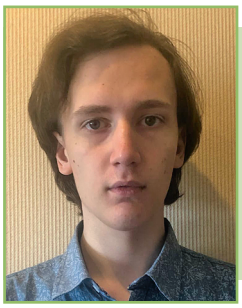
ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 004.49(045)
© Попов И. О., Марунько А. С., Петров О. И., Олейник А. А., 2020

Вирусы и антивирусные программы в информационной безопасности



Илья Олегович Попов, *студент факультета прикладной математики и информационных технологий, Финансовый университет, Москва, Россия*
Ilya O. Popov, *student, Faculty of Applied Mathematics and Information Technology, Financial University, Moscow, Russia*
ilya.pop.2014@yandex.ru

Анна Сергеевна Марунько, *студентка факультета прикладной математики и информационных технологий, Финансовый университет, Москва, Россия*
Anna S. Marunko, *student, Faculty of Applied Mathematics and Information Technology, Financial University, Moscow, Russia*
marunko.a@yandex.ru

Олег Игревич Петров, *студент факультета прикладной математики и информационных технологий, Финансовый университет, Москва, Россия*
Oleg I. Petrov, *student, Faculty of Applied Mathematics and Information Technology, Financial University, Moscow, Russia*
oleg.ptro737@gmail.com

Анастасия Александровна Олейник, *студентка факультета прикладной математики и информационных технологий, Финансовый университет, Москва, Россия*
Anastasia A. Oleynik, *student, Faculty of Applied Mathematics and Information Technology, Financial University, Moscow, Russia*
nastyadoma@mail.com

Научный руководитель: ***Терновсков В.Б.,*** *доцент, кандидат экономических наук, Финансовый университет, Москва, Россия /*
Scientific supervisor: ***Ternovskov V.B.,*** *Cand. Sci. (Econ.), Financial University, Moscow, Russia.*

АННОТАЦИЯ

В нынешних условиях беспрерывного развития технологий в области программирования, компьютерных сетей и сети Интернет не перестает расти и темная сторона прогресса: вирусное ПО. Рядовые пользователи зачастую не обращают внимания, когда они попадают на их компьютеры, и даже не имеют установленных антивирусных программ. Следовательно, необходимо исследовать все аспекты борьбы с вирусами: предотвращение заражения, методы обнаружения вредоносных программ, их уничтожение, а также ликвидация последствий. При достаточном объеме знаний о том, как сражаться с компьютерными вирусами, станет возможно эффективно информировать пользователей, не разбирающихся в данной сфере, и избегать вспышек вирусов, которые происходят и в компьютерном мире (например, вирус Petya). Для этого мы провели исследование основных научных источников по данной тематике и статистических данных. Как итог, в данной работе даются основные представления о вирусах и проводится анализ методов их классификации, обнаружения и уничтожения.

Ключевые слова: *вирусы; антивирусы; интернет; компьютеры; компьютерные сети; безопасность; информационная безопасность; ПО; браузеры; глобальные сети*

Для цитирования: **Попов И. О., Марунько А. С., Петров О. И., Олейник А. А. Вирусы и антивирусные программы в информационной безопасности.** ***Научные записки молодых исследователей.*** **2020;8(4):74-80.**

ORIGINAL PAPER

Viruses and Anti-viruses in Information Security

ABSTRACT

It is an open secret that no technology can be evolved without its dark side and all the disadvantages bring developed too. That is precisely why computer viruses are not surprising to anybody. However, it is genuinely astonishing that there are still a lot of people worldwide who are not aware of this dangerous phenomenon. They tend not to have anti-virus software installed and regard their computer malfunctions as something ordinary without any alarm. Therefore, our goal is to reconsider both methods of viruses' classification, detection, annihilation and how anti-virus software works itself. With that task completed, we have made a relatively recent and relevant analysis to help average computer users understand what a computer virus is and how to fight it.

Keywords: *viruses; anti-viruses; internet; computers; computer networks; security; information security; software; browsers; global networks*

For citation: **Popov I. O., Marunko A. S., Petrov O. I., Oleynik A. A. Viruses and anti-viruses in information security.** ***Nauchnye zapiski molodykh issledovatelei = Scientific notes of young researchers*****. 2020;8(4):74-80.**

Введение

Со времен появления первых компьютеров и по сей день вирусы являются одной из основных причин появления неполадок в работе ЭВМ, утечек информации, в том числе и конфиденциальных данных. При этом за все это время компьютерные вирусы успели эволюционировать и обрести новые многочисленные формы. Сейчас рядовому программисту ничего не стоит создать вирусную программу по разработанному шаблону, поэтому новое вредоносное ПО появляется чуть ли не каждую секунду.

Однако и эволюция антивирусных программ не стоит на месте. Методы обнаружения и предотвращения вредоносных действий продолжают развиваться. Также существуют платные версии большинства программ, предоставляющие более широкий функционал помимо работы с вирусами: например файервол (межсетевой экран), VPN и т.д. [1].

Несмотря на все достоинства, нынешнее защитное ПО далеко не идеально и имеет много недостатков. Как следствие, вопрос о борьбе с вирусными программами остается открытым.

Происхождение и классификация компьютерных вирусов

Идея и концепция механической структуры, способной к самовоспроизводству, активации, захвату и мутации, была выведена еще в 1959 г. американским ученым Л.С. Пенроузом, после чего Ф.Г. Сталь в качестве исследования реализовал эту идею при помощи машинного кода на IBM 650 [2].

Самой по себе проблемы компьютерных вирусов могло и не возникнуть, поскольку сами по себе ЭВМ сначала были только у крупных корпораций, правительственных организаций и подобных структур, так как сложность самой по себе ЭВМ делала ее крайне дорогим удовольствием для обычного человека, пока в 1979 г. компания Apple не выпустила первый доступный персональный компьютер Apple II. После того как многие пользователи получили в свое распоряжение личную ЭВМ, у вируса как у типа программы появилось то, что само по себе делает возможным его существование: потенциальная среда обитания и распространения.

С того момента было написано великое множество программ по распространению и борьбе с вирусами. Многие из них стали своего рода легендами. Как говорилось ранее, эволюция в мире информационных технологий не стоит на месте и различных видов вредоносных программ стало значительно больше, вследствие чего возникла необходимость в систематизированной классификации этих программ. Приведем такую характеристику.

Классифицировать весь спектр программ достаточно непростая задача в связи с различными аспектами, но можно дать вполне базовую классификацию по ключевым особенностям (см. *таблицу*).

Также можно добавить такие особенности, как поражаемая операционная система и выполняемые функции (например, слежка за пользователем, уничтожение данных, кража данных и т.д.).

Методы обнаружения компьютерных вирусов

Первым шагом в борьбе с вирусом и впоследствии восстановлении ЭВМ является, конечно же, обнаружение этого вредоносного ПО. В некоторых случаях это несложная задача: пользователь может самостоятельно понять, что его компьютер был заражен. Например, в интернет-браузере невозможно получить доступ к определенным веб-сайтам, регулярно меняется домашняя страница или сам браузер работает медленнее, чем обычно. Также пользователи зачастую замечают такие признаки:

- Медленная работа или зависания компьютера.
- Постоянно всплывающие оповещения на рабочем столе или в браузере.
- Неожиданные перезагрузки компьютера.
- Сообщения об ошибках, что системные файлы повреждены.
- Отсутствие доступа к командной строке диспетчеру задач и прочим системным приложениям [6].

Однако бывают и случаи, когда ошибки в работе операционной системы или браузера не так очевидны и пользователь спокойно выполняет всю необходимую ему работу, и тем не менее на компьютере имеются вирусы. Именно поэтому следует периодически сканировать все содержимое антивирусными программами, которые используют свои методы обнаружения вирусного ПО. Их можно поделить на две основных группы:

- Обнаружение вирусов по «словарю» [1].

Это достаточно простой способ. Антивирус просто сканирует все файлы и программы и сравнивает их со словарем, куда внесены существующие вирусы. Если есть совпадение, то антивирус удалит вредителя либо внесет в карантин.

Разумеется, чтобы данный метод справлялся со своей задачей, необходимо обновлять словарь и вносить в него новые вредоносные программы. Так как в наши дни их достаточно много, то, скорее всего, в словаре вашего антивируса будут далеко не все вирусы. Но чаще всего и этого достаточно, ведь большинство антивирусов используют именно метод словаря для обнаружения.

- Обнаружение вирусов по поведению программ.

Антивирусы, работающие по этому принципу, отслеживают то, как ведут себя программы и какие действия они выполняют. В основном вся подозрительная активность программ сводилась к записи новых данных в исполняемый файл, но теперь и обычные программы нередко делают то же самое. Как следствие, пользователь получает много ложных предупреждений, когда антивирус вновь принимает безобидный файл за вредоносный. Неудивительно, что этот способ применяется все реже и реже.

Таблица

Классификация компьютерных вирусов

Вредоносность	• Безвредные — такого рода программы просто способны распространяться в сети, переходя с одного ПК на другой, но при этом не выполняют какие-либо деструктивные функции по отношению к системе [3]. • Неопасные — вредоносные программы, способные перегружать память ПК или генерировать звуковые сигналы, изображения. • Опасные — программы, способные наносить урон системе. • Крайне опасные — вирусы, способные уничтожать данные, находящиеся в различных сегментах и секторах памяти, приводить к поломке механических частей ПК
Среда обитания	• Файловые — поражение исполняемых файлов, средой обитания являются соответственно COM и EXE файлы [3]. • Загрузочные — поражение секторов загрузки (Boot секторов) жестких дисков или секторов системного загрузчика. • Сетевые — поражение компьютерных сетей и систем. • Макро — поражение файлов программы Microsoft Office
Способ заражения	• Резидентные вирусы — вирусы, остающиеся в оперативной памяти после исполнения работы инфицированной программы. После перезагрузки системы будут удалены с устройства, если в коде программы не заложена функция автозапуска, при таком условии лишь произойдет повторное инфицирование системы [4]. • Нерезидентные вирусы — вирусы, не занимающие оперативную память устройства и выполняющиеся лишь однократно при исполнении вирусной программы
Особенности алгоритма работы	• Companion-вирусы — поражение EXE-файлов, при котором создается двойник COM-файла, после чего сначала исполняется файл с вирусом, потом файл самой программы. Содержимое EXE-файла при таком алгоритме не изменяется [5]. • Worms-вирусы — распространение в сети путем вычисления адресов других подключенных к этой сети устройств и отправка собственных копий на эти устройства. • Вирусы-паразиты — вирусы, способные изменять содержимое файлов и сегментов памяти зараженных устройств. • Stealth-вирусы — вирусы, способные перехватывать обращения дисковой операционный системы (DOS) к пораженным участкам диска и подставлять незараженные сегменты памяти. Помимо всего прочего, такие вирусы способны обманывать внутренние резидентные мониторы системы. • Вирусы-полиморфы — вирусы, не имеющие повторяющихся частей кода, в связи с этим такие вирусы очень трудно обнаружить. • Макровирусы — вирусы, поражающие макросы в файловых редакторах, таких как Microsoft Word и Microsoft Excel. • Вирусы, способные к самошифрованию,— вирусы, способные изменять свой программный код. • Вирусы с нестандартным алгоритмом — вирусы, имеющие свои собственные сигнатуры и структурные алгоритмы, сильно затрудняющие обнаружение вируса

Источник: составлено автором.

Также к методу обнаружения по поведению программы можно отнести принцип работы антивирусов, имитирующих небольшую часть кода запускаемой программы или имитирующих операционную систему (что-то вроде виртуальной машины) [4], а уже затем выполняющих программу на ней. Нетрудно догадаться, что такая проверка может занять слишком много времени, поэтому ею пользуются профессионалы, а не рядовые пользователи компьютеров. Зато она действительно является эффективной и может обнаружить все вирусы, оккупирующие ЭВМ.

Антивирусные программы

Говоря о методах обнаружения вирусов, мы уже упомянули, что, конечно же, главное средство борьбы с вредителями — это антивирусные программы. Они совмещают в себе все, что необходимо пользователю: находят вирус, ликвидируют его и его последствия, если был нанесен ущерб данным или другим программам.

При этом антивирусное ПО можно разделить на несколько видов, у которых все же несколько отличается функционал [7]:

- Детекторы.

Это как раз описанные выше антивирусы. Они находят проблему и «лечат» ее, используя метод словаря. К этому виду относят банальные и всем известные Doctor Web, антивирус Касперского.

- Фильтры.

Такие антивирусы следят за диском. При попытке любой программы записаться на него фильтр сообщит пользователю об этом и запросит у него разрешение на совершение операции. Таким образом можно бороться и с новыми неизвестными вирусами, если, конечно, они взаимодействуют с диском, а не с BIOS [8].

- Вакцинаторы.

Данный вид антивируса используется только для борьбы с конкретными известными вредоносными программами, поскольку вакцинатору необходимо взять признаки вируса. Затем он их записывает в безопасную программу пользователя, и вирус считает, что она уже заражена.

- Ревизоры.

Ревизоры хранят в себе сведения о состоянии программ и файлов, а при повторном сканировании используют их для сравнения и анализа изменений. Проверяется множество факторов: от размера файлов и времени их создания до состояния BOOT-сектора. Однако сам антивирус не определяет, вредоносный перед ним файл или нет. Он передает все данные об изменениях пользователю, который уже сам должен решить, что послужило им причиной. Если это, по мнению человека, вирус, то тогда уже ревизор удаляет небезопасные данные или помещает их в карантин [8].

Несмотря на то что существует множество видов антивирусов с различными функционалами и принципами работы, а также большой реестр разработчиков данного ПО, недостатков у антивирусов, к сожалению, тоже немало.

Все-таки еще ни одна антивирусная программа не сможет гарантировать вам стопроцентной защиты от любого вируса. Это может быть новый неизвестный вирус, пока еще не занесенный в словари, или вирус, который был сильно зашифрован. Тогда понадобится мощный распаковщик, чего, разумеется, нет во многих антивирусах.

Более того, антивирусы любят находить угрозу в абсолютно безопасных файлах. Поэтому рядовые пользователи сами пропускают мимо глаз предупреждения о вирусах и вредоносных файлах, что делает защиту менее надежной.

Исследование проблемы сетевых перехватчиков на антивирусах

Сетевой перехват — это процесс, производимый с помощью «атаки посредника». Особое ПО перенаправляет на себя шифрованное соединение пользователя с каким-либо сайтом, на который поступил запрос, и притворяется им. Затем перехватчик открывает новое соединение с изначальным веб-ресурсом и пропускает данные через себя между двумя соединениями. Поскольку тот, кто перехватывает трафик, получает доступ к большинству данных в рамках соединения, то он может считать, поменять и заблокировать любой контент, передающийся или получаемый клиентом. Это может использоваться как в хороших (блокировка вредоносных сайтов), так и в плохих целях (мошенничество, взлом устройств) [9, с. 101].

Зимой 2017 г. представителями Google, Mozilla, Cloudflare и нескольких университетов были резко раскритикованы процессы перехвата HTTPS-трафика антивирусами и сетевыми фильтрами.

Благодаря сделанному исследованию выяснили, что сетевой перехват HTTPS-трафика антивирусными программами может нести угрозу для безопасности пользователей и их подключения к всемирной сети.

Как правило, данное ПО не может получить доступ к HTTPS-пакетам, однако антивирусные компании нашли способ для анализа данных, идущих по зашифрованным подключениям: они стали устанавливать собственные корневые сертификаты на устройство пользователя, что значительно снижает безопасность подключения.

Более того, анализ показывает, что сканеры трафика, представленные в некоторых антивирусах, за счет своих недоработок имеют еще больше уязвимостей. Перехваченные подключения используют слабые криптографические алгоритмы и пользуются до этого взломанными шифрами, которые могут позволить проводить атаки на устройства и расшифровывать подключение [10, с. 20]. Таким образом, как минимум, около 10% трафика перехватывается не только антивирусами, но и сторонним ПО, которое пользуется им, с легкостью расшифровывает и анализирует в своих целях. Именно потому антивирусным компаниям стоит задуматься о новом способе сбора информации [11].

Но лишь полбеды заключается в том, что перехват HTTPS-пакетов снижает защищенность пользователя и его данных в сети. Другая проблема — это то, насколько часто встречается сетевой перехват.

Измерение количества перехватов — задача непростая, поэтому для обнаружения перехвата используется усовершенствованная версия технологии TLS fingerprinting (буквально сетевой отпечаток пальца). Так, будет определено, кто именно осуществляет соединение: перехватчик или браузер. Технология оценивает конструкцию клиентского TLS-пакета (в основном это наборы шифров и TLS-опции) и сравнивает ее с базой данных уже известных [9, с. 109].

Были оценены рабочие процессы интернет-магазина, сайта Cloudflare и серверов обновления Firefox. Рассматривали, сколько браузерного трафика они перехватывают. И результаты, в свою очередь, показали, что перехватывается от 4 до 10% трафика, при этом 4% — это сервера Firefox, а 10% — Cloudfare. Это немало, но необходимо помнить, что часть перехватов выполняется не злоумышленниками.

Если же разбить перехваченные HTTPS-пакеты по операционным системам, то выясняется, что с Windows перехватывается гораздо чаще, чем с MacOS или Linux. А трафик с мобильных устройств (Android и IOS) перехватывается реже, чем с ОС для ПК, но не в случае с серверами Firefox. Как ни странно, там чаще всего перехватом занимаются мобильные провайдеры [12]. Возможно, это происходит от того, что настольная версия Firefox использует отдельное хранилище для корневых SSL-сертификатов, что уменьшает вероятность данных быть перехваченными. На данный момент это один из маневров, который может быть временным решением проблемы перехвата HTTPS-трафика. Но минус маневра в том, что его предоставляет владелец сервера и запрошенного интернет-ресурса, а не антивирус, выступающий инициатором перехвата. Далеко не каждый сайт имеет возможность сделать это.

Таким образом, мы имеем возможность лишь наверняка определить масштаб урона, наносимого пользователю сетевыми перехватчиками, и лишь немного ликвидировать его, ведь все зависит от большого числа факторов: используемых ПО и соединений, запрашиваемого сайта, устройства пользователя и ОС на нем [13]. Но при этом абсолютно точно невозможно этого избежать, пока производители антивирусов не эволюционируют до менее уязвимого способа контроля HTTPS-трафика.

Выводы

Подводя итоги, невозможно не заметить, какое огромное количество вирусов существуют и создаются каждую минуту в мире, а также какой ущерб они наносят пользователям компьютеров и сети Интернет.

К счастью, существуют антивирусные программы, которые хоть и не полностью, но могут предотвратить урон или ликвидировать последствия. Поэтому пользователям одинаково необходимо научиться правильно использовать как антивирусы, так и незнакомые файлы и ссылки — в любой момент они могут оказаться вредоносными.

Более того, разработчикам антивирусного ПО тоже есть, над чем поработать. Методы обнаружения и уничтожения вирусов на компьютере далеко не идеальны, в чем можно убедиться и на примерах данной статьи, и на личном опыте. Да и создатели вредоносных программ не сидят на месте, постоянно улучшая код и шифрование.

Именно в такой гонке эффективности вирусов и антивирусов пользователи должны научиться при помощи различного ПО обеспечивать свою безопасность и безопасность ПК.

Список источников

1. Духан Е.И., Синадский Н.И., Хорьков Д.А. Программно-аппаратные средства защиты компьютерной информации. Екатеринбург: УрГУ; 2008. 240 с.
2. Курилов Ф.М. Оптимизационный метод проведения сравнительного анализа средств защиты информации от несанкционированного доступа. Технические науки: проблемы и перспективы: материалы III Междунар. науч. конф. (г. Санкт-Петербург, июль 2015 г.). СПб.: Свое издательство; 2015:40–44.
3. Власов Д.В., Минаев А.С. Методы противодействия анализу исполняемых файлов в информационных системах. *Информация и безопасность.* 2014;17(2):308–311.
4. Иванов В.Ю., Жигалов К.Ю. Методика обнаружения следов вредоносного программного обеспечения в дампах оперативной памяти. *Cloud of science.* 2018:5(2):2–5.
5. Рудниченко А.К., Шаханова М.В. Актуальные способы внедрения компьютерных вирусов в информационные системы. *Молодой ученый.* 2016;(11):221–223.
6. Кияев В.И. Безопасность информационных систем. М.: Открытый Университет «ИНТУИТ»; 2016. 192 с.
7. Гинодман В.А., Обелец Н.В., Павлов А.А. От первых вирусов до целевых атак. М.: МИФИ; 2014. 96 с.
8. Ложников П.С., Михайлов Е.М. Обеспечение безопасности сетевой инфраструктуры на основе операционной системы Microsoft. М.: Бином; 2008.
9. Хруска Ян. Борьба вирусов и антивирусов. Нью-Джерси, США: Издательство Саймона и Шустера; 1990.
10. Климентьев К.Е. Компьютерные вирусы и антивирусы. Д.А. Мовчан, ред. М.: ДМК-Пресс; 2015.
11. Антивирус Avast уличили в слежке за пользователями // iz.ru: ежедн. интернет-изд. 2019. 11 дек. URL: https://iz.ru/953277/2019–12–11/antivirus-avast-ulichili-v-slezhke-za-polzovateliami (дата обращения: 09.03.2020).
12. Панов С.С. Пять лучших антивирусов для защиты вашего смартфона. *Наука и образование сегодня.* 2018;(3):18–21.
13. Спицын В.Г. Информационная безопасность вычислительной техники. Томск: Эль Контент; 2011. 148 с.

References

1. Duhan E.I., Sinadskij N.I., Horkov D.A. Hardware and software protection of computer information. Ekaterinburg: UrGU; 2008. 240 p. (In Russ.).
2. Kurilov F.M. Optimization method for a comparative analysis of information security tools against unauthorized access. In: Engineering: problems and prospects. Materials of the III International scientific conference (St. Petersburg, July 2015). St. Petersburg: Svoe izdatelstvo; 2015:40–44. (In Russ.).
3. Vlasov D.V., Minaev A.S. Methods of counteracting the analysis of executable files in information systems. *Informatsiya i bezopasnost.* 2014;17(2):308–311. (In Russ.).
4. Ivanov V. Yu., Zhigalov K. Yu. Methodology for detecting traces of malware in core dumps. *Cloud of science.* 2018;5(2):2–5. (In Russ.).
5. Rudnichenko A.K., Shahanova M.V. Actual methods of introducing computer viruses into information systems. *Molodoy uchony.* 2016;(11):221–223. (In Russ.).
6. Kijaev V.I. Information System Security. Moscow: Otkrytyj Universitet INTUIT; 2016. 192 p. (In Russ.).
7. Ginodman V.A., Obelec N.V., Pavlov A.A. From the first viruses to targeted attacks. Moscow: MIFI; 2014. 96 p. (In Russ.).
8. Lozhnikov P.S., Mihajlov E.M. Securing the network infrastructure based on the operating system Microsoft. Moscow: Binom; 2008. (In Russ.).
9. Hruska Jan. Computer virus and anti-virus warfare. NJ: United States Imprint of Simon and Schuster; 1990. (In Russ.).
10. Klimentev K.E. Computer viruses and anti-viruses. D.A. Movchan, ed. Moscow: DMK-Press; 2015. (In Russ.).
11. Avast anti-virus got caught in users espionage. 2019, 11 December. URL: https://iz.ru/953277/2019–12–11/antivirus-avast-ulichili-v-slezhke-za-polzovateliami (accessed on 9.03.2020). (In Russ.).
12. Panov S.S. Top-5 anti-viruses for protecting your smartphone. *Science and education today.* 2018;(3):18–21. (In Russ.).
13. Spicyn V.G. Information security of computer technology. Tomsk: Jel Kontent; 2011. (In Russ.).