ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.491 **DOI: 10.18413/2518-1092-2020-5-3-0-1**

Гоголь А.С.
Маслова М.А.

ОСНОВНЫЕ ВИДЫ КОМПЬЮТЕРНЫХ УГРОЗ

Севастопольский государственный университет, ул. Университетская, д. 33, г. Севастополь, 299053, Россия

e-mail: andrey.gogol.99@mail.ru, info@sevsu.ru, machechka-81@mail.ru

Аннотация
Компьютер – устройство, созданное для выполнения на данном устройстве операций. Данные операции определяются и задаются пользователем, и эти последовательности операций называют программами. Чаще всего это математические расчеты, но к этим последовательностям можно относить и операции ввода данных и их вывода. Сегодня люди объединяют компьютеры и получают из них сети и системы с огромным множеством таких инструкций. В наше время практически у каждого человека имеется портативный компьютер, с которым он путешествует, с помощью которого он обменивается данными с друзьями, коллегами либо родными. Пользователи данных устройств обмениваются данными друг с другом по сети «Интернет» и не только. Так же они создают локальные сети для обеспечения внутреннего электронного документооборота на предприятии. Либо передают информацию посредством внешних накопителей. Учитывая, уровень информатизации и масштабы информационной инфраструктуры, можно понять, что существует немало уязвимостей. Используя данные уязвимости, любой злоумышленник может внедрить вредоносное программное обеспечение в наш компьютер. Цель статьи – провести анализ существующих видов компьютерных угроз, проанализировать уязвимости и составить рекомендации, которые позволят избежать нарушений в работе системы.
Ключевые слова: компьютерные программы; компьютерные угрозы; уязвимости; вредоносное программное обеспечение; информация.

UDC 004.491

Gogol A.S.
Maslova M.A.

MAIN TYPES OF COMPUTER THREATS

Sevastopol state University, 33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: andrey.gogol.99@mail.ru, info@sevsu.ru, machechka-81@mail.ru

Abstract
Computer – a device created for performing operations on this device. These operations are defined and specified by the user, and these sequences of operations are called programs. Most often these are mathematical calculations, but these sequences can also include data entry and output operations. Today, people combine computers and get networks and systems from them with a huge number of such instructions. Nowadays, almost every person has a portable computer with which they travel, with which they exchange data with friends, colleagues or relatives. Users of these devices exchange data with each other over the Internet and beyond. They also create local networks to ensure internal electronic document management at the enterprise. Or transmit information via external storage devices. Given the level of Informatization and the scale of the information infrastructure, we can understand that there are many vulnerabilities. Using these vulnerabilities, any attacker can inject malicious software into our computer. The purpose of the

article is to analyze existing types of computer threats, analyze vulnerabilities, and make recommendations that will help avoid system failures.
Keywords: computer programs; computer threats; vulnerabilities; malicious software; information.

ВВЕДЕНИЕ

Проведем анализ актуальных компьютерных угроз. При анализе компьютерных угроз необходимо помнить и о неопытности либо о неосведомленность пользователя. Пользователь и сам может скачать вредоносное программное обеспечение, которое через любой промежуток времени нарушит любое свойство информации. Человеческий фактор, является самой распространенной уязвимостью, которую злоумышленники успешно используют сегодня, тем самым нарушая конфиденциальность, целостность и доступность информации. Из-за доступных уязвимостей многие компании и иногда рядовые пользователи несут огромные финансовые убытки. Эти проблемы будут актуальны всегда, пока существует и хранится информация, которая имеет определенную ценность. При всём этом любой другой пользователь может потерять персональные данные, которые хранятся на его персональном компьютере либо на мобильном устройстве. Чаще всего вредоносное программное обеспечение не выбирает какую-либо определенную организацию, либо человека.

ОСНОВНАЯ ЧАСТЬ

Рассмотрим основные виды компьютерных угроз, существующих сегодня (Рисунок 1).

Вирус либо программа-троянец находятся в интернете и распространяются столько, сколько потребуется. Данное программное обеспечение может годами быть неактивным и просто ожидать. Например, вредоносная программа-троянец «Petya» в июне 2017 года распространилась по множеству стран мира и поразила огромное количество компьютеров. Сети больших нефтяных компаний и обычные медицинские лаборатории лишились информации, которая хранилась на их стационарных компьютерах. Данный вирус можно назвать не только троянским программным обеспечением, но и шифровальщиком. Он переписывал главные загрузочные записи пользователей операционной системы Microsoft Windows и после этого шифровал базы данных, в которых хранились сведения о содержимом тома с файловой системой [1].

Таким образом, пользователь терял доступ к операционной системе и данным, которые находились на носителях. Пользователю предлагалось купить ключ, который разблокирует его операционную систему.

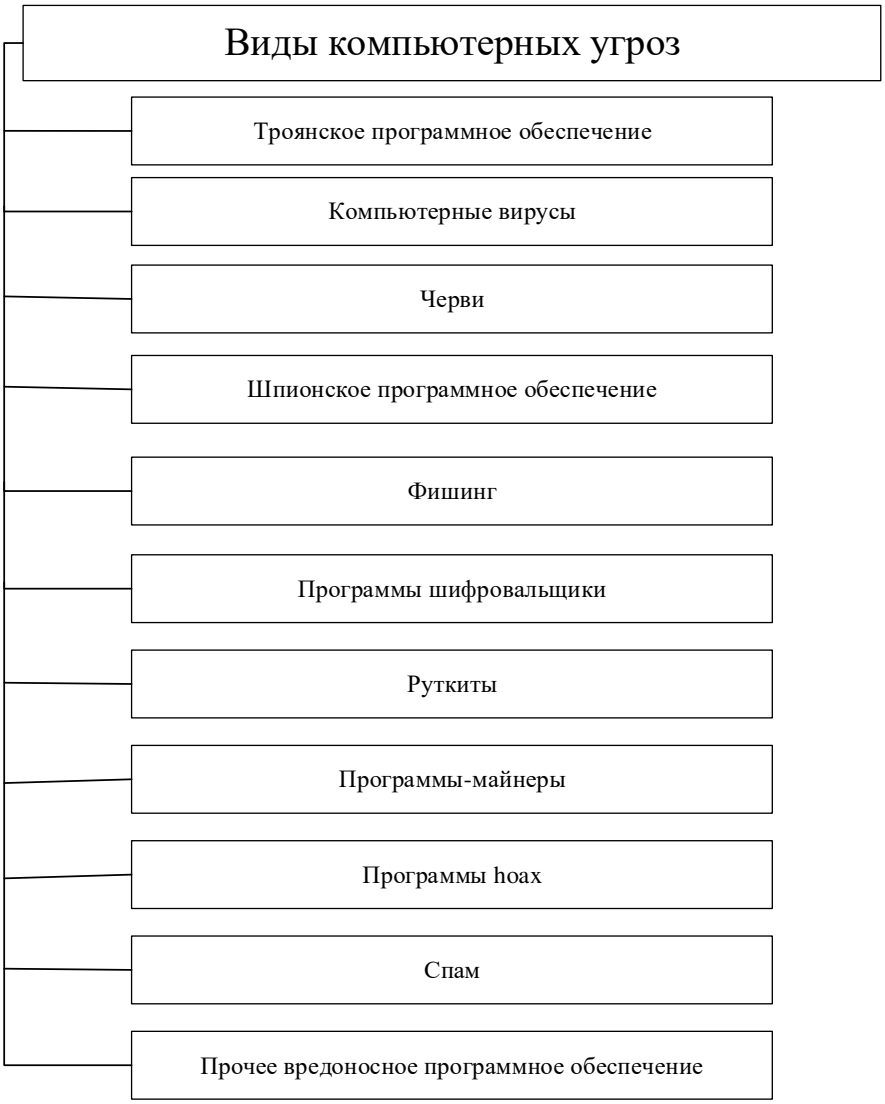

Рис. 1. Основные виды компьютерных угроз
Fig. 1. Main types of computer threats

Через некоторое время у вируса «Petya» появился помощник «Misha», который вступал в действие при неудачной попытке блокировки вирусом «Petya». Вирус «Misha», в свою очередь, блокировал .exe файлы и никак не затрагивал системные файлы. Пользователь входил в операционную систему и не мог использовать программы. По данным компании Касперский самый большой процент атак выдался на Украину и Россию из-за стремительного распространения данного вируса в системе для электронного документооборота компании M.E.Doc на территории Украины [9].

Таблица 1

Процентное соотношение заражения стран мира по данным Kaspersky.Lab

Table 1

Percentage of infection in countries of the world according to Kaspersky.Lab data

Страна	**Процент заражения**
Украина	60.0%
Россия	31.1%
Польша	6.0%
Италия	4.0%
Германия	2.0%
Беларусь	0.09%

После улучшения вирус распространился на другие государства и в большей степени от него пострадали крупные компании.

Таблица 2

Количество зафиксированных и отраженных атак за первое полугодие 2018 года по данным Kaspersky.Lab

Table 2

Number of recorded and repelled attacks for the first half of 2018 according to Kaspersky.Lab data

Вид отраженной атаки	**Количество атак/пользователей**
Веб-атака вредоносного программного обеспечения	243 749 050
Уникальные вредоносные зафиксированные URL	65 559 498
Пользователи, на компьютерах которых отражены атаки шифровальщиков	80 901
Пользователей, на компьютерах которых отражены атаки с использованием программ-майнеров	1 362 123

За годы развития информационной инфраструктуры злоумышленники придумали огромное количество разновидностей вредоносного программного обеспечения.

Сегодня каждая угроза может использоваться в связке с другой угрозой. Например, пользователь получает спам, читает сообщение и переходит по ссылке. Данное сообщение содержит такую информацию, которая определенно заинтересует данного пользователя и сыграет на его любопытстве. Далее пользователь переходит по ссылке либо скачивает вредоносный файл, и это вредоносное программное обеспечение в виде троянца начнёт действовать на его компьютере. Таким образом, будет нарушена доступность, целостность и конфиденциальность информации, которая хранится на данном устройстве. И мы получаем связку из трех и более угроз для компьютера, в которую входят: спам, фишинг, троянское программное обеспечение. Вместо троянского программного обеспечения может быть, любой другой вид компьютерной угрозы [4].

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

По данным лаборатории Касперского можно сгруппировать угрозы на три вида (Таблица 3).

Таблица 3

Данные из пирамиды киберугроз Kaspersky.Lab за 2018 г.

Table 3

Data from the Kaspersky cyber threat pyramid.Lab for 2018

Название вида	**Процент**
Кибероружие: уникальные угрозы	0,1%
Целевые атаки: изощренные угрозы	9,9%
Массовые атаки	90%

Можно понять, что большая часть атак – это массовые атаки, такие как вирус-шифровальщик «Petya».

Рассмотрим отдельно каждый из видов угроз:

1) Троянское программное обеспечение – вредоносное программное обеспечение, которое выполняет несанкционированное уничтожение файлов как системных, так и обычных приложений. Данные программы нарушают не только доступность к информации, но и целостность, конфиденциальность.

Данная угроза не похожа на червей либо вирусы, так как она не имеет свойство распространения на другие компьютеры, но попадая в систему, она может нанести системе огромный вред [6].

2) Компьютерные вирусы – программы, внедряющие вредоносные инструкции в любое программное обеспечение пользователя. Они были придуманы для распространения, и при этом распространении они стирают и изменяют файлы.

3) Черви – вредоносный код, который при своем распространении использует ресурсы сети. Отсюда и пошло это название. Так как черви имеют способность «ползти» из одного компьютера к другому по каналам связи. [7]

Черви распространяются с более высокой скоростью. Они обнаруживают IP-адреса других компьютеров и распространяются по ним. Иногда они могут воспользоваться лишь оперативной памятью компьютера. [2]

4) Шпионское программное обеспечение – программы, которые несанкционированно и целенаправленно собирают сведения о пользователе. Они могут быть скрыты и пользователь не узнает об их присутствии до конца их работы. [10]

Данные программы могут производить сканирование жесткого диска и собирать информацию об установленном программном обеспечении. Также они могут собирать информацию о сетевых настройках устройства.

Существует шпионское программное обеспечение, которое при всем этом позволяет контролировать компьютер жертвы. Существуют встраиваемые в браузер программы, которые перенаправляют трафик. Так при запросе одного сайта пользователя направляют на другой.

5) Фишинг – вид социальной инженерии, при котором происходит «выуживание» каких-либо данных у пользователя. Использует письмо с текстом, который заинтересует пользователя, далее он переходит по вредоносной ссылке. Также человек может оставить свои логин и пароль на поддельном сайте. [3]

6) Руткиты – утилиты, которые используются для маскировки подозрительной активности на устройстве человека. Данные утилиты маскируют деятельность вирусов, червей и троянцев.

Также они могут изменять функции операционной системы тем самым, маскируя себя и злоумышленника.

7) Программы шифровальщики – программное обеспечение, которое при попадании на устройство рядового пользователя, шифрует ценные для него файлы, а иногда и системные. Если данная программа шифрует системные файлы, то пользователь теряет доступ ко всей операционной системе и данным. Чаще всего такие программы требуют выкуп.

8) Программы-майнеры – программы, которые без ведома человека начинают эксплуатацию ресурсов его компьютера для майнинга криптовалюты. Вся мощность компьютера уходит на майнинг и работает на злоумышленника. Чаще всего можно заметить как на персональном компьютере падает производительность

9) Hoax-программы – программное обеспечение, которое навязывает пользователю покупку другого продукта путем обмана. Например, она может выдать пользователю баннер, на котором будет написано, что компьютер подвергся атаке.

10) Спам – корреспонденция нежелательного характера, которая рассылается массово и может использоваться злоумышленниками для кражи данных либо для распространения зловредного программного-обеспечения. [8]

Так же не стоит забывать о других угрозах. Такие угрозы как программы, которые созданы для создания других вредоносных программ и их распространения, организованные DDOS атаки на сервера и другие зловредные утилиты и приложения. [5]

Для предотвращения некоторых из угроз рекомендуется:

1) обновлять своевременно, вручную базы данных антивируса;

2) не платить выкуп, так как вскоре ключ от программы шифровальщика выложат в открытый доступ, и никто не будет идти на поводу у злоумышленника;

3) устанавливать последние обновления операционной системы;

4) убедится, что включены все компоненты антивируса;

5) сделать резервное копирование файлов.

ЗАКЛЮЧЕНИЕ

Безусловно, компьютер стал частью жизни практически каждого жителя нашей планеты, за счёт высокого уровня информатизации. Проанализированные виды компьютерных угроз показывают, что возросло и количество злоумышленников и созданных ими зловредных программ. Данные программные обеспечение направлены на уничтожение, искажение, распространение данной информации. Некоторое программное обеспечение создано для того, чтобы вымогать денежные средства у человека. Для обеспечения собственной безопасности, либо безопасности компании создают антивирусные программы, которые отвечают всем требованиям и способны защитить пользователя в полной мере от всех имеющихся и появляющихся угроз. Но при всем этом не стоит забывать о том, что сам пользователь может совершить ошибку и пустить вредоносный код в свою систему, что может привести к непоправимому ущербу. Таким образом, необходимо периодически проводить анализ новых угроз, чтобы всегда быть во «всеоружии». Особенно это важно для руководителей компаний. Они должны интересоваться сами и при этом осведомлять своих сотрудников о всех имеющихся компьютерных угрозах своевременно.

Список литературы

1. Всё что нужно знать о новой эпидемии [Электронный ресурс] URL: https://xakep.ru/2017/06/28/petya-write-up/.
2. Гуляев В. Р., Струнькина В. А. Компьютерные вирусы – проблема XXI века // Юный ученый. – 2017. – №1. – С. 54-56. – URL https://moluch.ru/young/archive/10/752/.
3. Гуськова А. М. Фишинг как основной метод социальной инженерии в схемах финансового мошенничества [Текст] // Исследования молодых ученых: материалы III Междунар. науч. конф. (г. Казань, октябрь 2019 г.). – Казань: Молодой ученый, 2019. – С. 3-6. – URL https://moluch.ru/conf/stud/archive/349/15208/
4. Как работает фишинг [Электронный ресурс] URL: https://www.kaspersky.ru/blog/how-to-avoid-phishing/5411/.
5. Общие сведения о компьютерных угрозах [Электронный ресурс] URL: https://support.kaspersky.ru/614#block1.
6. Трубачёв Евгений Сергеевич Троянские программы: механизмы проникновения и заражения // Вестник ВУиТ. – 2011. – №18. – URL: https://cyberleninka.ru/article/n/troyanskie-programmy-mehanizmy-proniknoveniya-i-zarazheniya.
7. Что такое компьютерный вирус и компьютерный червь? [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/threats/viruses-worms.
8. Что такое спам? [Электронный ресурс] URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-spam/.
9. Шифровальщик Petya/NotPetya/ExPetr [Электронный ресурс] URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/.
10. Шпионские программы [Электронный ресурс] URL: https://ru.malwarebytes.com/spyware/.

References

1. Everything you need to know about the new epidemic [Electronic resource] URL: https://xakep.ru/2017/06/28/petya-write-up/.
2. Gulyaev V. R., Strunkina V. A. Computer viruses-the problem of the XXI century // Young scientist. – 2017. – no. 1. – P. 54-56. – URL https://moluch.ru/young/archive/10/752/.
3. Guskova a.m. Phishing as the main method of social engineering in financial fraud schemes [Text] // Research of young scientists: materials of the III international conference. scientific conference (Kazan, October 2019). – Kazan: Young scientist, 2019. – P. 3-6. – URL https://moluch.ru/conf/stud/archive/349/15208/.
4. How phishing works [Electronic resource] URL: https://www.kaspersky.ru/blog/how-to-avoid-phishing/5411/.
5. General information about computer threats [Electronic resource] URL: https://support.kaspersky.ru/614#block1.
6. Trubachev Evgeny Sergeevich Trojan programs: mechanisms of penetration and infection // Vestnik Vuit. – 2011. – №18. – URL: https://cyberleninka.ru/article/n/troyanskie-programmy-mehanizmy-proniknoveniya-i-zarazheniya.

7. What is a computer virus and a computer worm? [Electronic resource] URL: https://www.kaspersky.ru/resource-center/threats/viruses-worms.
8. What is spam? [Electronic resource] URL: https://encyclopedia.kaspersky.ru/knowledge/what-is-spam/.
9. cryptographer Petya/NotPetya/ExPetr [Electronic resource] URL: https://www.kaspersky.ru/blog/new-ransomware-epidemics/17855/.
10. Spy programs [Electronic resource]. URL: https://ru.malwarebytes.com/spyware/.

Гоголь Андрей Сергеевич, студент 4 курса кафедры Информационная безопасность Института радиоэлектроники и информационной безопасности
Маслова Мария Александровна, аспирант, старший преподаватель кафедры «Информационная безопасность» Института радиоэлектроники и информационной безопасности

Gogol Andrey Sergeevich, 4th year student of the Department Information security, Institute of Radioelectronics and Information security
Maslova Maria Alexandrovna, post-graduate student, senior lecturer of the Department «Information security», Institute of Radioelectronics and Information security