УДК 004.8

Компьютерные вирусы: системный подход

А.Е. Воробьев[*1], А.Н. Корчевский[*2], К.А. Воробьев[*3]

[*1] д.т.н., профессор, Грозненский государственный нефтяной технический университет,
fogel_al@mail.ru, OrcID: 0000-0002-7324-428X, SPIN-код: 3457-6870

[*2] к.т.н., доцент, Донецкий национальный технический университет,
korchevskyial@mail.ru, OrcID: 0000-0002-2247-7833, SPIN-код: 1293-7006

[*3] аспирант, Российский университет дружбы народов им. П. Лумумбы,
k.vorobyev98@mail.ru, SPIN-код: 8425-7290

Аннотация

Представлены результаты системного подхода к компьютерным вирусам. Даны определения наиболее важных вредоносных программ: вируса, компьютерного червя, троянского коня, логической бомбы и др. Описана история их появления и негативный эффект, который они с собой несут. Дана классификация компьютерных вирусов. Показаны основные способы заражения компьютеров вирусами.

Практически все пользователи электронных услуг в своей деятельности так или иначе сталкиваются с компьютерными вирусами, которые, зачастую довольно сильно их обременяют. В связи с тем, что рядовой пользователь экономически мало кому интересен, то эти вирусы возможно являются или «эхом» тайных компьютерных войн и операций, или сознательным деструктивным воздействием недружеских стран или отдельных групп на противостоящее им общество (страну), что в целом весьма негативно отражается на состоянии национальной экономики, незаметно «съедая» миллиарды долларов (или аналогичный эквивалент, в другой, более привычной, валюте). Так, система автоматического распространения Agent.BTZ вышла далеко за пределы сетей Министерства обороны США, и в результате заражения ПК происходили по всему миру спустя многие годы после её первоначального выпуска.

В информационных войнах, чтобы нарушить функциональность существующей инфраструктуры и хранимых данных, а также для заражения компьютеров и сетей атакованной стороны, зачастую используется вредоносное программное обеспечение (такое, как различные вирусы).

Вирус – это программа или код, который копирует себя в других файлах, с которыми он контактирует [6], в более крупную программу, изменяя её. При этом вирус запускается только тогда, когда начинает работать его программа-носитель. Затем вирус реплицирует себя, заражая (по мере своего размножения) другие рабочие программы системы атакованного объекта. В результате любая программа, загрузочный сектор, документ, поддерживающий макросы и т.д., могут быть заражены путем изменения содержимого этих файлов и копирования в них вирусного кода.

Компьютерный вирус обычно состоит из двух частей [6]:

• первая часть – это самокопирующийся код, позволяющий вирусу распространяться;

• вторая часть – рабочая составляющая (которая может быть как безвредной, так и чрезвычайно опасной).

Некоторые компьютерные вирусы состоят только из самокопирующегося кода. Иногда вирусу для распространения требуется взаимодействие с человеком: например, необходим запуск компьютерной программы, содержащей вирус, или открытие зараженного файла.

История компьютерных вирусов началась в 1948 г. В это время, хотя компьютерные вирусы ещё не получили своего названия, их впервые теоретически сформулировал и обосновал венгерский математик Джон фон Нейман, разработавший самовоспроизводящуюся компьютерную программу (которую считают предшественницей современных компьютерных вирусов, хотя она так и не была внедрена в том виде, в каком они впоследствии появились).

Первым настоящим предком современных вирусов была программа Prevading, которая могла получать доступ к другим программам на компьютерной системе UNIVAC 1108 [6].

В 70-х годах XX в. аспирант Университета Южной Калифорнии Фред Коэн разработал безымянную вредоносную программу, способную контролировать работу операционной системы компьютера. Он также первым ввёл термин «компьютерный вирус».

Первый известный компьютерный вирус появился в 1971 г. и назывался Creeper [4]. Этот вирус был нацелен на некоторые мэйнфреймовые компьютеры, работающие под управлением TENEX. Первое подтвержденное обнаружение компьютерного вируса в «дикой природе» произошло в 1981 г. и он назывался Elk Cloner [6].

Этот вирус заражал сектор BOOT у компьютеров Apple II.

Вирус Brain, появившейся в 1986 г., заражал 5,2-дюймовые дискеты. Он был делом рук двух братьев, Басита и Амджада Фарука Альви, владельцев компьютерного магазина в Пакистане [5]. Устав от того, что клиенты нелегально копируют их программы, они разработали Brain, который заменял загрузочный сектор дискеты вирусом. Вирус, который также стал первым скрытым вирусом, и содержал скрытое сообщение об авторских правах, но фактически не повреждал имеющиеся данные.

Появившейся в 1988 г. вирус Jerusalem стирал все запущенные компьютерные программы, а разработанный в 1989 г. вирус Datacrime мог выполнять низкоуровневое форматирование нулевого пути жесткого диска.

Вирус Michelangelo, появившийся в 1992 году, стал одним из первых компьютерных вирусов, привлекших всеобщее внимание, поскольку некоторые поставщики непреднамеренно продавали оборудование и программное обеспечение, им зараженное [14].

Макровирусы – это вирусы, способные заражать документы, созданные в таких программах, как Microsoft Word, – стали популярными в середине-конце 1990-х годов. Одним из самых известных вирусов электронной почты был вирус Melissa [6], выявленный в 1999 г., который довольно быстро распространился среди систем Windows (всего лишь за несколько дней заразив 90 тыс. систем). Melissa не был предназначен для повреждения компьютерных систем, но он проявляется тем, что внезапно для пользователей из некоторых серверов электронной почты на экран вырывалось не планированное сообщение. Необходимо отметить, что доля глобальных вредоносных кибератак через электронную почту с 2018 по 2022 год выросла с 33 % до 86 % [10].

Появление надежных и высокоскоростных широкополосных сетей в начале XXI в. изменило способы распространения вредоносных программ [5], которые больше не ограничивались дискетами или корпоративными сетями, а могли довольно быстро распространяться по электронной почте, через популярные веб-сайты и даже напрямую через Интернет. В результате ландшафт угроз стал неоднородной средой, объединяющей вирусы, черви и трояны – отсюда и название «вредоносное ПО», как общее название для вредоносного программного обеспечения. Одной из самых серьезных эпидемий этой новой эпохи стало появивление 4 мая 2000 года компьютерного вирсу LoveLetter, еще следовавшего шаблону более ранних почтовых вирусов, но, в отличие от макровирусов, доминировавших в мире угроз с 1995 г., он не принимал форму зараженного документа Word, а приходил в виде VBS-файла.

Создатель ILOVEYOU, Онель де Гусман, спроектировал своего червя так, чтобы он перезаписывал существующие файлы и заменял их своими копиями, которые затем использовались для распространения червя по всем контактам электронной почты жертв [5]. Поскольку сообщение приходило новым жертвам от знакомых, то они с большей вероятностью открывали его, что делало ILOVEYOU высокоэффективным вирусом.

В июле 2001 г. червь Code Red попытался подвергнуть весь Интернет распределённой атаке типа «отказ в обслуживании» (DDoS) [14].

Эти ранние программные вирусы распространялись от одной компьютерной программы к другой или от диска к диску и используя каждую зараженную программу, файл или диск, чтобы сделать как можно больше своих копий [6]. Вирусное программное обеспечение обычно скрыто в операционной системе компьютера или в прикладных программах. Некоторые вирусы ничего не делают, кроме своего воспроизведения, другие – отображают какие-либо неожиданные сообщения на экране компьютера, в то время как третьи – уничтожают данные или удаляют информацию с дисков.

Один из последних крупных вирусов, Heartbleed, появился в 2014 г. и поставил под угрозу серверы по всему Интернету [5]. Heartbleed, в отличие от предыдущих вирусов и червей, проникает через уязвимости в OpenSSL, универсальной криптографической библиотеке с открытым исходным кодом, используемой компаниями по всему миру.

Вирус 2015 г Moker может обходить антивирусы, «песочницы», виртуальные машины и, эксплуатируя уязвимость системы контроля учётных записей (User Account Control), функции Windows, которая должна предупреждать пользователей о внесении программой изменений, требующих разрешения администратора. Эта вредоносная программа даже применяет методы защиты от отладки после обнаружения, чтобы избежать анализа вредоносного кода и ещё больше обмануть исследователей.

На конференции Black Hat USA 2018 исследователи IBM представили новое поколение высокоточных и уклончивых инструментов для кибератак, действующих на базе искусственного интеллекта [1], под названием Deeplocker [7]. Эта вредоносная программа «скрывает свои намерения, пока не достигнет конкретной жертвы» и «выполняет свои вредоносные действия, как только модель ИИ идентифицирует цель с помощью таких специальных индикаторов, как распознавание лица, голоса и геолокации.

Эти особенности позволили вредоносной программе Deeplocker скрывать информацию о своей цели и назначении глубоко в коде (отсюда и название) [7]. Более того, экспертами подчеркивается, что даже если она будет обнаружена, то аналитикам вредоносных программ будет очень сложно определить, для чего она предназначена или что она искала. Не зная этих вещей, невозможно расшифровать условия её срабатывания, а это означает, что вредоносная нагрузка никогда не будет разблокирована до часа X и поэтому останется недоступной для её изучения.

В 2024 г. киберпреступники значительно активизировали использование искусственного интеллекта (ИИ) и машинного обучения [11]. Эти технологии позволили разработать гораздо более сложное вредоносное программное обеспечение, способное обходить традиционные методы обнаружения.

Ещё одна продвинутая угроза, обнаруженная в 2024 года, – вирус Stealthy, нацеленный в первую очередь на государственные учреждения и крупные корпорации с целью кражи конфиденциальных данных. Stealthy использует полиморфный код, что позволяет ему довольно часто менять сигнатуру и избегать своего обнаружения. Он проникает в сети через фишинговые письма и эксплуатирует уязвимости нулевого дня. Громкие утечки данных, приписываемые Stealthy, привели к утечке миллионов личных и корпоративных данных.

Одним из наиболее значимых вариантов вируса-вымогателя, появившихся в 2024 г., стал Blackout (рис. 1). Этот вирус-вымогатель специально нацелен на критически важную инфраструктуру, в частности, электросети [11]. Попав в систему энергосети, Blackout быстро распространяется через уязвимости устаревшего программного обеспечения, шифруя важные файлы и требуя выкуп в криптовалюте.

В марте 2024 года произошла скоординированная кибератака, направленная на несколько глобальных финансовых учреждений, что привело к временному нарушению банковских услуг и финансовых транзакций [11]. В ходе этой атаки использовалась комбинация компьютерных вирусов и банковских троянов, включая новый вариант под названием FinSteal. В результате финансовый сектор понес миллиардные убытки, возникших из-за необходимости выплаты выкупа, расходов на восстановление и ущерба репутации.

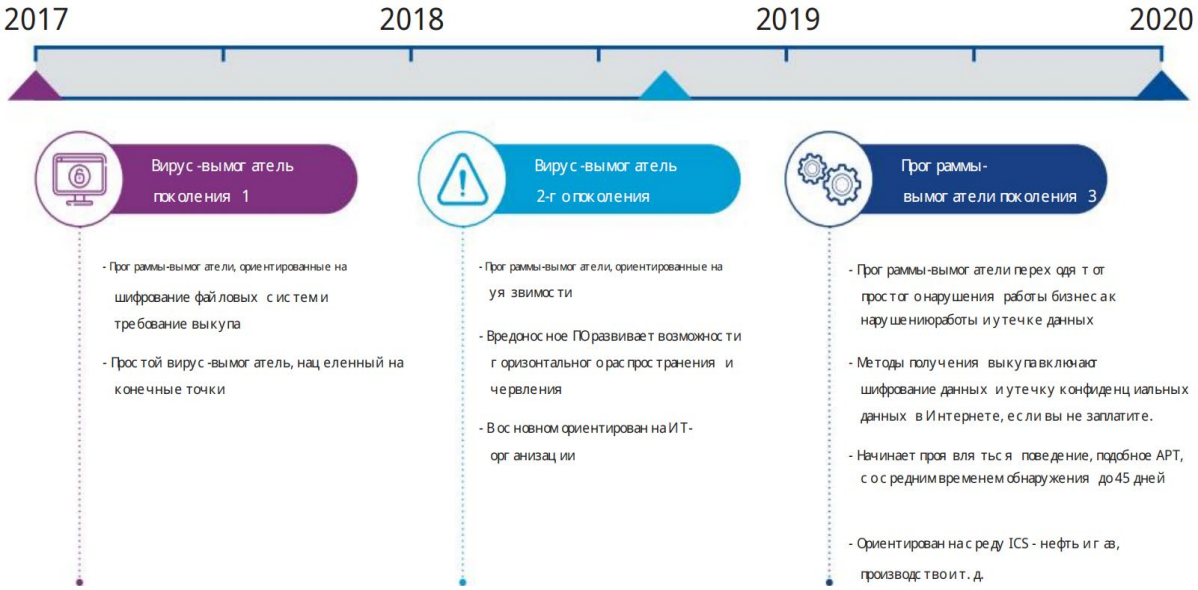

Рисунок 1 - Рост числа программ-вымогателей

На основе топологического анализа имеющихся вирусов и их действий была разработана их научная классификация [3], приведенная на рисунке 2.

Компьютерные черви – это вредоносные компьютерные программы [6], которые размножаются, путем своего копирования в полномасштабном режиме с одного компьютера на другой, обычно по сети Интернет [12], часто без участия человека. В отличие от традиционных вирусов, им не нужно заражать другие программы своими действиями. Компьютерные черви могут вызвать потерю связи, только лишь «поедая» имеющиеся ресурсы (уменьшая свободный объем памяти ПК) и распространяясь по сетям. Однако, такого червя можно легко модифицировать так, чтобы происходило удаление данных с ПК или что-то гораздо хуже и сложнее. Например, через них также можно получать доступ как к файлам в электронной почте, так и к самому компьютеру, что позволяет создавать бреши в операционных системах и приложениях. Кроме того, черви затрудняют работу сети, могут повреждать данные и снижать общую работоспособность компьютера.

Рисунок 2 - Классификация компьютерных вирусов [3]

Интернет-черви создают серьезные проблемы для зараженных компьютеров и могут нанести значительный ущерб из-за снижения объема свободного сетевого трафика. Например, червь SQL Slammer в январе 2003 г. каждые 8,5 секунд обеспечивал удвоение количества зараженных компьютеров.

Первый известный червь был создан в 1988 г. студентом Корнельского университета во время эксперимента и был совершенно случайно выпущен в Интернет. В результате, только в одних США он заблокировал 6000 компьютеров. Летом 2001 г. появился червь под названием Code Red. Его целью были интернет-сервисы, работающие под управлением серверов Microsoft.

В 2022 году детекторы вредоносных программ смогли заблокировать почти 206 млн. вредоносных программ-червей из вредоносных файлов (рис. 3). ***Троянские кони*** (трояны) – это вредоносные программы, которые маскируются под полезное программное обеспечение или расширяются, прикрепляясь к другим полезным программам [6].

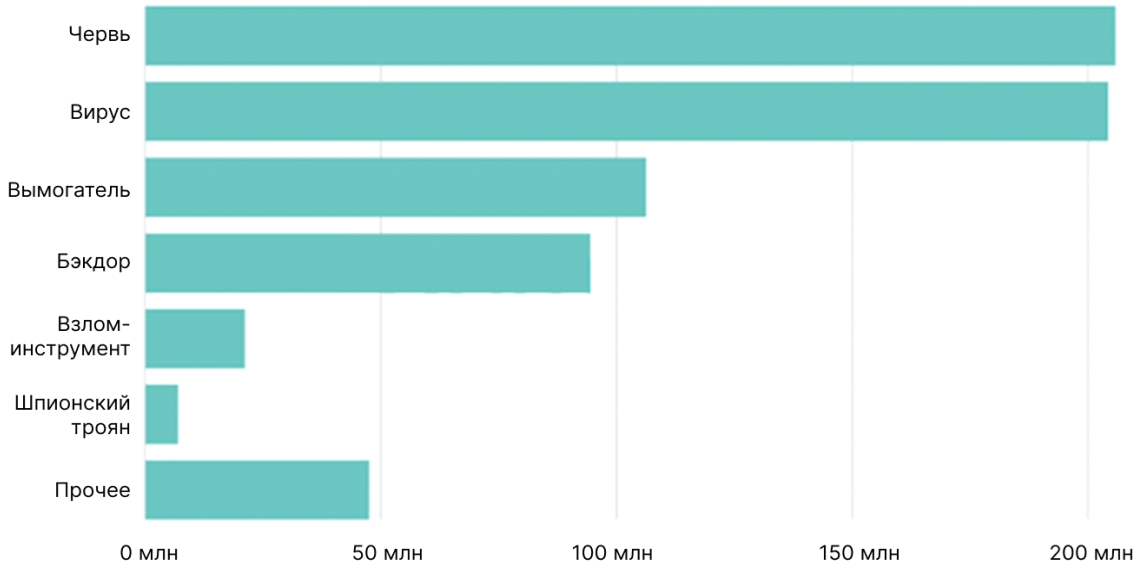

Рисунок 3 - Наиболее часто применяемое вредоносное программное обеспечение

«Трояны» обычно выполняют нежелательные действия на компьютере, скрытые в «фоне». Наиболее распространенным из этих нежелательных действий является раскрытие паролей пользователя, банковской информации и другой конфиденциальной информации, путем «подслушивания» обмена данными или просто путем чтения этих файлов и сообщения о них «владельцу» троянского коня. Первый троян под названием ANIMAL был разработан программистом Джоном Уокером в 1975 г.

В настоящее время троянские кони, существующие в виде вредоносных программ, а также скрытые в схемах оборудования, представляют собой одну из самых серьёзных угроз, с которыми могут столкнуться государства в случае войны, когда эффективность мобильной и другой связи и вооруженных сил напрямую будут зависить от компьютерных технологий [8]. Поскольку все самолёты, ракеты и радары используют бортовые компьютеры, то угроза подрывной деятельности во время кризиса, приводящая к сбоям в их работе или к тайному искажению критически важных данных, в значительной степени озадачивает военных стратегов и разработчиков программного (в том числе – антивирусного) обеспечения [2].

Троянские кони применяются и в полицейской службе, занимающейся сбором необходимой информации, осуществляемой с целью мониторинга и обнаружения криминальных структур и готовящихся преступлений.

Трояны распространяются путем установки или обновления коммерческих операционных систем и других программных и аппаратных компонентов компьютеров, а также через интернет-провайдеров, путем проникновения в существующие механизмы передачи данных (информации).

Наиболее известные троянские кони: Back Orifice; Netbus; SubSeven.

В 2025 г. были проведены целевые кибератаки на российские промышленные и научные организации трояном Batavia, который представляет собой вирус, специально разработанный для шпионажа, состоящий из VBA-скрипта и двух исполняемых файлов.

Отличительной особенностью Batavia является его узкая специализация на краже документов: эта программа собирает различные файлы, найденные на компьютере жертвы и подключённых съёмных носителях. Для этого Batavia получает доступ к системным журналам, спискам установленных программ, драйверов и компонентов операционной системы, а также к электронной почте и офисным документам различных форматов. Троян Batavia способен собирать таблицы, презентации и другие файлы, содержащие потенциально ценную корпоративную информацию.

При этом, на долю Trojan приходится 15,56 % мобильных вредоносных программ [10], а на долю его клона Troyan-spy – 4,55 % кибератак мобильных вредоносных программ.

Логическая бомба – это тип троянского коня, используемый для запуска вируса, червя или какой-либо другой системной кибератаки [12]. Логическая бомба представляет собой программный код, намеренно внедренный в программную систему, который повреждает или уничтожает её функциональность, при наступлении определенного условия (например, при достижении определенной даты или времени) или по специально отданной команде.

Люки (лазейки или черный ход) – это особый механизм, встроенный в систему её разработчиком [12]. Основная функция такой лазейки – дать возможность разработчику при необходимости нелегально пробраться обратно в компьютерную систему, обойдя существующую её защиту.

Сколы – современное программное обеспечение, которое может содержать деструктивные функции, а также может реализовывать подобные функции в компьютерном оборудовании [12]. Сегодняшние чипы содержат миллионы интегральных схем, которые производитель может легко настроить так, чтобы они заодно также содержали некоторые тайные и даже неожиданные функции. При этом эти электронные узлы и детали могут быть настроены таким образом, чтобы они отправляли радиосигналы (которые позволяют идентифицировать их точное местоположение), выходили из строя через определенное время или взрывались (после получения сигнала на определенной частоте) и т.д.

Так, компьютерные системы все больше полагаются на готовых и компоненты офшорных производителей, что вносит потенциальную уязвимость в систему безопасности.

Иностранные агенты или частные подрядчики могут предварительно загружать вредоносные программы и «заряженные» компоненты оборудования в продаваемые различные гаджеты (как для осуществления в последующем кибератак, так и для эксплуатационных целей). В 2009 г. Объединенный разведывательный комитет Великобритании предупредил, что китайские компоненты телефонной сети British Telecom могут быть предварительно загружены вредоносными программами или уязвимостями нулевого дня, что даст КНР возможность прервать поставки электроэнергии и продовольствия в эту страну. «Спящая» вредоносная нагрузка такого рода может быть удаленно запущена для достижения желаемого

результата в будущем, при возникновении политического или военного кризиса.

Кроме того, в 2012 г. Комитет по разведке Палаты представителей США предупредил, что детали для компьютеров, поставляемые Huawei, китайской компанией, основанной бывшим офицером Народно-освободительной армии, могут быть использованы для извлечения из памяти ПК конфиденциальных данных.

Наномашины и ***микробы*** – предоставляют возможность нанести серьезный вред компьютерной системе [12]. В отличие от вирусов, их можно использовать для кибератаки не на программное обеспечение, а на аппаратуру компьютерной системы. Наномашины – это крошечные роботы (меньше муравьев), которые могут быть распространены в информационном центре противника. Далее они распространяются по рабочим офисам, пока не найдут компьютер. Они настолько малы, что проникают в компьютер через имеющиеся в нем незначительные щели и отключают электронные схемы, нанося им существенные механические повреждения. Другой способ повредить компьютерное оборудование – представляет применение особой породы микробов, которые физически уничтожат кремниевые составляющие интегральных схем в компьютерной лаборатории.

Шпионское программное обеспечение – это широкая категория вредоносных программ, созданных для частичного перехвата информации или захвата контроля над компьютером, без ведома или разрешения пользователя [6].

Шпионское программное обеспечение тайно собирает информацию о пользователе через интернет-соединение, как правило, без его ведома, обычно в рекламных целях (так называемое Adware, которое показывает всплывающую рекламу и другие сообщения), но иногда для кражи конфиденциальной информации (такой, как имена пользователей, пароли и номера кредитных карт и др.). Шпионские приложения обычно встроены в качестве скрытого компонента в условно-бесплатные или бесплатные программы, загружаемых из Интернета [13]. После установки шпионское программное обеспечение отслеживает действия пользователя, а затем тайно передает эту информацию в фоновом режиме кому-то другому.

Шпион отличается от вируса и червя тем, что он, как правило, не воспроизводит себя. Как и многие новые вирусы, шпион предназначен для использования зараженных компьютеров в коммерческих целях (кража финансов, вымогательство и т.д.). В некоторых случаях, шпион используется для проверки соблюдения условий лицензии на использование той или иной компьютерной программы. Типичные тактики шпионского программного обеспечения – показ всплывающей рекламы, кража личных данных (включая финансовую информацию, такую как номера кредитных карт и пароли), отслеживание онлайн-активности в маркетинговых целях или перенаправление HTTP-запросов на рекламные страницы.

Ботнет – это набор скомпрометированных компьютеров, подключенных к Интернету, на которых запущено вредоносное программное обеспечение [13]. Каждое такое скомпрометированное устройство называется *ботом* (или зомби), а человек, управляющий ботнетом, называется *пастухом* ботов (или ботмастером). Управление и контроль ботнета обычно включают веб-серверы (называемые серверами управления и контроля или CnC), работающие для конкретной цели управления ботами, хотя некоторые старые ботнеты управляются пастухом ботов с помощью Internet Relay Chat (IRC).

Боты часто используются для совершения кибератак типа «отказ в обслуживании», рассылки спама, хранения украденных данных и/или загрузки дополнительных вредоносных программ на зараженный хост-компьютер.

Еще двумя наиболее часто используемыми методами эксплуатации существующих уязвимостей являются переполнение буфера ПК и кибератаки с использованием SQL-инъекций [13].

Переполнение буфера ПК – это кибератака, при которой хакер записывает в буфер памяти больше данных, чем рассчитанное для хранения информации. Часть этих данных попадает в соседнюю память, заставляя настольное или веб-приложение выполнять произвольный код с повышенными привилегиями или даже аварийно завершать работу ПК.

SQL-инъекция атакует базы данных через веб-сайт или веб-приложение. Для этого, хакер отправляет SQL-заявления в веб-форму, пытаясь заставить веб-приложение передать деструктивную SQL-команду в базу данных. Успешная атака SQL-инъекции может раскрыть содержимое базы данных (такое, как номера кредитных карт и социального страхования, пароли и т.д.) злоумышленнику.

Наименование и характеристики таких вредоносных вирусных программ было сведено в таблицу 1. Она наглядно отображает распространенные типы вредоносных программ, способы их распространения и потенциальные угрозы. Вирусы могут передаваться разными способами, но в настоящее время практически все вирусы передаются через Интернет, и лишь гораздо реже – через дискеты, сменные жесткие диски, компакт-диски и другие съемные носители [6]. Возможно, что в некоторых электронных узлах и деталях ПК иностранного производства заложены «спящие» вирусы или злонамеренные функции.

Таблица 1 - Наименование и основные характеристики распространенных типов вирусных программ

Вид	Название	Метод распространения	Цель
1	Файловые вирусы	Через зараженные исполняемые файлы	Повреждение данных, воровство информации
2	Макровирусы	Через зараженные документы MS Office	Изменение или разрушение файлов
3	Загрузочные вирусы	Запись в загрузочный сектор HDD/Floppy	Блокировка запуска ОС
4	Черви	Самораспространение через сети и e-mail	Порча данных, нагрузка на сеть
5	Трояны	Скрытая установка под видом полезных программ	Удалённое управление компьютером, кража данных
6	Логические бомбы	Автоматический запуск при определенном событии	Массивное повреждение данных
7	Polymorphic (полиморфные)	Постоянное изменение собственного кода	Сложность обнаружения
8	Stealth (невидимые)	Скрытие следов активности	Длительное паразитирование
9	Spyware	Сбор данных без ведома пользователя	Украденные пароли, история просмотров
10	Ransomware (вымогатели)	Шифрование файлов и требование выкупа	Заблокированный доступ к данным

Наиболее распространенными способами заражения компьютера вирусами являются [9]:

• Вложения в электронные письма. Большинство вирусов отправляются в виде вложений в электронные письма, которые якобы отправлены от имени знакомого пользователю человека или от имени легальной компании или организации.

• Посещение вредоносных веб-сайтов. Большинство пользователей думают, что они в безопасности, если никогда не нажимают ни на какие ссылки во время серфинга в Интернете. Однако многие веб-сайты содержат скрытый код, который автоматически загружает вредоносное программное обеспечение на атакуемый компьютер при просмотре без всякого предупреждения.

• Обмен файлами по технологии P2P. Эта процедура позволяет загружать музыку, фильмы, игры и программное обеспечение с других компьютеров. К сожалению, эти файлы часто заражены вирусами, которые проникают на компьютер при попытке их воспроизведения.

• Загрузка пиратского программного обеспечения или игр. Многие пользователи считают, что загрузка пиратских версий популярного программного обеспечения – это нормально, поскольку за нее не нужно платить. Однако это может подвергнуть их компьютер риску заражения вредоносным кодом, встроенным в такие файлы.

Из всей истории компьютерных вирусов, появившихся на сегодняшний день, наиболее разрушительными являются [9]:

• Love Bug – червь, вызвавший сбой в работе компьютеров по всему миру в мае 2000 года.

• Вирус ILOVEYOU представлял собой компьютерный вирус, который распространял любовное послание от филиппинца всем его онлайн-друзьям. Он был создан филиппинским программистом, который отправил его вложением к электронному письму с темой «ILOVEYOU». Вирус был разработан для заражения компьютеров под управлением Microsoft Windows 3 мая 2000 г. ровно в 10:00 по Гринвичу (манильское время).

• Червь Slammer, который заразил более 90 % всех уязвимых машин в Интернете в течение 10 минут после его появления в январе 2003 года.

• Code Red II и Nimda – оба червя, которые в июле 2001 года начали массированные атаки типа «отказ в обслуживании» на крупные веб-сайты.

• В ноябре 2003 года червь Blaster заразил более 250 тыс. компьютеров под управлением Windows менее чем за 24 часа. Червь Slammer считается самым быстро распространяющимся компьютерным вирусом, когда-либо выпущенным в киберпространство. В первый день он распространялся со скоростью около миллиона компьютеров в минуту и т. д.

• Программа-вымогатель Wannacry (также являющаяся разновидностью вируса) – это глобальная кибератака, начавшаяся 12 мая 2017 года. Изначально атака была направлена на Национальную службу здравоохранения (NHS) в

Англии, но вскоре распространилась по всему миру на другие организации и предприятия.

Программа-вымогатель – это тип вредоносного программного обеспечения, которое блокирует файлы атакуемого пользователя или удерживает его компьютерную систему в заложниках до тех пор, пока он не заплатит за её восстановление. В данном случае хакеры требовали 300 долл. в биткоинах за каждый заражённый компьютер.

Литература

1. Воробьев, А.Е. Введение в искусственный интеллект / А.Е. Воробьев, К.А. Воробьев, К.К. Кушеков. – Москва, Вологда: Инфра-Инженерия, 2026. – 132 с.

2. Воробьев, А.Е. Направления разработки компьютерных операционных систем / А.Е. Воробьев, К.А. Воробьев, К.А.Х. Алнассар // Сборник статей LXX международной научно-практической конференции. – Москва: Научно-издательский центр «Актуальность», 2025. - С. 69-75.

3. Основным определяющим признаком данной разновидности вредоносного ПО // https://kasheloff.ru/photos/osnovniym-opredelyayushim-priznakom-dannoy-raznovidnosti/76.

4. Популярные типы компьютерных вирусов // https://www.pctechguide.com/virus-removal/popular-computer-virus-types-and-their-effects.

5. A brief history of computer viruses & what the future holds // https://www.kaspersky.co.uk/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds.

6. Damjanovi Dragan Z. Types of information warfare and examples of malicious programs of information warfare // Technical Courier. Vol. 65, N 4. 2017. Pp. 1044-1059.

7. Fabio Cristiano, Dennis Broeders, François Delerue, Frédérick Douzet, and Aude Géry. Artificial intelligence and international conflict in cyberspace edited. New York. 2023. - 279 p. DOI: 10.4324/9781003284093.

8. Fred Schreier. On Cyberwarfare. Geneva Centre for the democratic control of armed forces. Switzerland, 2015. - 133 p.

9. History of computer virus // https://www.neumetric.com/history-of-computer-virus.

10. Naveen Kumar. 83 Cybersecurity statistics (2025): worldwide data & trends // https://www.demandsage.com/cybersecurity-statistics.

11. Notable computer viruses of 2024 // https://launchits.com/notable-computer-viruses-of-2024.

12. Reto E. Haeni. Information warfare an introduction. Washington. 1997. 16 p.

13. Steve Piper. Definitive Guide™ to next-generation threat protection. USA. 1997. 76 p.

14. Zephin Livingston. The history of computer viruses & malware // https://www.esecurityplanet.com/threats/computer-viruses-and-malware-history. 2022.

Воробьев А.Е., Корчевский А.Н., Воробьев К.А. Компьютерные вирусы: системный подход. *Представлены результаты системного подхода к компьютерным вирусам. Даны определения наиболее важных вредоносных программ: вируса, компьютерного червя, троянского коня, логической бомбы и др. Описана история их появления и негативный эффект, который они с собой несут. Дана классификация компьютерных вирусов. Показаны основные способы заражения компьютеров вирусами.*

Ключевые слова*: компьютерные вирусы, история появления, воздействие, классификация, распространение, деструктивное воздействие.*

Vorob'yov A.E., Korchevskyi A.N., Vorob'ev K.A. Computer viruses: system approach. *The article presents the results of a systematic approach to computer viruses. Definitions of the most important malicious programs are given: a virus, a computer worm, a Trojan horse, a logical bomb, etc. The history of their appearance and the negative effect they carry are described. A classification of computer viruses is given. The main ways of infecting computers with viruses are shown.*

Keywords*: computer viruses, history of appearance, impact, classification, distribution, destructive impact.*

Статья поступила в редакцию 18.09.2025
Рекомендована к публикации профессором Мальчевой Р. В.