**Машинное обучение и ИИ в области информационной безопасности**

Рассмотрим некоторые из примеров использования машинного обучения и ИИ в области кибербезопасности. Одной из основных областей применения машинного обучения и ИИ в кибербезопасности является *обнаружение и анализ аномалий*. Традиционные методы обнаружения вторжений, основанные на правилах и сигнатурах, имеют свои ограничения и могут пропускать новые и неизвестные виды атак. Машинное обучение позволяет создавать модели, которые способны обнаруживать аномальное поведение и атаки, основываясь на анализе больших объемов данных. Например, алгоритмы машинного обучения могут проанализировать данные о сетевом трафике и выявить аномальные паттерны, указывающие на наличие вредоносных программ или атакующих. Это позволяет операторам безопасности принять меры по защите системы раньше, чем будет нанесен значительный ущерб. А еще, машинное обучение и ИИ позволяют автоматизировать процессы обработки угроз и реагирования на инциденты безопасности. *Спам-сообщения* электронной почты стали неотъемлемой частью нашей повседневной жизни, системы машинного обучения могут классифицировать входящие электронные письма на основе их содержимого и метаданных, определять, является ли письмо спамом или содержит вредоносные вложения. Они могут обнаружить ключевые слова, фразы и синтаксические особенности, чтобы точно определить, является ли письмо спамом или нет. Так, например, в системе *AVSOFT KAIROS*, с использованием методов машинного обучения, выделяются ключевые слова, характерные для фишинга, а также определяется не только класс, но и категория письма, что обеспечивает эффективную защиту от нежелательной почты и мошенничества. *Рис 1. Пример отчета ML из системы AVSOFT KAIROS*



Рис 1. Пример отчета ML из системы AVSOFT KAIROS

 Методы обработки текстов на естественном языке (Natural Language Processing, NLP), используемые в AVSOFT ATHENA и AVSOFT KAIROS позволяют обнаружить тайпсквоттинг (англ. typosquatting ← typo опечатка + cybersquatting), поддельные домены и мимикрию под легитимные сайты. *Рис 2. Пример отчета по тайпсквоттингу из системы AVSOFT KAIROS*



Рис 2. Пример отчета по тайпсквоттингу из системы AVSOFT KAIROS



Рис 3. Пример отчета с поддельным сайтом авторизации из системы AVSOFT KAIROS

AVSOFT KAIROS применяет алгоритмы компьютерного зрения для распознавания поддельных веб-сайтов. Он анализирует визуальные элементы, такие как логотипы и макеты страниц, и сравнивает их с базой данных подлинных ресурсов.

Если AVSOFT KAIROS [https://avsw.ru/products/mail-gateway/kairos] обнаруживает подозрительные отличия, он предупреждает пользователя о возможной фишинговой атаке и блокирует доступ к подозрительным сайтам. *Рис 3. Пример отчета с поддельным сайтом авторизации из системы AVSOFT KAIROS*
Заключение

Применение ИИ в спам-фильтрации, борьбе с фишингом, обнаружении вторжений и анализе больших данных позволяет повысить эффективность защиты информации и обеспечить безопасность цифровых систем.
Для того чтобы справиться с рисками и ограничениями, связанными с машинным обучением и ИИ в области информационной безопасности, необходимо применять многоуровневую защиту. Важно комбинировать методы машинного обучения с традиционными методами обнаружения и предотвращения атак.