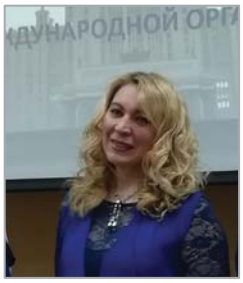
Список литературы
1. **Книберг Х.**, **Скарин М.** Scrum и Kanban: выжимаем максимум. – InfoQ, 2010
2. **Stephens M.**, **Rosenberg D.** Extreme Programming Refactored: The Case Against XP. - APress, USA, 2003
3. **Кент Бек**: Экстремальное программирование. - Питер, 2002
4. **Royce**, Winston. Managing the Development of Large Software Systems. - 1970.
5. **Книберг Х.** Scrum и XP: заметки с передовой = Scrum and XP from the trenches. - C4Media, 2007
6. **Richard W.** Selby. Software Engineering: Barry W. Boehm's Lifetime Contributions to Software Development, Management, and Research. — John Wiley & Sons, 2007-06-04. — 834 с. — ISBN 9780470148730.

АНАЛИЗ ЭФФЕКТИВНОСТИ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В СОВРЕМЕННЫХ ТЕХНОЛОГИЯХ ЗАЩИТЫ ИНФОРМАЦИИ

Югансон Анна Райвовна
Студент Московского политехнического университета

Овчинников Максим Владиславович
Студент Московского политехнического университета



Бритвина Валентина Валентиновна
Кандидат педагогических наук, доцент кафедры «Инфокогнитивные технологии» Московского политехнического университета

Аннотация. В данной статье проанализирована эффективность использования антивирусного ПО в современных способах защиты информации. Разработаны рекомендации по обеспечению безопасности хранения данных, находящихся на компьютерах. Сделан вывод о том, что антивирусные программы не всегда защищают от вирусных атак, что в свою очередь может привести к потере данных на устройстве.

Ключевые слова: антивирус, компьютер, защита, безопасность, вирус, вредоносная программа, уязвимость, информационная технология.

Annotation. This article analyzes the effectiveness of anti-virus SOFTWARE in modern methods of information protection. Recommendations to ensure the security of data storage on computers have been developed. It is concluded that antivirus programs do not always protect against virus attacks, which in turn can lead to loss of data on the device.

Keywords: antivirus, computer, protection, security, virus, malware, vulnerability, information technology.

Введение

Большинство пользователей при покупке нового компьютера сразу задаются вопросом установки антивирусной программы. Вредоносные файлы могут не только незначительно помешать работе устройства, но и украсть конфиденциальную ин-

формацию или вовсе вывести компьютер из строя. В 2017 году на продаже антивирусных программ Лаборатория Касперского заработала 698 миллионов долларов. Однако на самом деле, антивирусы не так эффективны, как мы думаем, как говорит Даррен Билби, специалист по безопасности из компании Google, они не являются обязательными атрибутами любого персонального компьютера и даже считаются бесполезными. Но люди с каждым годом продолжают доверять сохранность информации на своих компьютерах антивирусам.

Цель исследования

Изучить эффективность антивирусных программ, используемых на компьютерах.

Задачи исследования

- Проанализировать работу антивирусных программ против актуальных угроз;
- Рассмотреть методы внедрения вирусов на системное ПО;
- Разобрать рекомендации по обеспечению безопасности данных, находящихся на компьютерах.

Результаты исследования

Как показано на рис. 1, проанализировав работу антивирусных программ против давно сгенерированных угроз, было выяснено, что антивирусы показывают эффективность примерно 99,8%, но эти данные не являются актуальными, так как тесты проводились на образцах вредоносного ПО, которые в большинстве случаев уже не используются для проведения атак.

В Тель-Авивском университете было проведено исследование. Студенты нашли на российских запрещенных форумах 82 образца самого свежего вредоносного ПО и проверили его по базе VirusTotal против 42 популярных антивирусных движков. Они определили следующее:

1. Эффективность антивирусов против только что сгенерированных угроз оказалась менее 5%.
2. От появления вируса до начала его распознавания антивирусами проходит до четырех недель.
3. У антивирусов с самым высоким процентом определения угроз присутствует также высокий процент ложных срабатываний.

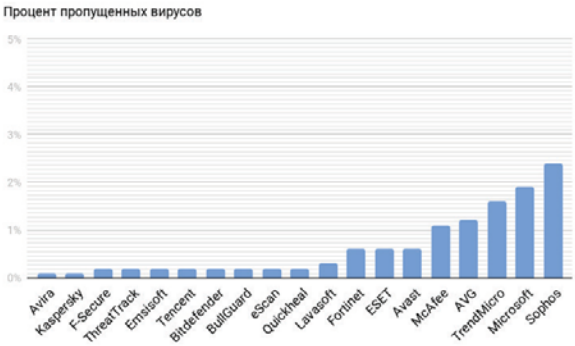


Рис. 1. Процент пропущенных вирусов

Для проведения аналогичного эксперимента по выявлению эффективности антивирусных программ против актуальных угроз, было выбрано 10 недавно обнаруженных вирусов, собранных на репозитории MalShare, и 68 антивирусных программ, представленных в базе VirusTotal. Из самых популярных в нем присутствуют такие антивирусы как: Microsoft Defender (13,3% рынка), ESET (11,5% рынка), Avira (5% рынка), Kaspersky (6,2% рынка), а также Dr.Web и встроенные по умолчанию в браузеры антивирусы (Opera, Google, Yandex). Распределение антивирусов по популярности показано на рис. 2.

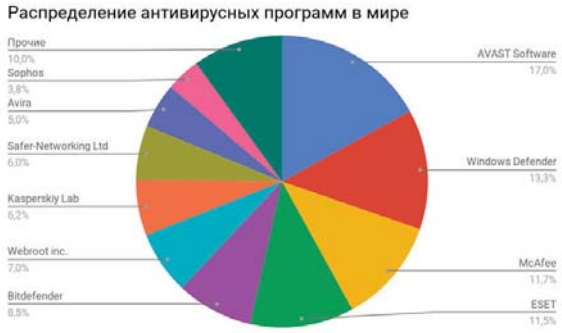


Рис. 2. Процентное распределение антивирусных программ

Таблица 1

Рассмотренные вирусы

Формат файла	Дата обнаружения	Ссылка на вирус
PE32	2019-02-23 14:49:42 UTC	http://upyourtext.com/infoabout.txt
PE32	2019-02-23 14:48:46 UTC	http://refkids.ir/wp-content/themes/nuovowp/assets/css/browser.jpg
gzip	2019-02-23 14:40:50 UTC	http://www.uffvfxgutuat.tw/dardoz/77435_0029299.html
gzip	2019-02-23 14:25:05 UTC	http://www.uffvfxgutuat.tw/xhqpup/2679390_882508.html
data	2019-02-23 14:11:07 UTC	http://lannavan.com/lau759
PE32	2019-02-23 14:01:54 UTC	http://song.lpbes.org/oKDGT3HnwA_9uй
PE32	2019-02-23 13:57:11 UTC	http://td-electronic.net/MbY14ajM/
gzip	2019-02-23 13:48:47 UTC	http://www.uffvfxgutuat.tw/mweubz/645406_486675.html
gzip	2019-02-23 13:48:42 UTC	http://www.elpqthnskbbf.tw/ltggle/030002_848137.html
gzip	2019-02-23 13:47:56 UTC	http://www.uffvfxgutuat.tw/dwrpdb/9463598_6787738.html

По результатам проверки, приведенным на рис. 3, из 68 антивирусов только 2 антивируса смогли обнаружить все угрозы. 49 антивирусов не определили даже одной. Общая эффективность обнаружения составляет 12,5%.

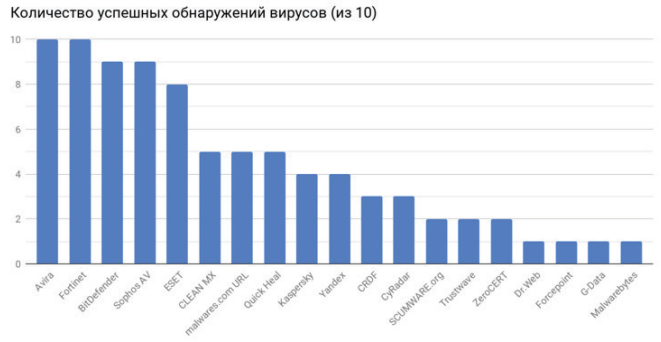


Рис. 3. Количество успешных обнаружений вирусов

Чтобы защитить информацию от вредоносного ПО, нужно определить методы внедрения вирусов на компьютер. Киберпреступники часто используют любые уязвимости в операционной системе или в установленных программах. Уязвимость — свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации [3]. Так как современные приложения содержат большой функционал, разработчикам сложно сделать программу, которая не содержала бы никаких ошибок. Также злоумышленники могут "склеивать" вредоносную программу с любым файлом в конечный формат ".exe". Например, взяв дистрибутив программы 2ГИС, можно связать его с вирусом и отправить как обычный загрузочный файл другому пользователю. А также можно скрыть расширение файла путем использования символов юникода. В названии файла будет отображаться не то расширение, какое есть на самом деле [1]. Существует пять основных методов заражения компьютерными вирусами, которые представлены на рис. 4.

Рис. 4. Методы заражения компьютерными вирусами

1. Открытие приложенных файлов и ссылок, присланных с неизвестных почтовых адресов. Это самый частый путь заражения вирусами. Люди могут не посмотреть на отправителя сообщения и нажать на заманчивую ссылку, поверив привлекательному предложению из спам-рассылки. Эти поддельные сообщения могут выглядеть как настоящие, так что даже опытный человек может быть застигнут врасплох. При переходе по ссылке может начаться загрузка зараженного файл или открыться фишинговый сайт.

2. Загрузка файлов с вредоносных сайтов.

Пользователи часто загружают файлы с непроверенных и ненадежных источников, фишинговых сайтов. На таких сайтах файлы представляют опасность, так как обычно являются зараженными.

3. Онлайн реклама.

Преступники часто размещают незараженную рекламу на надежных веб-сайтах и оставляют ее на некоторое время, чтобы завоевать доверие. Затем они помещают в рекламу вредоносный код, который заразит компьютер при нажатии.

4. Открытие файлов и ссылок, присланных в социальных сетях.

Люди, как правило, более спокойно относятся к ссылкам, опубликованным на сайтах социальных сетей, и ссылкам, которыми делятся их контакты. Злоумышленники могут взломать страницы социальных сетей и под видом сообщений от друзей отправлять ссылки на вредоносные сайты.

5. Загрузка нелицензионных программ.

Большинство россиян еще не привыкло покупать дорогостоящее программное обеспечение для компьютеров, предпочитая пользоваться "пиратскими" копиями. Поэтому данный путь заражения до сих пор остается актуальным. Злоумышленники могут распространять популярную программу вместе с вирусом, например, для кражи паролей.

Антивирусы в определенных случаях являются неэффективными, но в сети каждый день появляются новые вредоносные программы, и более 4 миллиардов пользователей со всего мира заходят в интернет каждый день. Поэтому нами, исходя из анализа, были разработаны рекомендации по обеспечению безопасности данных, находящихся на компьютерах [2, 4, 5]:

1. Следует делать резервные копии данных и своей компьютерной системы в нескольких облачных хранилищах. Их необходимо обновлять каждый месяц.

2. Не оставляйте свой компьютер в публичных местах. Особенно, если вы не вышли из своих страниц в социальных сетях. Злоумышленник может украсть ваш ноутбук или данные из него. Физическая безопасность вашей машины так же важна, как и техническая.

3. Игнорируйте письма, отправленные с неизвестных почтовых адресов. Остерегайтесь вложений, ссылок и форм в электронных письмах, которые приходят от людей, которых вы не знаете, или которые кажутся подозрительными. Избегайте ненадежных (часто бесплатных) загрузок.

4. Используйте только безопасные интернет-соединения. Это можно легко проверить: URL адрес сайта, на который вы переходите, должен начинаться с https://. Данная технология передачи данных шифрует все данные, которые вы отправляете на сервер сайта, в том числе пароли, номера кредитных карт.

5. Своевременно обновляйте свою компьютерную систему. Включите автоматическое обновление. Компании часто исправляют ошибки, найденные в своем ПО, удаляя уязвимости, тем самым увеличивая степень безопасности данных.

6. Используйте только сложные пароли, содержащие различные буквы, цифры и специальные символы – чем длиннее и сложнее, тем лучше. Используйте разные пароли для каждой учетной записи. Двухфазная аутентификация еще больше обезопасит ваши данные.

7. Устанавливайте только лицензионное ПО с официальных сайтов. Лучше один раз заплатить разработчикам за их работу, чем потерять все свои личные данные или «лечить» компьютер, вышедший из строя, за еще более высокую сумму денег.

8. Если компьютер подключен к сети, включите «брандмауэр» («файрволл»), то есть программу, ограничивающую как входящую, так и исходящую сетевую активность компьютера.

Вывод. Исходя из результатов эксперимента по выявлению эффективности антивирусных программ против только что сгенерированных угроз, было выяснено, что общая эффективность обнаружения вирусов составляет 12,5%. Против давно существующих вирусов антивирусы показывают эффективность примерно 99,8%. Таким образом, был сделан вывод, что антивирусные программы не так эффективны против только что сгенерированных угроз. Было рассмотрено пять методов внедрения вирусов на системное ПО и разработано восемь простых правил безопасности, которые следует соблюдать при пользовании компьютером, чтобы обезопасить его от большинства видов атак. Это позволит сохранить уникальную информацию, персональные данные, личные материалы.

Список литературы

1. **Рудниченко А.К.** Актуальные способы внедрения компьютерных вирусов в информационные системы [Электрон. ресурс] / А.К. Рудниченко, М.В. Шаханова // Молодой ученый. – 2016. – №11. – С. 221–223. – Режим доступа: https://moluch.ru/archive/115/30348.
2. **Климентьев К.Е.** Компьютерные вирусы и антивирусы: взгляд программиста / К.Е. Климентьев. – М.: ДМК-Пресс, 2013.
3. **Нестеров С.А.** Информационная безопасность и защита информации: учеб. пособие / С.А. Нестеров. – СПб.: Изд-во Политехн. ун-та, 2009.
4. Введение в информационную безопасность автоматизированных систем: учеб. пособие / В.В. Бондарев. – М.: МГТУ им. Н.Э. Баумана, 2016. – 250 с.
5. **Блинов А.М.** Информационная безопасность: учеб. пособие / А.М. Блинов. – Ч. 1. – СПб.: СПбГУЭФ, 2010. – 96 с.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ РАСЧЕТОВ НА ПРОЧНОСТЬ ТОНКОСТЕННЫХ ЭЛЕМЕНТОВ КОНСТРУКЦИИ ПРИ КОРРОЗИОННОМ ВОЗДЕЙСТВИИ

Тищенко Светлана Леонидовна
Студентка 1-го курса магистратуры Московского политехнического университета

Луганцев Леонид Дмитриевич
Доктор технических наук, профессор, профессор кафедры «Инфокогнитивные технологии» Московского политехнического университета

Аннотация. На основе линейной механики разрушения представлены метод и алгоритм расчетной оценки несущей способности и располагаемого ресурса тонкостенных оболочечных конструкций, работающих в коррозионных средах при сочетании термомеханического и коррозионного воздействий.

Ключевые слова: тонкостенный элемент конструкции, термомеханическое воздействие, коррозионный износ, коррозионная трещина, располагаемый ресурс, прочность.