УДК 004.056
https://doi.org/10.47533/2020.1606-146X.151

Б. С. АХМЕТОВ[1]*, В. А. ЛАХНО[2]

[1]Казахский национальный педагогический университет имени Абая, г. Алматы, Казахстан
[2]Национальнай университет биоресурсов и природопользования, г. Киев, Украина

ИСПОЛЬЗОВАНИЕ WAF ДЛЯ ЗАЩИТЫ ВНУТРЕННИХ СЕРВИСОВ УНИВЕРСИТЕТА В СТРУКТУРЕ ZERO TRUST

В статье изложены результаты пилотного исследования по использованию брандмауэра веб-приложений (Web Application Firewall или WAF) для защиты внутренних сервисов информационной образовательной среды университета (ИОСУ). Показано, что данная задача чрезвычайно важна в условиях глобализации образования. Использование WAF выполнено в структуре Zero Trust. Система тестировалась в два этапа. Во-первых, были использованы инструменты для автоматизации поиска веб-уязвимостей (сканеры веб-уязвимостей) ИОСУ. На втором этапе проводилось ручное тестирование приложений на уязвимости SQL-инъекций, межсайтового скриптинга и атак Path Traversal. Показано, что полученные результаты позволяют улучшить защиту сервисов в локальных сетях университета, что важно для достижения конечной цели – эффективная защита конечных пользователей и сервисов ИОСУ в условиях глобализации образования. Установлено, что использование WAF в системах с нулевым доверием – довольно распространенный вариант защиты сервисов внутри организаций, в том числе учебных. Показано, что использование открытых решений WAF в структуре Zero Trust позволяет более гибко и персонально подстраивать защиту под соответствующие нужды университетских сервисов.

***Ключевые слова**: web сервисы университета, информационная безопасность, брандмауэры, OWASP, WAF.*

Введение. В условиях продолжающейся пандемии, вызванной коронавирусом Covid-19, одним из важнейших направлений информатизации образования, в том числе в университетах Республики Казахстан (РК), стала организация учебного процесса, основанная на широком применении различных Интернет-сервисов. Например, к таким сервисам можно отнести: блоги и микроблоги; социальные сети; вики; медиа хранилища; поисковые системы и др. [1].

В условиях интенсивного развития систем дистанционного обучения (СДО) сформировались исключительно высокие требования к IT-инфраструктуре и компьютерным сетям университетов. Это, в свою очередь, вынуждает ИТ специалистов университетов усложнять эти инфраструктуры. Чем сложнее ИТ структура университетской сети и количество входящих в нее звеньев, тем выше вероятность появления уязвимых мест. На фоне роста популярности веб-приложений, используемых в процессе обучения [1-3], растет и необходимость их защиты от взлома и несанкционированного доступа (НСД). Это обусловлено тем, что более 75% хакерских атак направлены на уязвимости веб-приложений и сайтов. Последствия подобных злонамеренных действий достаточно очевидны и не очень приятны для компаний и организаций. Следствием такого доступа могут стать – потеря личных данных, включая платежную информа-

* E-mail корреспондирующего автора: bakhytzhan.akhmetov.54@mail.ru

цию, возможность получения доступа к коммерческой тайне и конфиденциальным документам. Кроме того, уязвимости веб-приложений могут стать точкой входа злоумышленников в корпоративную сеть университета.

Классические общепринятые методы сетевой защиты не предотвращают атаки на веб-сервисы. Межсетевые экраны ориентированы на угрозы сетевого и транспортного уровней, в то время как веб-приложения работают на прикладном уровне.

Брандмауэр веб-приложений (Web Application Firewall) – тип брандмауэра, который применяется для защиты веб-приложений. В то время как прямой прокси-сервер защищает идентификацию клиентского компьютера с помощью посредника, WAF (web application firewall) развертывается перед веб-приложениями (в режиме обратного прокси-сервера) и анализирует двунаправленный трафик HTTP/HTTPS, обнаруживая вредоносный трафик и блокируя его. WAF не является окончательным решением безопасности организации, например, университета. Скорее, WAF предназначены для использования в сочетании с другими решениями безопасности периметра сети, такими как брандмауэры нового поколения (NGFW) и системами предотвращения вторжений (IPS) [4-9].

Таким образом, на основании вышеизложенного, актуальность темы обеспечения кибербезопасности информационно-образовательной среды университета (ИОСУ) обуславливается массовым переходом учебных заведений РК на дистанционные форматы обучения, что, в частности, вызвано пандемией коронавируса Covid-19.

Основной материал статьи. Сегодня множество преподавателей и студентов университетов пользуются веб-приложениями для поиска необходимой информации. Преподаватели и студенты (или клиенты Интернет-сервисов) предоставляют свои имена (а также, например, данные платежных систем и иную информацию), которые могут стать золотой жилой для хакеров, стремящихся завладеть конфиденциальной информацией. При этом защита сайта университета – это также вопрос защиты физического оборудования. Хакеры могут не только украсть конфиденциальную клиентскую информацию, но и заразить университетский сайт вредоносным ПО. Это, в свою очередь, может повлиять на физическое оборудование.

В большинстве случаев СДО представляют собой распределенные приложения, строящиеся на базе информационной системы (ИС) университетов. Такие распределенные приложения широко задействуют web-ресурсы в процессах интерактивного взаимодействия учащихся и научно-педагогических работников университетов. В процессе своего функционирования данная система подвергается ряду негативных влияний случайного и преднамеренного характера, что в результате может привести к нарушению информационной (ИБ) и кибернетической безопасности (КБ) не только СДО, но и всей ИС учебного заведения, а также нанести вред всем участникам учебного процесса. Соответственно, для уменьшения негативного воздействия и предотвращения рисков ИБ необходимо задействовать специализированные средства и механизмы защиты.

Брандмауэр веб-приложений (Web Application Firewall или сокращённо WAF) – это устройство, которое защищает веб-приложения от большинства существующих на сегодняшний день атак (в том числе от OWASP Top Ten).

WAF находится между внешними пользователями и веб-приложениями и анализирует весь HTTP/HTTPS-трафик, выявляя и блокируя вредоносные запросы до того, как они смогут повлиять на пользователей или на веб-приложение. В результате WAF защищают критически важные для бизнеса веб-приложения и веб-серверы от атак, см. рис. 1.

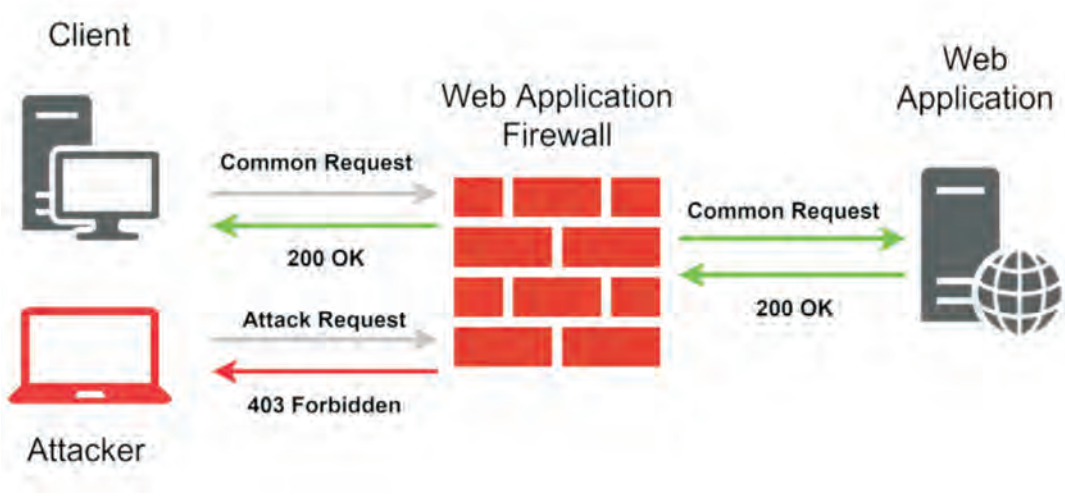

Рисунок 1 – Схема работы WAF

WAF работает на основе набора правил. Эти правила называют политиками, которые используются для фильтрации большинства известных на сегодняшний день атак. Многие службы WAF предоставляют набор правил по умолчанию. Данный список периодически обновляется.

WAF могут работать по модели отрицательной безопасности (черный список), положительной безопасности (белый список) или по гибридной модели.

На втором этапе проводилось ручное тестирование приложений на уязвимости SQL-инъекции, межсайтового скриптинга, атаки Path Traversal. При попытке провести атаку приложения, защищенного межсетевым экраном, были получены ответы «403 Forbidden», что свидетельствует о невозможности проведения атак. Для фиксации атак на веб-сервер ModSecurity использовались два типа журналов: журнал ошибок (error.log) и журнал аудита modsec_audit.log. Журнал ошибок создается при обнаружении ошибки или при попытке реализовать атаку. Поскольку ModSecurity работает в паре с Apache, все журналы ошибок (журналы ошибок Apache+журналы ошибок ModSecurity) создаются в одном файле. Журнал аудита начинает заполняться после фиксации события в журнале ошибок. В журнале аудита записывается более подробная информация о заблокированной атаке. Журналы аудита ModSecurity создаются в соответствии с уникальными идентификаторами журнала ошибок.

В качестве тест-сервера был выбран WAMP-сервер с установленным Wordpress и настроенной стандартной страницей. Для доступа используется IP-адрес 192.168.1.44 без WAF, и 192.168.1.251 – через WAF, см. рис 2.

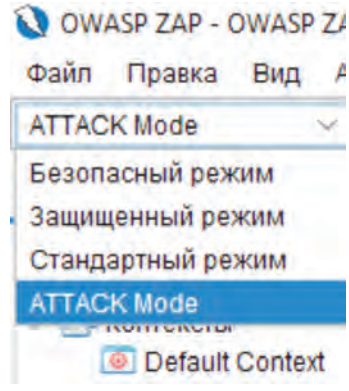

Рисунок 2 – Выбор режима сканирования

После завершения сканирования на вкладке «Уведомления», см. рис. 3, можно просмотреть результаты. Уведомления представлены 5 типами предупреждений, серьезность которых отображается определенным цветом флажка.

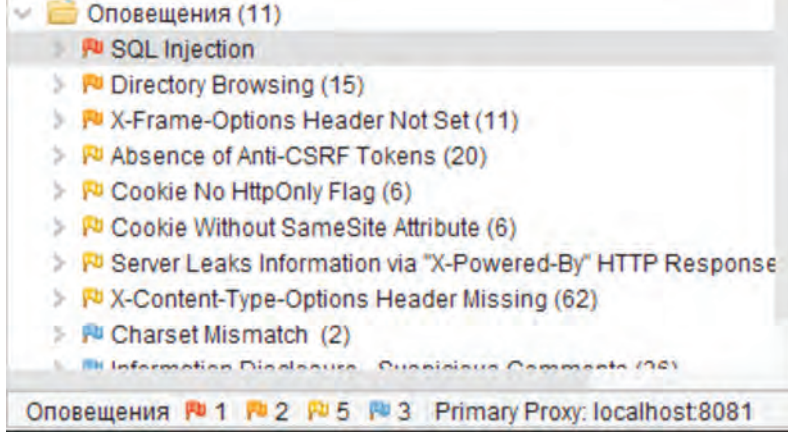

Рисунок 3 – Тестирование веб-страницы, которая не защищена WAF

В процессе исследования функции брандмауэра были возложены на программу ModSecurity. Для установки брандмауэра веб-приложений ModSecurity была выполнена установка веб-сервера Apache и произведена его настройка для дальнейшей работы в режиме обратного прокси-сервера.

Для блокировки атак на веб-сервер была загружена самая новая на данный момент версия правил OWASP CRS, загруженная с GitHub.

Для защиты от атак типа "отказ в обслуживании", "распределенный отказ в обслуживании" (DoS, DdoS) и bruteforce атак был установлен модуль mod_evasive. Основные настройки данного модуля находятся в файле /etc/apache2/mods-enabled/evasive.conf.

На рисунке 4 показаны настройки параметров сканирования.

Сканер смог найти только информацию о версии операционной системы, Apache и PHP, см. рис. 5.

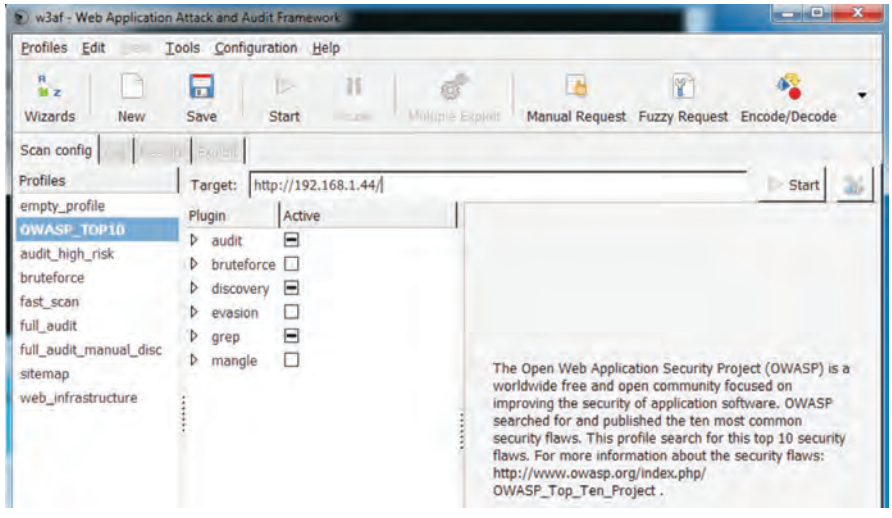

Рисунок 4 – Настройка параметров сканера

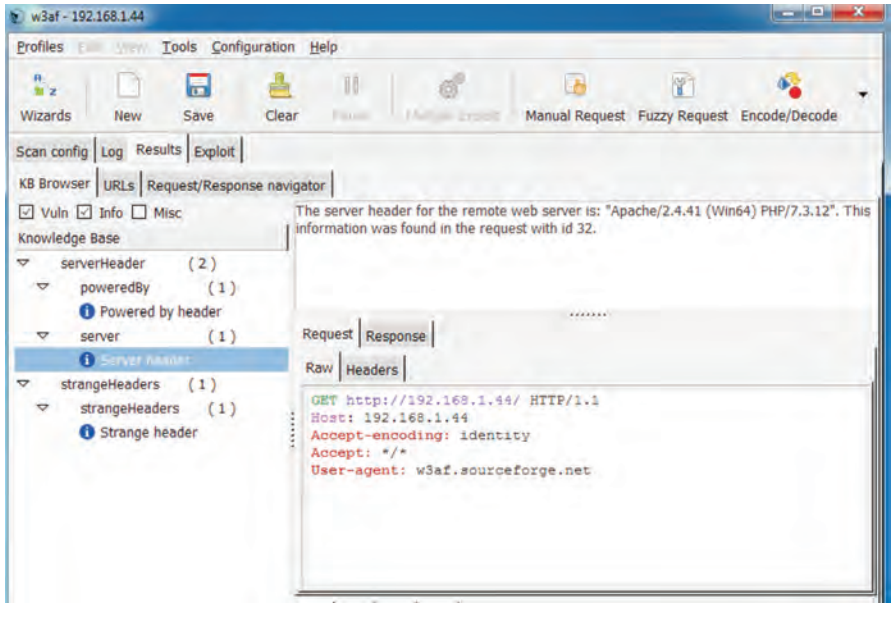

Рисунок 5 – Результаты сканирования без WAF

Сканирование через WAF закончилось быстрее, чем через без WAF. В результате сканер смог найти одну страницу с ошибкой веб-сервера Apache, см. рис. 6.

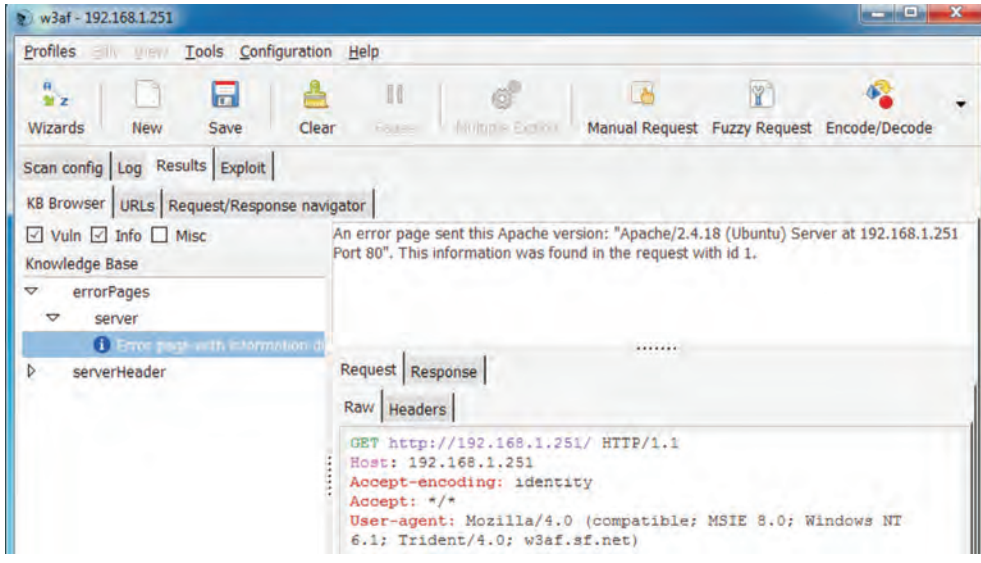

Рисунок 6 – Результаты сканирования через WAF

Традиционные сетевые брандмауэры защищают локальные сети от НСД. Их основная цель – отделить защищенную зону от менее безопасной и контролировать связь между ними. Ключевое техническое различие между брандмауэром уровня приложений и брандмауэрами сетевого уровня – это уровень, на котором они работают. Последнее определено моделью взаимодействия открытых систем, которая характеризует и стандартизирует функции связи в телекоммуникационных и вычислительных системах. WAF защищает от атак на седьмом уровне модели OSI – уровни приложений. Основными угрозами этого уровня являются атаки на разного рода фреймворки, манипуляция с файлами cookie, эксплуатация SQL-инъекций, атаки с использованием межсайтовых сценариев. Традиционные сетевые брандмауэры работают на уровнях 3 и 4 модели OSI, защищая сетевой трафик. По этой причине, традиционный сетевой брандмауэр сам по себе не защитит университетскую сеть от атак на веб-страницы.

Выводы. Проведено пилотное исследование по использованию WAF для защиты внутренних сервисов кибербезопасности ИОСУ в условиях глобализации образования. Использование WAF выполнено в структуре Zero Trust. Система тестировалась в два этапа. Во-первых, мы использовали инструменты для автоматизации поиска веб-уязвимостей (сканеры веб-уязвимостей) ИОСУ. На втором этапе проводилось ручное тестирование приложений на уязвимости SQL-инъекций, межсайтового скриптинга и атак Path Traversal. Показано, что полученные результаты позволяют улучшить защиту сервисов в локальных сетях университета. Проведенное исследование важно для достижения конечной цели – разработка методологии обеспечения кибербезопасности ИОСУ в условиях глобализации образования и эффективной защиты конечных пользователей и сервисов.

Установлено, что использование WAF в системах с нулевым доверием – довольно распространенный вариант защиты сервисов внутри организации. Но использование

открытых решений позволяет более гибко и персонально подстраивать защиту под соответствующие нужды университета.

Благодарности. Исследование финансируется Казахским национальным педагогическим университетом имени Абая (договор № ППС-ДН-01 от 12.02.2020).

ЛИТЕРАТУРА

1 Моглан Д.В. Образовательное сетевое сообщество как одна из эффективных форм активизации учебно-познавательной деятельности студентов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Серия «Гуманитарные и общественные науки». 2014. № 4 (208). С. 183–191.

2 Иванченко Д.А. Роль Интернет-пространства в формировании образовательной информационной среды // Дистанционное и виртуальное обучение. 2011. № 2. С. 19–31.

3 Поначугин А.В. Выбор веб-сервиса для проведения потоковых лекций у студентов инженерных специальностей // Вестник Минского университета. 2021. Т. 9, №3. С.7.

4 Appelt, Dennis, et al. A machine-learning-driven evolutionary approach for testing web application firewalls. IEEE Transactions on Reliability, 2018, 67.3: 733-757.

5 Appelt, Dennis, et al. Automated testing for SQL injection vulnerabilities: an input mutation approach. In: Proceedings of the 2014 International Symposium on Software Testing and Analysis. 2014. p. 259–269.

6 Demertzis, Konstantinos; Iliadis, Lazaros. Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks. Journal of Computations & Modelling, 2019, 9.2: 1–26.

7 Garbis, Jason; Chapman, Jerry W. Zero Trust Architectures. In: Zero Trust Security. Apress, Berkeley, CA, 2021. p. 19–51.

8 Jingyao, Sun, et al. Securing a Network: How Effective Using Firewalls and VPNs Are?. In: Future of Information and Communication Conference. Springer, Cham, 2019. p. 1050–1068.

9 Macdonald, Neil; ORANS, Lawrence; SKORUPA, Joe. The Future of Network Security Is in the Cloud. Gartner. Viitattu, 2019, 1: 2021.

REFERENCES

1 Moglan D.V. Obrazovatelnoye setevoye soobshchestvo kak odna iz effektivnykh form aktivizatsii uchebno-poznavatelnoy deyatelnosti studentov // Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Seriya «Gumanitarnyye i obshchestvennyye nauki». 2014. № 4 (208). S. 183–191.

2 Ivanchenko D.A. Rol Internet-prostranstva v formirovanii obrazovatelnoy informatsionnoy sredy // Distantsionnoye i virtualnoye obucheniye. 2011. № 2. S. 19–31.

3 Ponachugin A.V. Vybor veb-servisa dlya provedeniya potokovykh lektsiy u studentov inzhenernykh spetsialnostey // Vestnik Minskogo universiteta. 2021. T. 9. №3. S.7.

4 Appelt. Dennis. et al. A machine-learning-driven evolutionary approach for testing web application firewalls. IEEE Transactions on Reliability. 2018. 67.3: 733-757.

5 Appelt. Dennis. et al. Automated testing for SQL injection vulnerabilities: an input mutation approach. In: Proceedings of the 2014 International Symposium on Software Testing and Analysis. 2014. p. 259–269.

6 Demertzis. Konstantinos; Iliadis. Lazaros. Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks. Journal of Computations & Modelling. 2019. 9.2: 1–26.

7 Garbis. Jason; Chapman. Jerry W. Zero Trust Architectures. In: Zero Trust Security. Apress. Berkeley. CA. 2021. p. 19–51.

8 Jingyao. Sun. et al. Securing a Network: How Effective Using Firewalls and VPNs Are?. In: Future of Information and Communication Conference. Springer. Cham. 2019. p. 1050–1068.

9 Macdonald. Neil; ORANS. Lawrence; SKORUPA. Joe. The Future of Network Security Is in the Cloud. Gartner. Viitattu. 2019. 1: 2021.

Б. С. АХМЕТОВ[1]*, В. А. ЛАХНО [2]

[1]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы, Қазақстан
[2]Украинаның Ұлттық биоресурстар және табиғатты пайдалану университеті, Киев, Украина

ZERO TRUST ҚҰРЫЛЫМЫНДА УНИВЕРСИТЕТТІҢ ІШКІ ҚЫЗМЕТТЕРІН ҚОРҒАУ ҮШІН WAF ПАЙДАЛАНУ

Мақалада университеттің ақпараттық білім беру ортасының (УАББО) ішкі қызметтерін қорғау үшін веб-қосымшалардың (Web Application Firewall немесе WAF) брандмауэрін пайдалану бойынша пилоттық зерттеу нәтижелері көрсетілген. Бұл міндет білім берудің жаңдануы жағдайында өте маңызды екендігі көрсетілген. WAF қолдану Zero Trust құрылымында жүзеге асырылады. Жүйе екі кезеңде тестіленді. Біріншіден, УАББО веб-осалдықтарды іздеуді автоматтандыру үшін құралдар қолданылды (веб-осалдықтарды тексерушілер). Екінші кезеңде SQL-инъекцияларының, сайтаралық скриптингтің және Path Traversal шабуылдарының осалдығына қосымшаларды қолмен тестілеу жүргізілді. Алынған нәтижелер университеттің жергілікті желілерінде сервистерді қорғауды жақсартуға мүмкіндік беретіні көрсетілген, оның түпкі мақсаты – білім берудің жаңдануы жағдайында түпкі пайдаланушылар мен УАББО сервистерін тиімді қорғауға қол жеткізу. Нөлдік сенім жүйелерінде WAF қолдану көптеген ұйымдар, соның ішінде білім беру ұйымдары ішіндегі қызметтерді қорғаудың кең таралған нұсқасы екендігі анықталды. Zero Trust құрылымында ашық WAF шешімдерін пайдалану қорғауды университет қызметтерінің тиісті қажеттіліктеріне икемді және жеке реттеуге мүмкіндік беретіні көрсетілген.

Түйін сөздер*: университеттің web қызметтері, ақпараттық қауіпсіздік, брандмауэр, OWASP, WAF.*

B. S. AKHMETOV[1*], V. A. LAKHNO[2]

[1]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
[2] National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine

USING WAF TO PROTECT THE UNIVERSITY'S INTERNAL SERVICES IN THE ZERO TRUST STRUCTURE

The article presents the results of a pilot study on the use of a Web Application Firewall (Web Application Firewall or WAF) to protect the internal services of the information educational environment of the university (IEEU). It is shown that this task is extremely important in the context of globalization

of education. The use of WAF is performed in the Zero Trust structure. The system was tested in two stages. Firstly, tools were used to automate the search for web vulnerabilities (web vulnerability scanners) IEEU. At the second stage, manual testing of applications for vulnerabilities of SQL injection, cross-site scripting and Path Traversal attacks was carried out. It is shown that the results obtained make it possible to improve the protection of services in the university's local networks, which is important for achieving the ultimate goal - effective protection of end users and IEEU services in the context of globalization of education. It has been established that the use of WAF in systems with zero trust is a fairly common option for protecting services within organizations, including educational ones. It is shown that the use of open WAF solutions in the Zero Trust structure allows you to more flexibly and personally adjust protection to the appropriate needs of university services.

***Keywords**: university web services, information security, firewalls, OWASP, WAF.*