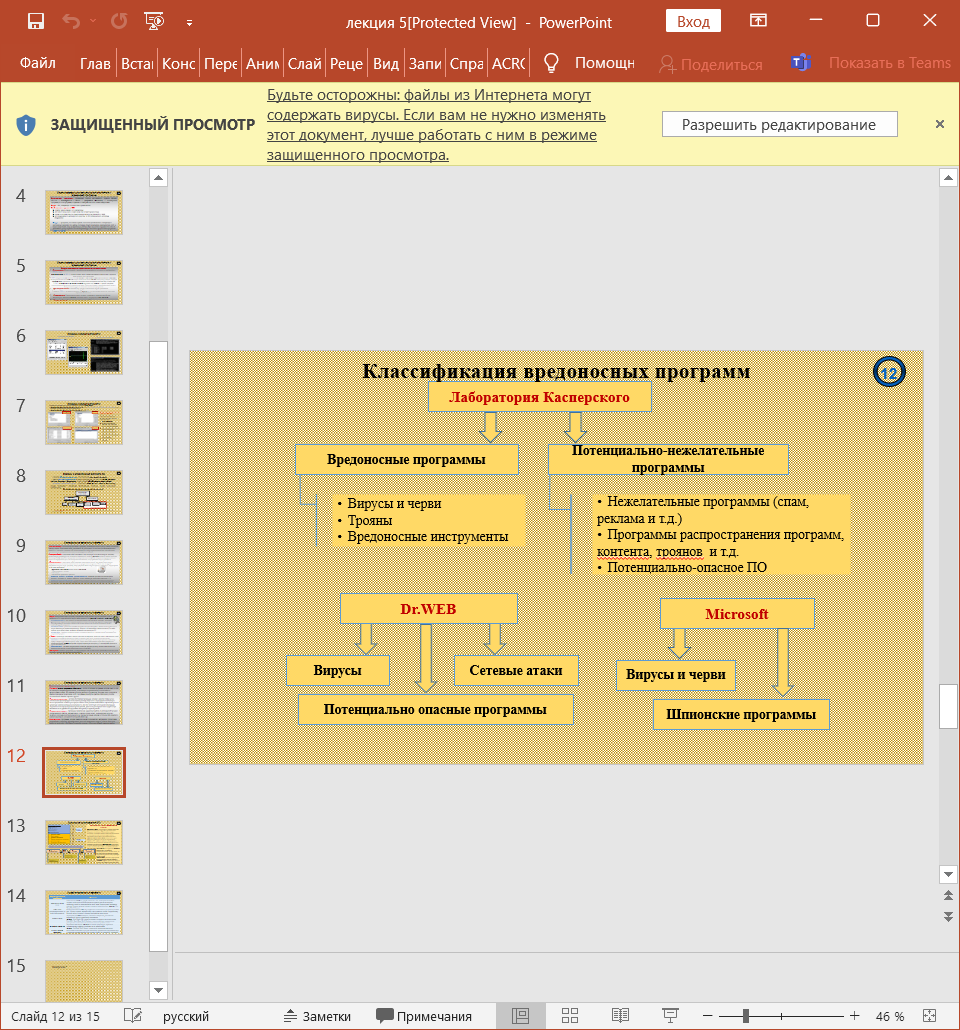


Рисунок 2

*Жизненный цикл вирусного ПО*.

Время показало, что наиболее эффективно организовать работу вируса можно в *две стадии*: подготовительную и активную. Во время *подготовительной стадии* действия вируса направлены только на внедрение в систему (подготовка своих вирусных копий, проникновение в системные объекты) – использует механизмы защиты. В этот период вирус наиболее уязвим, поэтому важно, чтобы он не был обнаружен. Поэтому действия вируса должны быть максимально скрыты. После вирус переходит к своей *активной стадии*, во время которой реализуются функции негативного воздействия на систему.

На стадии *поиска объектов для заражения* встречается два способа поведения вирусов:

1. Получив управление, вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту (зараженному объекту).
2. Получив управление, вирус так или иначе остается в памяти и производит поиск жертв непрерывно, до завершения работы среды, в которой он выполняется.

*Внедрение* вирусных копий может осуществляться двумя методами:

1. Внедрение вирусного кода непосредственно в заражаемый объект.
2. Замена объекта на вирусную копию. Замещаемый объект, как правило, переименовывается.

*Современные ОС многозадачные и многопользовательские*, с поддержкой сети. Современный компьютерный **вирус** должен обладать **рядом свойств**:

* наличие средств противодействия подсистеме безопасности (вирус должен обладать средствами преодоления механизмов разграничения доступа, систем аудита, аутентификации);
* корректная работа в условиях совместного использования файлов (для доступа процессов к разделяемым файлам используется механизм блокировок file sharing);
* использование современных средств передачи информации (сетей);
* согласование действий различных экземпляров вируса (не должно быть конфликтов между экземплярами вируса, отсутствие лишних экземпляров);
* накопление и использование «опыта» (фиксация и использование результатов своей работы);
* использование элементов случайности (функции вируса не привязываются к таймеру и др.).

Требования противоречивы, поэтому всегда ищется компромиссное решение.

*Черви* и *вирусы* могут осуществлять все те же действия, что и *трояны*. На уровне реализации это могут быть как отдельные троянские компоненты, так и встроенные функции. Кроме этого, за счет массовости, для вирусов и червей характерны также другие формы вредоносных действий, рисунок 3:

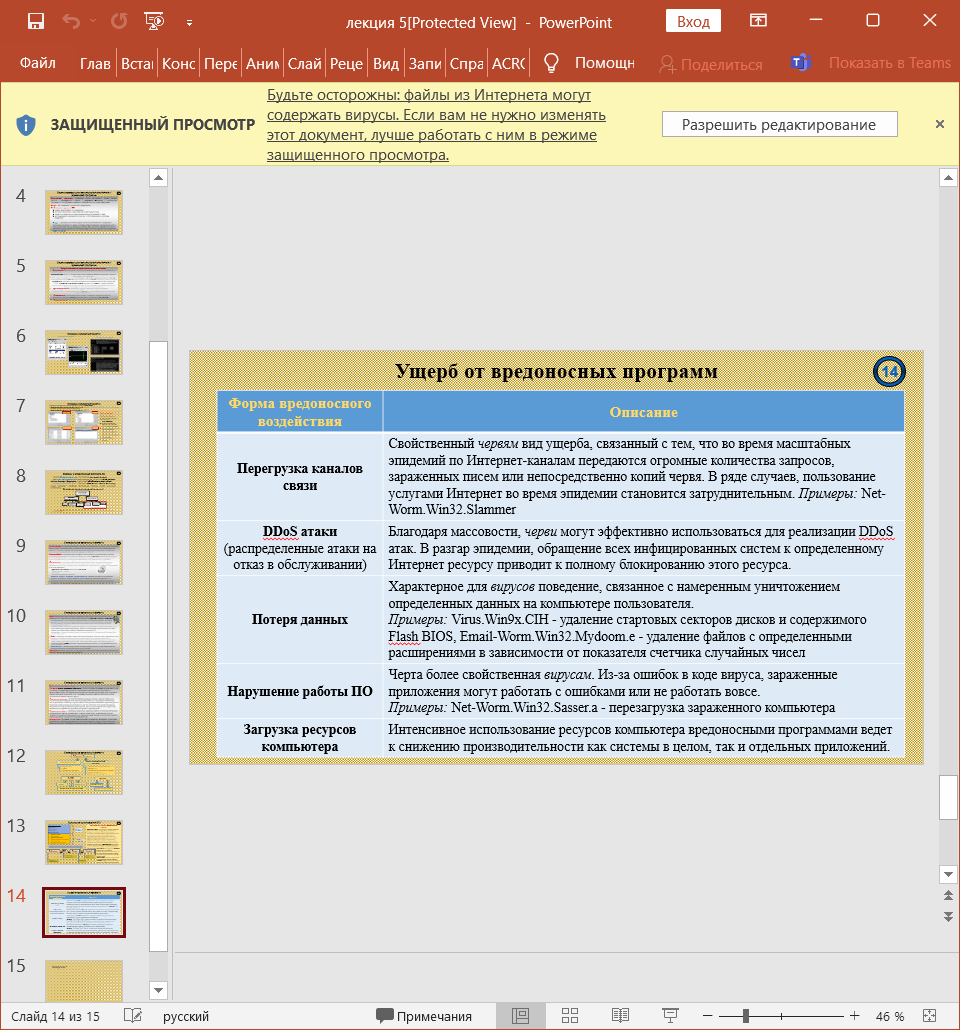


Рисунок 3 – Ущерб от вредоносных программ

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.