СРАВНИТЕЛЬНЫЙ АНАЛИЗ АНТИВИРУСНЫХ РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Д.С. Калининский, *магистрант*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2023-7-1-203-207

Аннотация. *В статье проводится детальный анализ популярных антивирусных решений для обеспечения безопасности данных: Symantec Endpoint Protection, McAfee Total Protection, Kaspersky Total Security и Microsoft Defender. Исследование основывается на критериях удобства использования, надежности, функциональности и стоимости. Результаты анализа представлены с целью помочь пользователям принимать информированные решения о выборе антивирусного программного обеспечения, учитывая их индивидуальные потребности и предпочтения.*

Ключевые слова: *безопасность данных, антивирусное программное обеспечение, Symantec Endpoint Protection, McAfee Total Protection, Kaspersky Total Security, Microsoft Defender, сравнительный анализ.*

Современные офисы – это сложные системы с множеством устройств и ПО, где ключевое внимание уделяется информационной безопасности. Небрежное отношение к защите может привести к утечке конфиденциальных данных, негативно отражаясь на финансах и репутации компании [1]. Существует множество компаний, предлагающих решения по защите информации, позволяющие ограничивать доступ и контролировать обработку данных.

Одно из наиболее популярных ПО для контроля доступа - Active Directory от Microsoft. Оно обеспечивает управление пользователями и компьютерами, автоматическую установку ПО и обновлений, обеспечивая высокий уровень безопасности [2].

Дополнительно предлагаются продукты Symantec Endpoint Protection и Kaspersky Endpoint Security, обеспечивающие защиту от вредоносного ПО. Однако они не поддерживают биометрическую аутентификацию, что может быть реализовано в новых решениях.

При разработке такого ПО необходимо изучить различные методы аутентификации, включая биометрические.

Существующие системы безопасности разделяются на типы в зависимости от задач, например, системы контроля доступа и системы видеонаблюдения, которые помогают контролировать работу сотрудников [3].

Сравнение и анализ существующих программных решений

Symantec Endpoint Protection

Symantec Endpoint Protection – это комплексное решение для безопасности, предлагающее функции предотвращения вторжений, брандмауэра и защиты от вредоносных программ [4]. Оно включает некоторые функции, специфичные для ПО для предотвращения потери данных, и обычно устанавливается на серверах с Windows, Linux или macOS.

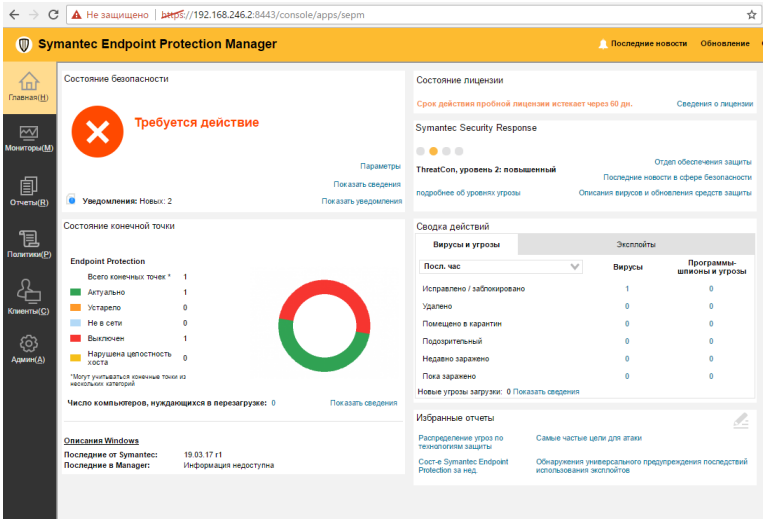

Рис. 1. Symantec Endpoint Protection

Главная функция Endpoint Protection – сканирование компьютеров на наличие угроз, предотвращение запуска неразрешенных программ и управление брандмауэром для контроля сетевого трафика. Он также идентифицирует и блокирует вредоносный трафик в корпоративных сетях и веб-браузерах. Symantec использует совокупные данные от 175 миллионов устройств, на которых установлена Endpoint Security, для обнаружения вредоносного ПО [5].

Endpoint Protection включает административную консоль, позволяющую менять политики безопасности для разных отделов и управлять сканированием файлов и программ. Он не управляет мобильными устройствами напрямую, но обеспечивает защиту компьютера при подключении мобильных устройств.

Однако у Symantec Endpoint Protection есть недостатки: в 2012 году его исходный код был украден и опубликован в Интернете, и в 2019 году была обнаружена серьезная ошибка, которая позволяла обойти механизм самозащиты.

McAfee Total Protection

McAfee – известный разработчик решений для онлайн-защиты, центрирующий свою работу на защите пользователей. Программные продукты McAfee адаптируются к требованиям клиентов, предлагая простые и интегрированные решения.

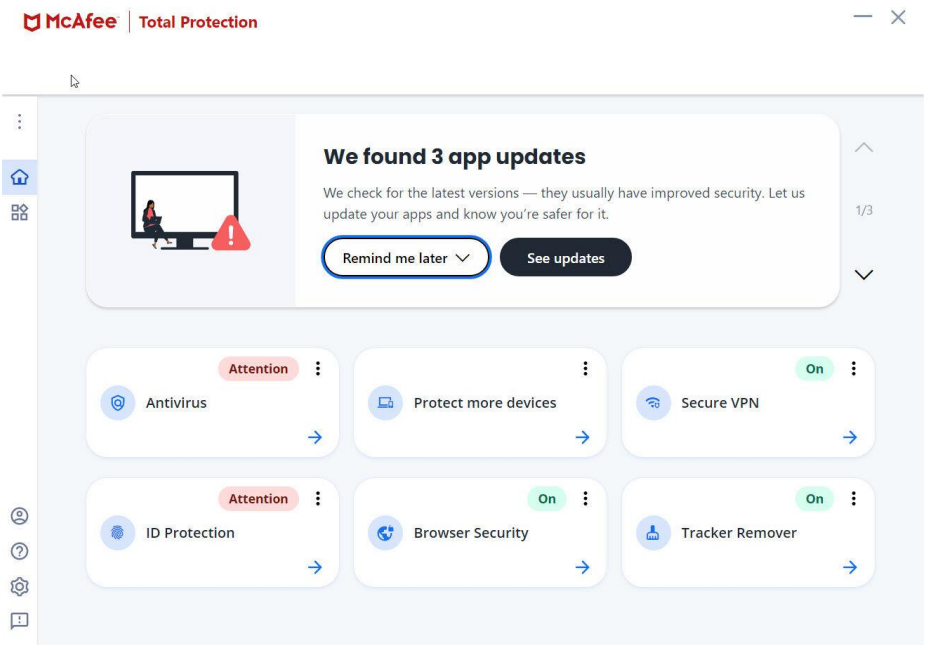

Рис. 2. McAfee Total Protection

McAfee Total Protection – это универсальное решение, обеспечивающее мониторинг кредитной активности, блокировку и замораживание кредитных файлов для предотвращения нежелательного открытия счетов, удаление личной информации с сайтов брокеров данных, отслеживание утечек информации в темной сети и помощь в восстановлении личной информации при ее утечке. Комплексная защита включает страхование от кражи личных данных на 1 млн долларов и дополнительное покрытие программ-вымогателей на 25 тыс. долларов [6].

Преимуществами McAfee Total Protection являются круглосуточная защита от вредоносных программ и онлайн-угроз, удобство использования через единый интерфейс управления, надежная защита для более чем 600 млн устройств, и гарантия возврата денег, если не удается удалить вирусы с устройств.

Необходимо подчеркнуть, что поддержание актуальности баз данных McAfee Total Protection и обновление операционной системы и программ является важным условием для эффективной работы этого решения [7].

Kaspersky Total Security

Kaspersky Total Security – это полноценное решение для защиты компьютеров от большинства вирусов и вредоносного ПО. Ключевые функции включают родительский контроль, защиту онлайн-платежей, автоматическое облачное резервное копирование, менеджер паролей, шифрование данных и удалённое управление защитой мобильных устройств [8].

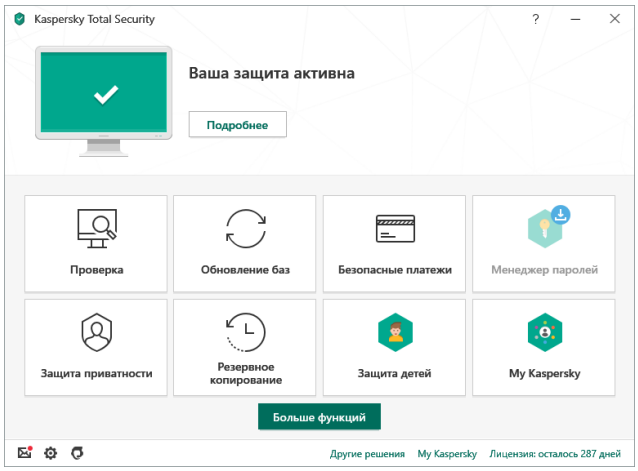

Рис. 3. Kaspersky Total Security

Преимущества Kaspersky Total Security включают быструю и надежную защиту от вирусов и атак, удобный интерфейс, своевременные обновления баз данных, продуманные модули и функции, а также гибкую систему настроек.

Среди недостатков – необходимость регулярной покупки лицензионного ключа, значительная системная нагрузка, которая может замедлять работу слабых компьютеров, и потребность в большом количестве места и оперативной памяти. Кроме того, некоторые функции могут быть слишком навязчивыми, и программа может ошибочно идентифицировать некоторые безопасные файлы как вредоносные.

В общем, Kaspersky Total Security является комплексным и надежным инструментом для защиты компьютеров и мобильных устройств от широкого спектра угроз [9].

Microsoft Defender

Microsoft Defender – это встроенный антивирус от Microsoft, предназначенный для защиты компьютеров на Windows от вредоносного ПО [10]. Он включает в себя модули безопасности, отслеживающие подозрительные изменения в системе в реальном времени, и позволяет удалять установленные приложения ActiveX.

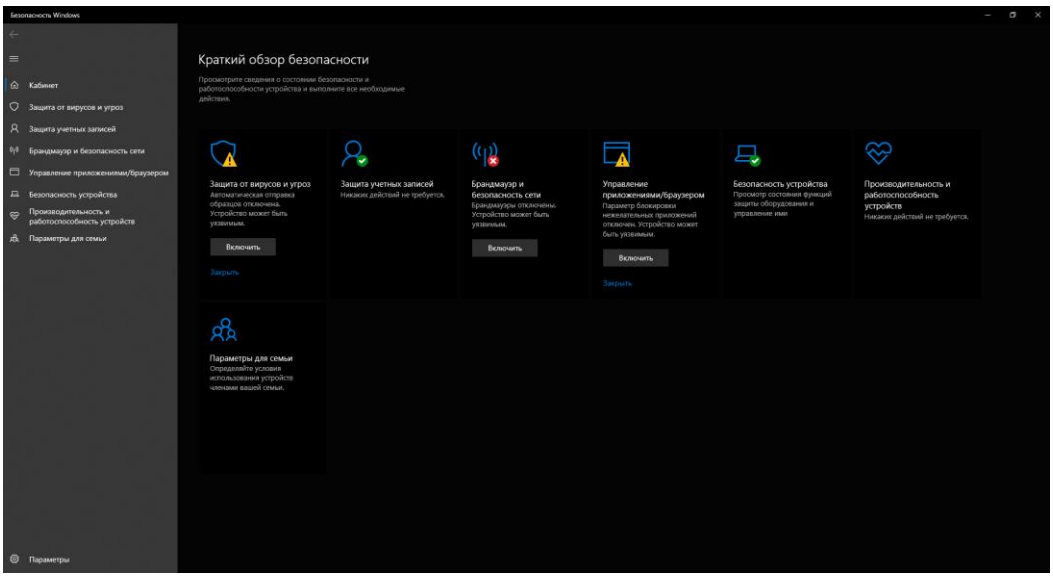

Рис. 4. Microsoft Defender

Преимущества Microsoft Defender включают глубокое сканирование системы, минимальные системные требования, низкий процент ложных срабатываний, отсутствие рекламы, автоматическую активацию и отсутствие сбора конфиденциальной информации для коммерческого использования.

С другой стороны, Microsoft Defender иногда может пропускать вредоносные программы, и его общая мощность и надежность могут быть ниже, чем у некоторых лидеров в этом сегменте. К тому же, в нем отсутствуют некоторые дополнительные функции, которые могут быть полезны пользователям.

Сравнительный анализ

После оценки различных решений для защиты данных, было проанализировано четыре популярных антивируса: Symantec Endpoint Protection, McAfee Total Protection, Kaspersky Total Security и Microsoft Defender. Основные критерии включали удобство использования, надежность, функциональность и стоимость [11, 12].

Symantec Endpoint Protection отличается интуитивным интерфейсом и высокой эффективностью в обнаружении угроз, но его стоимость может быть выше по сравнению с конкурентами. McAfee Total Protection также эффективно обнаруживает угрозы и предлагает дополнительные функции, однако его стоимость может быть высока.

Kaspersky Total Security предлагает обширный набор функций и высокую надежность, но его установка может быть сложнее, и он может замедлять систему. Microsoft Defender, встроенный в Windows, предоставляет базовую защиту с простым интерфейсом и автоматическими обновлениями.

В целом, каждое решение имеет свои преимущества и недостатки, и выбор зависит от индивидуальных потребностей пользователя. Например, для простоты использования подойдет Microsoft Defender, а для более высокого уровня защиты – Symantec Endpoint Protection, McAfee Total Protection или Kaspersky Total Security. Однако стоит помнить, что более мощные программы могут замедлять работу системы.

Заключение

В результате проведенного анализа выяснилось, что каждое из рассмотренных антивирусных решений имеет свои преимущества и недостатки. Выбор подходящего программного обеспечения для обеспечения безопасности данных во многом зависит от индивидуальных потребностей и предпочтений пользователя. Мощные антивирусные программы, такие как Symantec Endpoint Protection, McAfee Total Protection и Kaspersky Total Security, предлагают обширный набор функций и высо-

кую степень защиты, но могут потребовать больше системных ресурсов и замедлить работу системы. В то же время Microsoft Defender, встроенный в операционную систему Windows, обеспечивает базовую защиту и удобство использования. Таким образом, конечный выбор антивирусного решения должен учитывать баланс между необходимым уровнем безопасности, доступностью и возможностью эффективной работы системы.

Библиографический список

1. Федеральная служба безопасности (ФСБ). – [Электронный ресурс]. – Режим доступа: https://www.fsb.ru/.

2. "SANS Institute". – [Электронный ресурс]. – Режим доступа: https://www.sans.org/.

3. "National Institute of Standards and Technology (NIST)". – [Электронный ресурс]. – Режим доступа: https://www.nist.gov/.

4. "OWASP (Open Web Application Security Project)". – [Электронный ресурс]. – Режим доступа: https://owasp.org/.

5. "CISA (Cybersecurity and Infrastructure Security Agency)". – [Электронный ресурс]. – Режим доступа: https://www.cisa.gov/.

6. "Microsoft Security". – [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/security.

7. "IBM Security". – [Электронный ресурс]. – Режим доступа: https://www.ibm.com/security.

8. "Cisco Security". – [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/products/security/index.html.

9. "Kaspersky Lab". – [Электронный ресурс]. – Режим доступа: https://www.kaspersky.com/.

10. "Symantec". – [Электронный ресурс]. – Режим доступа: https://www.symantec.com/.

11. "McAfee". – [Электронный ресурс]. – Режим доступа: https://www.mcafee.com/.

12. Ross, D.A. Introduction to Cybersecurity: Understanding and Applying Principles and Practices. Wiley, 2018.

BENCHMARKING ANTIVIRUS SECURITY SOLUTIONS

D.S. Kalininskiy, *Graduate Student*
Moscow Technical University of Communications and Informatics
(Russia, Moscow)

Abstract. *The article provides a detailed analysis of popular antivirus solutions for data security: Symantec Endpoint Protection, McAfee Total Protection, Kaspersky Total Security and Microsoft Defender. The study is based on the criteria of usability, reliability, functionality and cost. The results of the analysis are presented to help users make informed decisions about choosing antivirus software based on their individual needs and preferences.*

Keywords: *data security, antivirus software, Symantec Endpoint Protection, McAfee Total Protection, Kaspersky Total Security, Microsoft Defender, benchmarking.*