УДК 004.056.53; 004.8

АДАПТИВНОЕ ОБУЧЕНИЕ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ: ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И CTF-ПЛАТФОРМ

К.Д. Янович, В.В. Васькевич

Учреждение образования «Гомельский государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В данной работе предложена концепция адаптивной образовательной среды для подготовки специалистов по кибербезопасности, объединяющая технологии искусственного интеллекта и CTF-платформ. Искусственный интеллект выступает в роли помощника: анализирует действия обучающегося, выявляет его слабые места и формирует индивидуальные практические задания. CTF-платформы помогают закрепить полученные знания на практике. Такая концепция обеспечивает персонализированную траекторию обучения, повышает мотивацию и эффективность обучения и сокращает время подготовки специалистов, готовых к решению реальных задач защиты информационных систем.

Ключевые слова: адаптивное обучение; искусственный интеллект; кибербезопасность; CTF-платформы; персонализация; индивидуальный маршрут; практические навыки; подготовка кадров; машинное обучение; образовательные технологии.

ADAPTIVE TRAINING OF CYBERSECURITY SPECIALISTS: USING AI AND CTF PLATFORMS

K.D. Yanovich, V.V. Vaskevich
Educational Institution "Francisk Skorina Gomel State University", Gomel, Republic of Belarus

Annotation. In the article, the concept of an adaptive educational environment for training cybersecurity specialists is proposed, combining artificial intelligence technologies and CTF platforms. Artificial intelligence acts as an assistant: it analyzes the student's actions, identifies his weaknesses and forms individual practical tasks. CTF platforms help to consolidate the acquired knowledge in practice. This concept provides a personalized learning trajectory, increases motivation and learning efficiency, and reduces the training time for specialists who are ready to solve real-world information system protection tasks.
Keywords: adaptive learning; artificial intelligence; cybersecurity; CTF platforms; personalization; individual route; practical skills; staff training; machine learning; educational technologies.

Введение

В условиях современной реальности сфера кибербезопасности является одной из ключевых для обеспечения национальной безопасности, устойчивого развития бизнеса, государства и общества, а глобальный рынок испытывает острую нехватку квалифицированных специалистов. Поэтому обучение данных специалистов становится приоритетным и включает в себя как теоретическую базу, так и применение различных инструментов на практике, в том числе созданных на основе искусственного интеллекта (ИИ), а также CTF-площадок.

Основная часть

ИИ для обучения кибербезопасности имеет широкое применение. Данный инструмент может быть использован в качестве помощника для всех специалистов (начинающих или опытных) с целью обучения, помощи при решении различных задач, освоении инструментов или для сбора полезных источников. Он персонализирует контент под конкретного человека, а также сопровождает его на протяжении всего времени использования. Например, российская платформа Avareange, в которую входят индивидуальные маршруты обучения с учетом анализа поведения (используя ML и LangChain), чат-ассистент на базе нейросети GigaChat, моделирование фишинговых атак с автоматической корректировкой сценариев под опыт пользователя, прогнозирующая аналитика и построение планов CISO через систему Pulse (скоринг уязвимостей и OSINT), а также интерактивная панель с визуализацией уровня готовности персонала и динамики угроз. Центральная составляющая

решения – адаптивное обучение, основанное на технологиях искусственного интеллекта. Применение платформ LangChain и моделей машинного обучения дает возможность проводить глубокий анализ поведения сотрудников и формировать персонализированные образовательные подходы. Такой подход способствует повышению информированности команды об угрозах и эффективной подготовке к реалиям кибербезопасности [1].

Для опытных специалистов ИИ – мощный инструмент для проведения пентеста, который способен обрабатывать огромные объемы данных, выявлять шаблоны и автоматизировать сложные задачи, структурировать процессы отчетности. Также он позволяет повысить работоспособность специалистов, автоматизируя рутинные операции и помогая выявлять уязвимости, которые могут быть пропущены или незамечены при ручном тестировании [2]. Одним из ключевых направлений применения искусственного интеллекта в пентестах выступает эксплуатация уязвимостей. Современные ИИ-системы способны модифицировать готовые экплойты или разрабатывать новые, ориентируясь на специфику целевой среды. Такой подход обеспечивает достоверную проверку наличия уязвимостей и снижает долю ошибочных срабатываний. Интеллектуальные платформы учитывают нюансы конфигурации системы и предлагают оптимальные способы подтверждения уязвимых мест.

В контексте обучения кибербезопасности, как было сказано ранее, важна не только теоретическая часть, но и практическая, в особенности практикоориентированность, поэтому платформы CTF (Capture The Flag) выступают связующим звеном между этими частями, позволяя применить полученные знания на практике. Там представлено множество различных категорий: OSINT, Forensics, PWN, Crypto, Web и другие. Основная цель данных платформ – «захватить флаг», то есть решить задания на определенные темы, ответом на которые выступает длинный код, состоящий из букв и цифр, зачастую обернутый в фигурные скобки. Примером таких платформ выступают площадки HackTheBox, TryHackMe, Codeby Academy и многие другие. Практикуясь в решении задач по различным темам, специалисты по кибербезопасности получают бесценный опыт для дальнейшей профессиональной карьеры, а также имеют возможность стать более конкурентноспособными на рынке труда.

Но не стоит забывать, что ИИ может использоваться как для обучения специалистами, так и злоумышленниками. ИИ также показывает высокий потенциал возможностей автоматизации компрометации защищаемой инфраструктуры. Оценка формируется на основе результатов тестирования ИИ в рамках программ Bug Bounty и соревнований типа CTF., например, в июне 2025 года ассистент Xbow занял лидирующую позицию в рейтинге HackerOne, выявив максимальное число уязвимостей в коде – что стало

историческим прецедентом для платформы. Система учитывает не только количество найденных багов, но и их критичность, анализируя безопасность программного обеспечения ведущих корпораций. Еще один случай – согласно исследованиям Palisade Research, агентный ИИ участвовал в CTF, где решил 19 из 20 заданий среди 400 команд, заняв позицию в топ-5% участников. На следующем этапе, в соревновании с участием почти 8000 команд, наиболее успешному ИИ-агенту удалось получить 20 флагов из 62, прочно войдя в Топ-10%. Недавно на темных форумах появились сообщения о новом инструменте Hexstrike-AI: он объединяет свыше 150 ИИ-агентов, способен автоматизированно проводить аудит инфраструктуры, эксплуатировать уязвимости, включая zero-day, и удерживать доступ в компрометированных системах – все это за считанные минуты. Подобные достижения наглядно демонстрируют высокий потенциал искусственного интеллекта, при этом его текущие успехи уже значительно превосходят те, которые были наблюдаемы всего год назад [3].

Заключение

Таким образом, применение ИИ и CTF-платформ для обучения специалистов по кибербезопасности имеет ключевую роль в качестве помощника для преподавателя, а не его замены.

Список использованных источников

1. Не учить, а адаптироваться. Российский стартап переизобрел тренировку по информационной безопасности с помощью ИИ. [Электронный ресурс] // Коммерсантъ. – 2025. – 28 августа. – URL: https://www.kommersant.ru/doc/7989327. – Дата доступа: 15.03.2026.

2. Огнивчук, М. Как искусственный интеллект усиливает возможности специалистов по кибербезопасности. [Электронный ресурс] / М. Огнивчук // Обзор ИИ-инструментов пентестов 2025. – 2025. – 4 июня. – URL: https://www.h-x.technology/ru/blog-ru/review-ai-tools-pentest-2025-ru. – Дата доступа: 15.03.2026.

3. Голушко, А. SOC будущего: ключевые тренды 2026-2028. [Электронный ресурс] / А. Голушко // Positive Technologies. – 2025. – 30 октября. – URL: https://ptsecurity.com/research/ analytics/the-future-soc-trends-defining-tomorrow-cyber-defense/#id2. – Дата доступа: 15.03.2026.

References

1. Not to teach, but to adapt. A Russian startup has reinvented information security training using AI. [Electronic resource] // Kommersant. – 2025. – August 28. – URL: https://www.kommersant.ru/doc/7989327. – Access date: 15.03.2026.

2. Ognivchuk, M. How artificial intelligence enhances the capabilities of cybersecurity specialists. [Electronic resource] / M. Ognivchuk // Review of AI tools for pentests 2025. – 2025. – June 4. – URL: https://www.h-x.technology/ru/blog-ru/review-ai-tools-pentest-2025-ru. – Access date: 15.03.2026.

3. Golushko, A. SOC of the future: key trends 2026-2028. [Electronic resource] / A. Golushko // Positive Technologies. – 2025. – October 30. – URL: https://ptsecurity.com/research/analytics/the-future-soc-trends-defining-tomorrow-cyber-defense/#id2 . – Access date: 15.03.2026.

Сведения об авторах

Янович К.Д., студентка факультета физики и информационных технологий, специальности «Кибербезопасность», учреждение образования «Гомельский государственный университет имени Франциска Скорины», karifox100@gmail.com.

Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, учреждение образования «Гомельский государственный университет имени Франциска Скорины», vaskevich@gsu.by.

Information about the authors

Yanovich K.D., student of the Faculty of Physics and Information Technologies, specialty "Cybersecurity", Education Institution "Francysk Skaryna Gomel State University", karifox100@gmail.com.

Vaskevich V.V., Senior Lecturer at the Department of Radiophysics and Electronics, Education Institution "Francysk Skaryna Gomel State University", vaskevich@gsu.by.