ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

САХНО Виталий Викторович
магистрант
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

В бурный этап развития информационных технологий, таких как, искусственный интеллект и машинное обучение, они широко применяются в информационных системах для увеличения эффективности труда и повышения продаж. Уже сейчас их применения в защите от киберпреступников становится одним из главных направлений в сфере информационной безопасности.
Ключевые слова: искусственный интеллект, информационная безопасность, киберприступники, уязвимость, атака.

В настоящее время чисто атак с быстрой скоростью увеличивается, а способы проявления угроз меняется. Например, компания Kaspersky, утверждает, что их продукт отражают более 700 млн онлайн-атак в квартал (2019 г.), а компания Cisco заявляет о блокировании более 20 млрд сетевых атак в день (за 2018 г.) [1]. При таких больших объёмах вредоносных программ, злоумышленники уже стали часто использовать средства автоматизации атак, и уже на сегодняшней день были зафиксированы случаи применения искусственного интеллекта обучения для их обновления и изменения под проявляющие средства защиты информации.

Так, уже в 2019 г. мировой рынок технологий искусственного интеллекта в сфере информационной безопасности оценивается в $8 млрд и с ежегодным ростом на 23% [2].

Эффективным прототипом использования искусственного интеллекта является известный троян Emotet [3]. Одним из каналов его распространения является спам-фишинг, а обновленная версия может передаваться через Wi-Fi и заражать все подключенные устройства. Группировка лиц, которая создала троян Emotet, использовала искусственный интеллект для усиления эффективности атаки, использовала в цепочке разговора анализ текста на естественном языке.

Еще одной областью использования искусственного интеллекта в корыстных целях является быстрый подбор паролей или обход двухфакторной аутентификации. Примерно, два года назад исследователи создали бота, который мог обходить проверки «CAPTCHA» с вероятностью на 90% с помощью искусственного интеллекта [4].

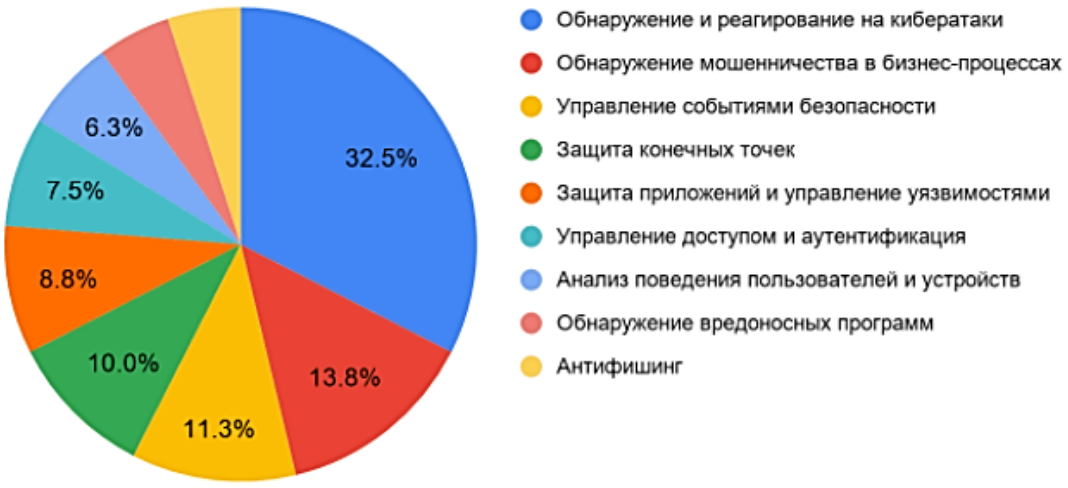

Рисунок 1. **Сценарии использование технологий искусственный интеллект**

Помимо использование искусственного интеллекта в злых целях, он также стал применяться для построения мощных систем защиты информации, далее разберем их (рисунок 1) [5]:

1. EDR (Endpoint Detection and Response) – платформы для обнаружения атак на рабочих станциях, которые могут оперативного реагирования на них. С помощью искусственного интеллекта они могут обнаруживать неизвестные вредоносные программы и автоматически классифицировать их по типу угрозы, а также самостоятельно реагировать на них. Система принимает решения на основе общей базы знаний. Некоторые продукты могут использовать искусственный интеллект для разметки расположения данных на конечных точках и контролировать любое их перемещения, чтобы выявлять внутренние угрозы.

2. NDR (Network Detection and Response) – устройства, а так могут применяться в виде платформы, которые обнаруживают сетевые атаки и оперативно на них реагируют. При использовании статистики и базы знаний об угрозах, продукты выявляют с помощью искусственного интеллекта угрозы в сетевом трафике и могут автоматически на них реагировать, изменяя конфигурацию сетевых устройств и шлюзов. Часть продуктов также специализируется на защите облачных технологий.

3. UEBA (User and Entity Behavior Analytics) – система, которая позволяет проводить анализ действий пользователей и информационных объектов. Она обнаруживает случаи аномального поведения и используют их для детектирования внутренних и внешних угроз. Основной сценарий применения искусственного интеллекта в продуктах UEBA – это автоматическое выявление аномалий в поведенческих моделях для пользователей и различных объектов информационных систем. Выявление анормальностей в поведение может выявляться в целях мониторинга и управления доступом, обнаружения мошенничества среди клиентов или сотрудников для защиты конфиденциальных данных и коммерческой тайны, а также для проверки соблюдения тех или иных требований политики безопасности и нормативных актов.

4. TIP (Threat Intelligence Platform) – платформы раннего предотвращения угроз и реагирования на них, которые работают на основе большого количества различного рода данных и индикаторов компрометации. Использования искусственного интеллекта позволяет увеличить эффективность обнаружения неизвестных угроз на ранних этапах их зарождения; сценарий чем-то схож с работой SIEM-систем, но только нацелен на внешние источники данных и внешние угрозы.

5. SIEM (Security Information and Event Management) – система, которая осуществляет мониторинг действия пользователей и информационных систем, в реальном времени анализируя события безопасности, направленных от сетевых устройств, средств защиты информации, сервисов, приложений. В системах данного типа накапливается большое количество данных из различных источников, а использования искусственного интеллекта даёт возможность выявления аномалий разными методами и сокращать ложные. Использования технологий искусственного интеллекта в SIEM-системах позволяет использовать высокого уровня автоматизации.

6. SOAR (Security Orchestration and Automated Response) – системы, которые могут обнаруживать угрозы безопасности и автоматически реагирование на инциденты нужным способом.

7. Средства защиты приложений (Application Security) – системы, которые позволяют выявить угрозы безопасности в прикладных приложениях и управлять мониторингом и устранением этих угроз. Основной сценарий применения искусственного интеллекта в системах защиты – это автоматический сбор информации об уязвимостях, атаках и заражениях, которые были допущены в открытых источниках.

8. Антифрод (Antifraud) – системы, которая позволяет выявлять угрозы в бизнес-процессах и реагировать на мошеннические операции в режиме реального времени на начальных этапах. В системах защиты от мошенничества искусственный интеллект применяется для выявления отклонений от установленных бизнес-процессов, тем самым

быстро реагировать на возможное финансовое преступление или уязвимость процессов. Применение искусственного интеллекта в таких системах всегда актуально, так как дает возможность быстро адаптироваться к изменению логики в бизнес-процессе.

СПИСОК ЛИТЕРАТУРЫ

1. Применение технологий искусственного интеллекта в информационной безопасности. – URL: https://www.anti-malware.ru/analytics /Technology_Analysis/using-artificial-intelligence-technologies-in-information-security (дата обращения 01.02.2021).
2. Искусственный интеллект (мировой рынок). – URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_(мировой_рынок) (дата обращения 01.02.2021).
3. *Тугенгольд А.К., Лукьянов Е.А., Волошин Р.Н., Бонилья В.Ф.* Интеллектуальная система мониторинга и управления техническим состоянием мехатронных технологических объектов // Вестник Донского государственного технического университета. – 2020. – № 20(2). – С. 188-195. – URL:https://doi.org/10.23947/1992-5980-2020-20-2-188-195.
4. Применение нейронных сетей для распознавания Captcha. – URL: https://istina.fnkcrr.ru/diplomas/coursework/162144908// (дата обращения 01.02.2021).
5. *Суханов А.В.* Разработка теоретических основ и методологии мониторинга безопасности информационных систем для критических сфер применения: дис. … доктора технических наук. – СПб, 2010.

USE OF INTELLIGENT SYSTEMS TO ENSURE INFORMATION SECURITY

SAKHNO Vitaly Viktorovich
undergraduate
Don State Technical University
Rostov-on-Don, Russia

In the turbulent stage of development of information technologies, such as artificial intelligence and machine learning, they are widely used in information systems to increase labor efficiency and increase sales. Already, their application in protection against cybercriminals is becoming one of the main directions in the field of information security.
Key words: artificial intelligence, information security, cyber attackers, vulnerability, attack.