Кривоногова Анастасия Евгеньевна,

студентка 3-го курса;

Зарипова Римма Солтановна,

канд. техн. наук, доцент,

ФГБОУ ВО «Казанский государственный энергетический университет»,

г. Казань. Республика Татарстан, Россия

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Большинство продуктов по обеспечению безопасности ориентированы исключительно на устранение вредоносных программ. Но, как известно, количество опасных беспилотных атак растет с арифметической прогрессией: ежегодно добавляются миллионы. В статье рассмотрен вопрос о возможностях искусственного интеллекта и машинного обучения в решении проблемы уменьшения площади атаки.

Ключевые слова: искусственный интеллект, машинное обучение, информационная безопасность.

Искусственный интеллект и машинное обучение могут помочь специалистам в области ИТ-безопасности достичь более высокого уровня защищенности данных. По статистике, организации тратят около 100 млрд долларов на огромное множество программных продуктов, обеспечивающих безопасность систем [4]. Однако никто из главных сотрудников компании не может быть уверен, что она не подвергается высокой опасности и не уязвима.

Искусственный интеллект (ИИ) и машинное обучение могут предложить специалистам в области ИТ-безопасности способ применения хороших методов обеспечения кибербезопасности и уменьшить степень поверхности атаки [1].

Существует множество причин, по которым информационная безопасность постоянно находится под угрозой. Основной из них является то, что злоумышленники находят уязвимости и новые способы атаки с огромной скоростью [2].

Большинство продуктов по обеспечению безопасности ориентированы исключительно на устранение вредоносных программ. Но, как известно,

количество опасных беспилотных атак растет с арифметической прогрессией: ежегодно добавляются миллионы. Может ли искусственный интеллект и машинное обучение помочь уменьшить площадь атаки?

Большинство утверждает, что искусственный интеллект может решить данную проблему и значительно повысить уровень информационной безопасности [5]. Не существует сомнений в том, что искусственный интеллект действительно нашел своё применение во многих сферах деятельности и облегчил выполнение ряда задач, таких как обнаружение объектов в изображениях и видео, распознавание речи, обработка естественного языка, беспилотные автомобили, игры, здравоохранение и многое другое.

Но для использования машинного обучения в области кибербезопасности недостаточно выполнение отведённых заранее алгоритмов с минимальной погрешностью весов. Невозможно задать начальную базу, которая смогла бы стать основой для глубокого обучения в виду большого количества уникальных случаев нападения. Следует учесть три главных фактора:

- постоянно растущее количество исключительных случаев;
- отсутствие определенных правил вторжения в системы;
- огромное количество несортированных данных о методах и способов атак.

На данный момент возможности обработки данных искусственным интеллектом имеют наибольшую ценность для следующих областей информационной безопасности [3]:

1) анализ и исследование: машинное обучение может быстро определить характер атаки, её распространение и влияние на систему;

2) готовность к угрозе: искусственный интеллект может обрабатывать более 100 ТБ данных ежедневно для определения наиболее вероятных угроз для организации;

3) диагностика: искусственный интеллект может постоянно контролировать данные и находить отклонения в рабочих процессах.

Методы искусственного интеллекта с каждым днем становятся актуальнее и идеально подходят для достижения информационной безопасности и сокращения количества атак в том случае, если учесть все особенности поставленной задачи.

СПИСОК ЛИТЕРАТУРЫ

1. Бикмухаметов И.И. Кибертерроризм как угроза информационной безопасности / И.И. Бикмухаметов, Р.С. Зарипова // Аллея науки. – 2018. – Т.1. – №2(18). – С. 266-268.

2. Злыгостев Д.Д. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий / Д.Д. Злыгостев, Р.С. Зарипова / Инновации в информационных технологиях, машиностроении и автотранспорте: Сборник материалов Международной научно-практической конференции. – Кемерово, 2017. – С. 23-25.

3. Кривоногова А.Е. Проблемы и перспективы развития индустрии искусственного интеллекта / А.Е. Кривоногова, Р.С. Зарипова // Аллея науки. – 2018. – Т.3. – №1(17). – С. 869-871.

4. Салтанаева Е.А. Методика управления информационными технологиями на предприятиях и в организациях / Е.А. Салтанаева, Р.И. Эшелиоглу // Аллея науки. – 2018. – Т.1. – №2(18). – С. 330-333.

5. Хайруллин А.М. Концепция и методы инженерно-технической защиты информации / А.М. Хайруллин, Р.С. Зарипова // Аллея науки. – 2018. – Т.1. – №2(18). – С. 290-293.

6. Шакиров А.А. Обеспечение информационной безопасности организаций / А.А. Шакиров, Р.С. Зарипова // Аллея науки. – 2018. – Т.3. – №1(17). – С. 841-843.

7. Шакиров А.А. Актуальность обеспечения информационной безопасности в условиях цифровой экономики / Шакиров А.А., Зарипова Р.С. / Инновационное развитие экономики. Будущее России: Сборник материалов и докладов V Всероссийской (национальной) научно-практической конференции. – 2018. – С. 257-260.