

МЕТОДЫ ОЦЕНКИ СОСТОЯНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ

Е.П. Зуенок

На сегодняшний день все большую ценность и значимость приобретают информационные ресурсы. И чем более они ценны, тем важнее ее безопасность. А значит безопасность ее носителей и каналов передачи. Потеря данных большой компании может принести ей огромные убытки. Следовательно, одной из первых ее задач – обеспечить защиту своих серверов и рабочих станций. Для оценки антивирусной защиты программы следует учитывать следующие критерии: качество эвристического анализа, скорость реакции обнаружения вирусов, качество сигнатурного анализа, качество поведенческого блокиратора, способность к лечению активных заражений, способность к выявлению активных руткитов, качество самозащиты, возможность поддержки упаковщиков, частота ложных срабатываний. Однако кроме этого имеют значение количество необходимых для корректной работы программы ресурсов, устойчивость к сбоям, количество ложных срабатываний, стоимость программы и прочее. Тестирование и анализ существующих антивирусных программ проводился неоднократно. В докладе рассматривается метод оценки антивирусных программ, учитывающий технические характеристики программ. В 2016 г. компанией Microsoft была проанализирована эффективность антивирусов с учетом распространенности угроз. Этот метод позволяет учитывать в большей степени те угрозы, которые чаще встречаются в различных регионах. В 2018 г. был проведен сравнительный анализ антивирусных программ на основе значений показателей защиты от вирусов. Этот метод позволяет глубже разобраться возможности антивирусных программ. При этом среднестатистический пользователь, не имеющий глубоких знаний в этой области, как правило, оценивает программу по тому, насколько ей удобно и просто пользоваться, не создает ли она неудобств для работы с компьютером. Если взять выборку по рейтингу всех этих анализов, то результаты будут отличаться. У каждой программы свои минусы и свои плюсы. И при этом ни одна из них не может обеспечить абсолютную защиту. И наиболее эффективным ее вариантом будет комплексная защита, при создании которой учитываются все особенности программ и условия их работы. Кроме того, для поддержания уровня защищенности необходимы постоянный мониторинг и развитие действующей системы защиты. Рассмотренный метод позволяет найти наиболее оптимальное решение защиты от вредоносных программ, учитывая возможности рабочей техники и запросы пользователей [1, 2].

Литература

1. Сравнительный анализ антивирусов. Сравнение антивирусов по эффективности защиты от новейших вредоносных программ Сравнение двух антивирусных программ по информатике [Электронный ресурс] – Режим доступа: <https://polarize.ru/game/sravnitelnyi-analiz-antivirusov-sravnenie-antivirusov-po>. – Дата доступа: 04.05.2021.

2. Эффективность антивирусов с учетом распространения угроз [Электронный ресурс] – Режим доступа: <https://www.comss.ru/page.php?id=3072>. – Дата доступа: 04.05.2021.