УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РЕШЕНИИ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ

А. С. Кечеджиев, О. Л. Цветкова
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. В последнее время наблюдается нехватка специалистов в области защиты информации. При этом организации задействуют все больше цифровых устройств и методов обработки информации, то есть растет число потенциально уязвимых объектов. Для решения этих проблем развиваются средства искусственного интеллекта. В статье показаны возможности его применения в целях обеспечения кибербезопасности. Однако у искусственного интеллекта есть собственные уязвимости, что необходимо учитывать, создавая и обслуживая информационные системы. Авторы предлагают алгоритм разработки и отладки методики, эффективной при использовании искусственного интеллекта в рассматриваемой сфере.

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

ARTIFICIAL INTELLIGENCE IN SOLVING CYBER SECURITY TASKS

Aleksandr S. Kechedzhiev, Olga L. Tsvetkova
Don State Technical University (Rostov-on-Don, Russian Federation)

Abstract. Recently, there has been a shortage of specialists in the field of information security. At the same time, organizations are using more and more digital devices and information processing methods, that is, the number of potentially vulnerable objects is growing. To solve these problems, artificial intelligence tools are being developed. The article shows the possibilities of its application in order to ensure cybersecurity. However, artificial intelligence has its own vulnerabilities, which must be taken into account when creating and maintaining information systems. The authors propose an algorithm for developing and debugging a technique that is effective when using artificial intelligence in the area under consideration.

Keywords: artificial intelligence, machine learning, cyber security, cyber threats, information security.

Введение. Киберпреступность — один из самых быстроразвивающихся видов экономической преступности [1]. Постоянно совершенствуются информационные и цифровые технологии, растет квалификация злоумышленников. Возникает необходимость в создании современных методов защиты информации, обеспечивающих требуемый уровень защищенности от новых угроз. Для этих целей хорошо подходят методы защиты, основанные на использовании искусственного интеллекта.

Наблюдаемый в настоящее время технологический скачок вызван достижениями в сфере искусственного интеллекта, в частности глубокого машинного обучения [2–4]. Последние разработки превосходят возможности человеческого мозга в решении таких задач, как распознавание изображений, обработка естественного языка и анализ данных. Однако широкое корпоративное использование систем искусственного интеллекта имеет и отрицательные стороны. Оно открывает возможности манипулирования, что приводит к серьезным последствиям для

безопасности, например, сетевого мониторинга, финансовых систем и автономных транспортных средств. Этим обусловлена актуальность создания методов защиты информационных систем.

Цель исследования — анализ возможностей и проблем применения средств искусственного интеллекта при решении задач кибербезопасности. Для достижения цели ставились и решались следующие задачи:

– анализ областей внедрения методов искусственного интеллекта,

– исследование проблемы увеличения потенциально уязвимых объектов при внедрении средств искусственного интеллекта,

– разработка алгоритма внедрения средств искусственного интеллекта при реализации заявленной цели.

Основная часть

Современные проблемы кибербезопасности. Каждый год мировая цифровая инфраструктура интегрирует сотни миллионов гаджетов и устройств интернета вещей, а также более ста миллиардов новых строк программного кода. Несомненно, цифровые технологии и интеллектуальные устройства значительно улучшили качество обслуживания клиентов, повысили гибкость бизнеса и открыли эру цифровых инноваций. При этом растет число объектов киберугроз и векторов атак.

Ежегодные опросы свидетельствуют о нехватке специалистов по информационной безопасности и кибербезопасности [5]. Согласно исследованию аудиторской компании PricewaterhouseCoopers (PwC, «ПрайсвотерхаусКуперс», англ.), расходы предприятий и организаций на кибербезопасность будут расти. В 2021 году опрос 3,6 тыс. руководителей различных организаций, подразделений информационных технологий показал примерно равную заинтересованность в инвестициях в кибербезопасность в мире и в России. При этом 56 % респондентов считают, что увеличение числа нарушений информационной безопасности будет обусловлено проблемами программного обеспечения. Для России актуальны также атаки на облачные сервисы и взлом рабочей почты.

Назовем основные проблемы защиты корпоративной информации:

– региональные коммерческие и государственные площадки не обеспечивают требуемый уровень защиты;

– IT-специалисты не обладают нужной квалификацией, не совершенствуют протоколы безопасности;

– средства защиты и программное обеспечение не обновляются, что открывает возможности атаковать систему;

– персонал слабо подготовлен, не выполняет элементарных требований по безопасности;

– ведомства не выработали согласованную политику противодействия угрозам.

Искусственный интеллект в решении задач кибербезопасности. Машинное обучение обладает большим потенциалом для обеспечения кибербезопасности. Главные решения в этой сфере генерируются по известной схеме: кибераналитики обучают приложение, используя существующие данные.

Ниже перечислены основные задачи средств искусственного интеллекта в сфере кибербезопасности.

1. Обнаружение вторжений. Машинное обучение помогает фиксировать вторжения и защищаться от них.

2. Выявление уязвимостей в программном коде. Это относительно новая область применения искусственного интеллекта. Машинное обучение позволяет сканировать большие объемы программного кода и находить потенциальные уязвимости.

3. Дополнение аналитики угроз. Комбинируются традиционная аналитика (список известных угроз) и машинное обучение для обнаружения новых.

4. Поиск аномалий. Мошеннические действия могут быть помечены и предотвращены в режиме реального времени путем обнаружения закономерностей и выявления отклонений от ожидаемого базового поведения.

Отметим возможность дополнять и расширять подходы с помощью искусственного интеллекта. Это позволяет сократить время выявления, анализа и реагирования на угрозы.

Проблемы увеличения поверхности атаки при внедрении средств искусственного интеллекта. Атаки на системы искусственного интеллекта в основном связаны с путаницей в базовой модели машинного обучения и взломом защиты. Например, генеративные состязательные сети (разновидность искусственных нейронных сетей) могут обмануть систему распознавания лиц [6]. К тому же такие сети используют для атаки на речевые приложения и голосовые биометрические системы.

Отметим также, что, обманув систему искусственного интеллекта, вредоносный файл может быть ошибочно классифицирован как безопасный.

С распространением искусственного интеллекта растут риски информационной безопасности. Поэтому IT-специалистам необходимо:

– регулярно проводить анализ и аудит систем защиты с целью своевременного выявления новых рисков;

– разбираться в технологиях машинного обучения, особенностях функционирования приложений искусственного интеллекта;

– оценивать восприимчивость систем к атакам.

Одна из возможностей вредоносного использования искусственного интеллекта [7] — фишинг. Электронные письма персонализируются с помощью искусственного интеллекта. Это максимально повышает вероятность, что жертвы откроют письма и перейдут по небезопасным ссылкам.

Еще одна модель работы злоумышленников — выбор жертвы по вероятности «конверсии». Точно так же обычный маркетолог задействует искусственный интеллект для взаимодействия с целевой аудиторией.

Все эти риски могут возрасти при удаленной работе коллектива, когда персонал находится вне периметра безопасности организации. Задача снижения таких рисков стимулирует наем экспертов по искусственному интеллекту и машинному обучению.

На основе проведенного анализа авторы разработали алгоритм внедрения средств искусственного интеллекта для решения задач обеспечения кибербезопасности. Практическая реализация такого подхода обеспечит эффективное использование искусственного интеллекта в области защиты информации (рис. 1).

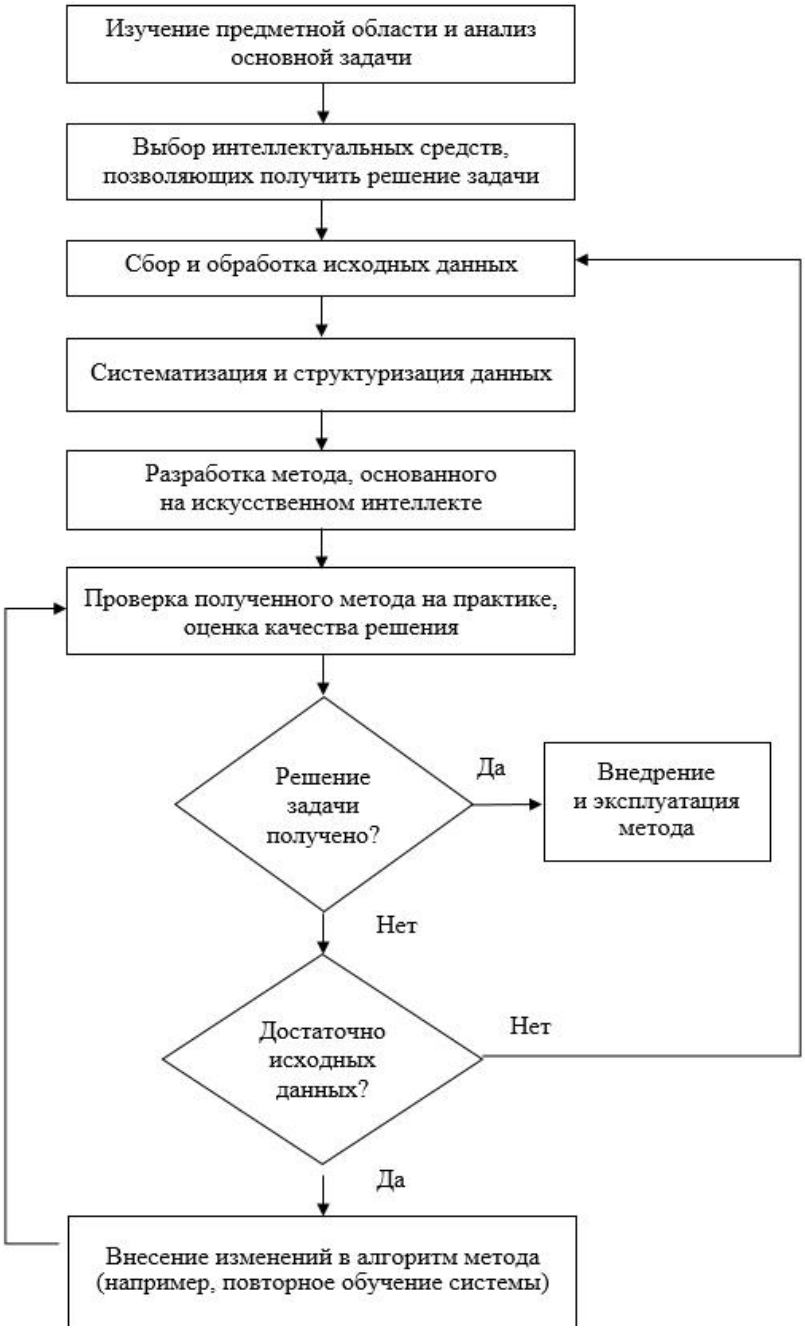

Рис. 1. Алгоритм внедрения средств искусственного интеллекта для решения задач обеспечения кибербезопасности

Итак, работа начинается с изучения предметной области и анализа основной задачи. Определяются средства, позволяющие получить решения задачи. Данные собираются, обрабатываются, систематизируются и структурируются. Затем создается метод, основанный на искусственном интеллекте. IT-специалисты обучают систему искусственного интеллекта для выполнения функций по защите информации.

Заключение. Обеспечение информационной безопасности — это непрерывное выявление и отражение киберугроз. Использование средств искусственного интеллекта позволяет предприятиям учитывать риски и работать на опережение.

Библиографический список

1. Приходько, Д. В. Киберпреступность как глобальная проблема современности / Д. В. Приходько, А. А. Белькова // Экономика и бизнес: теория и практика. — 2021. — № 4-2. — URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-globalnaya-problema-sovremennosti (дата обращения: 28.12.2022).

2. Unsupervised deep learning identifies semantic disentanglement in single inferotemporal neurons / I. Higgins, L. Chang, V. Langston [et al.] // Nature Communications. — 2021. — 12 (1), 6456. 10.1038/s41467-021-26751-5.

3. Randomized automatic differentiation / D. Oktay. N. McGreivy J. Aduol [et al.] // ResearchGate. — 2020. — Jul. — URL: https://www.researchgate.net/publication/343124368_Randomized_Automatic_Differentiation (дата обращения 26.12.2022).

4. On the spectral bias of neural networks / N. Rahaman, A. Baratin, D. Arpitet [et al.] // Proceedings.mlr.press : [сайт]. — URL: http://proceedings.mlr.press/v97/rahaman19a/rahaman19a.pdf (дата обращения: 02.04.2023).

5. Савосин, Д. Российские компании готовятся к увеличению расходов на кибербезопасность / Д. Савосин // RB.RU : [сайт]. — URL: https://rb.ru/news/companies-spending-cybersecurity/ (дата обращения 26.12.2022).

6. Боршигов, К. Генеративно-состязательная нейросеть / К. Боршигов // Neuro Hive : [сайт]. — URL: https://neurohive.io/ru/osnovy-data-science/gan-rukovodstvo-dlja-novichkov/ (дата обращения 26.12.2022).

7. Минбалеев, А. В. Проблемы использования искусственного интеллекта в противодействии киберпреступности // Вестник ЮУрГУ. — 2020. — № 4. — (Право). — URL: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-iskusstvennogo-intellekta-v-protivodeystvii-kiberprestupnosti (дата обращения: 26.12.2022).

Об авторах:

Кечеджиев Александр Сергеевич, магистрант кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), Kechedzhiev.alex@mail.ru.

Цветкова Ольга Леонидовна, доцент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), кандидат технических наук, доцент, olga_cvetkova@mail.ru.

About the Authors:

Aleksandr S. Kechedzhiev, Master's degree student of the Computing Systems and Information Security Department, Don State Technical University (344003, Russian Federation, Rostov-on-Don, Gagarin Square, 1), Kechedzhiev.alex@mail.ru

Olga L. Tsvetkova, associate professor of the Computing Systems and Information Security Department, Don State Technical University (344003, Russian Federation, Rostov-on-Don, Gagarin Square, 1), Cand. Sci. (Eng.), associate professor, olga_cvetkova@mail.ru