Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.415.53

Омуару
Алвелл Эллингтон

Методика тестирования антивирусного программного обеспечения

АВТОРЕФЕРАТ

на соискание ученой степени магистра технических наук
по специальности
1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Белоусова Е.С.,
кандидат технических наук

_____

Минск 2018

ВВЕДЕНИЕ

Быстрое развитие коммуникационных и информационных технологий привело к резкому увеличению числа пользователей сети. В настоящее время по состоянию на декабрь 2017 г. в мире насчитывается более 4 миллиардов пользователей Интернета. Любой пользователь компьютера должен сначала установить антивирусное программное обеспечение перед подключением к сети. На сегодняшний день существует множество программных продуктов, которые, как утверждают их разработчики, способны защитить компьютер от вредоносного программного обеспечения. По этой причине актуальной является задача тестирования антивирусов с целью выявления наиболее качественного программного продукта.

Сегодня тестирование стало обязательной частью процесса производства любого программного обеспечения, в том числе и антивирусного. Основная цель тестирования – это обнаружение и устранение ошибок. Следствием такой деятельности является повышение качества программной защиты персональных данных. Антивирусное тестирование также может помочь снизить риск несанкционированного доступа к данным, потери данных или утечки, нарушения обслуживания и плохого управления информационными системами. В последние десятилетия был предложен ряд методов оценки качества работы антивирусных программ. Каждый метод имеет свои достоинства и недостатки и может использоваться только для анализа некоторых параметров антивирусных программ.

В настоящее время существует 4 метода тестирования антивирусных программ: статическое тестирование, динамическое тестирование; тестирование скорости реакции, ретроспектива. Тесты продолжают развиваться по мере развития отрасли, продукты становятся более сложными, требуются более сложные тесты. Важно расширить методологию тестирования в областях, которые наиболее важны для защиты пользователей, используя индикаторы, которые важны как для пользователей, так и для разработчиков.

Исходя из выше сказанного целью данной работы является составление методологии определения качества программного обеспечения защиты обеспечения персональной информации с помощью антивирусных приложений. Причем, конечной целью автором поставлено исследование эффективности различных антивирусных программных продуктов с помощью разработанной

методики тестирования. Для тестирования выбраны следующие антивирусные программные обеспечения: Kaspersky, Avira, Avast, Eset NOD32. В работе производится оценка их эффективности исходя из следующих критериев: быстродействие, удобство использования, количество обнаруженных вредоносных файлов, количество удаленных и вылеченных файлов.

Автором изучен и систематизирован определенный объем сведений по теме диссертационной работы. Разработана и обоснована методика проведения тестирования антивирусных программных продуктов. Выбраны антивирусные программы для проведения тестирования по предлагаемой методике.

Теоретическая и практическая значимость работы заключается в разработке методики тестирования антивирусных программных продуктов, которая может быть использована для определения эффективности работы различных антивирусов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетным направлениям научных исследований Беларуси на 2016-2020 годы, утвержденным Постановлением Совета министров Беларуси от 12 марта 2015 года, № 190. Работа выполнена в образовании «Белорусский государственный университет информатики и радиоэлектроники».

Цель исследования работы

Цель – определение качества программного обеспечения защиты персональной информации с помощью методики тестирования антивирусных приложений.

Для достижения поставленной цели решены следующие задачи:

– провести статистическое исследование угроз информационной безопасности в компьютерных сетях;

– провести обзор различных антивирусных программных продуктов;

– проанализировать существующие методы антивирусной защиты;

– разработать методику тестирования антивирусной защиты компьютерных сетей;

– осуществить проверку разработанной методики для тестирования антивирусного программного обеспечения;

– разработать рекомендации по применению разработанной методики определения качества антивирусного программного обеспечения.

Личный вклад заявителя

Результаты исследований получены автором самостоятельно. Научный руководитель принимал участие в определении целей и задач исследования, интерпретации промежуточных результатов.

Положения, выносимые на защиту

1. Методика определения качества программного обеспечения защиты персональной информации с помощью антивирусных приложений, позволяющая

определять эффективность работы данных приложений по быстродействию, удобству использования, количеству обнаруженных вредоносных файлов, количеству удаленных и вылеченных файлов.

2. Тестирование с использованием методики определения качества антивирусных программных продуктов показывает невозможность обеспечения эффективной защиты персональной информации существующими программными методами.

Апробация результатов диссертации

Основные результаты диссертационной работы были представлены и обсуждены на научных конференциях различного уровня: 54-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР (Минск, 23 апреля 2018 г.); XVI Белорусско-российской научно-технической конференции (Минск, 5 июня 2018 г.).

По теме диссертации опубликован 1 тезис доклада в сборнике материалов конференции.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** определена область исследований и их актуальность. В общей характеристике работы сформулирована цель работы, изложены основные положения, выносимые на защиту.

В **первой главе** представлен обзор существующих угроз информационной безопасности и существующих методов защиты. Приводится классификация программных методов защиты от сетевых угроз. Проанализированы требования к антивирусным программным продуктам, на основе которых были сделаны выводы об необходимости составления методики тестирования антивирусных программ. На основе обзора современных антивирусных программ были выбраны антивирусы, на которых производилось тестирование разработанной методики.

В **второй главе** был произведен анализ существующих методов тестирования антивирусов, выделены их достоинства и недостатки. Разработана методика определения качества программного обеспечения защиты персональной информации с помощью антивирусных приложений.

В **третьей главе** представлено применение разработанной методики для тестирования выбранных антивирусных программных продуктов. Произведены качественные и количественные оценки влияния работы антивируса на быстродействие информационной системы, удобства использования, определено количество обнаруженных вредоносных файлов, удаленной и восстановленных файлов. Анализ результатов тестирования позволил сформировать требования по использованию каждого антивирусного программного обеспечения. Также была дана рекомендация по разработанной методологии тестирования антивирусного программного обеспечения.

В **Заключении** сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

С быстрым развитием технологий меняется и характер вирусных угроз для данных. Технологии, которые должны обеспечить защиту от этих угроз, должны адаптироваться. Разработчики антивирусных программ утверждают, что они обеспечивают эффективное реагирование на компьютерные вирусные инциденты. Однако в настоящее время нет сведений относительно наилучшего способа оценки эффективности таких требований. Поэтому особенно актуальным является разработка тестов антивирусных программных продуктов, которые измеряют эффективность функциональных возможностей антивируса. Используя этот подход, была разработана методика тестирования выполнения требований к функциональности антивирусных программ. Данная методика включает следующие этапы: загрузка, установка и обновление тестируемого антивирусного программного обеспечения; первичное сканирование фалов; дополнительная проверка файлов, не обнаруженных при первичной проверке; документирование результатов первичной и дополнительной проверки; исследование эффективности работы дополнительных сервисов и инструментов антивирусного программного обеспечения.

По данной методике производились тестирования антивирусных продуктов, используемых в диагностических программах, защите от вредоносных веб-приложений, фишинга, дополнительных сканеров. Для тестирования были выбраны следующие программные продукты: Kaspersky, Avira, Avast, Eset NOD32. На основе проведенных тестов можно заметить, что не один из тестируемых продуктов не обнаружил 100 % зараженных файлов, при этом все продукты осуществляли попытки лечения некоторых файлов, а не просто удалять обнаруженные ими угрозы. Антивирусный продукт Kaspersky обнаружил 97,65 % зараженных файлов, при этом из них более 60 % было удалено, и более 35 % излечились. Антивирусный продукт Eset NOD32 обнаружил 77,88 % зараженных файлов, восстановлено было около 47 % файлов были восстановлены и около 30 % были удалены. Антивирусный продукт Avira обнаружил 95,98 % зараженных файлов, удалил более 53% и восстановил более 53 %. Последнее антивирусное программное обеспечение Avast обнаружило 85,69 %, восстановлено более чем на 39 % и удалило 46 %.

На основе тестирования различных антивирусных продуктов можно сделать вывод, что нет антивирусной программы, которая обеспечивает 100 % защиту от вредоносного ПО. Между тем, рекомендуется устанавливать антивирусные программы для защиты персональных данных. Для лучшей производительности устройств лучше устанавливать не более одного антивируса. Кроме того, загрузка программного обеспечения с небезопасных веб-сайтов может нанести значительный вред. Основной рекомендацией на основе проведенного тестирования является установка и ежедневные обновления выбранного антивирусного программного обеспечения, профилактическая еженедельная проверка файловой системы устройства.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Омуару Алвелл Эллингтон. Методика тестирования антивирусного программного обеспечения / Омуару Алвелл Эллингтон, Е.С. Белоусова // Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно-технической конференции. – Минск, 2018. – С. 68.