

## ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СРЕДСТВАХ ЗАЩИТЫ ИНФОРМАЦИИ

**Степанов М.О., магистрант 1 курса института компьютерных  
технологий и защиты информации**

**Научный руководитель – Шарипов Р.Р., кандидат технических  
наук, доцент**

**Казанский национальный исследовательский технический  
университет им. А.Н. Туполева – КАИ**

***Ключевые слова:** искусственный интеллект, информационная  
безопасность, защита информации, автоматизация.*

*В данной статье рассматривается применение искусственного  
интеллекта в средствах защиты информации и его влияние на  
автоматизацию процессов и повышение эффективности.*

**Введение.** Современные угрозы информационной безопасности требуют применения инновационных подходов для защиты данных, как персональных, так и критически важных для предприятия, а также защиты корпоративных и технологических сетей. Сейчас особенно выделяется использование искусственного интеллекта в средствах защиты информации. Искусственный интеллект является «помощником» при выполнении рутинных задач, также при его использовании можно автоматизировать процессы анализа угроз, обнаружения вторжений, аномалий, тем самым увеличивая эффективность систем безопасности[1].

**Цель работы.** Целью данной работы является анализ применения искусственного интеллекта в современных средствах защиты информации, а также оценка эффективности решений, использующих ИИ для автоматизации процессов в области информационной безопасности.

**Результаты исследований.** Искусственный интеллект активно применяется в различных средствах защиты информации. В частности, решения класса SOAR, такие как SplunkPhantom, IBMResilient,

PaloAltoCortexXSOAR и SecurityVision активно используют ИИ для автоматизации реагирования на инциденты. Эти системы анализируют большие объемы данных, включая тактики и техники, применяемые злоумышленниками по матрице MITREи БДУ ФСТЭК (SecurityVision), а также выявляют угрозы и автоматически принимают решения, основанные на плейбуках. Встроенный ИИ в SOARсистему отечественного производителя SecurityVisionнеобходим для анализа вердиктов инцидентов и помощи в управлении новыми задачами, система анализирует все инциденты и состояния их жизненного цикла для определения возможных ложно-положительных срабатываний (FalsePositive) и снижения нагрузки на персонал. Благодаря этому функционалу система позволяет сократить время реагирования и минимизировать человеческий фактор[2].

Еще одним кейсом является применения ИИ в межсетевых экранах. Одним из наиболее интересных решений является продуктCloudflare главным отличием от других является наличие ИИ помощника – ассистента, который помогает писать правила на межсетевом экране при формировании запроса внутри платформы. аналитиком по информационной безопасности [3]. Один из примеров простого правила (Рис.1)

The screenshot shows the 'AI Assistant' interface in the Cloudflare dashboard. At the top, there's a header 'AI Assistant' with a 'Beta' badge and a close button. Below it, a 'New!' notification states: 'AI features on the Cloudflare Dashboard may provide inaccurate responses. Consider checking results before taking action. If you found these results useful or if they could use improvement, let us know!'. The main area has a text input field containing 'Match requests with a low bot score'. Below this, it says 'Try some example prompts:' followed by two buttons: 'Match all POST requests to /admin' and 'Match all requests from the UK'. Another button 'Match requests with a low bot score' is highlighted. Under 'Your rule explained', it says: 'Use cf.bot\_management.score to match bot scores, paired with the lt operator to match scores less than 30.' Below this, a section 'When incoming requests match...' contains a table with three columns: 'Field', 'Operator', and 'Value'. The 'Field' column has a dropdown menu with 'Bot Score' selected. The 'Operator' column has a dropdown menu with 'less than' selected. The 'Value' column has a text input field with '30' entered, and a note 'e.g. 5' below it. At the bottom, there's an 'Expression Preview' section showing the rule expression '(cf.bot\_management.score lt 30)' and an 'Edit expression' link. Finally, there are 'Discard' and 'Apply Rule' buttons at the very bottom.

Рис. 1. Правило «Сопоставление запросов с низким рейтингом»

**Выводы.** Применение искусственного интеллекта в средствах защиты информации открывает новые возможности для повышения эффективности систем безопасности. ИИ позволяет автоматизировать процессы анализа угроз, обнаружения аномалий и принятия решений, что значительно снижает время реагирования и повышает точность. Продукты, использующие ИИ, такие как SOAR-платформы, решения для генерации правил межсетевых экранов и другие, демонстрируют высокую эффективность в борьбе с современными угрозами. Дальнейшее развитие технологий ИИ в области информационной безопасности будет способствовать созданию более надежных и интеллектуальных систем защиты.

### **Библиографический список:**

1. Гришаев, Д. А. Актуальные тренды и перспективы использования искусственного интеллекта в обеспечении информационной безопасности / Д. А. Гришаев // Наука и бизнес: пути развития. – 2024. – № 1(151). – С. 85-90. – EDNGMTQPX.<https://elibrary.ru/item.asp?id=65644770> (дата обращения: 24.02.2025). - Режим доступа: Научная электронная библиотека eLIBRARY.RU.
2. Искусственный интеллект в информационной безопасности[Электронный ресурс]. – Режим доступа:<https://www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti/>. (дата обращения: 25.02.2025).
3. AIEverywherewiththeWAFRuleBuilderAssistant, CloudflareRadarAllInsights, andupdatedAIbotprotection[Электронный ресурс]. – Режим доступа:<https://blog.cloudflare.com/bringing-ai-to-cloudflare/>. (дата обращения: 25.02.2025).

**THE USE OF ARTIFICIAL INTELLIGENCE IN INFORMATION  
SECURITY MEDIA**

**Stepanov M.O.**

**Scientific supervisor - Sharipov R.R.**

**Kazan National Research Technical University named after A.N.**

**Tupolev – KAI**

**Keywords:** *artificial intelligence, information security, information security, automation.*

*This article examines the use of artificial intelligence in information security tools and its impact on process automation and efficiency improvement.*