# Вредоносные программы.

# Компьютерные вирусы.

Оглавление

[Вредоносные программы. 1](#_Toc340764913)

[Компьютерные вирусы. 1](#_Toc340764914)

[История 2](#_Toc340764915)

[Этимология названия 4](#_Toc340764916)

[Формальное определение 4](#_Toc340764917)

[Классификация 5](#_Toc340764918)

[По вредоносной нагрузке 6](#_Toc340764919)

[По методу размножения 7](#_Toc340764920)

[Признаки заражения 8](#_Toc340764921)

[Противодействие обнаружению 9](#_Toc340764922)

[Профилактика и лечение 10](#_Toc340764923)

[Юридические аспекты 10](#_Toc340764924)

[Экономика 11](#_Toc340764925)

[Кибер-оружие 12](#_Toc340764926)

[Литература 14](#_Toc340764927)

*Вредоносная программа* - (на жаргоне антивирусных служб «зловред», англ. malware, malicious software — «злонамеренное программное обеспечение») — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации.

*Компью́терный ви́рус* — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация). Кроме этого вирусы, без ведома пользователя (осознанного понимания происходящего и его последствий), но при его участии выполняют прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру.

Даже если автор вируса не программировал вредоносных эффектов, вирус, как любая другая программа, может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами, причем, особо не стараясь поставить в известность оператора компьютера. Скорее даже вовсе наоборот, как можно тщательнее скрывая подобные ситуации.

Запрограммированные вредоносные действия рассмотрим ниже.

Вирусы – это также в обиходной среде обобщенное название всевозможных других разновидностей вредоносных программ. Основной принцип вредоносности – это захват ресурсов вычислительной системы – компьютера, планшета, смартфона без прямого одобрения и выполнение поставленной задачи – кража данных, скрытие присутствия и др. Поэтому вирусы относят к вредоносным программам.

Известны сотни тысяч компьютерных вирусов, которые уже не могут воспользоваться своими способностями. Но каждый день выходят на свет все новые творения всевозможных умельцев из разных стран. Россия уверенно держится в первой пятерке вирусописателей.

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273). Согласно доктрине информационной безопасности РФ[2], в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детской порнографии и обеспечению информационной безопасности в сетях ЭВМ.

# История

Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.[3]

Первыми известными собственно вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Анди Хопкинса (англ. Andy Hopkins). В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу DPROTECT — первый резидентный антивирус.

Первые вирусные эпидемии относятся к 1987—1989 годам: Brain (более 18 тысяч зараженных компьютеров, по данным McAfee, Jerusalem, червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).

Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989[5]), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).

Параллельно оформляются организованные движения как про-, так и антивирусной направленности: в 1990 году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton AntiVirus. И в середине 90 Питер Нортон, автор мегахита Norton Commander, издает свой бестселлер на русском языке – «Пишем вирус и антивирус», что значительно пополнило ряды обоих лагерей.

В 1992 году появились первый конструктор вирусов для PC — VCL (для Amiga конструкторы существовали и ранее), а также готовые полиморфные модули (MtE, DAME и TPE) и модули шифрования для встраивания в новые вирусы.

В несколько последующих лет были окончательно отточены стелс- и полиморфные технологии (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а также испробованы самые необычные способы проникновения в систему и заражения файлов (Dir II — 1991, PMBS, Shadowgard, Cruncher — 1993). Кроме того, появились вирусы, заражающие объектные файлы (Shifter, 1994) и исходные тексты программ (SrcVir, 1994). С распространением пакета Microsoft Office получили распространение макровирусы (Concept, 1995).

В 1996 году появился первый вирус для Windows 95 — Win95.Boza, а в декабре того же года — первый резидентный вирус для неё — Win95.Punch.

С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (ShareFun, 1997 — макровирус MS Word, использующий MS-Mail для распространения; Win32.HLLP.DeTroie, 1998 — семейство вирусов-шпионов; Melissa, 1999 — макровирус и сетевой червь, побивший все рекорды по скорости распространения). Эру расцвета «троянских коней» открывает утилита скрытого удаленного администрирования BackOrifice (1998) и последовавшие за ней аналоги (NetBus, Phase).

Вирус Win95.CIH достиг апогея в применении необычных методов, перезаписывая FlashBIOS зараженных машин (эпидемия в июне 1998 считается самой разрушительной за предшествующие годы).

В конце 1990-x — начале 2000-x годов с усложнением ПО и системного окружения, массовым переходом на сравнительно защищенные Windows семейства NT, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий в обнаружении вирусов, построенных по сложным алгоритмам, последние стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный автозапуск, руткиты) и подменять полиморфизм огромным количеством видов (число известных вирусов растет экспоненциально).

Вместе с тем, обнаружение в Windows и другом распространенном ПО многочисленных уязвимостей открыло дорогу червям-эксплоитам. В 2004 году беспрецедентные по масштабам эпидемии вызывают MsBlast (по данным Microsoft — более 16 млн систем[6]), Sasser и Mydoom (оценочные ущербы 500 млн и 4 млрд долл. соответственно[7]).

Кроме того, монолитные вирусы в значительной мере уступают место комплексам вредоносного ПО с разделением ролей и вспомогательными средствами (троянские программы, загрузчики/дропперы, фишинговые сайты, спам-боты и пауки). Также расцветают социальные технологии — спам и фишинг — как средство заражения в обход механизмов защиты ПО.

Вначале на основе троянских программ, а с развитием технологий p2p-сетей — и самостоятельно — набирает обороты самый современный вид вирусов — черви-ботнеты (Rustock, 2006, ок. 150 тыс. ботов; Conficker, 2008—2009, более 7 млн ботов; Kraken, 2009, ок. 500 тыс. ботов).

Вирусы в числе прочего вредоносного ПО окончательно оформляются как средство киберпреступности.

# Этимология названия

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах»[8], опубликованном в журнале Venture в мае 1970 года.

Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в подпрограмме PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер и, вероятно, это и было то, что впервые было правильно обозначено как вирус.

# Формальное определение

Нет общепринятого определения вируса. В академической среде термин был употреблён Фредом Коэном в его работе «Эксперименты с компьютерными вирусами»[9][10], где он сам приписывает авторство термина Лену Эдлмэну[11][12].

Формально вирус определён Фредом Коэном со ссылкой на машину Тьюринга[13] следующим образом[14]:

M : (SM, IM, OM : SM x IM > IM, NM : SM x IM > SM, DM : SM x IM > d)

с заданным множеством состояний SM, множеством входных символов IM и отображений (OM, NM, DM), которая на основе своего текущего состояния s ∈ SM и входного символа i ∈ IM, считанного с полубесконечной ленты, определяет: выходной символ o ∈ IM для записи на ленту, следующее состояние машины s' ∈ SM и движения по ленте d ∈ {-1,0,1}.

Для данной машины M, последовательность символов v : vi ∈ IM может быть сочтена вирусом тогда и только тогда, когда обработка последовательности v в момент времени t, влечёт за собой то, что в один из следующих моментов времени t, последовательность v′ (не пересекающаяся с v) существует на ленте, и эта последовательность v′ была записана M в точке t′, лежащей между t и t″:

∀ CM ∀ t ∀ j:

SM(t) = SM0 ∧

PM(t) = j ∧

{ CM(t, j) … CM(t, j + |v| - 1)} = v ⇒

∃ v' ∃ j' ∃ t' ∃ t":

t < t" < t' ∧

{j' … j' +|v'|} ∩ {j … j + |v|} = ∅ ∧

{ CM(t', j') … CM(t', j' + |v'| - 1)} = v' ∧

PM(t") ∈ { j' … j' + |v'| - 1 }

где:

t ∈ N число базовых операций «перемещения», осуществлённых машиной

PM ∈ N номер позиции на ленте машины в момент времени t

SM0 начальное состояние машины

CM(t, c) содержимое ячейки c в момент времени t

Данное определение было дано в контексте вирусного множества VS = (M, V) — пары, состоящей из машины Тьюринга M и множества последовательностей символов V: v, v' ∈ V. Из данного определения следует, что понятие вируса неразрывно связано с его интерпретацией в заданном контексте, или окружении.

Фредом Коэном было показано[14], что «любая самовоспроизводящаяся последовательность символов: одноэлементный VS, согласно которой существует бесконечное количество VS, и не-VS, для которых существуют машины, по отношению к которым все последовательности символов является вирусом, и машин, для которых ни одна из последовательностей символов не является вирусом, даёт возможность понять, когда любая конечная последовательность символов является вирусом для какой-либо машины». Он также приводит доказательство того, что в общем виде вопрос о том, является ли данная пара (M, X) : Xi ∈ IM вирусом, неразрешим (то есть не существует алгоритма, который мог бы достоверно определить все вирусы), теми же средствами, которыми доказывается неразрешимость проблемы остановки.[13]

Другие исследователи доказали, что существуют такие типы вирусов (вирусы, содержащие копию программы, улавливающей вирусы), которые не могут быть безошибочно определены ни одним алгоритмом.

# Классификация

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

У каждой компании-разработчика антивирусного программного обеспечения существует собственная корпоративная классификация и номенклатура вредоносных программ. Приведённая здесь классификация основана на методике «Лаборатории Касперского».

### По вредоносной нагрузке

1. Помехи в работе заражённого компьютера: начиная от открытия-закрытия поддона CD-ROM и заканчивая уничтожением данных и поломкой аппаратного обеспечения. Поломками известен, в частности, Win32.CIH.
2. Блокировка антивирусных сайтов, антивирусного ПО и административных функций ОС с целью усложнить лечение.
3. Саботирование промышленных процессов, управляемых компьютером.
4. Инсталляция другого вредоносного ПО.
5. Загрузка из сети (downloader).
6. Распаковка другой вредоносной программы, уже содержащейся внутри файла (dropper).
7. Кража, мошенничество, вымогательство и шпионаж за пользователем. Для кражи может применяться сканирование жёсткого диска, регистрация нажатий клавиш (Keylogger) и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы.
8. Похищение данных, представляющих ценность или тайну.
9. Кража аккаунтов различных служб (электронной почты, мессенджеров, игровых серверов…). Аккаунты применяются для рассылки спама. Также через электронную почту зачастую можно заполучить пароли от других аккаунтов, а виртуальное имущество в MMOG — продать.
10. Кража аккаунтов платёжных систем.
11. Блокировка компьютера, шифрование файлов пользователя с целью шантажа и вымогательства денежных средств (см. Ransomware). В большинстве случаев после оплаты компьютер или не разблокируется, или вскоре блокируется второй раз.
12. Использование телефонного модема для совершения дорогостоящих звонков, что влечёт за собой значительные суммы в телефонных счетах.
13. Платное ПО, имитирующее, например, антивирус, но ничего полезного не делающее (fraudware или scareware).
14. Прочая незаконная деятельность:
    1. Получение несанкционированного (и/или дарового) доступа к ресурсам самого компьютера или третьим ресурсам, доступным через него, в том числе прямое управление компьютером (так называемый backdoor).
    2. Организация на компьютере открытых релеев и общедоступных прокси-серверов.
    3. Заражённый компьютер (в составе ботнета) может быть использован для проведения DDoS-атак.
    4. Сбор адресов электронной почты и распространение спама, в том числе в составе ботнета.
    5. Накрутка электронных голосований, щелчков по рекламным баннерам.
    6. Генерация монет платёжной системы Bitcoin.

Программы, не являющиеся истинно вредоносными, но в большинстве случаев нежелательные:

* Шуточное ПО, делающее какие-либо беспокоящие пользователя вещи.
* Adware — программное обеспечение, показывающее рекламу.
* Spyware — программное обеспечение, посылающее через интернет не санкционированную пользователем информацию.
* «Отравленные» документы, дестабилизирующие ПО, открывающее их (например, архив размером меньше мегабайта может содержать гигабайты данных и надолго «завесить» архиватор).
* Программы удалённого администрирования могут применяться как для того, чтобы дистанционно решать проблемы с компьютером, так и для неблаговидных целей.

Иногда вредоносное ПО для собственного «жизнеобеспечения» устанавливает дополнительные утилиты: IRC-клиенты[4], программные маршрутизаторы[5], открытые библиотеки перехвата клавиатуры…[6] Такое ПО вредоносным не является, но из-за того, что за ним часто стоит истинно вредоносная программа, детектируется антивирусами. Бывает даже, что вредоносным является только скрипт из одной строчки, а остальные программы вполне легитимны.[7]

### По методу размножения

*Через Эксплойт* — теоретически безобидный набор данных (например, графический файл или сетевой пакет), некорректно воспринимаемый программой, работающей с такими данными. Здесь вред наносит не сам файл, а неадекватное поведение ПО с ошибкой. Также эксплойтом называют программу для генерации подобных «отравленных» данных.

*Логическая бомба* в программе срабатывает при определённом условии, и неотделима от полезной программы-носителя.

*Троянская программа*  - не имеет собственного механизма размножения.

*Компьютерный вирус* - Каналы распространения:

• Дискеты. Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

• Флеш-накопители (флешки). В настоящее время USB-флешки заменяют не только дискеты, но и по объему превосходят следующих заменителей дискет –CD, DVD диски. Флешки повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя, скрытие папок и создание отравленных ярлыков на них – при открытии папки в процесс explorerа внедрялся вредоносный код как отладчик и получал полные права в системе.

• Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, как правило, всегда используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

• Системы обмена мгновенными сообщениями и СМС. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ, Skype и через другие программы мгновенного обмена сообщениями. Также есть случаи маскировки под них.

• Веб-сайты. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

• Интернет, локальные сети и bluetooth. Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет.

Механизм распространение вирусов.

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), или особенности обработки псевдо-объектов (папки .lnk например использовал Stuxnet) для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

*Сетевой червь* - способен самостоятельно размножаться по сети. Делятся на IRC-, почтовые, размножающиеся с помощью эксплойтов и т. д.

Вредоносное ПО может образовывать цепочки: например, с помощью эксплойта (1) на компьютере жертвы развёртывается загрузчик, устанавливающий из интернета червя или несколько.

# Признаки заражения

Существует ряд признаков, которые могут сопутствовать заражению вирусом: появление на экране непредусмотренных сообщений и запросов, изображений и звуковых сигналов; самопроизвольный запуск программ без участия пользователя; попытки неизвестных программ подключиться к Интернету без ведома пользователя и т. п. О поражении вирусом через почту может свидетельствовать то, что друзья и знакомые пользователя говорят о сообщениях от него, которые он не отправлял; наличие в почтовом ящике большого количества сообщений без обратного адреса и заголовков. Однако эти признаки не всегда являются следствием присутствия вирусов. Например, в случае с почтой заражённые сообщения могут рассылаться с обратным адресом пользователя с других компьютеров.

Среди косвенных признаков можно назвать частые зависания и сбои в работе компьютера, замедленная (по сравнению с изначальным поведением) работа компьютера при запуске программ, невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого, частое обращение к жёсткому диску (часто мигает лампочка на системном блоке), браузер Internet Explorer «зависает» или ведёт себя неожиданным образом (например, окно программы невозможно закрыть). Но основной причиной для подобных симптомов являются всё же не вирусы, а сбои в аппаратном обеспечении, конфликты между программами и баги («жучки», дефекты) в них.[15]

# Противодействие обнаружению

Во времена MS-DOS были распространены стелс-вирусы, перехватывающие прерывания для обращения к операционной системе. Вирус таким образом мог скрывать свои файлы из дерева каталогов или подставлять вместо зараженного файла исходную копию.

С широким распространением антивирусных сканеров, проверяющих перед запуском любой код на наличие сигнатур или выполнение подозрительных действий, этой технологии стало недостаточно. Сокрытие вируса из списка процессов или дерева каталогов для того, чтобы не привлекать лишнее внимание пользователя, является базовым приемом, однако для борьбы с антивирусами требуются более изощренные методы. Для противодействия сканированию на наличие сигнатур применяется шифрование кода и полиморфизм. Эти техники часто применяются вместе, поскольку для расшифрования зашифрованной части вируса необходимо оставлять расшифровщик незашифрованным, что позволяет обнаруживать его по сигнатуре. Поэтому для изменения расшифровщика применяют полиморфизм — модификацию последовательности команд, не изменяющую выполняемых действий. Это возможно благодаря весьма разнообразной и гибкой системе команд процессоров Intel, в которой одно и то же элементарное действие, например сложение двух чисел, может быть выполнено несколькими последовательностями команд.

Также применяется перемешивание кода, когда отдельные команды случайным образом разупорядочиваются и соединяются безусловными переходами. Передовым фронтом вирусных технологий считается метаморфизм, который часто путают с полиморфизмом. Расшифровщик полиморфного вируса относительно прост, его функция — расшифровать основное тело вируса после внедрения, то есть после того как его код будет проверен антивирусом и запущен. Он не содержит самого полиморфного движка, который находится в зашифрованной части вируса и генерирует расшифровщик. В отличие от этого, метаморфный вирус может вообще не применять шифрование, поскольку сам при каждой репликации переписывает весь свой код.[16]

# Профилактика и лечение

Абсолютной защиты от вредоносных программ не существует: от «эксплойтов нулевого дня» наподобие Sasser или Conficker не застрахован никто. Но с помощью некоторых мер можно существенно снизить риск заражения вредоносными программами. Ниже перечислены основные и наиболее эффективные меры для повышения безопасности:

* использовать современные операционные системы, не дающие изменять важные файлы без ведома пользователя;
* своевременно устанавливать обновления;
* если существует режим автоматического обновления, включить его;
* помимо антивирусных продуктов, использующих сигнатурные методы поиска вредоносных программ, использовать программное обеспечение, обеспечивающее проактивную защиту от угроз (необходимость использования проактивной защиты обуславливается тем, что сигнатурный антивирус не замечает новые угрозы, ещё не внесенные в антивирусные базы);
* постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
* ограничить физический доступ к компьютеру посторонних лиц;
* использовать внешние носители информации только от проверенных источников;
* не открывать компьютерные файлы, полученные от ненадёжных источников;
* использовать персональный Firewall (аппаратный или программный), контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь;
* Регулярно повышать свои знания в области компьютерной безопасности.

# Юридические аспекты

За создание, использование и распространение вредоносных программ предусмотрена различная ответственность, в том числе и уголовная, в законодательстве многих стран мира. В частности, уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ предусмотрена в Статье 273 УК РФ. Для того, чтобы программа считалась вредоносной, нужны три критерия:

Уничтожение информации или нарушение работы. Таким образом, взломщик защиты от копирования — не вредоносная программа.

Несанкционированная работа. Программа форматирования диска, входящая в комплект любой ОС, не является вредоносной, так как её запуск санкционируется пользователем.

Заведомость — явная цель несанкционированно уничтожить информацию. Программы с ошибкой могут пройти как нарушение прав потребителей или как преступная халатность — но не как вредоносные.

Более чёткие критерии, по которым программные продукты (модули) могут быть отнесены к категории вредоносных программ, до настоящего времени нигде четко не оговорены. Соответственно, для того, чтобы утверждение о вредоносности программы имело юридическую силу, необходимо проведение программно-технической экспертизы с соблюдением всех установленных действующим законодательством формальностей.

Стоит признать, что в РФ нарушение авторских прав часто квалифицируют как «создание и распространение вредоносных программ» — из-за более жёсткого наказания за последнее. Впрочем, создание вредоносных программ — преступление против оператора ЭВМ (владельца аппаратного обеспечения либо уполномоченного им человека), нарушение авторского права — против правообладателя.

# Экономика

В настоящее время кибер-пространство переживает перерождение кибер-преступности, количество переходит в качество – все чаще преступники объединяются для достижения конкретной цели – краже денег и все реже распространение вредоносных программ происходит по другим причинам. Появляются специфичные услуги, развивается их рынок. Сфера кибер-криминала успешно монетизируется, переходит на денежные рельсы.

Общий объем мирового рынка киберпреступности в 2011 году эксперты компании оценивают в $12,5 млрд. На долю американцев припадает 40% рынка. Еще 18% удерживают мошенники из Китая. Объединенные русским языком хакеры занимают “почетное” второе место в этом рейтинге с 36% доходов. Анализ проводился на данных международных организаций и компаний в сфере компьютерной безопасности, а также на информации из открытых источников.

Самый большой урон интернет-пользователям России в 2011 нанесли кибермошенники. Им удалось украсть около $942 млн. Первое место среди интернет-мошенничества занимают махинации в системах интернет-банкинга — 21,3% от общей суммы или $490 млн. При обналичивании денежных средств было похищено 16% или $367 млн долларов. Фишинговые атаки принесли преступникам 2,4% ($55 млн), а хищение электронных денег — 1,3% ($30 млн) от общей суммы, пишет издание «Ведомости».

Спамеры в прошлом году заработали в общей сложности $830 млн или 36,1% от общей суммы. Наиболее используемыми темами спам-сообщений в прошлом году были медикаменты, контрафактная продукция и пиратское ПО.

Внутренний рынок киберпреступности за год увеличил свой объем до 10% или $230 млн. Эти денежные средства были заработаны злоумышленниками на продаже трафика, эксплойтов, загрузок и “анонимизации”.

Нашумевшие в 2011 году DDoS-атаки, по подсчетам специалистов, принесли киберпреступникам всего $130 млн или 5,6% от общей суммы рынка.

Среди тенденций современного рынка можно отметить, во-первых, то, что отдельные хакеры постепенно объединяются в крупные преступные группировки. Во-вторых, углубляется степень взаимосвязи между главными игроками, которые все чаще делятся между собой данными, помогают друг-другу бот-сетями, оказывают содействие при обналичивании украденных средств. Все это усложняет расследование киберпреступлений.

Еще одной тенденцией является сращивание виртуальных преступных группировок с традиционными организованными преступниками, которые пытаются взять под свой контроль этот вид преступной деятельности. Все чаще организаторами и участниками киберпреступлений становятся не квалифицированные программисты, а люди из офлайна, владеющие достаточными средствами, связями и намерениями.

Сейчас создание вирусов превратилось из одиночного хулиганского занятия в серьёзный бизнес, имеющий тесные связи с бизнесом спама, партнерок, продажей трафика и другими видами противозаконной деятельности.[17] [18] Сами вредоносные программы перестают быть монолитным кодом, перерастая в сложные расширяемые комплексы как с автоматическим, так и командным управлением. Создание же сложных комплексов ставит на новый уровень вопрос безопасности в кибер-пространстве – вопрос противодействия кибер-оружию.

# Кибер-оружие

До недавнего времени такое понятие было лишь уделом научной фантастики. Сегодня же это действительная реальность. Рассмотрим потенциального прародителя этого класса угроз червя Stuxnet.

win32/Stuxnet — компьютерный червь, поражающий компьютеры под управлением операционной системы Microsoft Windows. 17 июня 2010 года его обнаружил антивирусный эксперт Сергей Уласень из белорусской компании «ВирусБлокАда». Вирус был обнаружен не только на компьютерах рядовых пользователей, но и в промышленных системах, управляющих автоматизированными производственными процессами.

Это первый известный компьютерный червь, перехватывающий и модифицирующий информационный поток между программируемыми логическими контроллерами марки Simatic Step 7 и рабочими станциями SCADA-системы Simatic WinCC фирмы Siemens. Таким образом, червь может быть использован в качестве средства несанкционированного сбора данных (шпионажа) и диверсий в АСУ ТП промышленных предприятий, электростанций, аэропортов и т. п.

Уникальность программы заключалась в том, что впервые в истории кибератак вирус физически разрушал инфраструктуру.

Существует предположение, что Stuxnet представляет собой специализированную разработку израильских спецслужб, направленную против ядерного проекта Ирана. В качестве доказательства упоминаются завуалированные упоминания слова MYRTUS, содержащиеся в коде червя. Этим словом буквально переводится с иврита имя библейского персонажа, персидской царицы иудейского происхождения Эсфири, которая помогла сорвать планы полного уничтожения иудеев в Персидском царстве. Кроме того, в коде однажды встречается никак не объясненная дата 9 мая 1979 года (19790509). В этот день произошла казнь известного иранского промышленника Хабиба Эльганяна, еврея по национальности.

Американский журналист Дэвид Сангер в книге «Противостоять и скрывать: тайные войны Обамы и удивительное использование американской силы» утверждает, что Stuxnet был частью антииранской операции «Олимпийские игры» американского правительства.

Данный вирус использует четыре уязвимости системы Microsoft Windows (уязвимость «нулевого дня» (zero-day) и три ранее известные уязвимости) направленная на распространение при помощи USB-flash накопителей. Оставаться незамеченным антивирусными программами ему помогало наличие настоящих цифровых подписей (два действительных сертификата, выпущенных компаниями Realtek и JMicron) из той же зоны, что и атакуемые цели.

Объём исходного текста вируса составляет примерно 500 КБ кода на языке ассемблера, С и С++.

# Литература

[1] Спамооборона // KP.RU (недоступная ссылка — история)

[2] Доктрина информационной безопасности Российской Федерации

[3]McIlroy et al. Darwin, a Game of Survival of the Fittest among Programs

[4] Вирус RCE-1813 (Jerusalem — Иерусалим)

[5]George Smith. The Original Anti-Piracy Hack SecurityFocus, 12 августа 2002

[6]AlgoNet — Эпидемия MSBlast оказалась гораздо обширнее, чем предполагалось

[7]Cost of Sasser is $500m and counting Silicon.com

[8]The Scarred Man (англ.)

[9]Fred Cohen. Computer Viruses — Theory and Experiments (англ.)

[10]Коэн Ф. Компьютерные вирусы — теория и эксперименты (рус.)

[11]Leonard Adleman. An Abstract Theory of Computer Viruses (англ.)

[12] Цитируется по: Diomidis Spinellis. Reliable Identification of Bounded-length Viruses is NP-complete IEEE Transactions on Information Theory, 49(1), pp. 280—284, January 2003

[13] Alan M. Turing. On computable numbers, with an application to the Entscheidungs Problem. Proceedings of the London Mathematical Society, vol. 2, № 42, pp. 230—265, 1936, Corrections in 2(43): pp. 544—546

[14] Fred Cohen. Computational aspects of computer viruses Computers & Security, vol. 8, № 4, pp. 325—344, June 1989

[15]Признаки заражения компьютера. Лаборатория Касперского. Архивировано из первоисточника 28 мая 2012. Проверено 10 апреля 2012.

[16]Billy Belcebu. Метаморфизм Xine#4, перев. с англ. v0id

[17]Виталий Камлюк. Ботнеты. Вирусная энциклопедия. Лаборатория Касперского .

[18]Роман Боровко. Экономический ущерб от вирусов. Рынок информационной безопасности 2003. CNews-Аналитика. Архивировано из первоисточника 22 августа 2011.

[19] Статья 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ.