ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное

учреждение высшего образования

**Уральский государственный университет путей сообщения**

**(ФГБОУ ВО УрГУПС)**

Факультет Электротехнический

Кафедра Информационные технологии и защита информации

Специальность 10.03.01 Информационная безопасность

# Реферат на тему: «Вредоносные программные средства»

Выполнил:

студент гр. ИБ-110

Мизгирев Д. В.

Проверил:

ассистент кафедры «ИТиЗИ»

Ганженко Н.В.

Екатеринбург

2021

**СОДЕРЖАНИЕ**

## Возможные действия деструктивных программных средств.

По деструктивным возможностям вирусы можно разделить на:

• *безвредные,* т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

• *неопасные,* влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и т.п. эффектами;

• *опасные* вирусы, которые могут привести к серьезным сбоям в работе компьютера;

• *очень опасные,* в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожению данных, утрате необходимой для работы компьютера информации, записанной в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов — вводить в резонанс и разрушать головки некоторых типов винчестеров.

На сегодняшний день сложились установившиеся названия для некоторых типов вирусов.

Так, *«ловушками»* называют вирусы, использующие имеющиеся неточности в действующих программах или их несовершенство (например, изменяющие адрес входа из программы в подпрограммы и обратно).

*«Логические бомбы»,* или *«бомбы замедленного действия»* осуществляют длительную и разнообразную подготовку к проведению деструктивных действий и затем срабатывают при выполнении определенного комплекса условий (например, выполнении определенного этапа работ, наступлении

заданного времени, при обращении к программе определенного пользователя и т.п.). Эти вирусы особенно опасны в силу длительности периода, в течение которого они себя практически не обнаруживают, хотя уже ведут разрушительную работу. Факт проявления этих вирусов сопряжен с такой степенью порчи данных, что в установленной версии ОС оказываются неработоспособными практически все (или большинство) программ. Таким образом, машина становится полностью неработоспособной.

*Вирусы-«черви»* вызывают неуправляемое функционирование, например, сетевых или периферийных устройств (бесконечный «прогон» бумаги в принтере, постоянную перезагрузку операционной системы и т.п.).

*«Троянскими конями»* называют вирусы, распространяемые вместе с программным обеспечением специального назначения, причем для пользователя оказываются крайне неожиданными их деструктивные действия (например, таким вирусом могут быть заражены сами анти-вирусные программы).

Внешне «троянцы» могут даже выполнять некие полезные функции (фиктивно оптимизировать распределение памяти на компьютере, проводить уплотнение информации на диске и т.д.), но на самом деле либо разрушают систему (например, форматируют ваш винчестер на низком уровне или операцией многократного и оперативного считывания-записи информации способствуют механическому выведению из строя дисковода вашего компьютера), либо отдают контроль в руки другого человека. Пород «троянцев» множество: некоторые из них вообще не выполняют полезных функций, а просто скрытно «живут» на диске ЭВМ и совершают различные деструктивные действия, а некоторые, наоборот, совершенно не скрываются от пользователя, при этом производя некоторые манипуляции, о которых никто не подозревает (или не должен подозревать).

Пример вируса первого типа — известный вирус Back Orifice, дающий «врагу» почти полный контроль над вашим компьютером в компьютерной сети и для вас невидимый. Пример вируса второго типа — подделки под браузер MS Internet Explorer, который при соединении с сайтом фирмы Майкрософт развивает небывалую активность по пересылке данных с компьютера на сервер Майкрософт, объем которых явно превосходит простой запрос скачиваемого HTML документа (Web-страницы с ИНТЕРНЕТ).

## Способы проникновения ВПС в систему

### Социальная инженерия.

Методы социальной инженерии тем или иным способом заставляют пользователя запустить заражённый файл или открыть ссылку на заражённый веб-сайт. Эти методы применяются не только многочисленными почтовыми червями, но и другими видами вредоносного программного обеспечения.

Задача хакеров и вирусописателей — привлечь внимание пользователя к заражённому файлу (или HTTP-ссылке на заражённый файл), заинтересовать пользователя, заставить его кликнуть по файлу (или по ссылке на файл). «Классикой жанра» является нашумевший в мае 2000 года почтовый червь LoveLetter, до сих пор сохраняющий лидерство по масштабу нанесённого финансового ущерба, согласно данным от Computer Economics.

Почтовый червь Mydoom, «рванувший» в интернете в январе 2004 г., использовал тексты, имитирующие технические сообщения почтового сервера.

### Технологии внедрения.

Эти технологии используются злоумышленниками для внедрения в систему вредоносного кода скрытно, не привлекая внимания владельца компьютера. Осуществляется это через уязвимости в системе безопасности операционных систем и в программном обеспечении. Наличие уязвимостей позволяет изготовленному злоумышленником сетевому червю или троянской программе проникнуть в компьютер-жертву и самостоятельно запустить себя на исполнение.

Уязвимости являются, по сути, ошибками в коде или в логике работы различных программ. Современные операционные системы и приложения имеют сложную структуру и обширный функционал, и избежать ошибок при их проектировании и разработке просто невозможно. Этим и пользуются вирусописатели и компьютерные злоумышленники.

Уязвимостями в почтовых клиентах Outlook пользовались почтовые черви Nimda и Aliz. Для того чтобы запустить файл червя, достаточно было открыть заражённое письмо или просто навести на него курсор в окне предварительного просмотра.

В последние годы одним из наиболее популярных способов заражения стало внедрение вредоносного кода через веб-страницы. При этом часто используются уязвимости в интернет-браузерах. На веб-страницу помещается заражённый файл и скрипт-программа, которая использует уязвимость в браузере. При заходе пользователя на заражённую страницу срабатывает скрипт-программа, которая через уязвимость закачивает заражённый файл на компьютер и запускает его там на выполнение. В результате для заражения большого числа компьютеров достаточно заманить как можно большее число пользователей на такую веб-страницу.

## Одновременное использование технологий внедрения и методов социальной инженерии.

Достаточно часто компьютерными злоумышленниками используются сразу оба метода. Метод социальной инженерии — для привлечения внимания потенциальной жертвы, а технический — для увеличения вероятности проникновения заражённого объекта в систему.

Например, почтовый червь Mimail распространялся как вложение в электронное письмо. Для того чтобы пользователь обратил внимание на письмо, в него вставлялся специально оформленный текст, а для запуска копии червя из вложенного в письмо ZIP-архива — уязвимость в браузере Internet Explorer. В результате при открытии файла из архива червь создавал на диске свою копию и запускал её на исполнение без каких либо системных предупреждений или дополнительных действий пользователя. Кстати, этот червь был одним из первых, предназначенных для воровства персональной информации пользователей интернет-кошельков системы e-gold.

Другим примером является рассылка спама с темой «Привет» и текстом «Посмотри, что про тебя пишут». За текстом следовала ссылка на некую веб-страницу. При анализе выяснилось, что данная веб-страница содержит скрипт-программу, которая, пользуясь еще одной уязвимостью в Internet Explorer, загружает на компьютер пользователя троянскую программу LdPinch, предназначенную для воровства различных паролей.

## Классификация вредоносных программ

### Вирус.

Если просто, то это самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя. Вирусы можно разделить по типу объектов, которые они заражают, по методам заражения и выбора жертв. Вирусы можно подцепить разными способами: от нажатия вредоносной ссылки или файла в неизвестном письме до заражения на вредоносном сайте. При этом вирус может выполнять множество разных задач, направленных в первую очередь на принесение вреда операционной системе. В настоящее время вирусы довольно редки, так как создатели вредоносов стараются держать свои программы и их распространение под контролем. В противном случае вирус довольно быстро попадает в руки антивирусных компаний.

### **Червь**.

Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ. Однако черви не могут заражать существующие файлы. Вместо этого червь поселяется в компьютер отдельным файлом и ищет уязвимости в Сети или системе для дальнейшего распространения себя. Черви также могут подразделяться по способу заражения (электронная почта, мессенджеры, обмен файлами и пр.). Некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые поселяются лишь в оперативной памяти компьютера.

### **Троян**.

По своему действию является противоположностью вирусам и червям. Его предлагают загрузить под видом законного приложения, однако вместо заявленной функциональности он делает то, что нужно злоумышленникам. Троянцы получили свое название от одноименного печально известного мифологического коня, так как под видом какой-либо полезной программы или утилиты в систему проникает деструктивный элемент. Трояны не самовоспроизводятся и не распространяются сами по себе. Однако с увеличением вала информации и файлов в Интернете трояна стало довольно легко подцепить. Нынешние трояны эволюционировали до таких сложных форм, как, например, бэкдор (троян, пытающийся взять на себя администрирование компьютера) и троян-загрузчик (устанавливает на компьютер жертвы вредоносный код).

**Руткит**.

В современном мире руткит представляет собой особую часть вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения. Это возможно благодаря тесной интеграции руткита с операционной системой. А некоторые руткиты могут начать свою работу прежде, чем загрузится операционная система.

**Загрузчик**.

Эта зараза является небольшой частью кода, используемой для дальнейшей загрузки и установки полной версии вредоноса. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь вредонос.

## Заключение

Для того, чтобы защитить свой ПК от вирусных программ достаточно выполнять пару правил:

1. Не открывайте сомнительные ссылки и сайты.
2. Не запускайте незнакомые программы на своём компьютере и не открывайте неизвестные почтовые вложения.
3. Делайте резервные копии важной информации и храните их в безопасном удалённом от вашего компьютера месте.
4. Не вводите персональные данные на сомнительных сайтах.
5. Используйте лицензионные программные продукты и регулярно обновляйте их.
6. Используйте качественное антивирусное ПО.

## Список литературы

1. https://remik.ru/advices/?ELEMENT_ID=2453
2. https://www.kaspersky.ru/blog/klassifikaciya-vredonosnyx-programm/2200/
3. https://www.info-tehnologii.ru/komp_vir/kl_vir/destr_vir/index.html
4. https://encyclopedia.kaspersky.ru/knowledge/how-malware-penetrates-systems/