Обзорная статья
УДК 004.032.26.056
ББК 32.972.53
Д 58
DOI: 10.53598/2410-3225-2022-2-301-67-77

Обеспечение информационной безопасности веб-сайта в условиях импортозамещения

(*Рецензирована*)

Виталий Анатольевич Довгаль[1], Денис Игоревич Шередько[2]

[1] *Майкопский государственный технологический университет, Адыгейский государственный университет, Майкоп, Россия, urmia@mail.ru*
[2] *Майкопский государственный технологический университет, Майкоп, Россия, sheredkoden@yandex.ru*

Аннотация. *В статье рассматриваются угрозы, которым подвергаются веб-сайты, и способы их нейтрализации. Защита веб-сайтов в настоящее время часто осуществляется с применением решений, разработанных за рубежом. Наличие рисков, связанных с выведением из строя Интернет-ресурсов объектов критической инфраструктуры России, требует организации системной работы по ликвидации указанных информационных атак. В связи с необходимостью обеспечения бесперебойной работы веб-сайтов органов власти, средств массовой информации, финансовых учреждений, массовых социально значимых порталов и сетей необходимо обеспечить замещение иностранных средств защиты информации отечественными. В работе предлагаются варианты замены зарубежного программного обеспечения, используемого в стране, аналогичному ему по реализуемым функциям отечественным в рамках тенденции импортозамещения.*

Ключевые слова: *информационная безопасность, угрозы информационной безопасности, веб-сайт, обеспечение безопасности веб-сайтов, импортозамещение*

Review Paper

Ensuring the information security of the website in the conditions of import substitution

Vitaliy A. Dovgal[1], Denis I. Sheredko[2]

[1] *Maikop State University of Technology, Adyghe State University, Maikop, Russia, urmia@mail.ru*
[2] *Maikop State University of Technology, Maikop, Russia, sheredkoden@yandex.ru*

Abstract. Abstract. *The paper discusses the threats to which websites are exposed and ways to neutralize them. The protection of websites is now often carried out using solutions developed abroad. The presence of risks associated with the disabling of Internet resources of critical infrastructure facilities in Russia requires the organization of systematic work to eliminate these information attacks. Due to the need to ensure the smooth operation of government websites, mass media, financial institutions, socially significant mass portals and networks, it is necessary to ensure the replacement of foreign means of information protection with domestic ones. The paper offers options for replacing foreign software used in the country, with the domestic one similar to it in terms of the implemented functions within the framework of the import substitution trend.*

Keywords: *information security, threats to information security, website, ensuring the security of websites, import substitution*

Введение

Одной из задач обеспечения устойчивой работы информационной инфраструктуры, поставленных Президентом Российской Федерации на заседании Совета безопасности страны, является кардинальное снижение рисков, связанных с использованием зарубежных программ и оборудования [1]. В условиях киберагрессии недружественных стран и резко возросшими рисками информационной безопасности актуальным становится вопрос использования программного и аппаратного обеспечения защиты информации, созданных отечественными разработчиками. Мишенью хакеров оказываются в том числе веб-сайты, информационную защиту которых обеспечивает в большинстве случаев импортное программное обеспечение.

Цель исследования заключается в изучении и анализе возможностей по замене иностранных средств защиты веб-сайтов отечественным программным обеспечением.

1. Угрозы, присущие сайтам, и способы их нейтрализации

Сайт, или веб-сайт – одна или несколько логически связанных между собой веб-страниц, а также место расположения контента сервера [2]. Защита сайтов от возможных угроз информационной безопасности – важная задача для его владельца, так как возможны такие последствия, как, например, утечка персональных данных, неполучение от потенциальных клиентов прибыли вследствие недоступности сайта, снижение позиции сайта в результатах поиска, падение репутации организации и т.п. [3].

Веб-сайтам присущи следующие типы угроз [4]:

- изменение контента веб-сайта – то есть размещение на сайте злоумышленником любой информации;
- удаление данных злоумышленником, в том числе информации о паролях, базах данных клиентов;
- внедрение вредоносных программ, которые могут производить зловредные действия (например, кража персональных данных пользователя, переадресация на мошеннический сайт или заражение посетителей веб-сайта вирусными программами);
- рассылка спама веб-приложением сайта – угроза, приводящая к включению веб-сайта в спам-листы и невозможности в дальнейшем отправки санкционированных сообщений;
- DDoS-атака – угроза, затрудняющая или прекращающая доступ легальных пользователей к сайту.

К средствам защиты веб-сайтов относятся следующие [4]:

- межсетевой экран веб-приложений (Web application firewall, WAF);
- средства анализа веб-сайтов на наличие вирусов;
- балансировщики нагрузки на веб-приложения;
- средства защиты от DDoS-атак;
- сканеры защищенности веб-приложений.

Рассмотрим каждое средство в отдельности. Принцип работы межсетевого экрана веб-приложений основан на использовании его основного компонента защиты – машинного обучения, с помощью которого формируется «белый» список допустимых идентификаторов доступа (на данный момент в веб-приложениях используются три типа идентификатора доступа: HTTP-параметры, идентификатор ресурса, идентификатор сессии, он же cookie). Задача межсетевого экрана веб-приложений, реализованного как физическое или виртуальное устройство, состоит в выявлении допустимых значений идентификаторов для веб-приложения (реализация в виде агента на веб-сервере не рекомендована к использованию). Классический способ размещения WAF в сети – в режиме обратного прокси-сервера, перед защищаемыми веб-серверами – показан на ри-

сунке 1 [5]. Файрволы веб-приложений могут защитить от таких атак, как изменение и удаление данных веб-сайта, внедрение вредоносных программ, рассылка спама [6].

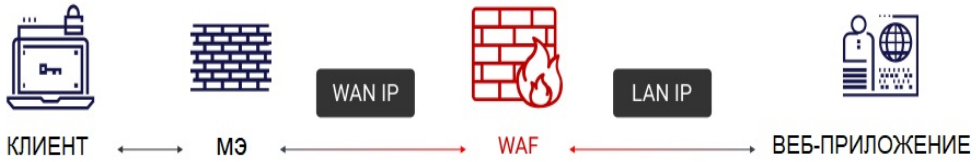

Рис. 1. Размещение межсетевого экрана веб-приложений в сети в режиме обратного прокси-сервера

Fig. 1. Placing a web application firewall on a network in reverse proxy mode

Средства анализа веб-сайтов на наличие вирусов позволяют обнаруживать вредоносное программное обеспечение (ПО) в файлах сайта или в его коде. Среди способов и средств проверки веб-сайта на наличие вредоносных программ можно выделить следующие: онлайн-сервисы (выполняющие статический и динамический анализ кода веб-страницы), антивирусные программы (сканирующие файлы на локальном веб-сервере, а также компьютеры администраторов сайта) [7].

Балансировка нагрузки на веб-приложения позволяет распределить нагрузку между несколькими сетевыми устройствами, такими как серверы, маршрутизаторы, межсетевые экраны [8]. Данная операция может быть реализована в виде дополнительного ПО или на отдельном сервере [9]. На рисунке 2 изображена схема, на которой балансировщик распределяет нагрузку между серверами [10]. Балансировка нагрузки позволяет избежать чрезмерной загруженности сервера и, как следствие, трудностей с доступом клиентов к сайту [11].

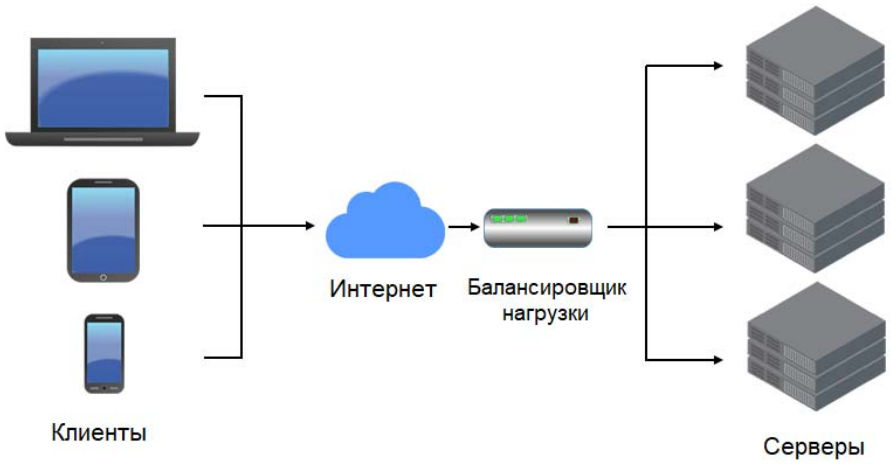

Рис. 2. Схема доступа клиентов к ресурсам сервера посредством балансировки нагрузки

Fig. 2. Schematic diagram showing how clients access server resources by load balancing

Для защиты от DDoS-атак применяются два подхода – создание программно-аппаратного комплекса в инфраструктуре организации-владельца сайта или выбор специального стороннего сервиса. В данной работе будет рассмотрен подход с использованием сторонних специальных сервисов [12]. На рисунке 3 показана схема защиты от DDoS-атак сторонним сервисом. При попытке пользователя зайти на сайт запрос от него отправляется в облако компании, предоставляющей сервис. В этом облаке происходит проверка и фильтрация трафика. Если трафик признан атакующим, то он блокируется. Остальной отправляется на веб-сервер, на котором хранится нужный пользователю сайт [3].

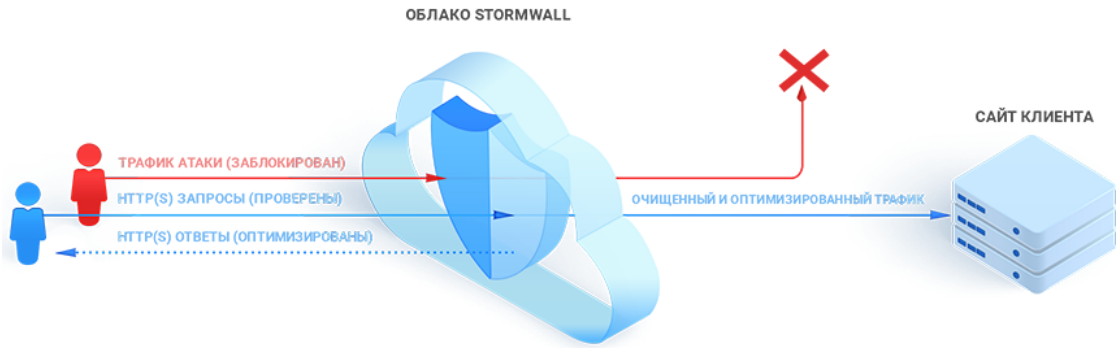

Рис. 3. Схема защиты от DDoS-атак с помощью стороннего сервиса

Fig. 3. DDoS-attack protection schematic diagram using a third-party service

Сканеры защищенности веб-приложений как средство защиты веб-сайтов предназначены для поиска уязвимостей в веб-приложениях [13].

2. Обеспечение безопасности сайта с помощью отечественных решений

Для защиты сайтов в данный момент используются различные средства и сервисы от иностранных производителей. Так, в качестве межсетевого экрана веб-приложений популярно решение американской компании Imperva, предназначенное для обеспечения безопасности критичных веб-приложений, – Imperva SecureSphere Web Application Firewall [14].

Для его замещения можно найти много других вариантов программного обеспечения указанного назначения, обеспечивающего услуги в области кибербезопасности и гарантирующего защиту корпоративных данных. Одним из отечественных межсетевых экранов веб-приложений является Solid Wall WAF [15]. Данное решение может быть реализовано в виде ПО, виртуального устройства, программно-аппаратного комплекса или как облачный сервис [16]. Преимущество Solid Wall WAF перед Imperva SecureSphere Web Application Firewall в том, что он присутствует в едином реестре российских программ для электронных вычислительных машин и баз данных [17].

Также отечественным файрволом веб-приложений является решение PT Application Firewall от компании Positive Technologies [5], отличия которого от американского Imperva SecureSphere Web Application Firewall состоят в следующем:

- российский комплекс включен в единый реестр российских программ для электронных вычислительных машин и баз данных [18];
- отечественный продукт имеет ретроспективный анализ (анализ логов трафика, осуществляющий верификацию атаки с использованием встроенного динамического сканера) [19].

В категории импортных антивирусных средств для защиты веб-сайтов можно назвать ПО Trend Micro Web Security от японской компании Trend Micro, считающейся мировым лидером среди разработчиков программного обеспечения для кибербезопасности [20].

Однако в нашей стране существует отечественное антивирусное ПО высокого уровня, в котором прежде всего можно выделить различные средства, разработанные компанией Kaspersky. Так, для серверных операционных систем (ОС) Windows разработан Kaspersky Security для Windows Server [21]. Данное ПО поддерживает такие версии ОС, как Windows Server 2012/2012 R2, Windows Server 2016, Windows Multi Point Server 2011, Windows Hyper-V Server 2012/2012 R2/2016, Windows Storage Server 2012/2012 R2/2016 [22].

Решение Kaspersky Endpoint Security для Linux может быть установлено на

большом количестве различных ОС [23]. К 32-битным относятся Ubuntu 16.04 LTS и выше, Альт 8 СП Рабочая Станция, Альт 8 СП Сервер и Гослинукс 6.6 и прочие. В число 64-х разрядных входят такие операционные системы, как Ubuntu 16.04 LTS и выше, SUSE Linux Enterprise Server 15 и выше, openSUSE Leap 15 и выше, Альт 8 СП Рабочая Станция, Альт 8 СП Сервер, Amazon Linux 2, Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5), Гослинукс 6.6 и AlterOS 7.5 и выше [24].

Необходимо обратить внимание на то, что решение Kaspersky Endpoint Security для Windows (версия 11.6.0.394) и Kaspersky Endpoint Security 11 для Linux сертифицированы ФСТЭК на соответствие требований ко второму уровню доверия, а также требованиям к средствам антивирусной защиты (САВЗ) – Профиль защиты САВЗ (Б, В и Г второго класса защиты) [25].

Разработкой антивирусного ПО также занимается и другой российский разработчик – компания Dr.Web. Ее продукт предоставляет возможность проверки сайта в качестве онлайн-сервиса, для чего на сайте разработчика нужно указать ссылку сайта, который необходимо проверить [26]. Непосредственно для защиты веб-сервера существует решение Dr.Web Server Security Suite [27].Одно из преимуществ данного продукта состоит в том, что версии для ОС Windows и Linux имеют сертификат ФСТЭК, подтверждающий соответствие требований ко второму уровню доверия, а также требований к средствам антивирусной защиты (САВЗ) – Профиль защиты САВЗ (А, Б, В и Г второго класса защиты) [25]. Dr.Web Enterprise Security Suite версия 10 и 12 (как для ОС Windows, так и для Linux) сертифицированы ФСБ России по соответствию требований к программным антивирусным средствам, используемым в средствах вычислительной техники, эксплуатируемых в органах федеральной службы безопасности, классов А2, Б2, В2, Г2 и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований эксплуатационной документации согласно формуляру RU.72110450.40012-01 30 01 [28]. Версия для ОС Linux сертифицирована Минобороны России [29]. Также преимуществом решений компании Dr.Web является их совместимость с отечественными ОС (например, такими, как ОС МСВС, ALT Linux, Astra Linux, ОС ROSA, Ред ОС 7.1 Муром, ОС Аврора, Р-Платформа) [29];

В качестве балансировщика нагрузки на веб-приложения используется модуль Local Traffic Manager, разработанный американской транснациональной корпорацией F5 Networks, Inc., специализирующейся на услугах, связанных с Интернет-сайтами и приложениями [30]. Модуль, входящий в комплекс BIG-IP, может поставляться в виде аппаратного обеспечения, виртуального устройства или облачного сервиса [30]. В его веб-интерфейсе TMUI (Traffic Management User Interface) российские специалисты уже нашли уязвимость [31].

Заменить скомпрометированный контроллер доставки приложений может отечественный балансировщик нагрузки Elastic Load Balance, разработанный в компании Сбер, который может использоваться только как облачный сервис и только с серверами, арендуемыми у облачного провайдера услуг SberCloud [32].

Еще одним российским балансировщиком нагрузки является Yandex Network Load Balancer, который также работает как облачный сервис и только при аренде серверов в сервисе Yandex Cloud [33].

Также на отечественном рынке присутствует «Отказоустойчивый балансировщик нагрузки», разработанный компанией Selectel, который также работает в виде облачного сервиса и только с арендованными у Selectel серверами [34].

Среди зарубежных сервисов по защите от DDoS-атак популярен Cloudflare DDoS protection, разработанный в американской компании Cloudflare [35]. Для его замещения можно порекомендовать отечественного представителя сервиса по защите от DDoS-

атак – «Сервис мониторинга трафика и защиты от DDoS-атак», созданного компанией Ростелеком [36]. Данный сервис позволяет выполнять требования российских нормативно-правовых актов, относящихся к защите объектов критической информационной инфраструктуры, персональных данных, информационных систем, автоматизированных систем управления технологическим процессом на критически важных объектах и финансовых операций [36]. Кроме того, сервис российской компании отличается от Cloudflare DDoS protection следующими преимуществами [12]:

- возможность использования услуги по защите от DDoS центра обработки данных (ЦОД), подразумевающей физическое перемещение оборудования в ЦОД, предоставляемый компанией Ростелеком;
- наличие фильтрации Hyper Text Transfer Protocol Secure (HTTPS) без раскрытия ключей.

Также услугу по защите сайтов от DDoS-атак предоставляет сервис «Защита и ускорение сайта», разработанный компанией DDoS-Guard [11]. Преимущества данного сервиса перед продуктом от Cloudflare [12]:

- возможность использования услуги по защите от DDoS ЦОД, подразумевающей физическое перемещение оборудования в предоставляемый компанией DDoS-Guard ЦОД;
- наличие фильтрации HTTPS без раскрытия ключей.

Для сканирования веб-приложений можно использовать фреймворк с открытым исходным кодом Metasploit, созданный в американской компании Rapid7 [37]. С помощью этого мощнейшего инструмента, имеющегося в распоряжении как киберпреступников, так и «белых хакеров» и специалистов по проникновению, можно исследовать уязвимости в сетях и на серверах, применяя готовый или создавая пользовательский код и вводя его в сеть для поиска слабых мест.

Рассмотрим отечественные решения для замещения средств устранения системных недостатков. В качестве примера можно привести Сканер-ВС, разработанный в компании АО «НПО «Эшелон» [38]. Данный продукт сертифицирован ФСТЭК по соответствию требований к четвертому уровню доверия и технических условий, а также внесен в единый реестр российских программ для электронных вычислительных машин и баз данных [39, 40]. Кроме этого, преимуществом данного сканера перед Metasploit является возможность проверки контрольных сумм заданных папок и файлов по 13-ти алгоритмам, включая ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 [41].

Другим примером отечественного сканера является решение XSpider, разработанное в компании Positive Technologies [42], которое предназначено для компаний с количеством сетевых узлов до 10000 [43].Программа-сканер XSpider имеет сертификат ФСТЭК, подтверждающий соответствие требований к четвертому уровню доверия и технических условий, и внесен в реестр российского программного обеспечения [25, 44].

Для крупных предприятий компания Positive Technologies предлагает комплексное решение для мониторинга защищенности сети предприятия MaxPatrol 8 [45], который по сравнению с Metasploit обладает следующими преимуществами:

- наличие сертификата ФСТЭК по соответствию требований к четвертому уровню доверия и внесено в реестр российского программного обеспечения [25, 46];
- возможность проверки системы управления базами данных [43];
- наличие режима контроля соответствия стандартам, который позволяет проверить выполнение требований отечественных регулирующих органов, международных и отраслевых стандартов, а также корпоративных регламентов [45].

Основная особенность российских сканеров уязвимостей состоит в том, что из-за требований различных нормативно-правовых актов определенные предприятия, на-

пример, операторы персональных данных должны обязательно иметь сканер уязвимостей, а сам продукт должен иметь сертификат ФСТЭК [43].

Заключение

В данном исследовании рассмотрена возможность замены иностранных средств защиты веб-сайта на российские. Был проведен сравнительный анализ различных популярных средств защиты. Исходя из выполненного анализа, можно сделать вывод, что в четырех из пяти групп средств защиты возможно произвести замену зарубежных на отечественные, исключение составляют балансировщики нагрузки.

Примечания

1. Путин поручил создать госсистему защиты информации // Сетевое издание «РИА Новости». URL: https://ria.ru/20220520/voyna-1789757869.html (дата обращения: 08.05.2022).

2. Интернет-энциклопедия «Википедия». URL: https://ru.wikipedia.org/wiki/Сайт (дата обращения: 12.03.2022).

3. Защита веб-сайтов от DDoS-атак без смены хостинга проксированием // Web-сайт компании “StormWall”. URL: https://stormwall.pro/website-protection (дата обращения: 07.05.2022).

4. Средства защиты веб-сайтов (приложений) // Интернет-издание “Anti-Malware.ru”. URL: https://www.anti-malware.ru/security/application-security (дата обращения: 12.03.2022).

5. PT Application Firewall // Web-сайт продукта ”PT Application Firewall”. URL: https://www.ptsecurity.com/ru-ru/products/af/ (дата обращения: 12.03.2022).

6. WAF (Web Application Firewall) // Web-сайт компании “StormWall”. URL: https://stormwall.pro/knowledge-base/termin/waf (дата обращения: 16.03.2022).

7. Проверка веб-сайта на вирусы // Интернет-издание “Anti-Malware.ru”. URL: https://www.anti-malware.ru/security/check-website-for-viruses (дата обращения: 29.03.2022).

8. Балансировка нагрузки на веб-приложения // Интернет-издание «Anti-Malware.ru». URL: https://www.anti-malware.ru/security/load-balancing (дата обращения: 12.03.2022).

9. Балансировка нагрузки // Web-сайт компании “SberCloud”. URL: https://sbercloud.ru/ru/warp/balansirovka-nagruzki (дата обращения: 12.03.2022).

10. Что такое балансировка нагрузки в сети? // Web-сайт компании «Мерион Нетворкс». URL: https://wiki.merionet.ru/seti/73/chto-takoe-balansirovka-nagruzki-v-seti/ (дата обращения: 16.03.2022).

11. Защита и ускорение сайта // Web-сайт сервиса «Защита и ускорение сайта». URL: https://ddos-guard.net/ru/store/web (дата обращения: 22.03.2022).

12. Сравнение сервисов по защите от DDoS-атак // Интернет-издание “Anti-Malware.ru”. URL: https://www.anti-malware.ru/compare/DDoS-attack-protection-services (дата обращения: 22.03.2022).

13. Аудит безопасности веб-сайта (сканер уязвимостей веб-сайта) // Интернет-издание “Anti-Malware.ru”. URL: https://www.anti-malware.ru/security/security-audit-website (дата обращения: 25.03.2022).

14. Брандмауэр веб-приложений // Веб-сайт продукта “Imperva Secure Sphere Web Application Firewall”. URL: https://www.imperva.com/products/web-application-firewall-waf/ (дата обращения: 26.03.2022).

15. SolidWall WAF // Web-сайт продукта “SolidWall WAF”. URL: https://solidwall.ru/ (дата обращения: 09.05.2022).

16. Интеллектуальный сетевой экран для защиты веб-приложений SolidWall // Web-сайт продукта “SolidWall WAF”. URL: https://solidwall.ru/features.html#architecture (дата обращения: 09.05.2022).

17. Интеллектуальный сетевой экран для защиты веб-приложений SolidWall // Web-сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет». URL: https://reestr.digital.gov.ru/reestr/309803/?sphrase_id=1372933 (дата обращения: 04.05.2022).

18. Система защиты приложений от несанкционированного доступа Positive Technologies Application Firewall (PTAF) // Web-сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет». URL: https://reestr.digital.gov.ru/reestr/441322/?sphrase_id=1267679 (дата обращения: 30.03.2022).

19. Сравнение фаерволов для защиты веб-сайтов (Web Application Firewall – WAF) // Интернет-издание “Anti-Malware.ru”. URL: https://www.anti-malware.ru/compare/web-application-firewall-waf-2017 (дата обращения: 25.03.2022).

20. Безопасность веб-приложений // Web-сайт продукта “Trend Micro Web Security”. URL: https://www.trendmicro.com/ru_ru/business/products/user-protection/sps/web-security.html (дата обращения: 05.05.2022).

21. Security для Windows Server // Web-сайт продукта “Kaspersky Security для Windows Server”. URL: https://www.kaspersky.ru/small-to-medium-business-security/windows-server-security (дата обращения: 30.03.2022).

22. Отказоустойчивая защита для важнейших бизнес-процессов, выполняемых на серверах Windows // Web-сайт продукта «Kaspersky Security для Windows Server». URL: https://media.kaspersky.com/ru/business-security/Kaspersky_Security_for_Windows_Server_10.1_Datasheet_Ru_web.pdf (дата обращения: 31.03.2022).

23. Kaspersky Endpoint Security для Linux // Web-сайт продукта “Kaspersky Endpoint Security для Linux”. URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-linux (дата обращения: 30.03.2022).

24. Надежная защита для серверов и рабочих станций под управлением Linux // Web-сайт продукта “Kaspersky Security для Windows Server”. URL: https://media.kaspersky.com/ru/business-security/Kaspersky_Endpoint_for_Linux_Datasheet_Ru_web.pdf (дата обращения: 31.03.2022).

25. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации // Web-сайт ФСТЭК, государственный реестр сертифицированных средств защиты информации. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения: 04.05.2022).

26. Проверить ссылку (URL) // Web-сайт онлайн-проверки стороннего web-сайта на вирусы. URL: https://vms.drweb.ru/online/ (дата обращения: 30.03.2022).

27. Dr.Web Server Security Suite // Web-сайт продукта “Dr.Web Server Security Suite”. URL: https://products.drweb.ru/fileserver/ (дата обращения: 29.03.2022).

28. Выписка из перечня средств защиты информации, сертифицированных ФСБ России. // Web-сайт ФСБ, перечень средств защиты информации, сертифицированных ФСБ России. URL: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_28.03.2022.doc (дата обращения: 11.04.2022).

29. Dr.Web Enterprise Security Suite // Web-сайт продукта “Dr.Web Server Security Suite”. URL: https://products.drweb.ru/fileserver/unix/ (дата обращения: 04.05.2022).

30. Интеллектуальное управление трафиком приложений // Web-сайт продукта “LocalTrafficManager”. URL: https://www.f5.com/products/big-ip-services/local-traffic-manager (дата обращения: 21.04.2022).

31. Большая дыра в BIG-IP. Как работает новая уязвимость в продуктах компании F5 // Интернет-издание «Хакер». URL: https://xakep.ru/2020/08/12/f5-big-ip-rce/ (дата обращения: 06.05.2022).

32. Техническая документация // Web-сайт сервиса “Elastic Load Balance”. URL: https://sbercloud.ru/ru/products/elastic-load-balance#tehnicheskaya-dokumentatsiya (дата обращения: 22.04.2022).

33. Yandex Network Load Balancer // Web-сайтсервиса “Yandex Network Load Balancer”. URL: https://cloud.yandex.ru/services/network-load-balancer (дата обращения: 22.04.2022).

34. Отказоустойчивый балансировщик нагрузки // Web-сайт сервиса «Отказоустойчивый балансировщик нагрузки». URL: https://selectel.ru/lab/general-load-balancer/ (дата обращения: 09.05.2022).

35.Комплексная защита от DDoS // Web-сайт продукта “Cloudflare DDoS protection”. URL: https://www.cloudflare.com/ddos/ (дата обращения: 22.04.2022).

36. Сервис мониторинга трафика и защиты от DDoS-атак // Web-сайт сервиса «Сервис мониторинга трафика и защиты от DDoS-атак». URL: https://rt-solar.ru/services/anti-ddos/ (дата обращения: 22.03.2022).

37. Metasploit // Web-сайт продукта “Metasploit”. URL: https://www.rapid7.com/products/metasploit/ (дата обращения: 11.03.2022).

38. Сканер-ВС анализ защищенности // Web-сайт продукта «Сканер-ВС». URL: https://scaner-vs.ru/ (дата обращения: 07.05.2022).

39. Описание // Web-сайт продукта «Сканер-ВС». URL: https://scaner-vs.ru/about/ (дата

обращения: 05.05.2022).

40. Средство анализа защищенности «Сканер-ВС» // Web-сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет». URL: https://reestr.digital.gov.ru/reestr/301522/?sphrase_id=1426619 (дата обращения: 05.05.2022).

41. Возможности // Web-сайт продукта «Сканер-ВС». URL: https://scaner-vs.ru/capabilities/ (дата обращения: 02.05.2022).

42. XSpider // Web-сайт продукта "XSpider". URL: https://www.ptsecurity.com/ru-ru/products/xspider/ (дата обращения: 05.05.2022).

43. Сканеры уязвимостей – обзор мирового и российского рынков // Интернет-издание "Anti-Malware.ru". URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets (дата обращения: 25.03.2022).

44. XSpider // Web-сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет». URL: https://reestr.digital.gov.ru/reestr/464566/?sphrase_id=1432114 (дата обращения: 05.05.2022).

45. MaxPatrol 8 // Web-сайт продукт "MaxPatrol 8". URL: https://www.ptsecurity.com/ru-ru/products/mp8/ (дата обращения: 03.05.2022).

46. MaxPatrol // Web-сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет». URL: https://reestr.digital.gov.ru/reestr/469631/?sphrase_id=1432197 (дата обращения: 05.05.2022).

References

1. Putin instructed to create a state information security system // RIA Novosti online edition. URL: https://ria.ru/20220520/voyna-1789757869.html (access date: 08/05/2022).

2. Internet encyclopedia "Wikipedia". URL: https://ru.wikipedia.org/wiki/Website (access date: 12/03/2022).

3. Protection of websites from DDoS-attacks without changing the hosting by proxying // Website of the StormWall company. URL: https://stormwall.pro/website-protection (access date: 07/05/2022).

4. Tools for protecting websites (applications) // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/security/application-security (access date: 12/03/2022).

5. PT Application Firewall // PT Application Firewall product web site. URL: https://www.ptsecurity.com/en-us/products/af/ (access date: 12/03/2022).

6. WAF (Web Application Firewall) // Website of the StormWall company. URL: https://stormwall.pro/knowledge-base/termin/waf (access date: 16/03/2022).

7. Checking a website for viruses // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/security/check-website-for-viruses (access date: 29/03/2022).

8. Load balancing for web applications // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/security/load-balancing (access date: 12/03/2022).

9. Load balancing // SberCloud company website. URL: https://sbercloud.ru/ru/warp/balansirovka-nagruzki (access date: 12/03/2022).

10. What is network load balancing? // Merion Networks company website. URL: https://wiki.merionet.ru/seti/73/chto-takoe-balansirovka-nagruzki-v-seti/ (access date: 16/03/2022).

11. Website protection and acceleration // Website of the Website Protection and Acceleration service. URL: https://ddos-guard.net/ru/store/web (access date: 22/03/2022).

12. Comparison of services for protection against DDoS attacks // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/compare/DDoS-attack-protection-services (access date: 22/03/2022).

13. Website security audit (website vulnerability scanner) // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/security/security-audit-website (access date: 25/03/2022).

14. Web Application Firewall // Website of the "Imperva Secure Sphere Web Application Firewall" product. URL: https://www.imperva.com/products/web-application-firewall-waf/ (access date: 26/03/2022).

15. SolidWall WAF // Website of the "SolidWall WAF" product. URL: https://solidwall.ru/ (access date: 09/05/2022).

16. Intelligent firewall to protect Solid Wall web applications // Website of the "SolidWall WAF" product. URL: https://solidwall.ru/features.html#architecture (access date: 09/05/2022).

17. Intelligent firewall to protect Solid Wall web applications // Website of the operator of the

unified register of Russian programs for electronic computers and databases in the “Internet” information and telecommunication network. URL:
https://reestr.digital.gov.ru/reestr/309803/?sphrase_id=1372933 (access date: 04/05/2022).

18. Positive Technologies Application Firewall (PTAF) system for protecting applications from unauthorized access // Website of the operator of the unified register of Russian programs for electronic computers and databases in the “Internet” information and telecommunications network. URL: https://reestr.digital.gov.ru/reestr/441322/?sphrase_id=1267679 (access date: 30/03/2022).

19. Comparison of firewalls for protecting websites (Web Application Firewall – WAF) // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/compare/web-application-firewall-waf-2017 (access date: 25/03/2022).

20. Web Application Security // Web site of “Trend Micro Web Security” product. URL: https://www.trendmicro.com/ru_ru/business/products/user-protection/sps/web-security.html (access date: 05/05/2022).

21. Security for Windows Server // Web-сайт of “Kaspersky Security for Windows Server” product. URL: https://www.kaspersky.ru/small-to-medium-business-security/windows-server-security (access date: 30/03/2022).

22. Fault-tolerant protection for the most important business processes running on Windows servers // Web site of “Kaspersky Security for Windows Server” product. URL:
https://media.kaspersky.com/ru/business-security/Kaspersky_Security_for_Windows_Server_10.1_Datasheet_Ru_web.pdf (access date: 31/03/2022).

23. Kaspersky Endpoint Security for Linux // Web site of “Kaspersky Endpoint Security for Linux” product. URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-linux (access date: 30/03/2022).

24. Reliable protection for servers and workstations running Linux // Website of “Kaspersky Security for Windows Server” product. URL: https://media.kaspersky.com/en/business-security/Kaspersky_Endpoint_for_Linux_Datasheet_Ru_web.pdf (access date: 31/03/2022).

25. Documents on certification of information security tools and certification of informatization objects according to information security requirements // FSTEC website, state register of certified information security tools. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001- 01bi00 (access date: 04/05/2022).

26. Check link (URL) // Web site for online checking of a third-party web site for viruses. URL: https://vms.drweb.ru/online/ (access date: 30/03/2022).

27. Dr. Web Server Security Suite // Website of “Dr. Web Server Security Suite” product. URL: https://products.drweb.ru/fileserver/ (access date: 29/03/2022).

28. Extract from the list of information security tools certified by the FSB of Russia // Website of the FSB, a list of information security tools certified by the FSB of Russia. URL: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_28.03.2022.doc (access date: 11/04/2022).

29. Dr. Web Enterprise Security Suite // Website of “Dr.Web Server Security Suite” product. URL: https://products.drweb.ru/fileserver/unix/ (access date: 04/05/2022).

30. Intelligent traffic management of applications // Website of the “Local Traffic Manager” product. URL: https://www.f5.com/products/big-ip-services/local-traffic-manager (access date: 21/04/2022).

31. Big hole in BIG-IP. How a new vulnerability works in F5 company products // Hacker online edition. URL: https://xakep.ru/2020/08/12/f5-big-ip-rce/ (access date: 06/05/2022).

32. Technical documentation // Website of the “Elastic Load Balance” service. URL: https://sbercloud.ru/ru/products/elastic-load-balance#tehnicheskaya-dokumentatsiya (access date: 22/04/2022).

33. Yandex Network Load Balancer // Website of the “Yandex Network Load Balancer” service. URL: https://cloud.yandex.ru/services/network-load-balancer (access date: 22/04/2022).

34. Fault-tolerant load balancer // Website of the Fault-tolerant load balancer service. URL: https://selectel.ru/lab/general-load-balancer/ (access date: 09/05/2022).

35. Comprehensive DDoS protection // Website of the “Cloudflare DDoS protection” product. URL: https://www.cloudflare.com/ddos/ (access date: 22/04/2022).

36. Service for monitoring traffic and protection against DDoS attacks // Website of the “Service for monitoring traffic and protection against DDoS attacks”. URL: https://rt-solar.ru/services/anti-ddos/ (access date: 22/03/2022).

37. Metasploit // Website of the “Metasploit” product. URL:
https://www.rapid7.com/products/metasploit/ (access date: 11/03/2022).

38. Scanner-VS security analysis // Web-site of the Scanner-VS product. URL:

https://scanner-vs.ru/ (access date: 07/05/2022).

39. Description // Web-site of the Scanner-VS product. URL: https://scanner-vs.ru/about/ (access date: 05/05/2022).

40. Scanner-VS security analysis tool // Website of the operator of the unified register of Russian programs for electronic computers and databases in the Internet information and telecommunication network. URL: https://reestr.digital.gov.ru/reestr/301522/?sphrase_id=1426619 (access date: 05/05/2022).

41. Capabilities // Web-site of the Scanner-VS product. URL: https://scanner-vs.ru/capabilities/ (access date: 02/05/2022).

42. XSpider // Website of the "XSpider" product. URL: https://www.ptsecurity.com/en-us/products/xspider/ (access date: 05/05/2022).

43. Vulnerability scanners: an overview of the world and Russian markets // Anti-Malware.ru Internet edition. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Vulnerability-scanners-global-and-Russian-markets (access date: 25/03/2022).

44. XSpider // Website of the operator of the unified register of Russian programs for electronic computers and databases in the "Internet" information and telecommunications network. URL: https://reestr.digital.gov.ru/reestr/464566/?sphrase_id=1432114 (access date: 05/05/2022).

45. MaxPatrol 8 // Website "MaxPatrol 8" product. URL: https://www.ptsecurity.com/en-us/products/mp8/ (access date: 03/05/2022).

46. MaxPatrol // Website of the operator of the unified register of Russian programs for electronic computers and databases in the "Internet" information and telecommunications network. URL: https://reestr.digital.gov.ru/reestr/469631/?sphrase_id=1432197 (access date: 05/05/2022).

Авторы заявляют об отсутствии конфликта интересов.

The authors declare no conflicts of interests.

Статья поступила в редакцию 10.05.2022; одобрена после рецензирования 10.06.2022; принята к публикации 11.06.2022.

The article was submitted 10.05.2022; approved after reviewing 10.06.2022; accepted for publication 11.06.2022.