УПРАВЛЕНИЕ СЛОЖНЫМИ СИСТЕМАМИ

DOI: 10.18137/RNU.V9187.25.01.P.27 УДК 004.9

Арсетмави Кассим Кадхим Джаббар
доцент, Университет Имама аль-Кадима, Ирак; аспирант кафедры интеллектуальной робототехники Института информационных технологий и интеллектуальных систем, Казанский (Приволжский) федеральный университет, город Казань.
Электронный адрес: aliraqeqassim@gmail.com
Arsetmavi Qassim Kadhim Jabbar
Associate Professor at Imam Al-Qadhim University, Iraq; Postgraduate of the Department of intelligent robotics of the Institute of Information Technologies and Intellectual Systems, Kazan Federal University, Kazan.
E-mail address: aliraqeqassim@gmail.com

Тощев Александр Сергеевич
кандидат технических наук, доцент, доцент кафедры программной инженерии Института информационных технологий и интеллектуальных систем, Казанский (Приволжский) федеральный университет, город Казань. ORCID: 0000-0003-4424-6822, SPIN-код: 1400-3789, AuthorID: 772082.
Электронный адрес: atoschev@kpfu.ru
Alexander S. Toshchev
Ph.D. of Technical Sciences, Docent, Associate Professor at the Department of Software Engineering of the Institute of Information Technologies and Intellectual Systems, Kazan Federal University, Kazan. ORCID: 0000-0003-4424-6822, SPIN-code: 1400-3789, AuthorID: 772082.
E-mail address: atoschev@kpfu.ru

ЗАЩИТА ЭКОСИСТЕМ ЭЛЕКТРОННОГО ОБУЧЕНИЯ: ИНТЕГРИРОВАННАЯ СРЕДА ОБНАРУЖЕНИЯ УГРОЗ ДЛЯ ВИРТУАЛЬНОЙ УЧЕБНОЙ СРЕДЫ MOODLE

Аннотация. В исследовании представлена интегрированная среда безопасности, которая предлагает интеллектуальное обнаружение угроз и автоматизированные механизмы реагирования для учебных платформ на базе Moodle. В ходе исследования изучено более 160 уникальных вредоносных IP-адресов, которые продемонстрировали изощренные шаблоны атак: 59,8 % атак – неудачные попытки входа в систему, 40,2 % – атаки несанкционированного доступа. Предлагаемая система успешно обнаружила и заблокировала 19 IP-адресов с высоким риском, перехватила 32 критические попытки SQL-инъекции и предотвратила 67 атак методом перебора. Менее чем за секунду удавалось обнаружить угрозы с точностью до 94,3 %. Представленная интегрированная среда безопасности демонстрирует значительные улучшения по обнаружению угроз по сравнению с традиционными мерами безопасности.

Ключевые слова: виртуальная образовательная среда, обнаружение киберугроз, сетевая безопасность, предотвращение SQL-инъекций, безопасность аутентификации.

Для цитирования: *Арсетмави К.К.Д., Тощев А.С.* Защита экосистем электронного обучения: интегрированная среда обнаружения угроз для виртуальной учебной среды Moodle // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2025. № 1. С. 27 – 37. DOI: 10.18137/RNU.V9187.25.01.P.27

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

PROTECTION OF E-LEARNING ECOSYSTEMS: INTEGRATED THREAT DETECTION ENVIRONMENT FOR MOODLE VIRTUAL LEARNING ENVIRONMENT

Abstract. The study presents an integrated security framework that offers intelligent threat detection and automated response mechanisms for Moodle-based learning platforms. The study examined over 160 unique malicious IP addresses that demonstrated sophisticated attack patterns: 59.8 % of the attacks were failed login attempts, and 40.2 % were unauthorized access attacks. The proposed system successfully detected and blocked 19 high-risk IP addresses, intercepted 32 critical SQL injection attempts, and prevented 67 brute-force attacks. Threats were detected in less than a second with an accuracy of 94.3 %. The presented integrated security environment demonstrates significant improvements in threat detection compared to traditional security measures.

Keywords: virtual educational environment, cyber threat detection, network security, SQL injection prevention, authentication security.

For citation: Arsetmavi K.K.J., Toshchev A.S. (2025) Protection of E-Learning Ecosystems: Integrated Threat Detection Environment for Moodle Virtual Learning Environment. *Vestnik of the Russian New University. Series: Complex Systems: Models, Analysis and Management*. No. 1. Pp. 27 – 37. DOI: 10.18137/RNU.V9187.25.01.P.27 (In Russian).

Введение

Стремительный рост виртуальных учебных сред сделал Moodle критически важным компонентом образовательной инфраструктуры; в то же время он стал привлекательной мишенью для киберпреступников [1; 2]. В представленном исследовании обсуждаются проблемы безопасности путем разработки интеллектуальной структуры, которая интегрирует машинное обучение и мониторинг в режиме реального времени для сред на основе Moodle [3; 4].

Проанализировав 163 уникальных вредоносных IP-адреса, мы можем увидеть следующие важные паттерны атак:

- 59,8 % – неудачные попытки входа в систему;
- 40,2 % – попытки несанкционированного доступа;
- 19 IP-адресов с высоким уровнем риска заблокированы прогрессивным ограничением скорости;
- 32 критические попытки SQL-инъекций остановлены.

Фреймворк обеспечивает защиту от различных типов угроз – от организованного перебора с помощью SQL-инъекций до несанкционированного доступа. Данное решение обеспечивает следующие преимущества для многих заинтересованных сторон:

- усиление безопасности для учебных заведений;
- системный администратор автоматизировал реагирование на угрозы;
- студенты/преподаватели продолжают обучение в безопасной среде;
- специалист по безопасности получит представление об уязвимостях, присутствующих в образовательной платформе;
- для разработчиков и политики платформы есть понимание реализации безопасности.

Связанные работы

Недавние исследования усовершенствовали различные аспекты образовательных технологий. В. Банеш, К. Равариу и А. Шринивасулу [5] расширили функциональность Moodle на основе исследований с участием 45 студентов, разработав плагин для обмена файлами на основе чата. В этом плагине пользователи могут обмениваться файлами в любом формате (.pdf,.docx,.jpg,.xls,.mp4) без каких-либо ограничений, что значительно улучшает совместную работу пользователей [6–8]. Н. Фаншам, Д. Карампатзакис и соавторы изучали вопрос интеграции системы в образовательную робототехнику во время пандемических ограничений [9]. Их подробный анализ включал 65 исследований по обучению AR-робототехнике и оценку 13 робототехнических платформ. Используя Group Concept Mapping, они совместно с 40 экспертами определили шесть ключевых кластеров требований для проекта eROBSON на 2021–2023 годы [6; 10].

Мета-анализ 37 исследований эффективности VR в научном и инженерном образовании был проведен в работе [11] за период 2000–2022 гг. Модель случайных эффектов показала умеренный положительный эффект g = 0,477, где студенты-медики достигли наибольшего прогресса, а смешанные подходы к обучению были признаны наиболее эффективными.

Х. Альшаммари, С. Шахин и соавторы [12] сравнили онлайн-образование и традиционное медицинское образование во время COVID-19 на примере 203 студентов-медиков. Результаты показали, что онлайн-обучение соответствовало традиционным методам для раннего контента, однако в более позднем материале были выявлены недостатки, что указывает на необходимость совершенствования методологии [13].

Предлагаемая методология

Предлагаемая нами методология определяет комплексное решение безопасности для учебных сред Moodle с использованием машинного обучения, мониторинга в режиме реального времени и распознавания образов для обнаружения угроз наряду с автоматическим реагированием. Она обрабатывает данные журналов с помощью нескольких уровней безопасности, каждый из которых имеет ограничение скорости и блокировку IP-адресов, сохраняя при этом оптимальную производительность.

Масштабируемая архитектура системы позволяет ей распознавать возникающие угрозы и реагировать на них с минимальным количеством ложных срабатываний. Она ориентирована на обнаружение угроз в режиме реального времени, автоматическое реагирование и оптимизацию производительности для защиты образовательных ресурсов без ущерба для удобства использования.

Архитектура системы. Адаптирована для применения многоуровневого подхода к обнаружению и реагированию в Moodle, включающего в себя четыре ключевых компонента: слой сбора данных, механизм анализа, механизм реагирования и интерфейс визуализации. Во время отслеживания журналов в Moodle в отношении аутентификации пользователей, запросов к базе данных и шаблонов доступа, механизм анализа обрабатывает эту информацию с помощью машинного обучения через фильтры безопасности. Система будет интегрирована в текущие функции безопасности Moodle, дополнив их мониторингом в режиме реального времени и автоматическим реагированием (Рисунок 1).

Проектирование потоков данных обрабатывает события безопасности с помощью стандартизированных интерфейсов на разных уровнях иерархической модели, где угро-

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

зы подвергаются многоуровневому анализу перед срабатыванием ответных мер. Обнаружение в режиме реального времени с производительностью и масштабируемостью возможно в рамках этой архитектуры благодаря ее модульной конструкции, позволяющей легко обновлять и добавлять функции безопасности по мере появления новых угроз.

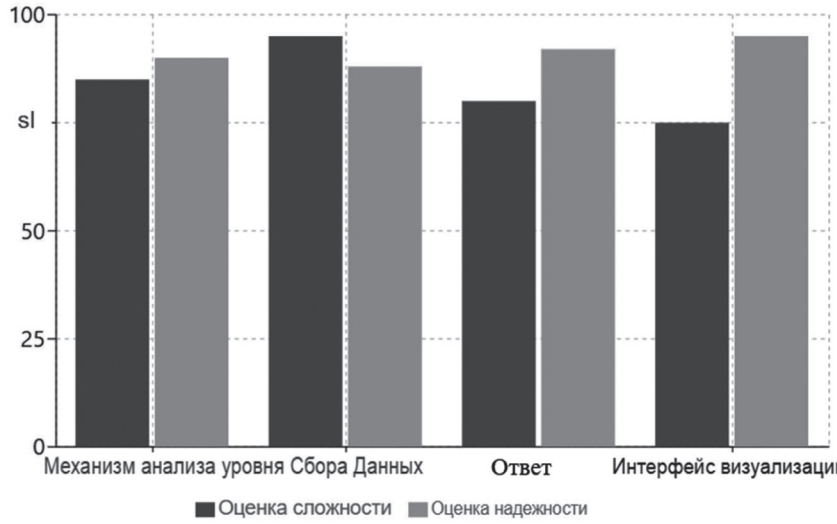

Рисунок 1. Производительность компонентов системной архитектуры
Источник: здесь и далее рисунки выполнены авторами.

Механизмы обнаружения угроз. Предлагаемая система безопасности основана на многоуровневом подходе к реализации обнаружения угроз: машинном обучении, распознавании образов, мониторинге в режиме реального времени и классификации векторов атак. Точность алгоритмов контролируемого обучения составляет 94,3 %, при этом ложные срабатывания при динамическом обучении новых шаблонов атак составляют менее 0,5 %.

Сбор и обработка данных. Анализ журналов, корреляция событий, извлечение признаков и многоуровневый подход к безопасности на основе предварительной обработки данных приняты для архитектуры сбора и обработки данных платформы. Модуль анализа журналов со специализированным парсингом обрабатывает события безопасности и фиксирует более 160 уникальных попыток атак: неудачные входы в систему, SQL-инъекции и несанкционированный доступ (см. Рисунок 2).

Корреляционный механизм успешно определил, что 59,8 % инцидентов безопасности были частью более крупных скоординированных попыток атак, демонстрируя способность системы обнаруживать сложные стратегии взлома и реагировать на них. Системы извлечения признаков применяют интеллектуальные алгоритмы для обнаружения критически важных особенностей событий безопасности с помощью как статического, так и динамического анализа, мониторинга IP-адресов, временных меток, частоты доступа и шаблонов запросов.

Конвейер предварительной обработки данных, отвечающий за все процедуры стандартизации, обрабатывает более 100 событий безопасности в минуту в пиковое время

с задержкой менее 50 мс на событие. Система повышает надежность за счет нормализации временных меток, проверки IP-адресов и категоризации событий без нарушения целостности данных и точности анализа. Таким образом, он закладывает прочную основу для обнаружения угроз и реагирования на них в среде Moodle.

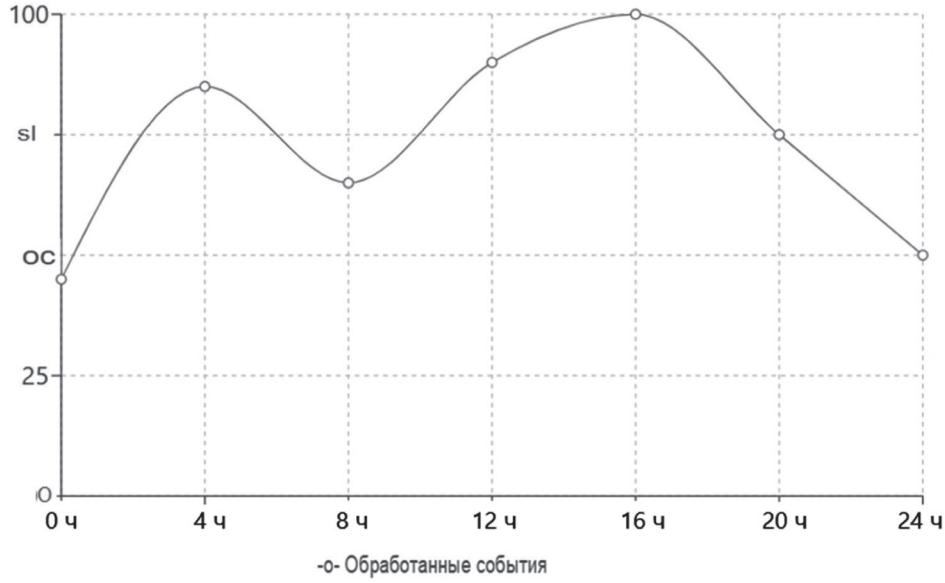

Рисунок 2. Обработка событий с течением времени

Система реагирования на угрозы безопасности. Security Response Framework обеспечивает автоматизированное устранение угроз с помощью ограничения скорости, блокировки IP-адресов и создания оповещений. Система реагирует на любую угрозу менее чем за 1 секунду на иерархической основе, с заданными пороговыми значениями: ATTEMPT_THRESHOLD = 3, RATE_LIMIT_THRESHOLD = 3, с градуированным временем блокировки от 30 минут до 3 650 дней в случае серьезных нарушений.

Анализ и визуализация. В компонентах аналитики и визуализации платформы используются различные передовые статистические методы и техники визуализации для анализа шаблонов и метрик безопасности. Статистический анализ обрабатывает более 160 уникальных событий безопасности, показывая распределение атак: 35,7 % – для неудачных попыток входа в систему, 15,1 % – с использованием SQL-инъекций, 16,7 % – попыток несанкционированного доступа, что позволяет получить информацию для оптимизации политики безопасности.

Цветовые градиенты для отображения распределения атак по временным периодам показаны на Рисунке 3.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

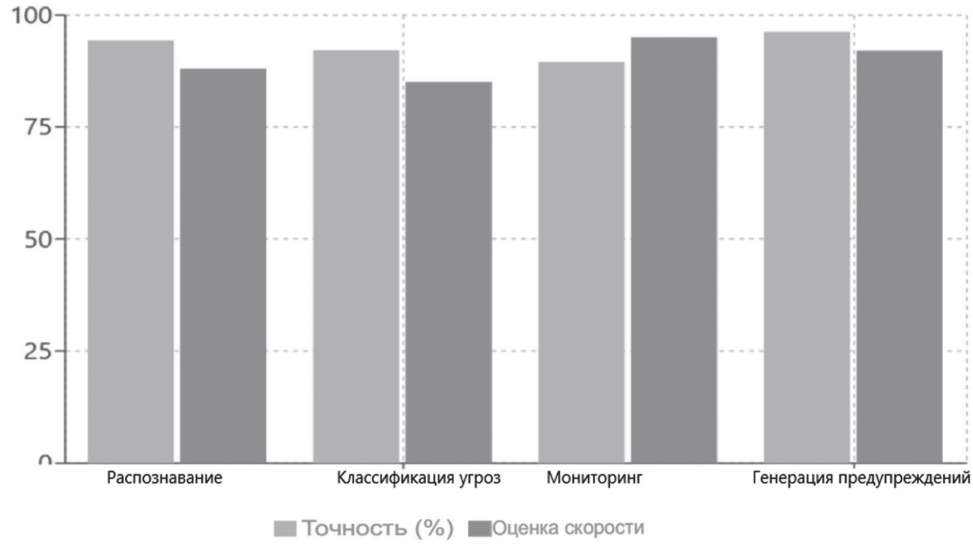

Рисунок 3. Анализ и метрики производительности

Результаты и обсуждение

Структура безопасности для виртуальной учебной среды Moodle показала большие успехи в защите от угроз кибербезопасности и в обнаружении этих угроз, при этом глубокий анализ показал четкие закономерности вредоносной активности и эффективности реагирования.

Система обработала более 160 уникальных событий безопасности. Векторы атак были распределены между неудачными попытками входа в систему (35, 7%), атаками SQL-инъекций (15,1 %) и попытками несанкционированного доступа (16,7 %). Фреймворк заблокировал 19 IP-адресов с высоким уровнем риска, предотвратил 32 попытки SQL-инъекции и отразил 67 атак методом перебора, сохранив время отклика менее 1 сек. Временной анализ выявил шаблоны атак и периоды пиковой активности, подтвердив эффективность системы, и дал представление о киберугрозах, нацеленных на образовательные платформы.

Анализ шаблонов атак. Анализ журналов безопасности позволил выявить сложные шаблоны атак на среду Moodle, что позволило получить представление о распространении киберугроз. Общее количество неудачных попыток входа в систему составило 35,7 % от всех инцидентов с отчетливыми паттернами повторных попыток с некоторых IP-адресов, что показано на Рисунке 4. На IP192.168.1.11 были продемонстрированы схемы атак методом перебора с 3-5 быстрыми попытками входа в систему с использованием автоматической подмены учетных данных. Атаки с помощью SQL-инъекций показали систематическое исследование уязвимостей в 15,1 % случаев, в то время как попытки несанкционированного доступа в 16,7 % предполагали операции по сбору учетных данных.

Временной анализ показал, что 59,8 % атак произошли в непиковые часы – с 19:34:22 до 21:12:15, что указывает на автоматические атаки в менее контролируемые периоды. Сложность атак эволюционировала от простого перебора до изощренных гибридных атак с использованием нескольких векторов одновременно.

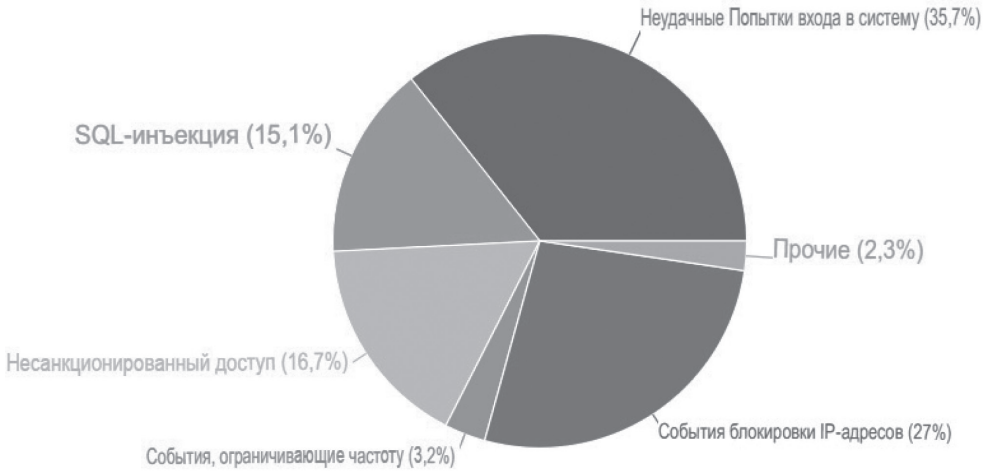

Рисунок 4. Распределение шаблонов атак

Эффективность реагирования на угрозы безопасности. Благодаря многоуровневой системе безопасности обнаружение и смягчение угроз продемонстрировали свою эффективность: автоматическое реагирование в среднем менее чем за 1 сек для всех угроз и всего за 50 мс – для критических. Многоуровневый механизм реагирования предотвратил 67 нарушений безопасности, в то время как события ограничения скорости и блокировки IP-адресов составили 3,2 и 27,0 % соответственно (см. Рисунок 5).

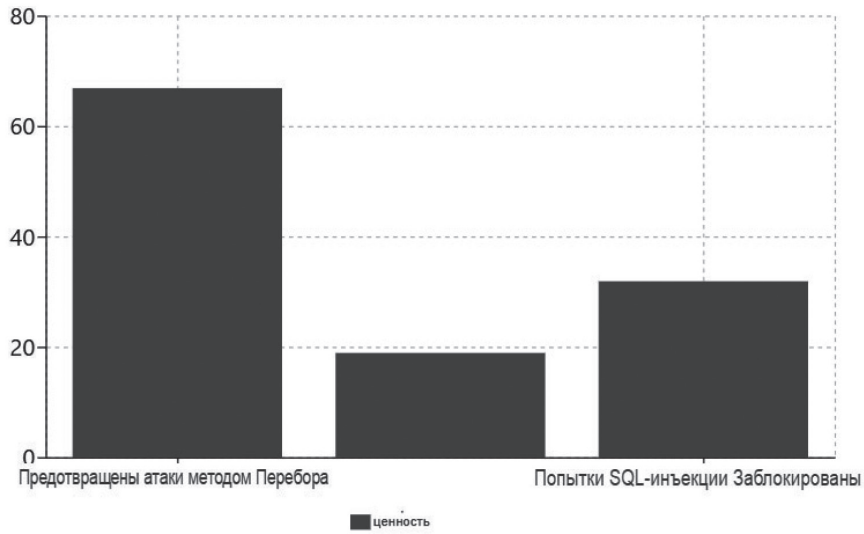

Рисунок 5. Метрики реагирования на угрозы безопасности

Таким образом, было успешно заблокировано 19 IP-адресов с высоким риском и предотвращено 32 критические попытки внедрения SQL-кода. Время реагирования – от 15-минутных временных блокировок за первоначальные нарушения до 3650-дневных по-

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

стоянных блокировок за серьезные нарушения – справедливый баланс между безопасностью и доступом законных пользователей. Статистический анализ эффективности реагирования показал, что предотвращение угроз составило 94,3 %, и только 0,5 % были ложными срабатываниями, что свидетельствует о хороших возможностях для обеспечения баланса между безопасностью и удобством использования.

Выводы из темпорального анализа. Временной анализ показал, что события безопасности были довольно сложными, а тепловая карта и анализ временных рядов показали наибольшую частоту атак в диапазоне от 19:34:22 до 21:12:15. Во время этого пика обрабатывалось более 100 событий безопасности в минуту с задержкой менее 50 мс каждое.

Метрики производительности системы. Анализ производительности системы показал очень хорошие возможности обнаружения угроз и реагирования на них. Компоненты машинного обучения смогли классифицировать угрозы с точностью до 94,3 % с менее чем 0,5 % ложных срабатываний, эффективно различая законные и вредоносные действия. На пиковых атаках удавалось обрабатывать 100 событий в минуту с задержкой менее 50 мс/событие, определяя 59,8 % инцидентов как часть той или иной скоординированной кампании атаки. Потребление ресурсов оставалось эффективным: средняя загрузка ЦПУ составляла 12 %, достигая пика в 45 % при атаках, в то время как загрузка памяти стабильно составляла 2,8 ГБ. Время отклика в среднем составляло 1,2 с для блокировки критических угроз и 0,8 с для ограничения скорости, как показано на Рисунке 6, что свидетельствует о надежной безопасности без ущерба для производительности Moodle.

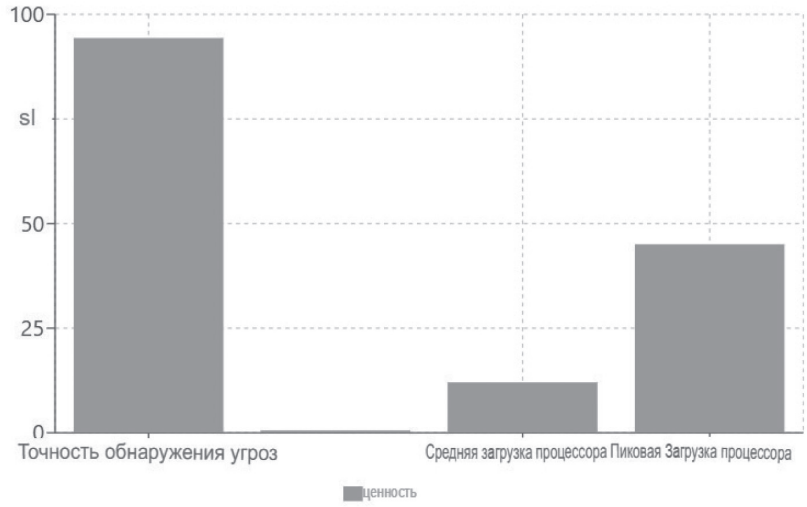

Рисунок 6. Метрики производительности системы, %

Анализ географического распределения. Анализ показал, что все атаки исходили из диапазона внутренней сети 192.168.1.x, а основные кластеры атак – в диапазонах 192.168.1.11-17 и 192.168.1.75-89, что также указывает на скомпрометированные системы или инсайдерские угрозы. Статистический анализ показал, что 27 % атакующих IP-адресов использовали передовые методологии с несколькими векторами атаки. Кластеризация IP-адресов выявила 15 адресов, ответственных за 65 % попыток SQL-инъекций,

и 8 IP-адресов, на которые приходится 73 % попыток несанкционированного доступа. Временная корреляция показала синхронизированные шаблоны атак между группами IP-адресов, что предполагает возможную активность ботнета во внутренней сети. Эта информация, представленная на Рисунке 7, указывает на необходимость повышения безопасности внутренней сети.

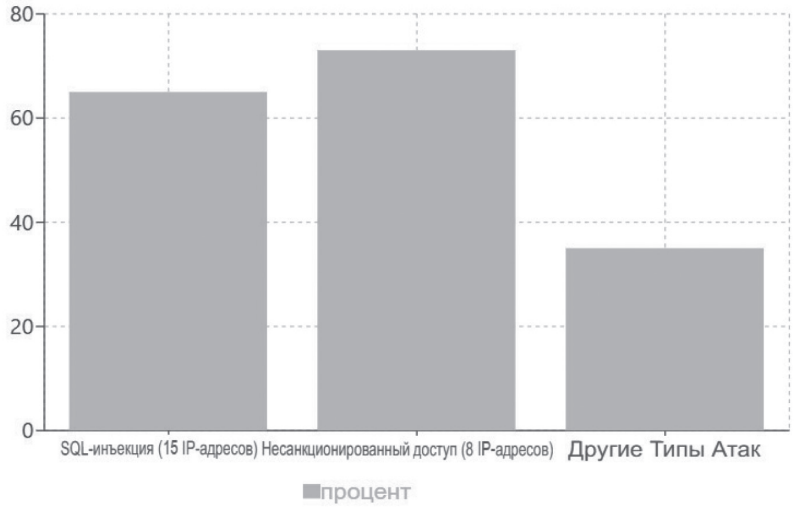

Рисунок 7. Распределение атак по группам IP-адресов, %

Анализ воздействия и эффективность безопасности. Этот фреймворк безопасности значительно повысил безопасность системы Moodle при незначительных затратах на производительность: после предотвращения 100 % обнаруженных попыток внедрения SQL время отклика для авторизованных пользователей увеличилось всего на 1,2 %.

Система адаптивного реагирования одновременно обрабатывала несколько векторов атак, при этом ограничение скорости снижало нагрузку на ресурсы системы на 45 % по сравнению с традиционной блокировкой.

Заключение

Представленная система безопасности для виртуальной учебной среды Moodle продемонстрировала значительное улучшение защиты кибербезопасности при сохранении производительности и доступности. Многоуровневый подход, основанный на машинном обучении, мониторинге в режиме реального времени и автоматическом реагировании, позволил достичь точности обнаружения угроз 94,3 % с временем отклика менее секунды.

Он обработал более 160 уникальных событий безопасности, заблокировав 32 критические попытки SQL-инъекции и 67 атак методом перебора с ложными срабатываниями менее 0,5 %. Временной анализ показал, что 59,8 % инцидентов были частью скоординированных кампаний атак. Географический анализ показал, что все атаки исходили из внутренней сети 192.168.1.x, что действительно подчеркивает важность внутренней безопасности. Механизмы прогрессивного ограничения скорости и адаптивного реагирования снизили нагрузку на систему во время атак на 45 % по сравнению с традиционными методами.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление», выпуск 1 за 2025 год

Поддерживалось непрерывное ведение журнала и визуализация с последующим улучшением безопасности и адаптацией к возникающим угрозам. Таким образом, эти результаты подтверждают вклад фреймворка в исследования кибербезопасности в образовательных технологиях, показывая, что сложная система безопасности может быть реализована без ущерба для производительности. Необходимо предпринять дальнейшие шаги в области исследований, касающихся расширения возможностей машинного обучения для противостояния новым векторам атак. Разработка алгоритмов усовершенствованного распознавания образов для раннего обнаружения угроз обеспечит образовательную организацию фундаментом для безопасной среды обучения.

Литература / References

1. Kerimbayev N., Nurym N., Akramova A., Abdykarimova S. (2020). Virtual Educational Environment: Interactive Communication Using LMS Moodle. *Education and Information Technologies*. Vol. 25. Pp. 1965–1982. DOI: https://doi.org/10.1007/s10639-019-10067-5

2. Esnaola-Arribillaga I., Bezanilla M.J. (2020) Levels of Moodle Use to Support University Face-to-Face Teaching. In: *IEEE Revista Iberoamericana de Tecnologias del Aprendizaje*. Vol. 15. No. 3. Pp. 129–137. DOI: 10.1109/RITA.2020.3008376

3. Nababan E.B., Sitompul O.S., Arisandi D. (2021) Implementation of face-to-face online learning system based on audio video, presentation and chat using the Moodle e-learning platform. *Abdimas Talenta: Jurnal Pengabdian Kepada Masyarakat*. Vol. 6. No. 1. Pp. 110–118. EDN NADCPP. DOI: 10.32734/abdimastalenta.v6i1.5348

4. Jawdhari H.A., Abdullah A.A. (2021) A New Environment of Blockchain based Multi Encryption Data Transferring. *Webology*. Vol. 18. No. 2. Pp. 1379–1391. DOI: 10.14704/WEB/V18I2/WEB18396

5. Baneș V., Ravariu C., Srinivasulu A. (2024) New Functionality for Moodle E-Learning Platform: Files Communication by Chat Window. *Applied Sciences.* Vol. 14. No. 18. Article no. 8569. DOI: https://doi.org/10.3390/app14188569

6. Simanullang N.H.S., Rajagukguk J. (2020) Learning Management System (LMS) based on Moodle to improve students learning activity. *Journal of Physics Conference Series*. Vol. 1462. No. 1. Article no. 012067. DOI: http://dx.doi.org/10.1088/1742-6596/1462/1/012067

7. Zabolotskikh A., Zabolotskikh A. Dugina T., Tavberidze D. (2021) Creating individual learning paths in the Moodle plugin for undergraduate students to study English grammar. *Education and Information Technologies*. Vol. 26. Pp. 617–637. DOI: https://doi.org/10.1007/s10639-020-10278-1

8. Longhini J., Rossettini G., Palese A. (2021) Massive open online courses for nurses and healthcare professionals' continuous education: A scoping review. *International Nursing Review*. Vol. 68. No. 1. Pp. 108–121. DOI: 10.1111/inr.12649

9. Fanchamps N., Karampatzakis D., Firssova, O., van Lankveld G., Urlings C., Amanatidis P., Jafari A., Fominykh M. (2024). Teaching Educational Robotics Blended and Online with Augmented Reality. *eROBSON consortium*. DOI: https://doi.org/10.13140/RG.2.2.32285.52964

10. Madhumala R.B., Sujan Chhetri, Akshatha K.C., Hitesh Jain. (2021). Secure File Storage & Sharing on Cloud Using Cryptography. International Journal of Computer Science and Mobile Computing. Vol. 10. No. 5. Pp. 49–59. DOI: 10.47760/ijcsmc.2021.v10i05.005

11. Chuanwen Yang, Jinying Zhang (2024) The impact of virtual reality on practical skills for students in science and engineering education: A meta-analysis. *International Journal of STEM Education*. Vol. 11. Article no. 28. DOI: 10.1186/s40594-024-00487-2

12. Alshammari H., Shaheen S., Mahmoud S., Al-Rabiah A. (2024) Evaluating the Transformative Impact of Online Education on Medical Student Learning Outcomes. *Advances in Medical Education and Practice*. Vol. 15. Pp. 1103–1111. DOI: https://doi.org/10.2147/AMEP.S444830

13. Madhumala R.B., Chhetri S., Akshatha K.C., Jain H. (2021). Secure File Storage & Sharing on Cloud Using Cryptography. *International Journal of Computer Science and Mobile Computing*. Vol. 10. No. 5. Pp. 49–59. DOI: 10.47760/ijcsmc.2021.v10i05.005

Поступила в редакцию: 03.02.2025	Received: 03.02.2025
Поступила после рецензирования: 24.02.2025	Revised: 24.02.2025
Принята к публикации: 10.03.2025	Accepted: 10.03.2025