УДК 004.056 Вестник УрФО № 2(56) / 2025, с. 65–73

**Частикова В. А., Алиев М. К.,
Тесленко А. А., Игнатенко И. С.**

DOI: 10.14529/secur250207

НЕЙРОННЫЕ СЕТИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Данная работа посвящена применению машинного обучения для повышения безопасности веб-приложений. Рассмотрены ограничения традиционных методов защиты, таких как файрволы веб-приложений (WAF), непрерывный мониторинг с использованием SIEM систем и тестирование на проникновение. Были проанализированы принципы работы нейронных сетей, их классификация и потенциал их применения для автоматизации анализа трафика, выявления аномалий и защиты от уязвимостей нулевого дня. Описаны преимущества и недостатки нейронных сетей, обоснована их интеграция с существующими инструментами и проведён сравнительный анализ современных WAF с машинным обучением.

Ключевые слова: *безопасность веб-приложений, нейронные сети, файрвол веб-приложений, система безопасности информации и управления событиями, киберугрозы, непрерывный мониторинг*

Chastikova V. A., Aliev M. K., Teslenko A. A. Ignatenko I. S.

NEURAL NETWORKS FOR WEB APPLICATION SECURITY

The publication focuses on the application of machine learning to enhance the security of web applications. It examines the limitations of traditional protection methods, such as web application firewalls (WAF), continuous monitoring using SIEM systems, and penetration testing. The principles of neural networks, their classification, and their potential for automating traffic analysis, detecting anomalies, and protecting against zero-day vulnerabilities have been analyzed. The advantages and disadvantages of neural networks are described, their integration with existing tools is justified, and a comparative analysis of modern WAFs with machine learning is conducted.

Keywords: *web application security, neural networks, Web Application Firewall (WAF), SIEM systems, cyber threats, continuous monitoring*

Введение

Цифровые технологии развиваются со стремительной скоростью, из-за чего вопрос обеспечения безопасности веб-приложений становится с каждым днем все более актуальным. Веб-приложения стали неотъемлемой частью нашего быта, охватывая огромное множество аспектов нашей жизни. Это делает их крайне привлекательной целью для киберпреступников. Рост числа и сложности кибератак на веб-приложения подчеркивает необходимость поиска все более эффективных решений для их защиты. Современные угрозы требуют современных подходов, способных противостоять как уже известным, так и совершенно новым неизведанным видам атак.

В данной статье комплексно рассмотрен вопрос применения нейронных сетей для обеспечения безопасности веб-приложений. Проанализированы ограничения традиционных методов защиты, описаны принципы работы нейронных сетей, рассмотрены их возможности и вызовы в контексте повышения надежности защиты, а также проведен сравнительный анализ ряда современных WAF от разных производителей.

Традиционные методы защиты и их ограничения

Традиционные методы защиты веб-приложений, такие как использование файрволов веб-приложений (WAF) на основе правил и сигнатур, непрерывный мониторинг трафика и поведения системы с использованием систем безопасности информации и управления событиями (SIEM), а также тестирование на проникновение долгое время составляли основу обеспечения безопасности. Однако их эффективность ограничена рядом факторов.

Традиционные WAF представляют собой инструменты, предназначенные для анализа HTTP/HTTPS-трафика и блокировки запросов на основе заранее заданных правил или сигнатур. Сигнатуры представляют собой характерные признаки уже известной вредоносной активности. Правила могут включать в себя черные списки, содержащие известные сигнатуры атак, а также белые списки, определяющие допустимые запросы [1, 2].

Однако, несмотря на свою эффективность, такой подход имеет ряд недостатков. Традиционный WAF, основанный на правилах и сигнатурах атак, не способен выявлять атаки, использующие неизвестные доселе уязвимости, именуемые «уязвимостями нулевого дня». Кроме того, WAF требует регулярной настройки и обновления правил и баз сигнатур атак, что увеличивает затраты времени и ресурсов. Дополнительной проблемой является большое количество ложных срабатываний, которые возникают при попытке охватить в правилах широкий спектр угроз.

Непрерывный мониторинг представляет собой процесс постоянного наблюдения за состоянием веб-приложения и анализа входящего трафика, осуществляемый центром мониторинга информационной безопасности (SOC). Этот метод позволяет своевременно выявлять подозрительную активность и реагировать на инциденты [3–5].

Главным недостатком данного подхода является то, что его реализация сопряжена с высокими затратами человеческих ресурсов, поскольку требует привлечения специалистов для обработки логов, настройки фильтров и анализа данных. Даже при интеграции с SIEM системами, которые автоматизируют сбор и корреляцию событий, значительная часть работы остается ручной, что снижает скорость реагирования на новые угрозы.

Тестирование на проникновение, или пентестинг, заключается в имитации атак на веб-приложение с целью выявления уязвимостей до их непосредственной эксплуатации злоумышленниками. Этот метод позволяет оценить уровень безопасности системы и разработать меры по устранению слабых мест [6].

Данный подход имеет ряд ограничений. Тестирование проводится разово или с определенной периодичностью, что не обеспечивает защиты в реальном времени. Кроме того, эффективность метода напрямую зависит от квалификации специалистов и используемых инструментов, а выявленные уязвимости требуют дополнительных ресурсов для их исправления, что замедляет процесс реагирования на нововыявленные угрозы.

Ниже представлена сравнительная таблица рассмотренных выше традиционных методов защиты веб-приложений по ряду критериев.

Таблица 1

Традиционные методы защиты и их ограничения

Критерий	WAF	Непрерывный мониторинг	Пентестинг
Скорость реагирования на новые угрозы	Высокая	Низкая	Низкая
Адаптация к изменяющимся угрозам	Низкая	Средняя	Низкая
Степень потребности в ручной настройке	Высокая	Высокая	Высокая
Точность выявления неизвестных угроз	Низкая	Средняя	Низкая

Нейронные сети: базовые принципы

Традиционные методы защиты не обладают достаточной гибкостью и не способны адаптироваться к быстро меняющимся условиям. В связи с этим технологии машинного обучения, в частности нейронные сети, становятся перспективным инструментом для повышения уровня безопасности веб-приложений.

Нейронные сети различаются по архитектуре и применимости к задачам безопасности веб-приложений. Многослойные перцептроны (MLP) используются для классификации запросов, например, для выявления потенциальных угроз, таких как SQL-инъекции или межсайтовый скриптинг. Сверточные нейронные сети (CNN) эффективны для анализа структурированных данных, таких как сетевые пакеты, помогая обнаруживать аномалии, указывающие на вторжения. Рекуррентные нейронные сети (RNN), особенно сети с долгой краткосрочной памятью (LSTM), обрабатывают последовательности событий, выявляя сложные атаки, такие как попытки захвата учетной записи, учитывая временные зависимости в поведении пользователей или паттернах запросов [7].

Если сеть содержит множество скрытых слоев, ее называют глубокой нейронной сетью (DNN). Глубокими могут быть любые из трех вышеперечисленных типов (MLP, CNN или RNN). Глубокие нейросети хорошо справляются с более сложными задачами, такими как прогнозирование неизвестных угроз на основе исторических данных [8].

Основное преимущество нейронных сетей заключается в их способности обрабатывать сложные и неструктурированные данные, такие как сетевой трафик, логи или последовательности пользовательских действий. Это позволяет им выявлять скрытые закономерности, что недоступно традиционным методам, основанным на статических правилах и сигнатурах. Кроме того, нейронные сети способны масштабироваться для анализа больших объемов информации, что делает их эффективным инструментом для обеспечения безопасности в условиях динамичных и разнообразных киберугроз.

Применение нейросетей в безопасности веб-приложений

Нейронные сети находят применение в различных аспектах обеспечения безопасности веб-приложений, позволяя преодолевать ограничения традиционных методов. Их способность анализировать большие объемы данных и выявлять скрытые закономерности делает возможным автоматизацию процессов, которые ранее требовали значительных ресурсов или были попросту невозможны.

Традиционные WAF основаны на использовании статических правил и сигнатур угроз, что приводит к необходимости их регулярной актуализации. Применение методов машинного обучения способно улучшить работу WAF путем автоматического формирования и адаптации правил на основе анализа трафика. Например, нейронные сети могут обучаться на примерах вредоносных запросов, таких как попытки SQL-инъекций, и отличать их от легитимных без заранее заданных сигнатур. Это снижает количество ложных срабатываний и повышает точность фильтрации. Кроме того, такая автоматизация уменьшает потребность в ручной настройке, что сокращает затраты времени и ресурсов [9].

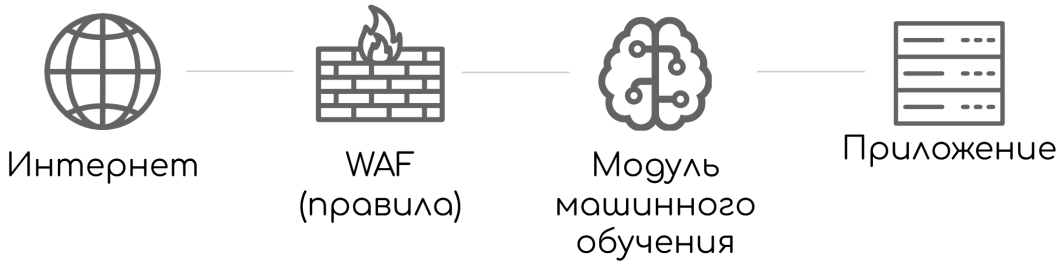

Рис. 1. Схема работы WAF с применением нейросетей

Помимо совершенствования WAF, нейронные сети открывают новые возможности и для оптимизации непрерывного мониторинга. Непрерывный мониторинг, реализуемый через центры мониторинга информационной безопасности (SOC) с использованием SIEM систем, традиционно требует значительных усилий специалистов для анализа логов и поведения пользователей. Интеграция машинного обучения, включая нейронные сети, в SIEM позволяет автоматизировать анализ больших объемов данных. Например, нейронные сети могут выявлять аномалии, указывающие на сложные атаки, такие как попытки эксплуатации бизнес-логики или несанкционированный доступ, обнаруживая скрытые паттерны в трафике. Это снижает нагрузку на команду SOC, ускоряет обнаружение инцидентов и повышает точность реагирования [10].

Преимущества и недостатки использования нейросетей

Использование нейронных сетей в обеспечении безопасности веб-приложений связано как с очевидными преимуществами, так и с определенными недостатками. Эти аспекты определяют их потенциал и ограничения в сравнении с традиционными методами защиты.

Основным преимуществом нейронных сетей является автоматизация процессов. Они способны самостоятельно анализировать данные и принимать решения, что снижает потребность в ручной настройке и участии специалистов. Например, автоматическое обновление правил WAF или обработка логов сокращают затраты времени и ресурсов.

Вторым важным достоинством выступает адаптивность. Нейронные сети обучаются на новых данных, что позволяет им реагировать на ранее неизвестные угрозы, такие как уязвимости нулевого дня, в отличие от статических методов, ограниченных заранее заданными правилами.

Кроме того, высокая скорость обработки больших объемов информации обеспечивает оперативное обнаружение аномалий, что критично для защиты от атак в реальном времени.

Однако применение нейронных сетей сопряжено с рядом вызовов. Во-первых, для их эффективной работы требуется значительный объем данных для обучения. Недостаток качественных данных может снизить точность анализа и привести к ошибкам в обнаружении угроз.

Во-вторых, настройка и оптимизация нейронных сетей представляют собой сложный процесс, требующий специализированных знаний и вычислительных ресурсов. Это увеличивает затраты на внедрение по сравнению с традиционными инструментами.

Наконец, нейронные сети часто функционируют как «черный ящик»: их решения трудно интерпретировать, что затрудняет анализ причин срабатывания и устранение ложных срабатываний.

Сравнительный анализ WAF с применением машинного обучения

Для оценки практической применимости нейронных сетей в области обеспечения безопасности веб-приложений был проведен сравнительный анализ существующих решений WAF, использующих машинное обучение. Сравнение проводилось по следующим критериям: качество безопасности (True Positive Rate), качество обнаружения (False Positive Rate) и сбалансированная оценка.

Качество безопасности (TPR) рассчитывалось по формуле (1).

$$TPR = \frac{TP}{P} = \frac{TP}{TP+FN} = 1 - FNR, \quad (1)$$

где

а) FNR – доля пропущенных атак (FN/P)

б) TP – правильно обнаруженные атаки

в) P – общее количество реальных атак ($TP+FN$)

г) FN – пропущенные атаки

Качество обнаружения (TNR) рассчитывалось по формуле (2).

$$TNR = \frac{TN}{N} = \frac{TN}{TN+FP} = 1 - FPR, \quad (2)$$

где

а) FPR – доля ложных срабатываний (FP/N)

б) TN – правильно пропущенные легитимные запросы

в) N – общее количество безопасных запросов ($TN+FP$)

г) FP – ложные срабатывания

Сбалансированная оценка (BA) рассчитывалось по формуле (3).

$$BA = \frac{TPR+TNR}{2}, \quad (3)$$

где

а) TNR – качество обнаружения

б) TPR – качество безопасности

Анализ основан на открытых тестах OpenAppSec 2024, а также на документациях производителей и отзывах пользователей. Результаты представлены в таблице 2. [11]

Таблица 2

Сравнительный анализ WAF с применением машинного обучения

WAF Solution	Configuration	Security Quality (True Positive Rate)	Detection Quality (False Positive Rate)	Balanced Accuracy
Microsoft Azure WAF	OWASP CRS 3.2 ruleset	97.526%	54.242%	71.642%
AWS WAF	AWS managed ruleset	79.751%	5.8%	86.976%
AWS WAF	AWS managed ruleset and F5 Ruleset	80.372%	5.879%	87.246%
CloudFlare WAF	Managed and OWASP Core Rulesets	69.3%	0.062%	84.619%
F5 NGINX App Protect WAF	Default profile	77.9%	1.808%	88.046%
F5 NGINX App Protect WAF	Strict profile	97.849%	22.084%	86.882%
NGINX ModSecurity	OWASP CRS 4.3.0	92.028%	17.523%	87.253%
open-appsec / CloudGuard WAF	Default (High Confidence)	99.368%	1.436%	98.966%
open-appsec / CloudGuard WAF	Critical Confidence	99.087%	0.81%	99.139%
Imperva Cloud WAF	Default configuration	11.97%	0.009%	55.981%
F5 BIG-IP Advanced WAF	Rapid Deployment Policy configuration	78.89%	2.8%	88.045%
Fortinet FortiWeb	Default configuration	68.971%	20.925%	74.023%
Google Cloud Armor	Preconfigured ModSecurity rules (Sensitivity level 2)	83.537%	50.283%	66.627%

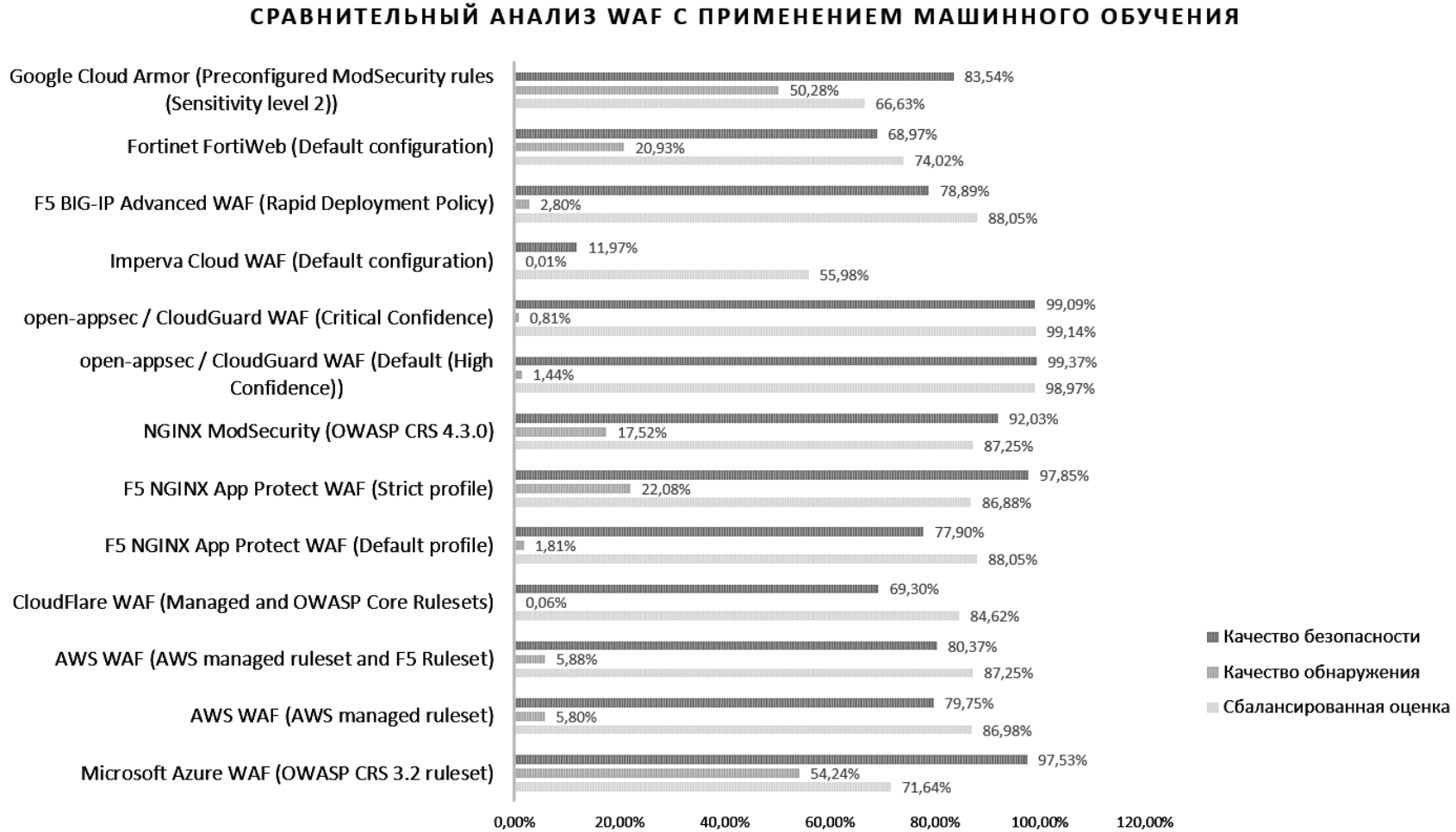

Рис. 2. Сравнительный анализ WAF с применением машинного обучения, гистограмма

На рис. 2 также представлена линейчатая гистограмма, наглядно представляющая данные анализа.

Из анализа видно, что решение openappsec CloudGuard WAF в конфигурации Default и Critical Confidence демонстрирует наивысшую сбалансированную оценку BA (примерно 99%), сочетая максимально высокий TPR (более 99%) с минимальным FPR (менее 1.5%). Это указывает на его способность надежно обнаруживать атаки при почти нулевых ложных срабатываниях, что делает его наиболее перспективным для практического применения.

Заключение

Нейронные сети представляют собой перспективное развитие традиционных подходов к обеспечению безопасности веб-приложений. Они устраняют ряд ограничений классических методов, таких как необходимость частой ручной настройки и неспособность противостоять неизвестным угрозам, за счет автоматизации, адаптивности и высокой скорости обработки данных. Их внедрение не исключает использования существующих инструментов -межсетевых экранов уровня приложения и непрерывного мониторинга, а дополняет их.

Перспективы дальнейшего применения нейронных сетей связаны с их интеграцией в текущие системы защиты. Комбинированный подход, сочетающий точность WAF и возможности анализа аномалий нейронными сетями, может повысить эффективность обнаружения и предотвращения атак. Аналогично, автоматизация мониторинга с использованием нейронных сетей способна снизить нагрузку на специалистов, сохраняя при этом высокую надежность защиты. Нейронные сети открывают новые возможности для повышения уровня безопасности веб-приложений в условиях растущей сложности киберугроз, однако использование их требует преодоления некоторых технических и организационных ограничений.

Литература

1. Solar MSS. WAF (Web Application Firewall): как устроен и где применяется. RT Solar, 2025. URL: https://rt-solar.ru/services/mss/blog/5367/ (дата обращения: 25.03.2025).

2. Yandex Cloud. Введение в WAF (Web Application Firewall). Yandex Cloud, 2025. URL: https://yandex.cloud/ru/docs/glossary/waf?utm_referrer=https%3A%2F%2Fyandex.ru%2F (дата обращения: 27.03.2025).

3. DigitalTatarstan. Security Operation Center (SOC) на пальцах: из чего состоит и кому нужен. Habr, 2023. URL: https://habr.com/ru/companies/digital_tatarstan/articles/775844/ (дата обращения: 23.03.2025).

4. SolarSecurity. Проблема непрерывной защиты веб-приложений. Взгляд со стороны исследователей и эксплуатантов. Habr, 2017. URL: https://habr.com/ru/companies/solarsecurity/articles/331786/ (дата обращения: 28.03.2025).

5. Avpavlov. Проблема непрерывной защиты веб-приложений. Взгляд со стороны исследователей и эксплуатантов. Часть 2. Habr, 2017. URL: https://habr.com/ru/companies/solarsecurity/articles/332846/ (дата обращения: 24.03.2025).

6. Al Shelbli H.M. A study on penetration testing process and tools // 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). Farmingdale, NY, USA, 2018. Pp. 1-5.

7. Розенко Ю. Что такое модели и архитектуры нейросетей. AdminVPS, 2025. URL: https://adminvps.ru/blog/chto-takoe-modeli-i-arhitektury-nejrosetej/ (дата обращения: 23.03.2025).

8. Boesch G. Глубокая нейронная сеть: 3 популярных типа (MLP, CNN и RNN). Viso.ai, 2021. URL: https://viso.ai/deep-learning/deep-neural-network-three-popular-types/ (дата обращения: 27.03.2025).

9. Elvin_GSNV. Как я создал межсетевой экран с помощью свёрточных нейронных сетей для веб-приложений с микросервисной архитектурой. Habr, 2022. URL: https://habr.com/ru/articles/677232/ (дата обращения: 25.03.2025).

10. Ptsecurity. Учимся на чужих ошибках: как прокачать SIEM с помощью machine learning. Habr, 2024. URL: https://habr.com/ru/companies/pt/articles/848986/ (дата обращения: 28.03.2025).

11. Rozenfeld B. Лучшие WAF решения в 2024-2025 годах: сравнение в реальных условиях. OpenAppSec, 2024. URL: https://www.openappsec.io/post/best-waf-solutions-in-2024-2025-real-world-comparison (дата обращения: 24.03.2025).

References

1. Solar MSS. WAF (Web Application Firewall): kak ustroen i gde primenyaetsya. RT Solar, 2025. URL: https://rt-solar.ru/services/mss/blog/5367/ (data obrashhenija: 25.03.2025).

2. Yandex Cloud. Vvedenie v WAF (Web Application Firewall). Yandex Cloud, 2025. URL: https://yandex.cloud/ru/docs/glossary/waf?utm_referrer=https%3A%2F%2Fyandex.ru%2F (data obrashhenija: 27.03.2025).

3. DigitalTatarstan. Security Operation Center (SOC) na pal'tsakh: iz chego sostoit i komu nuzhen. Habr, 2023. URL: https://habr.com/ru/companies/digital_tatarstan/articles/775844/ (data obrashhenija: 23.03.2025).

4. SolarSecurity. Problema nepreryvnoj zashhity veb-prilozhenij. Vzglyad so storony issledovatelej i ekspluatantov. Habr, 2017. URL: https://habr.com/ru/companies/solarsecurity/articles/331786/ (data obrashhenija: 28.03.2025).

5. Avpavlov. Problema nepreryvnoj zashhity veb-prilozhenij. Vzglyad so storony issledovatelej i ekspluatantov. Chast' 2. Habr, 2017. URL: https://habr.com/ru/companies/solarsecurity/articles/332846/ (data obrashhenija: 24.03.2025).

6. Al Shelbli H.M. A study on penetration testing process and tools. 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). Farmingdale, NY, USA, 2018. Pp. 1-5. DOI: 10.1109/LISAT.2018.8378035.

7. Rozenko Yu. Chto takoe modeli i arkhitektury nejrosetej. AdminVPS, 2025. URL: https://adminvps.ru/blog/chto-takoe-modeli-i-arhitektury-nejrosetej/ (data obrashhenija: 23.03.2025).

8. Boesch G. Deep Neural Network: The 3 Popular Types (MLP, CNN and RNN). Viso.ai, 2021. URL: https://viso.ai/deep-learning/deep-neural-network-three-popular-types/ (data obrashhenija: 27.03.2025).

9. Elvin_GSNV. Kak ya sozdal mezhsetevoj ekran s pomoshh'yu svyortochnykh nejronnykh setej dlya veb-prilozhenij s mikroservisnoj arkhitekturoj. Habr, 2022. URL: https://habr.com/ru/articles/677232/ (data obrashhenija: 25.03.2025).

10. Ptsecurity. Uchimsya na chuzhikh oshibkakh: kak prokachat' SIEM s pomoshh'yu machine learning. Habr, 2024. URL: https://habr.com/ru/companies/pt/articles/848986/ (data obrashhenija: 28.03.2025).

11. Rozenfeld B. Best WAF Solutions in 2024-2025: Real-World Comparison. OpenAppSec, 2024. URL: https://www.openappsec.io/post/best-waf-solutions-in-2024-2025-real-world-comparison (data obrashhenija: 24.03.2025).

ЧАСТИКОВА Вера Аркадьевна, кандидат технических наук, доцент, доцент кафедры кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: chastikova_va@mail.ru

ТЕСЛЕНКО Александр Александрович, студент кафедры кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: alextesl2018@mail.ru

АЛИЕВ Мунир Казбекович, студент кафедры кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: opennauka24@gmail.com

ИГНАТЕНКО Илья Сергеевич, студент кафедры кибербезопасности и защиты информации ФГБОУ ВО «Кубанский государственный технологический университет». 350000, г. Краснодар, ул. Красная, 135. E-mail: ilaignatenko1010@gmail.com

CHASTIKOVA Vera Arkadyevna, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cybersecurity and Information Protection of the Kuban State Technological University. 350000, Krasnodar, Krasnaya street, 135. E-mail: chastikova_va@mail.ru

TESLENKO Alexander Alexandrovich, student of the Department of Cybersecurity and Information Protection of the Kuban State Technological University. 350000, Krasnodar, Krasnaya street, 135. E-mail: alextesl2018@mail.ru

ALIEV Munir Kazbekovich, student of the Department of Cybersecurity and Information Protection of the Kuban State Technological University. 350000, Krasnodar, Krasnaya street, 135. E-mail: alextesl2018@mail.ru

IGNATENKO Ilya Sergeevich, student of the Department of Cybersecurity and Information Protection of the Kuban State Technological University. 350000, Krasnodar, Krasnaya street, 135. E-mail: ilaignatenko1010@gmail.com