УДК 004.491.22

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ ИНФОРМАЦИИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Андрей Алексеевич Хохлов
студент
garlic142@gmail.ru
Наталия Владимировна Пчелинцева
старший преподаватель
natas79@mail.ru
Алла Борисовна Лыкова
студент
lukovaalla3@gmail.com
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье рассматриваются компьютерные вирусы и вредоносные программы. Описана классификация вирусов и признаки заражения компьютера, действия, необходимые для предотвращения заражения ПК.

Ключевые слова: ПК, вирус, классификация, угроза, антивирус, уязвимости, система, файлы.

Компьютерные вирусы – это вредоносные программы, которые разрабатываются для проникновения в компьютер и наносить различные виды ущерба, такие как уничтожение данных, кража личной информации, блокировка компьютера и многие другие.

Варианты проникновения угроз в систему представлены в таблице 1.

Таблица 1

Варианты проникновения вредоносный ПО в систему компьютера

Способ проникновения	**Как происходит заражение**
При скачивании с сайтов	1. Во время скачивания в файле загрузчика может находиться встроенный вирус, который никаким образом заранее обнаружить не получиться; 2. Скачивание дополнительных пакетов, помимо основного файла, т.е. не снятие галочек в нужных местах
Брешь в системе безопасности	Отключенный для скачки файла на какое-то время антивирус может быть причиной временного отсутствия безопасности и попадания вируса в систему
Через электронную почту	Мошенники рассылающие по почте письма с вирусами не являются исключением. При открытии документа из письма на компьютер переносится зараженная программа
Предоставление доступа третьим лицам	При расширении круга лиц, имеющих доступ к ПК может произойти несанкционированный вход и получения прав ко всем файлам
Программы-обманщики	Выдают ложные уведомления, что на вашем ПК есть вирусы и предлагают скачать антивирус перейдя по ссылке
Носители информации	При подключении, к примеру, флешки к ПК вирусы сидящее на ней

	автоматически могут перенестись на компьютер
Бэкоды	Намеренные или произвольно созданные дефекты ПО, сетей или систем защиты

Рассмотрим классификации вирусов.

По способу заражения выделяют резидентные и нерезидентные программы. Первые ищут «жертв» постоянно. Ко вторым относятся вирусы, специализирующиеся на разовом инфицировании.

По местонахождения вирусы делятся на:

1. Загрузочные – работают только после включения операционной систему и начинают буйствовать;
2. Файловые – поступают вместе с основными программами и при открытии заражают систему;
3. Макровирусы – по большей части работают с редакторами (текстовыми, табличными, видеоредакторами);
4. Сетевые – попадают через сеть при скачивании файлов.

Про построение алгоритмов вирусы разделяют на шифровальные и перезаписывающие. Первый вид основан на зашифровке своих данных для худшего обнаружения. Второй перезаписывает себя самого частично или полностью, заполняя систему ненужным «хламом».

По степени опасности вирусы подразделяются на:

1. Безвредные – не несущие абсолютно никакого вреда системе;
2. Представляющие низкую угрозу – в большей степени это вирусы, забивающие ОЗУ, что в свою очередь ведет к зависаниям ПК;
3. Потенциально опасные – часто антивирусы могут путать программы ускорители с потенциально опасными программами;
4. Опасные – вирусы, наносящие значительный урон ОС (произвольное изменение файлов);
5. Чрезвычайно опасные - такие вирусы как трояны, полностью ломающие систему и ведущие к утечке важных файлов в сеть.

Некоторые вирусы нельзя отнести к какой-то одной группе, потому что бывают такие виды вирусов, которые могут какое-то время быть неактивными на ПК, а в определенный момент начать работать. Другие же могут подавляться системой безопасности и вовсе не иметь шансов проявить себя из-за ограничений возможностей.

Рассмотрим классификацию вирусов по механизму зараженя (рисунок 1) [4].

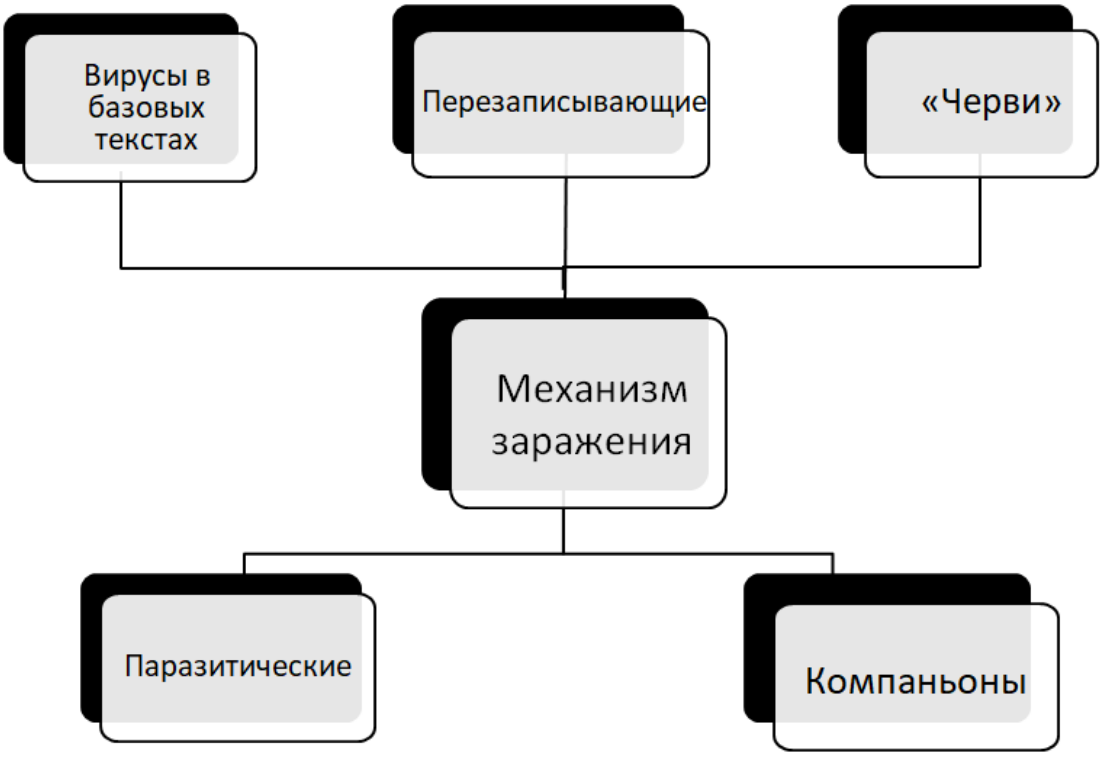

Рисунок 1 – Классификация деления вирусов по механизму заражения

Перезаписывающие вирусы изменяют программный код и подстраивают его под себя. Этот вирус является простым, так как файл у которого был заменен код очень быстро обнаруживается системой и сразу восстанавливается компьютером. Поэтому данный вирус особой опасности не несет.

Паразитические являются более опасным видом вирусов, за счет внедрения себя в любую точку файлу, будь то конец, середина или начало.

Если вирус проникает в начало файла, он записывает его код в конец. Таким образом первым, что будет запускаться это вредоносный файл. Но ведь так система не сможет работать и сразу выявить проблему. Как только файл перестает работать, он перезаписывает его начало, тем самым снова запуская его,

затем снова занимает свое место и ждет пока файл опять перестанет работать. Происходит дублирование системы.

Если вирус изменяет конец файла, то его задачей является приписаться в конце, при этом не забыв внести изменения в запуске файла для получения доступа к работе.

Третьим вариантом может стать добавление своего кода в середину файла. Более подробно процесс будет выглядеть так: вирус «раздвигает» для себя пространство или перезаписывает часть кода файла в его конец, при этом не забыв скомпенсировать его размер. Часто такой способ встречается при проникновении вируса в «дыры» системы, что вызывает сбои в работе. Также это могут быть «файлы-экзешники», которые имеют уязвимости, либо же неиспользуемые пространства.

Вирусы-черви являются своего рода бесполезными в большинстве случаев, так как для нанесения вреда компьютеру нужно их самостоятельное открытие. Они поступают в систему вместе с загрузочными файлами, а далее копируя свой код размножаются, но не могут нанести вреда пользователю. Как уже описывалось чуть выше, современные вирусы могут подстраиваться под ситуацию, так происходит и здесь. Для привлечения внимания они часть переименовывают себя в файлы с названиями install.exe или подобного плана.

Компаньоны – это необычный вид вирусов, который производит дублирование файла с его переименованием. Он не изменяет код файла, а просто меняет его имя, а себя в свою очередь называет главным именем, тем самым маскируясь. При запуске системы происходит запуск файла-хозяина, а доступ получает компаньон.

Вирусы в базовых текстах – поражают компиляторы, модули и исходные коды системных файлов [1,2].

Вирусы-ссылки не представляют собой потенциальной опасности. Ведь при открытии письма не происходит заражения, оно может произойти только после загрузки документа или перехода по ссылки в письме.

Вирусы-зомби. Долгое время не проявляют себя и большую часть времени являются неактивными. Но как только они получат сигнал от другого пользователя, который управляет ими, они сразу начнут свою вредоносную деятельность. Происходит резкое заражение системы. Как понятно из названия вирусы-зомби клонируют себе подобных, пытаясь подорвать систему безопасности и найти брешь. Компьютер начинает рассылать спам. Их цель заключается в достаточном количестве вирусов для достижения определенных задач. Таким образом, многие крупные компании подвергались такому заражению.

Еще одним интересным видом, с которым также имели дело крупные организации, особенно игровой индустрии – это эксплойт-вирусы. Они не дают прав для управления ПК, но пытаются найти точки воздействия, происходит сильный перегруз серверов (DDoS атака) и как следствие сбой в работе программ, игр и вылеты пользователей из аккаунтов. В большей степени этим занимаются хакеры в качестве забавы или умышленного вреда. В качестве примера можно привести вирус Sweet Orange.

Логические бомбы. Их опасность заключается в подставлении части кода в программу и последующего ожидания. Каждый раз, когда при входе в браузер, игры, приложения он будет анализировать наши запросы и ждать, когда мы будем на сайтах с введением логина и пароля. После чего они запоминают их и передают третьему пользователю. Так происходит кража личных данных, в том числе банковских счетов. Их коварность заключается в том, что антивирус часто не может их обнаружить и решить проблему оперативно не получается. Одним из таких представителей является вирус – Jerusalem.

Backdoor-вирусы. Если дословно переводить название, то получится возвращаемые вирусы. Они работают в паре с теми самыми безобидными червями. После первичного доступа хакеры повторно засылают в компьютер вирус для получения доступа ко всем важным файлам системы, с целью ее управления. Происходит утечка информации, а потом со счетов людей могут

сниматься деньги. Примечательной особенностью является размножение вируса и передача его на другие устройства. Представителем является – DoublePulsar.

Компьютерные вирусы мутанты содержат алгоритмы шифрования и расшифровки, за счет которых копии одной и той же программы не имеют одинаковых цепочек байтов. Их трудно выявить из-за сложных алгоритмов и модификаций. Все последующие версии мутирующего вируса имеют более развитый функционал и не похожи на своего родителя. Вирус мутант может нанести существенный вред компьютеру. Самые известные среди них - Grog, Dudley, Fly, Freddy.

Трояны – самый опасный вид вирусов, наносящий большой урон системе. Трояны активизироваться только после их открытия. Находятся они в безопасных местах и спят до определённого момента. После активации пользователи замечают утечку информации, ее удаление или замену.

Рассмотрим способы защиты от вредоносных программ. Распознать, что на вашем устройстве есть вирусу можно по следующим факторам (рисунок 2) [3].

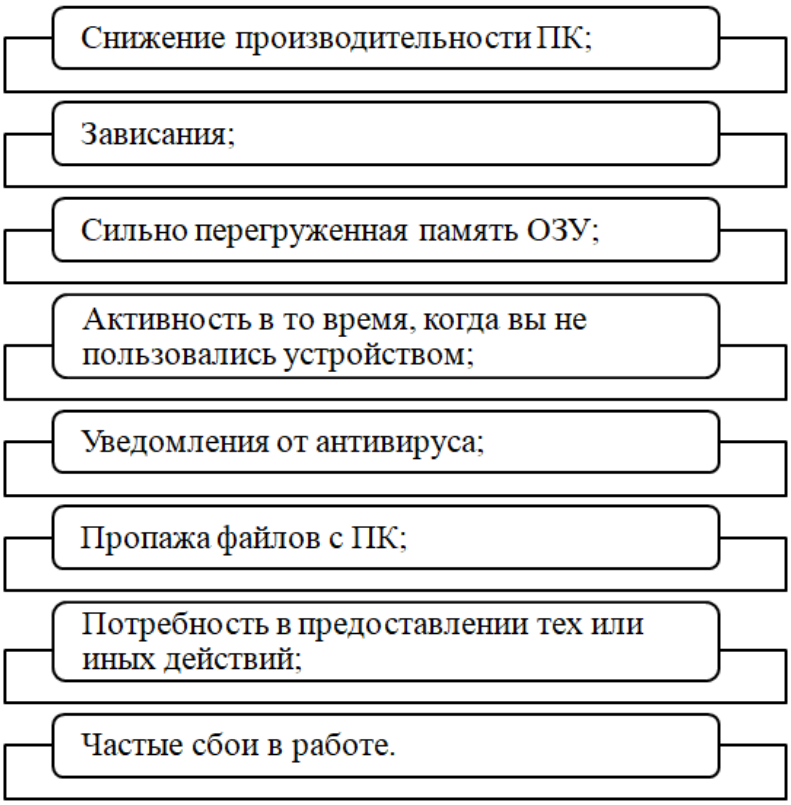

Рисунок 2 – Возможные факторы наличия вирусов в системе

Необходимо периодически сканировать систему на наличие вирусов или назначить время автоматического сканирования. Далее стоит настроить доступ разрешений для всех пользователей ПК и не предоставлять права третьим лицам. Регулярно обновлять программное обеспечение операционной системы и системы безопасности (защитник Windows или любой другой антивирусник). В купе со сканированием системы на вирусы, стоит проводить сканирование на наличие шпионских программ. Можно в дополнение включать настройки безопасности, предлагаемыми браузерами. Стоит помнить, что скачивать программы необходимо только с официальных сайтов. Как правило, в адресной строке нет лишних букв и некорректных доменов. В браузер стоит добавить антибаннер помогающий от навязчивой рекламы, так как обычно эти ссылки ведут на подозрительные сайты [5].

Соблюдение перечисленных способов защиты позволит снизить риски потери доступа к устройству и сохранит ваши личные данные. Большая часть вирусов, принимаемых в ПК вызвана невнимательностью пользователей и как правило отсутствия защиты.

Список литературы:

1. Алеексеев П., Козлов Д., Прокди Р. Антивирусы. Настраиваем защиту компьютера от вирусов // М.: СПб: Наука и Техника. 2008. 854с.

2. Александров К.П., Прокди Р.Г. Компьютер без сбоев, вирусов и проблем // М.: Наука и техника. 2008. 192 с.

3. Вульф М.М., Разумовский Н.Т. Защита компьютера от вирусов (книга + видеокурс на DVD) // М.: СПб: Наука и Техника. 2009. 160с.

4. Тимофеев А.В. Информатика и компьютерный интеллект // М.: Педагогика. 2012. 128с.

5. Пчелинцева Н.В., Гущина А.А. Компьютерная революция: положительное и отрицательное влияние на общество // Наука и образование: актуальные вопросы теории и практики. материалы Международной научно-

методической конференции. Оренбургский институт путей сообщения. Оренбург. 2021. С. 57-58.

UDC 004.491.22

ON THE ISSUE OF INFORMATION SECURITY AND INFORMATION PROTECTION IN MODERN SOCIETY

Andrey Al. Khokhlov
student
garlic142@gmail.com
Natalia V. Pchelintseva
senior lecturer
natas79@mail.ru
Vladislava M. Voroshilova
student
voroshilova.vladislava@inbox.ru
Alla B. Lykova
student
lukovaalla3@gmail.com
Michurinsk State Agrarian University
Michurinsk, Russia

Annotation. The article discusses computer viruses and malware. The classification of viruses and signs of infection of the computer, the actions necessary to prevent infection of the PC are described.

Keywords: PC, virus, classification, threat, antivirus, vulnerabilities, system, files.

Статья поступила в редакцию 03.05.2024; одобрена после рецензирования 13.06.2024; принята к публикации 27.06.2024.

The article was submitted 03.05.2024; approved after reviewing 13.06.2024; accepted for publication 27.06.2024.