

УДК 004.738.5:004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Гурский С.М., Полубенцев В.А.

Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, e-mail: vka@mil.ru

Информационно-телекоммуникационная сеть (ИТКС) «Интернет» в настоящее время объединяет более 4,88 млрд пользователей примерно в 180 странах мира. Архивы бесплатного доступа в ИТКС «Интернет» содержат информацию практически по всем сферам человеческой деятельности, от последних научных открытий до прогнозов погоды на завтра. Разработанная для удовлетворения потребностей и интересов исследовательских и образовательных групп, стремящихся получить доступ к суперкомпьютерам и мощным серверам, ИТКС «Интернет» набирает популярность. В то время как новые границы киберпространства открывают (или создают) более широкие возможности для всех видов инноваций, предпринимательства и получения прибыли, есть те, для кого ИТКС «Интернет» стала источником знаний, и те, для кого это просто рабочая утилиты. В то же время почти всем пользователям становится все труднее представить один день без приятного онлайн-общения, ежедневных новостных постов или актуальных видеоклипов (загрузок). Однако, несмотря на все свои преимущества, ИТКС «Интернет», как известно, является опасным и даже вредным местом для некоторых потребителей. Многочисленные мошенники (спамеры), шпионы и вирусы представляют угрозу для пользователей ИТКС «Интернет», и число вредоносных интернет-атак растет. В статье представлены определение информационной безопасности ИТКС «Интернет», анализ и выбор с помощью метода анализа иерархий Томаса Саати наилучших зарубежных и российских антивирусных программ с учётом выбранных критериев.

Ключевые слова: информационно-телекоммуникационная сеть «Интернет», информационная безопасность, задачи информационной безопасности, анализ показателей антивирусных программ

INFORMATION SECURITY IN THE INTERNET INFORMATION AND TELECOMMUNICATION NETWORK

Gurskiy S.M., Polubentsev V.A.

MSA named after A.F. Mozhaiskiy, St. Petersburg, e-mail: vka@mil.ru

The Information and Telecommunications Network (ITC Internet) currently connects more than 4.88 billion users in around 180 countries around the world. The archives of the free internet access contain information on almost all areas of human activity, from the latest scientific discoveries to the weather forecasts of tomorrow. designed to meet the needs and interests of research and education groups seeking access to supercomputers and powerful servers, the internet is gaining popularity. There are those for whom the internet has become a source of knowledge, and ones for whom it is just a working utility (job), while the new frontiers of cyberspace have opened up (or forged) broader opportunities for all kinds of innovation, entrepreneurship, and profit making. At the same time, it is becoming increasingly difficult for almost all users to imagine one day without congenial online communication, daily news lines or relevant video clips (downloads). However, despite all its advantages, «the Internet» is known to be a risk and even a harmful place for certain consumers. Numerous scammers (spammers), spies and viruses are posing a threat to network users and bank cardholders, and the number of malicious internet attacks is on the rise. This article provides an overview of the «Internet» in general and information security in particular. It focuses on the objectives (tasks) of cybersecurity as well as on the methods and techniques of violation prevention (antihacking). The authors present and describe the most reliable antivirus programs («antiviruses») that ensure a safe use and storage of personal data in the network.

Keywords: information and telecommunication network «Internet», information security, information security tasks, analysis of indicators of antivirus programs

Информационно-телекоммуникационная сеть (ИТКС) «Интернет» – неотъемлемая часть жизни каждого человека. Она служит средством связи с партнерами и заказчиками, обеспечивает поиск полезной информации. Количество пользователей ИТКС «Интернет» нарастает с каждым годом (рис. 1).

По данным Международного института маркетинговых и социальных исследований GfK-Russia к началу 2019 г. аудитория интернет-пользователей в России среди населения 16+ составила 90 млн чел. (+3 млн чел. к предыдущему году), т.е. превысила 2/3 взрослого населения страны [2]. Но тем не менее ИТКС «Интернет» – это публичная открытая сеть, поэтому существует

угроза негативного влияния вредоносных программ на персональные компьютеры пользователей. Поэтому вопросы совершенствования информационной безопасности в ИТКС «Интернет» продолжают оставаться актуальными [3–5].

Цель исследования: проанализировать основные способы информационной безопасности в ИТКС «Интернет», основанные на использовании антивирусных программ.

Материалы и методы исследования

В статье проведён обзор работ, посвящённых вопросам информационной безопасности при работе в ИТКС «Интернет» [5–7]. На основе рассмотрения

показателей антивирусных программ [8] с помощью метода анализа иерархий, разработанного американским профессором математики Томасом Л. Саати (МАИ, Analytic Hierarchy Process, АНР), предложены лучшие из них. МАИ представляет собой теорию, которая базируется на экспертных оценках и суждениях индивидуальных участников или групп и позволяет найти лучший из альтернативных вариантов антивирусных программ [9, 10].

ИТКС «Интернет» – это глобальная информационная система, которая логически взаимосвязана пространством глобальных уникальных адресов, основанных на интернет-протоколе (IP) или на последующих расширениях или преемниках IP; способна поддерживать коммуникации с использованием семейства Протокола управления передачей/интернет-протокола (TCP/IP) или его последующих расширений/преемников и/или других IP-совместимых протоколов; обеспечивает, использует или делает доступными, на общественной или частной основе, высокоуровневые сервисы, настроенные над описанной здесь коммуникационной и иной связанной с ней инфраструктурой [11].

Под термином «информационная безопасность» будем понимать состояние защищенности информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования [3, 4].

Главной функцией информационной безопасности является защита информации

от случайного или преднамеренного воздействия, исключая ее уничтожение, раскрытие или искажение. Для решения указанных задач используются антивирусные программы [3, 4, 8].

Для достижения цели исследования рассмотрены способы информационной безопасности в ИТКС «Интернет», основанные на использовании следующих антивирусных программ [8].

1. Dr.Web (Россия) – это антивирусная программа, которая обеспечивает комплексную защищенность всех элементов персонального компьютера (ПК) – системной памяти, твердотельных накопителей и сменных носителей – от угроз, шпионского и коммерческого программного обеспечения (ПО), взламывающих приложений и всевозможных опасных объектов из различных источников; преграждает вход в защищенную систему вирусам и вредоносному ПО; уничтожает проникнувшие вирусы; обеспечивает проверку веб-страниц; осуществляет возможность управления антивирусными программами Dr.Web, установленными на ПК для одной локальной сети [8, 12].

2. Антивирус Касперского (Россия) / Kaspersky Total Security – это антивирусная программа, которая обеспечивает комплексную защиту: от различных видов информационных угроз, сетевых и хакерских атак, а также спама; от вирусов, фишинга и вредоносных WEB-сайтов; имеет сильную защищенность без затормаживания системы; организует управление безопасностью из любой точки доступа; обеспечивает защиту ПК и мобильных устройств с одной лицензией; позволяет создавать резервные копии и шифровать ценные файлы на ПК [8, 13].

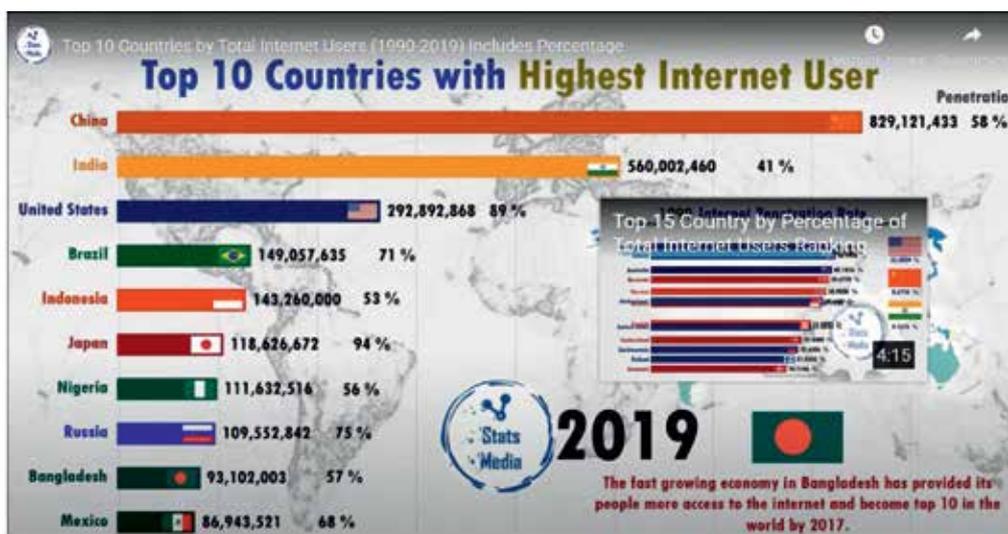


Рис. 1. Рейтинг стран мира по количеству интернет-пользователей [1]

3. McAfee (США) предлагает готовые реализации антивирусных программ, которые могут обеспечивать защиту, различных сетей, а также мобильных устройств во всех странах, помогая клиенту веб-обозревателя безопасно использовать сетевые сервисы. Основываясь на своей системе Global Threat Intelligence, McAfee реализует новаторские продукты, которые повышают возможности пользователей, организаций и представителей, позволяя им обезопасить свои данные, устранять системные сбои, а также обнаруживать недостатки системы [8, 14].

4. ESET NOD32 (Essential Security against Evolving Threats или эффективная защита от эволюционирующих угроз) – международный разработчик антивирусного программного обеспечения) Internet Security (Словакия), создавший антивирусную программу, включающую: антивирус, антишпион, антивирус, антиспам, охрану различных транзакций, родительский контроль, расширенное сканирование памяти [8, 15].

5. AVG Internet Security (Чехия) – антивирусная программа, которая включает в себя: хранилище данных, сканер электронной почты, сканер сайтов, антиспам, WEB-защиту компьютера и защиту электронной почты, защиту от атак злоумышленников, а также включает защиту для мобильных устройств [8, 16].

Для определения наиболее эффективной антивирусной программы предложено использовать следующие этапы МАИ [8–10].

1. Выделение проблемы – выбор наилучшей антивирусной программы с учётом выделенных основных критериев антивирусных программ: количество найденных вредоносных программ; процент определения вредоносных программ; время на поиск вредоносных программ; загрузка центрального процессора (ЦП); цена.

2. Выделение группы альтернатив – две российские Антивирус Касперского (Россия)/Kaspersky Total Security, Dr. Web (Россия)/ Dr. Web Security Space и три зарубежные McAfee (США), AVG Internet Security

(Чехия), ESET NOD32 Internet Security (Словакия) антивирусные программы. В ходе исследования приведенных выше антивирусных программ проведено сравнение их основных показателей (табл. 1).

3. Построение иерархии. Дерево иерархии (рис. 2) дает наглядное представление процедуры принятия решения.

4. Построение матрицы попарных сравнений критериев по цели – определение нормированных элементов b_{kj} матрицы-столбца $B_{n \times p}$ весовых критериев по цели для анализируемых антивирусных программ (табл. 2).

5. Построение матриц сравнений отдельных альтернатив по каждому из избранных критериев.

6. Применение методики анализа полученных матриц, предполагающей проведение нормировки элементов матриц и определение весов строк и столбцов для каждого из выбранных критериев.

Вышеперечисленные действия повторяем для всех матриц попарного сравнения альтернатив по выбранным критериям. В результате получаем матрицу весов альтернатив для рассматриваемых антивирусных программ по избранным критериям (табл. 3).

Введена в рассмотрение матрица нормированных показателей эффективности антивирусных программ, определяемая уравнением

$$C_{m \times p} = A_{m \times n} \times B_{n \times p}, \quad (1)$$

вычисленные элементы которой

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj} \text{ и дадут значения норми-$$

рованных показателей эффективности для анализируемых в качестве альтернатив антивирусных программ, где a_{ik} , b_{kj} – нормированные элементы матриц весов альтернатив по избранным критериям $A_{m \times n}$ (табл. 3) и матрицы-столбца $B_{n \times p}$ весовых критериев по цели для анализируемых антивирусных программ (табл. 2).

Таблица 1

Сравнение основных показателей антивирусных программ [8, 17]

Наименование антивирусной программы	Значения основных показателей антивирусных программ				
	Количество найденных вредоносных программ	% определения вредоносной программы	Время на поиск вредоносной программы	Загрузка цп, %	Цена, руб.
Антивирус Касперского (Россия)	3695	96,3	23 мин	80–95	4479
McAfee (США)	3489	90,1	12 мин	60–80	1432
Dr. Web (Россия)	2968	77,3	1 мин 10 сек	50–60	6123
AVG Internet Security (Чехия)	2840	74	5 мин 32 сек	15–30	1740
ESET NOD32 Internet Security (Словакия)	1949	50,8	1 мин 10 сек	40–50	1600

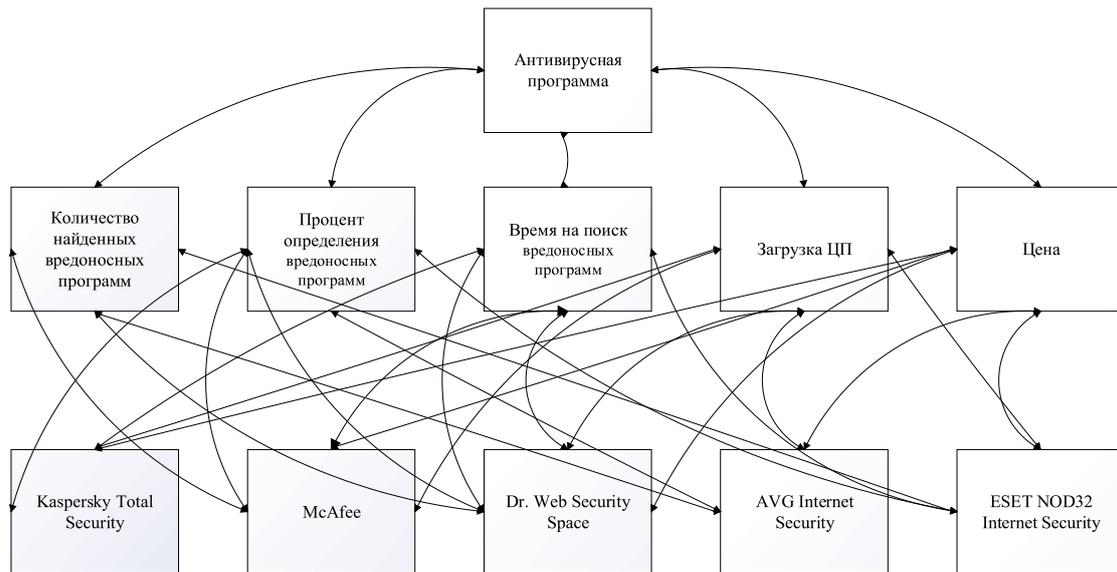


Рис. 2. Построение дерева иерархии (разработано авторами)

Таблица 2

Нормированные элементы b_{kj} матрицы-столбца $B_{n \times p}$ весовых критериев по цели для анализируемых антивирусных программ [Разработано авторами]

Наименование показателей	Значения нормированных элементов b_{kj} матрицы-столбца $B_{n \times p}$ весовых критериев по цели
Количество угроз	0,26
Процент определения	0,24
Время на поиск	0,12
Загрузка ЦП	0,06
Цена	0,32

Примечание: разработано авторами.

Таблица 3

Нормированные элементы a_{ik} матрицы весов альтернатив по избранным критериям $A_{m \times n}$ для анализируемых антивирусных программ [Разработано авторами]

Наименование антивирусной программы	Значения нормированных элементов a_{ik} матрицы $A_{m \times n}$ весов альтернатив по избранным критериям для анализируемых антивирусных программ				
	Количество найденных вредоносных программ	Процент определения вредоносных программ	Время на поиск вредоносных программ	Загрузка ЦП	Цена
Антивирус Касперского (Россия)/ Kaspersky Total Security	0,24	0,26	0,07	0,13	0,17
McAfee (США)	0,24	0,24	0,13	0,17	0,28
Dr. Web (Россия)/ Dr. Web Security Space	0,20	0,19	0,30	0,19	0,12
AVG Internet Security (Чехия)	0,19	0,18	0,20	0,28	0,22
ESET NOD32 Internet Security (Словакия)	0,13	0,13	0,30	0,23	0,21

Подставляя вычисленные нормированные значения (табл. 2 и 3) матриц a_{ik} , b_{kj} в уравнение (1), получаем матрицу-столбец $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$ нормированных значений показателей эффективности антивирусных программ (2) (рис. 3).

Решение:

$$C = A \cdot B = \begin{pmatrix} 0.24 & 0.26 & 0.07 & 0.13 & 0.17 \\ 0.24 & 0.24 & 0.13 & 0.17 & 0.28 \\ 0.2 & 0.19 & 0.3 & 0.19 & 0.12 \\ 0.19 & 0.18 & 0.2 & 0.28 & 0.22 \\ 0.13 & 0.13 & 0.3 & 0.23 & 0.21 \end{pmatrix} \cdot \begin{pmatrix} 0.26 \\ 0.24 \\ 0.12 \\ 0.06 \\ 0.32 \end{pmatrix} = \begin{pmatrix} 0.1954 \\ 0.2354 \\ 0.1834 \\ 0.2038 \\ 0.182 \end{pmatrix}$$

Компоненты матрицы C вычисляются следующим образом:

$$c_{11} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31} + a_{14} \cdot b_{41} + a_{15} \cdot b_{51} = 0.24 \cdot 0.26 + 0.26 \cdot 0.24 + 0.07 \cdot 0.12 + 0.13 \cdot 0.06 + 0.17 \cdot 0.32 = 0.0624 + 0.0624 + 0.0084 + 0.0078 + 0.0544 = 0.1954$$

$$c_{21} = a_{21} \cdot b_{11} + a_{22} \cdot b_{21} + a_{23} \cdot b_{31} + a_{24} \cdot b_{41} + a_{25} \cdot b_{51} = 0.24 \cdot 0.26 + 0.24 \cdot 0.24 + 0.13 \cdot 0.12 + 0.17 \cdot 0.06 + 0.28 \cdot 0.32 = 0.0624 + 0.0576 + 0.0156 + 0.0102 + 0.0896 = 0.2354$$

$$c_{31} = a_{31} \cdot b_{11} + a_{32} \cdot b_{21} + a_{33} \cdot b_{31} + a_{34} \cdot b_{41} + a_{35} \cdot b_{51} = 0.2 \cdot 0.26 + 0.19 \cdot 0.24 + 0.3 \cdot 0.12 + 0.19 \cdot 0.06 + 0.12 \cdot 0.32 = 0.052 + 0.0456 + 0.036 + 0.0114 + 0.0384 = 0.1834$$

$$c_{41} = a_{41} \cdot b_{11} + a_{42} \cdot b_{21} + a_{43} \cdot b_{31} + a_{44} \cdot b_{41} + a_{45} \cdot b_{51} = 0.19 \cdot 0.26 + 0.18 \cdot 0.24 + 0.2 \cdot 0.12 + 0.28 \cdot 0.06 + 0.22 \cdot 0.32 = 0.0494 + 0.0432 + 0.024 + 0.0168 + 0.0704 = 0.2038$$

$$c_{51} = a_{51} \cdot b_{11} + a_{52} \cdot b_{21} + a_{53} \cdot b_{31} + a_{54} \cdot b_{41} + a_{55} \cdot b_{51} = 0.13 \cdot 0.26 + 0.13 \cdot 0.24 + 0.3 \cdot 0.12 + 0.23 \cdot 0.06 + 0.21 \cdot 0.32 = 0.0338 + 0.0312 + 0.036 + 0.0138 + 0.0672 = 0.182$$

Рис. 3. Решение-вычисление $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$

Вычисление значений $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$ получено с помощью онлайн-калькулятора (рис. 3) [18]:

$$C_{m \times p} = A_{m \times n} \times B_{n \times p} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{pmatrix} \times \begin{pmatrix} b_{11} \\ b_{21} \\ b_{31} \\ b_{41} \\ b_{51} \end{pmatrix} = \begin{pmatrix} 0,24 & 0,26 & 0,07 & 0,13 & 0,17 \\ 0,24 & 0,24 & 0,13 & 0,17 & 0,28 \\ 0,20 & 0,19 & 0,30 & 0,19 & 0,12 \\ 0,19 & 0,18 & 0,20 & 0,28 & 0,22 \\ 0,13 & 0,13 & 0,30 & 0,23 & 0,21 \end{pmatrix} \times \begin{pmatrix} 0,26 \\ 0,24 \\ 0,12 \\ 0,06 \\ 0,32 \end{pmatrix} = \begin{pmatrix} 0,19 \\ 0,23 \\ 0,18 \\ 0,20 \\ 0,18 \end{pmatrix} \quad (2)$$

Окончательные результаты расчётов нормированных показателей эффективности зарубежных и российских антивирусных программ по избранным критериям согласно уравнению (2) округлены до двух значащих цифр и сведены в табл. 4. Как следует из результатов вычисления нормированных показателей эффективности антивирусных программ (табл. 4), наиболее эффективной зарубежной антивирусной программой с учётом выбранных критериев является McAfee (США), так как значение вычисленного показателя эффективности для неё составило наибольшее значение 0,23 (рис. 4) – больше значений соответствующих показателей для других антивирусных программ.

Таблица 4

Значения вычисленных нормированных показателей эффективности $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$ зарубежных и отечественных антивирусных программы по избранным критериям

Наименование антивирусной программы	Значение вычисленного показателя эффективности $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$ антивирусной программы
McAfee (США)	0,23
AVG Internet Security (Чехия)	0,20
Антивирус Касперского (Россия)/Kaspersky Total Security	0,19
Dr. Web (Россия)/ Dr. Web Security Space	0,18
ESET NOD32 Internet Security (Словакия)	0,18

Примечание: разработано авторами.

Значение вычисленного показателя эффективности

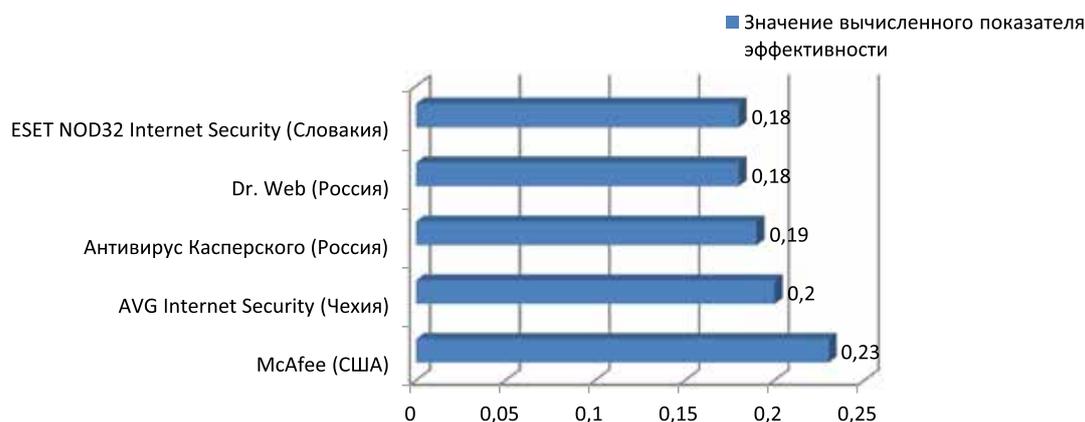


Рис. 4. Сравнение значений вычисленных нормированных показателей эффективности

$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$ российских и зарубежных антивирусных программ (разработано авторами)

Заключение

Для достижения цели исследования были рассмотрены способы информационной безопасности в ИТКС «Интернет», основанные на использовании антивирусных программ, а также выбор наилучшей из них с использованием МАИ.

Для определения наилучшего варианта антивирусной программы на основании использования МАИ введена матрица показателей эффективности антивирусных программ (1). В работе проведен расчет нормированных значений элементов матрицы эффективности антивирусных программ по уравнению (1) с использованием МАИ Томаса Л. Саати. Полученные значения вычисленных показателей эффективности

зарубежных и российских антивирусных программ по избранным критериям с использованием МАИ Томаса Л. Саати сведены в табл. 4. Наибольшее значение показателя эффективности антивирусных программ составило 0,23 (рис. 4), что соответствует характеристикам антивирусной программы McAfee (США). Поэтому для обеспечения информационной безопасности в ИТКС «Интернет» рекомендовано использовать среди зарубежных антивирусных программ – McAfee, а среди российских антивирусных программ наиболее эффективной следует признать антивирусную программу Антивирус Касперского (Россия)/Kaspersky Total Security (значение показателя эффективности, как следует из результатов расчетов в табл. 4 и рис. 4, составило 0,19).

Список литературы

1. Тюлягин С. Рейтинг стран мира по количеству Интернет-пользователей. [Электронный ресурс]. URL: <https://tyulyagin.ru/ratings/rejting-stran-mira-po-kolichestvu-internet-polzovatelej.html> (дата обращения: 07.12.2021).
2. Пескин А.Е., Смирнов А.В., Тюхтин М.Ф. Телевидение и Интернет / Под ред. канд. техн. наук А.В. Балобанова. М.: Горячая линия – Телеком, 2020. 340 с.
3. Малюк А.А., Горбатов В.С., Королев В.И. и др. Введение в информационную безопасность. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2018. 288 с.
4. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. СПб.: ВКА имени А.Ф. Можайского, 2016. 461 с.
5. Пилькевич С.В., Еремеев М.А. Модели социально значимых интернет-ресурсов // Труды СПИИРАН. 2015. Вып. 2 (39). С. 62–83. [Электронный ресурс]. URL: <http://www.proceedings.spiiras.nw.ru> (дата обращения: 07.12.2021).
6. Коржик В.И., Просихин В.П., Яковлев В.А. Основы криптографии: учебное пособие. СПб.: СПбГУТ, 2014. 276 с.
7. Сمارт Н. Криптография. Пер. с англ. С.А. Кулешова под ред. С.К. Ландо. М.: Техносфера, 2005. 528 с.
8. Климентьев К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. Издание рекомендовано в качестве учебного пособия для студентов технических вузов. М.: ДМК Пресс, 2013. 658 с.
9. Саати Томас Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Науч. ред. А.В. Андрейчиков, О.Н. Андрейчикова. М.: Издательство ЛКИ, 2008. 360 с.
10. Саати Томас Л. Принятие решений. Метод анализа иерархий. Пер. с англ. Р.В. Вачнадзе. М.: Радио и связь, 1993. 278 с.
11. Интернет: Официальное определение термина [Электронный ресурс]. URL: <https://medium.com/bazanov-org/интернет-официальное-определение-термина-e8374398892> (дата обращения: 07.12.2021).
12. Dr.Web Security Space [Электронный ресурс]. URL: https://products.drweb.ru/win/security_space (дата обращения: 07.12.2021).
13. Kaspersky Internet Security [Электронный ресурс]. URL: <https://www.kaspersky.ru/internet-security>. (дата обращения: 07.12.2021).
14. McAfee достоинства и недостатки [Электронный ресурс]. URL: <https://web-shpargalka.ru/mcafee-dostoinstva-i-nedostatki.php>. (дата обращения: 07.12.2021).
15. Что входит в ESET NOD32 Internet Security [Электронный ресурс]. URL: <https://www.esetnod32.ru/home/products/internet-security/>. (дата обращения: 07.12.2021).
16. AVG Internet Security Лучшая в своем классе защита для всех ваших устройств [Электронный ресурс]. URL: <https://www.avg.com/ru-ru/internet-security> (дата обращения: 07.12.2021).
17. Сравнение антивирусных программ [Электронный ресурс]. URL: <http://smartsourcing.ru/blogs/informatsionnaya-bezopasnost/1595> (дата обращения: 07.12.2021).
18. Онлайн калькулятор. [Электронный ресурс]. URL: <https://ru.onlinschool.com/math/assistance/matrix/multiply> (дата обращения: 07.12.2021).