Дата поступления рукописи в редакцию: 28.05.2026 г.
Дата принятия рукописи в печать: 30.06.2026 г.
DOI: 10.24412/3034-4271-2026-3-53-58

ЗУФАРОВА Анна Сергеевна,
старший преподаватель,
Тихоокеанский государственный университет,
e-mail: 006694@togudv.ru

ВЕРХОЗИНА Анастасия Федоровна,
студент,
Тихоокеанский государственный университет,
e-mail: 2018101805@togudv.ru

ПРЕИМУЩЕСТВА РЕШЕНИЙ EDR НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СВЕТЕ МОДЕЛИ УГРОЗ MITRE ATT&CK

Аннотация. *В современном мире атаки в сети становятся все сложнее, и важной частью защиты является не только обнаружение угроз, но и их прогнозирование. Статья посвящена исследованию преимуществ решений класса Endpoint Detection and Response (EDR), построенных на технологиях искусственного интеллекта (ИИ), применительно к модели угроз MITRE ATT&CK. Сегодня современные подходы к обеспечению информационной безопасности требуют новых подходов к обнаружению и предотвращению угроз. Традиционные защитные механизмы оказываются недостаточно эффективными против продвинутых атак, направленных на критически важные ресурсы предприятий. Искусственный интеллект в составе решений EDR способен существенно повысить уровень защиты благодаря способности выявлять нестандартные и ранее невиданные угрозы, минимизируя количество ложных срабатываний. Описаны основные преимущества решений EDR на основе ИИ, среди которых особое внимание уделено автоматизированному выявлению сложных угроз, уменьшению количества ложных тревог, проведению глубокого поведенческого анализа и улучшению прогнозирования возможных сценариев развития инцидентов. Рассматриваются ключевые компоненты модели MITRE ATT&CK, позволяющие оценивать эффективность различных этапов атаки и предлагать действенные меры защиты. Примеры конкретных техник и методик отражают актуальные аспекты современных угроз, подчеркивая необходимость интеграции интеллектуальных компонентов в процесс выявления вторжений. Заключение подчеркивает важность комплексного подхода к информационной безопасности, основанного на применении передовых технологий, позволяющих своевременно выявлять и устранять любые проявления киберпреступности. Таким образом, статья демонстрирует практическую значимость внедрения решений EDR с искусственным интеллектом для устойчивого роста устойчивости бизнеса в цифровую эпоху.*

Ключевые слова: *Endpoint Detection and Response (EDR); искусственный интеллект (ИИ); MITRE ATT&CK; кибератака; угроза; защита; машинное обучение; прогнозирование угроз.*

ZUFAROVA Anna Sergeevna,
Senior Lecturer,
Pacific State University

VERHOZINA Anastasia Fedorovna,
Student,
Pacific State University

ADVANTAGES OF EDR CLASS SOLUTIONS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE CONTEXT OF THE MITRE THREAT MODEL OF ATT&CK

Annotation. *In today's world, online attacks are becoming more complex, and an important part of protection is not only detecting threats, but also predicting them.*

The article is devoted to the study of the advantages of Endpoint Detection and Response (EDR) class solutions based on artificial intelligence (AI) technologies in relation to the MITRE ATT&CK threat model. Today, modern approaches to information security require new approaches to threat detection and prevention. Traditional defense mechanisms are proving insufficiently effective against advanced attacks targeting critical enterprise resources. Artificial intelligence in EDR solutions is able to significantly increase the level of protection due to the ability to identify non-standard and previously unseen threats, minimizing the number of false positives. The main advantages of AI-based EDR solutions are described, among which special attention is paid to the automated identification of complex threats, reducing the number of false alarms, conducting in-depth behavioral analysis and improving the prediction of possible incident scenarios. The key components of the MITRE ATT&CK model are considered, which make it possible to evaluate the effectiveness of various stages of an attack and propose effective protection measures. Examples of specific techniques and techniques reflect current aspects of modern threats, emphasizing the need to integrate intelligent components into the intrusion detection process. The conclusion underlines the importance of an integrated approach to information security based on the use of advanced technologies that allow timely detection and elimination of any manifestations of cybercrime. Thus, the article demonstrates the practical importance of implementing EDR solutions with artificial intelligence for the sustainable growth of business sustainability in the digital age.

Key words: *Endpoint Detection and Response (EDR); artificial intelligence (AI); MITRE ATT&CK; cyberattack; threat; protection; machine learning; threat forecasting.*

Введение

Любая организация хранит оцифрованную информацию, имеет выход в глобальную сеть интернет и уязвима перед киберпреступниками. Защищать и анализировать становиться все труднее. Появляется все больше объектов критической информационной инфраструктуры (КИИ). КИИ делиться на значимые и незначимые и присваивается категория (первая, вторая, третья). Такие категории необходимы для определения мер защиты, направленных на предотвращения компьютерных атак [1]. КИИ имеют значимость: социальную, политическую, экономическую, экологическую, значимость для обороны страны. Если важные КИИ атакуют, то парализуется важные отрасли страны. Человеческими силами трудно анализировать и защищать большие данные. На помощь приходит искусственный интеллект.

«Искусственный интеллект – это направление в науке основано на точных науках (математике, информатике, физика и другие), лингвистике, биологии, медицине, психологии, машиностроение и другое. На основе информации (в зависимости от научного направления) при помощи машинного обучения вычислительные системы имитируют человеческий интеллект. Так же искусственный интеллект может обнаружить хакерские атаки, угрозы и взломы из вне, а также автоматически принять необходимые меры для устранения угроз» [7; 8].

Тема применение искусственного интеллекта в защите информации сейчас актуальна. В нашей статье затронем понятия искусственного интеллекта, EDR (Endpoint Detection and Response), MITRE ATT&CK.

Симбиоз искусственного интеллекта и EDR позволяют системам обучатся на основе данных о безопасности. Благодаря такому обучению, у систем существенно повышается их способность к предсказанию и нейтрализации угроз до атаки. Такие возможности появляются благодаря анализу поведения в сети и на конечных точках. Это все позволяет обнаружить аномалии, уязвимости, ошибки, которые могут указывать на область атаки. Подход и анализ на основе ИИ в нынешней ситуации особенно актуален и ценен в контексте модели MITRE ATT&CK [1].

MITRE ATT&CK это матрица включает в себя огромный объем данных об угрозах (рисунок 1).

Рисунок 1. Матрица MITRE ATT&CK

Эти данные собраны из открытых источников, что дает богатую базу для анализа и обучения ИИ.

С развитием динамики угроз, простое обновление баз данных уже не может обеспечить достаточный уровень информационной безопасности.

EDR (Endpoint Detection and Response) – это средство, предназначенное для мониторинга и анализа активности на конечных устройствах [3]. Таких как компьютеры, сервера, мобильные устройства и т.д. Оно помогает выявлять подозрительные действия и реагировать на них.

В связке EDR на основе ИИ выступает как важный инструмент для адаптации к меняющимся тактикам злоумышленников, представленным в MITRE ATT&CK.

Системы могут не только распознавать известные атаки, но и предсказать новые изменения или свежие угрозы, тем самым системы опережают действия злоумышленников и защищают организации от возможных рисков [2]. Так, объединение ИИ и EDR систем с данными MITRE ATT&CK открывает новые пути в сфере ИБ предлагая глубокий анализ угроз и высокий уровень защиты. Это представляет большой шаг вперед в борьбе с киберпреступностью обеспечивая целостный подход к нахождению, предотвращению и реагированию на угрозы безопасности в реальном времени.

Материалы и методы

Рассмотрим, что такое MITRE ATT&CK. MITRE ATT&CK – это сокращение от Adversarial Tactics, Techniques, and Common Knowledge. Это общедоступная база знаний, она описывает тактики и техники, которые используют злоумышленники на каждом этапе своей атаки [5]. Матрица создана экспертами из организации MITRE чтобы дать общее понимание возможных угроз и сделать защиту информационных систем более эффективной. Зная определённые аспекты этой матрицы, специалисты могут предсказывать действия злоумышленников и разрабатывать меры защиты от атак. Матрица MITRE ATT&CK основывается на нескольких ключевых принципах: тактика, техника и процедуры (TTPs); структурирование и визуализация данных; большая база знаний; адаптивность; интеграция с другими инструментами [4]. Эти принципы делают матрицу MITRE ATT&CK эффективным инструментом для анализа тактики и защиты от киберугроз.

EDR-решение обеспечивает наглядное отображение происходящего в режиме реального времени и помогает активно выявлять потенциальные угрозы. В работе оно проходит через следующие основные этапы:

1. Сбор сведений с клиентских устройств.

На устройствах генерируется информация о сетевых коммуникациях, процессах и действиях пользователей. Вся эта информация передается централизованной платформе EDR (которая может размещаться в облаке, локально или иметь гибридную архитектуру), чтобы потом подвергнуться обработке.

2. Анализ полученных данных.

Используя методы машинного обучения, инструменты EDR анализируют собранные сведения, ориентируясь на стандартные модели поведения. Таким образом устанавливается нормальный режим работы системы, что упрощает выявление отклонений и потенциальных нарушений.

3. Уведомления о подозрительных событиях.

Система EDR оповещает специалистов службы информационной безопасности и другие подразделения компании обо всех необычных инцидентах. Помимо этого, она автоматически инициирует запрограммированные реакции согласно установленным правилам.

4. Архивирование данных.

Пока специалисты занимаются устранением инцидента, система сохраняет всю необходимую информацию, полученную во время обнаружения атаки. Эти данные впоследствии пригодятся для проведения расследований, изучения долгосрочных угроз либо поиска скрытых уязвимостей.

Использование базы знаний MITRE ATT&CK в работе с системами EDR на базе ИИ дает большое преимущество. ИИ помогает делать процесс поиска угроз проще, основываясь на том, что уже известно о методах и тактиках, упомянутых в матрице MITRE ATT&CK. Это значит, что системы EDR могут самостоятельно учиться на больших объемах данных об атаках, замечая закономерности и предугадывая возможные направления атак еще до их начала. Такой подход не только увеличивает скорость и точность нахождения угроз, но также значительно снижает количество ложных срабатываний обеспечивая тем самым более высокий уровень безопасности [5].

В работе оно проходит через следующие основные этапы: сбор сведений с клиентских устройств, анализ полученных данных, уведомления о подозрительных событиях, архивирование данных [7].

Нами был реализован эксперимент, по сравнению эффективности поиска и анализа атаки человеком и искусственным интеллектом. Целью эксперимента, оценить различия в скорости и анализа кибератаки человеком-аналитиком и системой на основе искусственного интеллекта.

На первом этапе была разработана виртуальная инфраструктура, имитирующая реальный критически важный объект. (промышленная система управления технологическими процессами). Потом произведены симуляция реалистичных кибератак различной степени сложности (от простых попыток несанкционированного доступа до сложных целевых атак).

Следующий этап, это наблюдение, анализ и измерение данных. Мы запускали два парал-

лельных сценария анализа: человек-аналитик и система искусственного интеллекта.

Первый это человек-аналитик по информационной безопасности. Специалист по кибербезопасности проводил ручной анализ журналов безопасности, использовал традиционные инструменты мониторинга и реагировал на сигналы тревоги.

Второй процесс, это система искусственного интеллекта (ИИ). Использовалась специализированная система EDR (Endpoint Detection and Response) с элементами искусственного интеллекта, настроенной на непрерывный мониторинг и автоматический анализ поведения системы.

Потом происходит сбор метрик. Идет регистрация временных показателей каждого этапа анализа и фиксации момента обнаружения атаки каждым участником.

Основные критерии, по которым будем анализировать.

• Время обнаружения атаки (от начала атаки до первого сигнала тревоги).

• Скорость идентификации типа атаки (время от сигнала тревоги до точной квалификации атаки).

• Качество анализа (точность определения причины и масштаба атаки).

• Эффективность реакции (скорость принятия контрмер и локализации угрозы).

По результатам эксперимента была составлена следующая таблица сравнительного анализа поиска и анализа атаки человеком и искусственным интеллектом (Таблица 1).

Таблица 1. Сравнительная характеристика

Тип анализа	Среднее время обнаружения человеком (мин.)	Среднее время обнаружения ИИ (сек.)
Предварительная разведка	135	11
Первичный мониторинг сети	60	5
Идентификация подозрительной активности	186	15
Выявление начальной фазы атаки	240	20
Определение типа атаки	360	30
Локализация вторжения	480	45
Оценка ущерба	600	60
Реакция и блокировка атаки	720	90

ИИ показал существенное превосходство по скорости обнаружения и анализа атаки практически на каждом этапе.

Наиболее заметное ускорение наблюдалось на этапах предварительной разведки, первичного мониторинга и идентификации подозрительной активности.

Несмотря на высокую производительность ИИ, этап полной ликвидации атаки занял чуть больше времени, поскольку финальная реакция зачастую требует подтверждения оператором-человеком.

Качество анализа и точность диагностики оказались выше у ИИ-системы, что позволило сократить среднее время восстановления работоспособности объекта.

Таким образом, эксперимент подтвердил гипотезу о существенном преимуществе искусственного интеллекта перед традиционными методами анализа и реагирования на кибератаки, особенно в условиях критически важных объектов, где каждая минута задержки имеет решающее значение.

Искусственный интеллект играет важную роль в современных системах EDR. Он помогает находить и реагировать на угрозы в реальном времени. С помощью машинного обучения и глубокого обучения, системы EDR на базе ИИ могут обрабатывать большие объемы данных с конечных устройств. Это позволяет обнаруживать даже самые сложные атаки, которые раньше могли оставаться незамеченными [10].

Одно из главных преимуществ ИИ в EDR – это его способность учиться и адаптироваться. Традиционные системы часто используют заранее заданные сигнатуры или шаблоны поведения, что делает их менее эффективными против новых угроз. В отличие от них, ИИ может изучать поведение и, основываясь на прошлых данных, настраивать свои модели для выявления новых типов атак. ИИ также улучшает процесс классификации и приоритезации угроз. Системы могут автоматически оценивать уровень риска и определять, какие угрозы наиболее важны. Это особенно полезно в контексте матрицы MITRE ATT&CK, которая содержит информацию о тактиках и методах, используемых злоумышленниками [11].

Интеграция ИИ с этой матрицей помогает системам EDR точно определить, какие атаки

произошли или могут произойти, и предлагает лучшие стратегии реагирования. В целом, ИИ значительно улучшает эффективность EDR. Он помогает справляться с современными угрозами и предсказывать будущие атаки. Интеграция ИИ с матрицей MITRE ATT&CK дает специалистам по кибербезопасности мощный инструмент для защиты организаций.

Заключение

Внедрение EDR на основе ИИ представляет собой революционный подход к защите компаний от современных угроз. Эта технология ключевой элемент стратегии защиты, соответствующей стандартам MITRE ATT&CK. Использование ИИ в EDR также значительно увеличивает скорость реагирования на инциденты, позволяя быстро идентифицировать атаки. Решение также помогает эффективно противодействовать угрозам в автоматическом режиме. Это освобождает ресурсы команды безопасности, давая возможность сосредоточить внимание на более важных задачах. Кроме того, интеграция EDR на основе ИИ с матрицей MITRE ATT&CK позволяет организациям детально прослеживать векторы атак и анализировать тактики противника, что является сильным инструментом при планировании защиты. В итоге, применение EDR на основе ИИ в контексте MITRE ATT&CK обеспечивает комплексное и глубокое понимание угроз, повышая общий уровень безопасности организаций. Внедрение и постоянное развитие EDR на основе ИИ является ключевой стратегией для тех организаций, которые стремятся не просто справиться с современными угрозами, но и предвосхитить их, обеспечивая надежную защиту своих цифровых активов.

Список литературы:

[1] Reiber, J. MITRE ATT&CK for dummies: AttackIQ Special Edition / J. Reiber, C. Wright. — 2021. — 42 p.

[2] Пашаев Ф. Г. Разработка программно-технических средств защиты технологических процессов от киберугроз / Ф. Г. Пашаев, Д. И. Зейналов, Г. Т. Наджафов // Проблемы информационной безопасности. Компьютерные системы. — 2024. — № 2 (59). — С. 104–116.

[3] Кривчун Н. А. Кибератаки и методы их предотвращения в информационных системах / Н. А. Кривчун, Д. В. Солодовников, А. К. Соколов и др. // Дискуссия. — 2024. — № 7 (128). — С. 120–126.

[4] Беляева О. Н. Значение и роль кибербезопасности в современном мире / О. Н. Беляева, К. М. Малышева // Reports Scientific Society. — 2024. — № 2 (46). — С. 5–8.

[5] Горда М. Д. Модель расследования киберпреступлений / М. Д. Горда, А. А. Чечулин // Информатизация и связь. — 2023. — № 3. — С. 92–97.

[6] Васильев В. И. Искусственный интеллект: история в лицах / В. И. Васильев. — 2-е изд., доп. — Москва: Машиностроение, 2015. — 111 с.

[7] Гибадуллин А. А. Мифы и легенды искусственного интеллекта / А. А. Гибадуллин // Академическая публицистика. — 2024. — № 1–1. — С. 553–556.

[8] Зуфарова А. С. Путь искусственного интеллекта: от компьютерной игры до средств познавательного развития учащихся ChatGPT / А. С. Зуфарова, А. В. Самойлов, М. Р. Мулявка и др. // Управление образованием: теория и практика. — 2023. — № 7 (65). — С. 76–90.

[9] Шевченко А. В. Защита искусственного интеллекта и объяснимого искусственного интеллекта от состязательных атак / А. В. Шевченко, А. Н. Аверкин // Мягкие измерения и вычисления. — 2024. — Т. 85, № 12. — С. 103–113.

[10] Пикалов П. А. Кибермошенничество с использованием искусственного интеллекта / П. А. Пикалов // Актуальные вопросы борьбы с преступлениями. — 2024. — № 2. — С. 56–59.

[11] Аланурова О. Цифровая безопасность и инновационные подходы к защите данных / О. Аланурова, Дж. Шохрадова // Символ науки: международный научный журнал. — 2024. — Т. 2, № 12–1. — С. 67–68.

[12] Маленков М. Г. Защита от атак с использованием ИИ с помощью ИИ / М. Г. Маленков // Инновации. Наука. Образование. — 2021. — Т. 2, № 44. — С. 49–53.

References:

[1] Reiber, J. MITRE ATT&CK for dummies: AttackIQ Special Edition / J. Reiber, C. Wright. — 2021. — 42 p.

[2] Pashayev, F. G. Development of software and hardware tools to protect technological processes from cyber threats / F. G. Pashayev, D. I. Zeynalov, G. T. Nadzhafov // Problems of information security. Computer systems. — 2024. — No. 2 (59). — P. 104–116.

[3] Krivchun, N. A. Cyberattacks and methods for their prevention in information systems / N. A. Krivchun, D. V. Solodovnikov, A. K. Sokolov, et al. // Discussion. — 2024. — No. 7 (128). — P. 120–126.

[4] Belyaeva O. N. The meaning and role of cybersecurity in the modern world / O. N. Belyaeva, K. M. Malysheva // Reports Scientific Society. - 2024. - No. 2 (46). — P. 5–8.

[5] Gorda M. D. Model for investigating cybercrimes / M. D. Gorda, A. A. Chechulin // Informatization and communication. - 2023. - No. 3. - P. 92–97.

[6] Vasiliev V.I. Artificial intelligence: history in faces / V.I. Vasiliev. — 2nd ed., add. — Moscow: Mechanical Engineering, 2015. — 111 p.

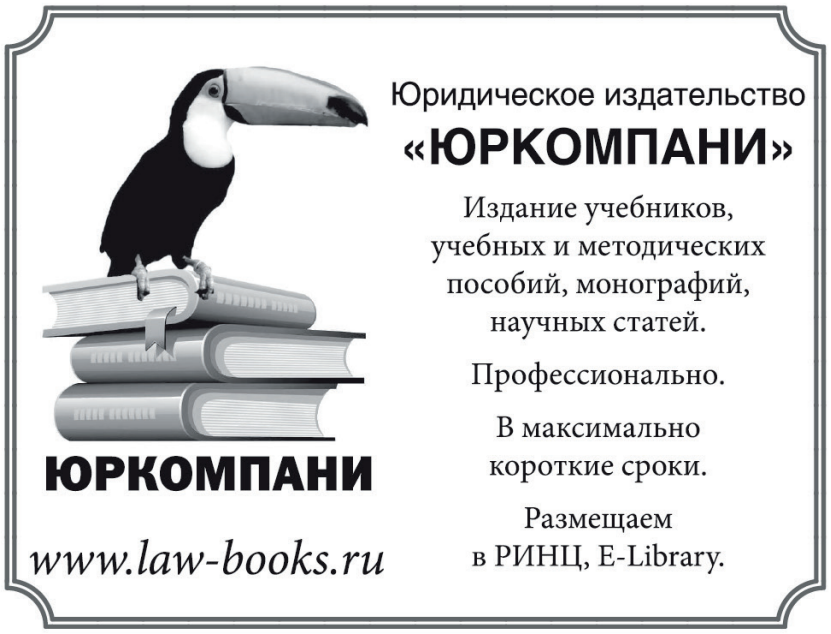
[7] Gibadullin A. A. Myths and legends of artificial intelligence / A. A. Gibadullin // Academic journalism. — 2024. — No. 1–1. — P. 553–556.

[8] Zufarova A. S. The Path of Artificial Intelligence: From a Computer Game to Means of

Cognitive Development of Students ChatGPT / A. S. Zufarova, A. V. Samoilov, M. R. Mulyavka, et al. // Education Management: Theory and Practice. — 2023. — No. 7 (65). — P. 76–90.

[9] Shevchenko A. V. Protecting Artificial Intelligence and Explainable Artificial Intelligence from Adversarial Attacks / A. V. Shevchenko, A. N. Averkin // Soft Measurements and Computations. — 2024. — Vol. 85, No. 12. — P. 103–113.

[10] Pikalov P. A. Cyberfraud Using Artificial Intelligence / P. A. Pikalov // Current Issues in Combating Crime. - 2024. - No. 2. - Pp. 56-59.

[11] Alanurova O. Digital Security and Innovative Approaches to Data Protection / O. Alanurova, J. Shokhradova // Symbol of Science: International Scientific Journal. - 2024. - Vol. 2, No. 12-1. - Pp. 67-68.

[12] Malenkov M. G. Defense against AI-Using Attacks with AI / M. G. Malenkov // Innovations. Science. Education. - 2021. - Vol. 2, No. 44. - Pp. 49-53.