ВикипедиЯ

Компьютерный вирус

Материал из Википедии — свободной энциклопедии

Компью́терный ви́рус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

```
text    segment   'code'
        assume cs:text,ds:text
        org     100h     main

main    proc
        jmp     VirStart            ;Переход на вирус
        db      'A'                 ;Маркер заражённости
        mov     ax,4C00h            ;Штатное завершение
        int     21h

VirStart:
        call    $+3                 ;Определение адреса
FindIP: pop     bp                  ;начала вируса
        sub     bp,offset FindIP

        mov     di,100h             ;Восстановление
        lea     si,[bp+OldBytes]    ;оригинального начала
        movsw                       ;заражённого файла
        movsw

        mov     ax,2524h            ;Переопределение int 24h
        lea     dx,[bp+New_24h]
        int     21h

        call    FindVictimFiles     ;Подпрограмма поиска и заражения
                                    ;жертв

        mov     ah,1Ah              ;Восстановление int 24h
        mov     dx,80h
        int     21h
```

Начало исходного кода вируса для MS-DOS на языке ассемблера

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В обиходе «вирусами» называют всё вредоносное ПО[1], хотя на самом деле это лишь один его вид.

Содержание

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[2].

Первыми известными 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 Энди Хопкинса (англ. *Andy Hopkins*). В начале 1985 года Ги Вон (англ. *Gee Wong*) написал программу DPROTECT — первый резидентный антивирус.

Первые вирусные эпидемии относятся к 1986-1989 годам: Brain (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию), Jerusalem (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске[3]), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч заражённых ПЭВМ только в Нидерландах).

Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989[4]), 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.

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 удалённого администрирования BackOrifice (1998) и последовавшие за ней аналоги (NetBus, Phase).

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

В конце 1990-х — начале 2000-х годов с усложнением ПО и системного окружения, массовым переходом на сравнительно защищённые 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 распространённом ПО многочисленных уязвимостей открыло дорогу червям-эксплоитам. В 2004 году беспрецедентные по масштабам эпидемии вызывают MsBlast (по данным Microsoft, более 16 млн систем[5]), Sasser и Mydoom (оценочные ущербы 500 млн и 4 млрд долл. соответственно[6]).

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.

В начале 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»[7], 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»[8][9], где он сам приписывает авторство термина Леонарду Адлеману[10][11].

Формально вирус определён Фредом Коэном со ссылкой на машину Тьюринга следующим образом[12]:

$M : (S_M, I_M, O_M : S_M \times I_M > I_M, N_M : S_M \times I_M > S_M, D_M : S_M \times I_M > d)$

с заданным множеством состояний S_M, множеством входных символов I_M и отображений (O_M, N_M, D_M), которая на основе своего текущего состояния $s \in S_M$ и входного символа $i \in I_M$, считанного с полубесконечной ленты, определяет: выходной символ $o \in I_M$ для записи на ленту, следующее состояние машины $s' \in S_M$ и движения по ленте $d \in \{-1,0,1\}$.

Для данной машины M последовательность символов $v : v_i \in I_M$ 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'':

$$
\begin{aligned}
&\forall\ C_M\ \forall\ t\ \forall\ j: \\
&S_M(t) = S_{M_0}\ \wedge \\
&P_M(t) = j\ \wedge \\
&\{\ C_M(t,\ j)\ \ldots\ C_M(t,\ j + |v| - 1)\} = v\ \Rightarrow \\
&\exists\ v'\ \exists\ j'\ \exists\ t'\ \exists\ t'': \\
&t < t'' < t'\ \wedge \\
&\{j'\ \ldots\ j' + |v'|\} \cap \{j\ \ldots\ j + |v|\} = \varnothing\ \wedge \\
&\{\ C_M(t',\ j')\ \ldots\ C_M(t',\ j' + |v'| - 1)\} = v'\ \wedge \\
&P_M(t'') \in \{\ j'\ \ldots\ j' + |v'| - 1\ \}
\end{aligned}
$$

где:

- $t \in \mathbf{N}$ число базовых операций «перемещения», осуществлённых машиной
- $P_M \in \mathbf{N}$ номер позиции на ленте машины в момент времени t
- S_{M_0} начальное состояние машины
- $C_M(t, c)$ 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: $v, v' \in V$. Из данного определения следует, что понятие вируса неразрывно связано с его интерпретацией в заданном контексте, или окружении.

Фредом Коэном было показано[12], 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 $(M, X) : X_i \in I_M$ 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 локальные и

глобальные (Интернет) сети. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);
- по используемым технологиям (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

Распространение

Через Интернет, локальные сети и съёмные носители.

Механизм

Вирусы распространяются, копируя своё тело и обеспечивая его последующее исполнение: вписывая себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск через реестр 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), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплойтом, использующим уязвимость.

После того как вирус успешно внедрился в коды программы, файла или документа, он будет находиться в состоянии сна, пока обстоятельства не заставят компьютер или устройство выполнить его код. Чтобы вирус заразил ваш компьютер, необходимо запустить заражённую программу, которая, в свою очередь, приведёт к выполнению кода вируса. Это означает, что вирус может оставаться бездействующим на компьютере без каких-либо симптомов поражения. Однако, как только вирус начинает действовать, он может заражать другие файлы и компьютеры, находящиеся в одной сети. В зависимости от целей программиста-вирусописателя, вирусы либо причиняют незначительный вред, либо имеют разрушительный эффект, например удаление данных или кража конфиденциальной информации.

Каналы

- 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-накопители заменяют дискеты и 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. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.
- 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, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.
- Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.
- Веб-страницы. 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 и локальные сети (черви). 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 удалённо 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. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

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 заражённого файла исходную копию.

С широким распространением антивирусных сканеров, проверяющих перед запуском любой код на наличие сигнатур или выполнение подозрительных действий, этой технологии стало недостаточно. Скрытие вируса из списка процессов или дерева каталогов для того, чтобы не привлекать лишнее внимание пользователя, является базовым приёмом, однако для борьбы с антивирусами требуются более изощрённые 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[14].

Профилактика и лечение

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости (учётная запись администратора в Windows).
2. Не запускать незнакомые программы из сомнительных источников.
3. Стараться блокировать возможность несанкционированного изменения системных файлов.
4. Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
6. Пользоваться только доверенными дистрибутивами.
7. Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
8. Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Экономика

Некоторые производители антивирусов утверждают, что сейчас создание вирусов превратилось из одиночного хулиганского занятия в серьёзный бизнес, имеющий тесные связи с бизнесом спама и другими видами противозаконной деятельности[15].

Также называются миллионные и даже миллиардные суммы ущерба от действий вирусов и червей[16]. К подобным утверждениям и оценкам следует относиться осторожно: суммы ущерба по оценкам различных аналитиков различаются (иногда на три-четыре порядка), а методики подсчёта не приводятся.

Криминализация

Создателю вируса *Scores*, нанесшего в 1988 ущерб пользователям компьютеров Macintosh, не было предъявлено обвинений, поскольку его действия не подпадали под имеющийся на тот момент в США закон *Computer Fraud and Abuse Act* либо другие законы. Этот случай привёл к разработке одного из первых законов, имеющих отношение к компьютерным вирусам: *Computer Virus Eradication Act* (1988)[17]. Сходным образом создатель самого разрушительного вируса ILOVEYOU в 2000 году избежал наказания из-за отсутствия на Филиппинах соответствующих ситуации законов[18].

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в некоторых странах как отдельный вид правонарушений: в России согласно Уголовному кодексу РФ (глава 28, статья 273), в США согласно *Computer Fraud and Abuse Act*, в Японии[19]. Во многих странах, однако, создание вирусов само по себе не является преступлением, и нанесенный ими вред подпадает под более общие законы о компьютерных правонарушениях[20].

Компьютерные вирусы в искусстве

В 2007 году украинский медиа-художник Степан Рябченко визуализировал виртуальную сущность компьютерных вирусов, придав им форму и образ[21][22].

Изображение компьютерного вируса Chernobyl, созданного украинским медиа-художником Степаном Рябченко в 2011 году.

См. также

- Троянская программа
- Хронология компьютерных вирусов и червей

Примечания

1. *А.Савицкий.* Опрос: Самая непонятная киберугроза (https://blog.kaspersky.ru/opros-samaya-neponyatnaya-kiberugroza/2960/). Лаборатория Касперского (10 февраля 2014).
2. McIlroy et al. Darwin, a Game of Survival of the Fittest among Programs (http://vx.netlux.org/lib/mdm00.html) Архивировано (https://web.archive.org/web/20050809073458/http://vx.netlux.org/lib/mdm00.html) 9 августа 2005 года.
3. Вирус RCE-1813 (Jerusalem — Иерусалим) (https://stfw.ru/page.php?id=9038)
4. George Smith. The Original Anti-Piracy Hack (http://www.securityfocus.com/columnists/102) SecurityFocus, 12 августа 2002
5. AlgoNet — Эпидемия (http://www.algonet.ru/?ID=446327)MSBlast оказалась гораздо обширнее, чем предполагалось
6. Cost of Sasser is $500m and counting (http://www.silicon.com/technology/security/2004/05/12/cost-of-sasser-is-500m-and-counting-39120627/) Silicon.com
7. The Scarred Man (http://vx.netlux.org/lib/mgb00.html) Архивная копия (http://web.archive.org/web/20110927080546/http://vx.netlux.org/lib/mgb00.html) от 27 сентября 2011 на Wayback Machine (англ.)

8. Fred Cohen. Computer Viruses — Theory and Experiments (http://vx.netlux.org/lib/afc01.html) (англ.) Архивировано (https://web.archive.org/web/20110321175646/http://vx.netlux.org/lib/afc01.html) 21 марта 2011 года.
9. Коэн Ф. Компьютерные вирусы — теория и эксперименты (http://www.nf-team.org/drmad/stuff/cohen.htm) Архивная копия (http://web.archive.org/web/20070930123209/http://www.nf-team.org/drmad/stuff/cohen.htm) от 30 сентября 2007 на Wayback Machine (рус.)
10. Leonard Adleman. An Abstract Theory of Computer Viruses (http://vx.netlux.org/lib/ala01.html) (англ.) Архивировано (https://web.archive.org/web/20051029165425/http://vx.netlux.org/lib/ala01.html) 29 октября 2005 года.
11. Цитируется по: Diomidis Spinellis. Reliable Identification of Bounded-length Viruses is NP-complete (http://vx.netlux.org/lib/ads03.html) Архивировано (https://web.archive.org/web/20051029163103/http://vx.netlux.org/lib/ads03.html) 29 октября 2005 года. IEEE Transactions on Information Theory, 49(1), pp. 280—284, January 2003
12. Fred Cohen. Computational aspects of computer viruses (http://vx.netlux.org/lib/afc10.html) Архивировано (https://web.archive.org/web/20060221061339/http://vx.netlux.org/lib/afc10.html) 21 февраля 2006 года. Computers & Security, vol. 8, № 4, pp. 325—344, June 1989
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. Billy Belcebu. Метаморфизм (http://www.wasm.ru/article.php?article=mmei) Архивная копия (http://web.archive.org/web/20110705180819/http://www.wasm.ru/article.php?article=mmei) от 5 июля 2011 на Wayback Machine Xine#4, перев. с англ. v0id
15. *Виталий Камлюк.* Ботнеты (http://www.viruslist.com/ru/viruses/analysis?pubid=204007610) (недоступная ссылка — *история* (https://web.archive.org/web/*/http://www.viruslist.com/ru/viruses/analysis?pubid=204007610)). *Вирусная энциклопедия*. Лаборатория Касперского (13 мая 2008). Дата обращения: 13 декабря 2008.
16. *Роман Боровко.* Экономический ущерб от вирусов (http://rnd.cnews.ru/reviews/free/security/part1/eco_loss.shtml). *Рынок информационной безопасности 2003*. CNews-Аналитика. Дата обращения: 13 декабря 2008.
17. *Charles Ritstein.* Virus Legislation // Executive Guide to Computer Viruses (https://books.google.com/books?id=iXBXgPqwkJIC&pg=PA37&lpg=PA37&dq=%22Computer+Virus+Eradication+Act%22&source=bl&ots=NE6ny0vaOT&sig=x8TI4Dv9s2Kfv3Md2lXi3JQqwjI&hl=ru&sa=X&ved=0CD8Q6AEwBWoVChMIp9WGzp-JyQIVQXxyCh0RoQ-e#v=onepage&q=%22Computer%20Virus%20Eradication%20Act%22&f=false). — NCSA, 1992.

18. *Jody R. Westby.* Laws on Crimes against Computer Systems // International Guide to Combating Cybercrime (https://books.google.com/books?id=wMqk28WPOf0C&printsec=frontcover&dq=international+cybercrime+law&hl=ru&sa=X&ved=0CBsQ6AEwAGoVChMI7Ieys6GJyQIVRScPCh0CYQpR#v=onepage&q=virus&f=false). — ABA Publishing, 2003.
19. Legislation Criminalizing Creation of Computer Viruses Enacted (http://cacm.acm.org/news/109785-legislation-criminalizing-creation-of-computer-viruses-enacted/fulltext)
20. *Авторы: Thomas J Holt,Adam M Bossler,Kathryn C Seigfried-Spellar.* Legal challanges in dealing with malware // Cybercrime and Digital Forensics: An Introduction (https://books.google.com/books?id=NsWgBgAAQBAJ&lpg=PA103&ots=SnJPUkb-Z7&dq=malware%20criminalization&hl=ru&pg=PA103#v=onepage&q=malware%20criminalization&f=false). — New York: Routledge, 2015. — С. 103.
21. Смотрите: Серия работ “Компьютерные вирусы” Степана Рябченко (https://officiel-online.com/lifestyle-2/art/stepan-ryabchenko-computer-viruses-art-works-serie/). *officiel-online.com*. Дата обращения: 15 июня 2020.
22. Цвет Чернобыля в работе украинского художника Степана Рябченко (https://artslooker.com/cvet-chernobyla-v-rabote-ukrainskogo-kh/). *ArtsLooker* (26 апреля 2020). Дата обращения: 15 июня 2020.

Ссылки

- Harold Thimbleby, Stuart Anderson, Paul Cairns. A framework for modelling trojans and computer virus infection (https://web.archive.org/web/20051120020756/http://vx.netlux.org/lib/aht01.html) (англ.)
- Truth about computer security histeria (http://www.vmyths.com/) (англ.) VMYTHS
- Развитие мобильных вирусов (https://web.archive.org/web/20070927205916/http://www.mobimag.ru/Articles/1044/Razvitie_mobilnyh_virusov.htm)
- Материалы и статьи по компьютерным вирусам на разных языках (http://vxheavens.com)
