УДК 004.056

М.П. КАРПЕНКО, А.Ю. СИМАЧЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА В SIEM- И SOAR-СИСТЕМАХ ДЛЯ ПОВЫШЕНИЯ ИХ РЕЗУЛЬТАТИВНОСТИ В УПРАВЛЕНИИ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Исследована возможность применения искусственного интеллекта (ИИ) в SIEM-системах и SOAR-системах в целях повышения их результативности в управлении инцидентами информационной безопасности (УИИБ). Проанализированы актуальные области применения ИИ в рамках SIEM и SOAR.

Исследуется применимость ИИ в системах управления информационной безопасностью (SIEM) и автоматизации реакции на инциденты (SOAR) для повышения результативности систем SIEM и SOAR в решении задач обеспечения информационной безопасности (ИБ).

Новизна проведенного исследования заключается в интеграции различных подходов использования ИИ на всех этапах управления инцидентами ИБ.

Цель исследования состоит в определении применимости ИИ для создания типологии инцидентов ИБ, создания правил сработки систем обнаружения инцидентов ИБ и их автоматического преобразования в формализованное описание. Такие системы способны обрабатывать данные и выполнять задачи значительно быстрее, чем любой человек, что позволяет повысить общую производительность и безопасность труда. В частности, в области ИБ технологии ИИ предоставляют возможность создавать решения существенно более высокой эффективности [1].

В данном исследовании проведен анализ возможности использования ИИ с целью генерации потенциальных сценариев инцидентов ИБ. Далее планируется разработать алгоритмы и модели, способные анализировать агрегированные данные в системе SIEM, SOAR и на основе этого анализа предсказывать возможные угрозы ИБ. Применение ИИ в SIEM-системах позволяет достигнуть очень высокого уровня автоматизации. В отличие от SIEM, ИИ в SOAR помогает не только проводить анализ угрозы информационной безопасности, но и автоматически реагировать на них надлежащим образом.

Важной частью анализа данных является определение наиболее эффективные стратегий реагирования на инциденты, основанных на

информации о состоянии SOAR и SIEM систем. Также определена ключевая роль специалистов по ИБ и ИИ в совместной разработке правил и стратегий реагирования.

В исследовании определена и обоснована необходимость внедрения различных ИИ на разных этапах обработки инцидентов ИБ [2], что подчеркивает важность совместного взаимодействия человеческого и искусственного интеллекта в этой области.

В настоящее время количество атак продолжает расти, а ландшафт угроз меняется с молниеносной скоростью, поэтому особое внимание уделено интеграции ИИ в системы управления инцидентами информационной безопасности (SIEM) и автоматизации управления инцидентами (SOAR) с целью повышения эффективности их работы, основанной на автоматизации процессов обнаружения и управления инцидентами ИБ, снижению времени реагирования на инциденты. Дает возможность сотруднику ИБ рассматривать угрозы, исключая ошибки второго рода (ложная сработка), что снижает нагрузку на системы и персонал [3].

Результатами применения ИИ для формулировки и разработки правил и стратегий реагирования на инциденты ИБ, стало снижение времени реагирования на инциденты, повышение эффективности в расследовании ИБ-инцидентов, обнаружение угроз, уменьшение ложных сработок рассматриваемых специалистом. Исходя из данных о текущем состоянии системы, ИИ смог предположить о новых возможных угрозах.

Список литературы

1. Артамонов В.А., Артамонова Е.В. Искусственный интеллект в системах безопасности // Защита информации. Инсайд. – 2022. – № 5. – С. 2–11.

2. ИИ в ИБ // хакер.ru [Электронный ресурс]. – URL: https://xakep.ru/2021/07/21/nn-in-ib/

3. MaxPatrol O2 // ptsecurity.com [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/products/mp-o2/#how-the-meta-product-works