УДК 004.89+004.056 Вестник УрФО № 4(46) / 2022, с. 76–87

Ручай А.Н., Токарев И.В., Грибачёв А.С.

DOI: 10.14529/secur220409

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТАВ СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

В настоящее время обработка информации и работа с большим объемом данных является важными задачами, поэтому огромную роль играет защита этой информации, разработка и улучшение моделей безопасности, основанных на реальных наборах данных. Безопасность компьютерных систем и сетей передачи данных имеет определяющее значение не только для коммерческих структур и граждан, но и для государства в целом. Данная проблема подтверждается также тем, что количество компьютерных атак каждый год увеличивается, а их уровень подготовленности и направленности усиливается. Такое увеличение атак объясняется ростом зависимости промышленности от цифровой инфраструктуры и других сфер жизнедеятельности, а также трудностями поддержания компетенций специалистов в области кибербезопасности. В статье рассматривается научная литература по методам машинного обучения и искусственного интеллекта, которые применяются в сфере компьютерной безопасности.

Ключевые слова: *кибербезопасность, интеллектуальный анализ данных, искусственный интеллект, машинное обучение.*

METHODS OF MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE IN THE FIELD OF INFORMATION SECURITY: ANALYSIS OF THE CURRENT STATE AND PROSPECTS FOR DEVELOPMENT

Currently the processing of information and work with a large amount of data is important,therefore, the protection of this information, the development and improvement of security models based on real data sets, plays a huge role. The security of computer systems and data transmission networks is of decisive importance not only for commercial structures and citizens, but also states. This problem is also confirmed by the fact that the number of computer attacks is increasing every yearand they turn into be moresophisticated and distributed. This increase in attacks is due to the growing dependence of the industry on digital infrastructure and other areas of life, as well as the difficulties in maintaining the competencies of cybersecurity specialists. This article is review of scientific papers on the methods of machine learning and artificial intelligence used in the field of computer security.

Keywords: *cyber security, data mining, artificial intelligent, machine learning.*

1. Введение

Киберпространство в последние годы меняется так быстро, что не только обычные пользователи, но и специалисты в области компьютерных технологий и информационной безопасности не могут поспеть. С каждым днем растет объем обрабатываемых данных, добавляются новые устройства, приложения и сервисы, использующие сеть Интернет. Цифровизация дала мощный толчок к переводу большинства бизнес-процессов в онлайн, развитию концепций и технологий во всех сферах жизни человека.

Тренд цифровизации и скорость ее развития объясняется появлением принципиально новых технологий и инструментов. Массовое использование языков программирования, фреймворков и сред разработки, перевод инфраструктуры организации в «облака», контейнеризация и виртуализация, – все эти инструменты способствуют реализации серьезных проектов в максимально короткий срок. Однако, такие инструменты доступны и злоумышленникам, которые могут использовать их в своих целях, скорость появления новых киберугроз впечатляет, что способствует увеличению значимости области компьютерной безопасности, необходимости противодействиязлоумышленникам, которые используют такие же высокоэффективные инструменты разработки, но в иных целях.

Учитывая темп развития технологий, можно с уверенностью сказать, что в ближайшее время искусственный интеллект может стать сильным инструментом при обеспечении компьютерной безопасности. И несмотря на то, что участие человека остается достаточно важным аспектом не только вэтой сфере, но и в других отраслях, в решении некоторых определенных задач машина постепенно начинает нас опережать.

Диалоги о практическом использовании искусственного интеллекта, в частности, в области компьютерной безопасности, ведутся уже достаточно давно, однако применение продуктов с машинным обучением в корпоративной среде стало возможным лишь тогда, когда качество и эффективность работы начало оправдывать вложенные в них средства, а уровень подготовленности и оснащенности киберпреступников вырос настолько, что эффективно и своевременно оказывать противодействие им возможно лишь с использованием современных технологий.

Теме искусственного интеллекта в области кибербезопасности уделено внимание во многих специальных, педагогических, научно-популярных и художественных изданиях, такая литература доступна для широкого круга читателей [1, 2].

Развитие применения информационных технологий в различных областях способствует совершенствованию работы институтов государственной власти. Наряду с совершенствованием технологий, реализация задач цифровой трансформации системы государственного управления сталкивается с определенными сложностями, наблюдается рост направленных компьютерных атак на создаваемые информационные системы. При этом практика централизованного внедрения единых цифровых решений без одновременного создания системы обеспечения их информационной безопасности существенно повышает риски проявления угроз безопасности и, как следствие, нанесение ущерба интересам личности, общества и государства [3]. Новые технологии машинного обучения позволяют достигать значительного прогресса как в развитии информационно-вычислительной техники, так и в совершенствовании процессов обеспечения информационной безопасности компьютерного оборудования и информационных систем.

Согласно работам Ozlem Yavanoglu (2017) [4] и Sumeet Dua (2011) [5], компьютерная безопасность является важной областью исследований, поскольку абсолютно все сферы деятельности, а также обычные граждане, собирают, обрабатывают и хранят огромный объем данных на электронно-вычислительных машинах. Для обеспечения безопасности существования информационной системы компаниям требуется прикладывать огромные усилия. Компонентами информационной безопасности являются: обеспечение безопасности сетей, данных, конечных хостов, мобильная безопасность и многое другое. Сегодня значимость использования сети Интернет и компьютерных систем серьезно расширились, и они являются неотъемлемой частью жизни современного человека. В связи с экспоненциальным ростом компьютерных систем и использованием сетей, безопасность становится все более значимым условием обеспечения бесперебойной работы. Киберпреступники могут использовать различные пути, чтобы нанести ущерб конечным пользователям компьютерных сетей и систем, что является риском для утечки данных либо их потери. Огромную роль в обнаружении таких угроз безопасности информационных систем играет искусственный интеллект и машинное обучение [4 – 9].

Для того, чтобы оценить значимость применения искусственного интеллекта и машинного обучения необходимо явно представлять на какой стадии развития находится данная сфера. Для более подробного раскрытия выбранной темы структура данного обзора строится следующим образом: в первой части даются основные понятия, принципы и определения машинного обучения, краткая история развития искусственного интеллекта, в основной части освещены научные труды, анализирующие методы машинного обучения и искусственного интеллекта, приводятся примеры практического применения искусственного интеллекта и машинного обучения в области информационной безопасности, в заключении описаны наиболее значимые современные задачи и проблемы, а также ограничения данных методов в сфере информационной безопасности и направления дальнейшего исследования.

2. Искусственный интеллект и информационная безопасность

Прежде чем переходить к определениям и принципам машинного обучения, необходимо разобраться в определениях основных понятий информационной безопасности.

Кибербезопасность представляет собой набор мер по обеспечению безопасности, конфиденциальности, целостности и доступности данных [4]. Авторами Ankush Meshram (2017) [10] и Maryam Feily (2009) [11] объясняется известная триада конфиденциальности, целостности и доступности данных при обеспечении защиты информации.

Конфиденциальность направлена на ограничение раскрытия информации и пре-

доставления доступа информации только уполномоченным лицам. Благодаря конфиденциальности, компании могут защитить свои данные и активы от злоумышленников. В работе Malek BenSalem (2008) [12] описываются основные способы обеспечения конфиденциальности: шифрование, контроль доступа и стеганография.

Понятие целостности требует защиты данных последовательным, точным и надежным способом. Необходимо гарантировать, что данные не будут изменены в течение заданного периода времени. Для того, чтобы предотвратить внесение изменений неавторизованными пользователями, необходимо применять правильные процессы и действия. Такие инструменты и алгоритмы как хеширование, цифровые подписи, сертификаты, строгое выполнение инструкций обеспечивают целостность данных. [11, 12].

Доступность – это еще одна концепция безопасности, в соответствии с которой данные и ресурсы должны быть доступны тогда, когда людям нужен доступ к ним, особенно во время чрезвычайных ситуаций или стихийных бедствий. Специалисты по кибербезопасности должны справляться с тремя основными проблемами доступности: отказ в обслуживании, потеря информационной системы при возникновении чрезвычайной ситуации и отказы оборудования при нормальной работе [12].

Для более детального понимания проблематики искусственного интеллекта прежде всего нужно дать определения таким важным терминам как искусственный интеллект, нейронная сеть и машинное обучение и другим.

Под искусственным интеллектом понимается исполнение задач принятия решений непосредственно самими информационными системами, а также способность их обучению, подобно интеллекту живого существа.

Нейронная сеть – это набор искусственных нейронов, связанных между собой, которые выполняют простые логические операции, имеющие способность машинного обучения.

Машинное обучение представляет собой один из методов искусственного интеллекта, основой которого является не прямое решение задачи, а прежде всего обучение за счет использования решения большого количества сходных задач.

Существует несколько подходов машинного обучения:

• При использовании способа машинного обучения с учителем применяются определенные наборы данных, классифицированные по характерным признакам, для которых используется обучающая выборка, либо человек, который определяет корректные пары «вопрос – ответ». Подробнее с этим способом машинного обучения можно ознакомиться в [13].

• При обучении без учителя информационная система должна сама, посредством известных свойств объектов определить взаимосвязь между ними, при этом не применяются размеченные наборы данных и не задаются корректные пары «вопрос – ответ».

• Машинное обучение с частичным привлечением учителя заключается в том, что берется комбинация некоторого количества размеченных наборов данных и значительно большее количество неразмеченных.

• При применении машинного обучения с подкреплением, «учитель» представляет собой определенную среду функционирования, которая дает ответ информационной системе с учетом принятых данной системой решений.

При этом в машинном обучении возможно использование других алгоритмов, например градиентный бустинг, байесовские сети, цепи Маркова.

Глубокое обучение – один из частных случаев машинного обучения, который заключается в использовании сложной многослойной искусственной нейронной сети для эмуляции работы человеческого мозга, а также для возможности обработки речи, звуковых и визуальных образов. Подробнее ознакомиться с глубоким обучением можно в [14]. Сегодня использование машинного зрения представлено в системах обеспечения безопасности, контроля транспорта и пассажиров. Обработка речи и распознавание слов помогают голосовым ассистентам Siri, Алиса или Маруся взаимодействовать с пользователями таких систем.

Большие данные представляют собой огромный набор различных данных, имеющих определенные характеристики: объем, скорость изменения и разнообразие. Важной задачей является повышение ценности больших данных, для этого необходимо реализовать переход от разнородных данных к структурированным, а в дальнейшем – к знаниям. Полученный из релевантного массива больших данных набор данных, – один из самых

ценных компонентов для машинного обучения в современных системах.

Глубокий анализ данных – процесс получения необходимой информации из неструктурированного набора больших данных.

Нечёткая логика – использование нестрогих правил и ответов при решении задач в системах нейронных сетей и искусственного интеллекта. Одно из применений – моделирование поведения человека, например, для сужения или ограничения условий поиска ответа на вопрос в зависимости от контекста.

В исследованиях Micah Musser и AshtonGarriott (2021) [18] машинное обучение представляется как раздел науки о том, как компьютер станет действовать без явной типизации. Основная задача машинного обучения – это создание моделей, которые смогут обрабатывать набор входных данных и работать с ними, применяя статистический анализ для прогнозирования выходного значения в границах с подходящим диапазоном [4]. В сфере компьютерных наук машинное обучение – одно из самых быстроразвивающихся разделов с комплексным практическим применением. Алгоритмы машинного обучения классифицируются как контролируемое, неконтролируемое обучение и обучение с учителем. Контролируемые алгоритмы делятся на регрессию и классификацию [15 – 26].

Искусственный интеллект (ИИ) представляет собой область научных исследований, которая направлена на увеличение вычислительной мощности.

ИИ, как правило, применяется для решения сложных задач, которые не удалось решить без объединенного интеллекта, обнаружения скрытых закономерностей из данных и разработки интеллектуальных машин [2].

ИИ имеет множество практических применений для представления знаний, поиска информации, распознавание речи, распознавания естественного языка, компьютерного зрения, а также, он важен в биоинформатике, в экспертных системах, в робототехнике, в разработках игр и киберзащиты с помощью различных алгоритмов, таких как нечеткая логика, генетические алгоритмы, стохастические алгоритмы, искусственная нейронная сеть.

Искусственные нейронные сети (ИНС) представляют собой метод искусственного интеллекта, который включает в себя набор компьютерных алгоритмов для имитации процесса обработки нейронами головного мозга человека информации. ИНС собирают свои знания, обнаруживая модели и отношения между данными, и учатся через их архитектуры, передаточные функции и алгоритмы обучения.

Существует множество типов нейронных сетей для различных целей. Многослойные нейронные сети персептронного типа являются самыми простыми и наиболее часто используемой архитектурой нейронных сетей, которые обучаются с помощью множества алгоритмов обучения.

3. Применение искусственного интеллекта в кибербезопасности

После того, как рассмотрены основные принципы и определения машинного обучения, можно перейти к вопросу практического применения систем искусственного интеллекта в области компьютерной безопасности. В настоящее время наблюдается развитие угроз безопасности, а также рост возникающих инцидентов в информационных системах. Нехватка квалифицированных специалистов по защите информации, а также необходимость оперативного реагирования при наступлении киберинцидента прежде всего объясняет важность использования искусственного интеллекта в области информационной безопасности.

Необходимость выявления аномалий в большом количестве событий информационной безопасности объясняет незаменимость системы защиты на основе искусственного интеллекта. Один из примеров выявления аномалий – анализ журналов систем защиты информации, данных из SIEM-систем (систем реагирования на киберинциденты) или SOAR-решений (программ для координации и управления системами безопасности). Эта информация, в совокупности с данными уже отработанных и закрытых инцидентов, будет представлять собой качественный размеченный набор данных, на котором системе можно будет легко обучиться.

Выявление аномалий позволяет обеспечивать защиту пользовательских данных. Банковские сервисы могут собирать, обрабатывать и анализировать данные об определенных признаках в работе пользователей в целях оперативного определения скомпрометированных учетных записей.

Обладая знаниями о типичном поведении пользователей, система искусственного интеллекта может бороться с внутренними

нарушителями путем оповещения администраторов таких систем о возникновении нештатной ситуации, в случае изменения модели поведения пользователя.

Одной из самых серьезных проблем безопасности является то, что технологии доступны большой массе людей и могут использоваться не только во благо, но и во вред различными киберпреступниками, что в свою очередь определяет необходимость использования современных средств и методов защиты для своевременного реагирования на компьютерные инциденты.

Сформулируем наиболее значимые современные научно-исследовательские задачи в сфере искусственного интеллекта в области кибербезопасности: защита от сетевых атак с использованием технологии больших данных и эвристического анализа; создание моделей использования нейросетевых методов в задачах кибербезопасности; исследование и создание технологии автоматического управления информационной безопасностью; создание технологии защищенного доступа; разработка технологии высокопроизводительной обработки и визуализации больших массивов данных;анализ угроз кибербезопасности.

Приведем конкретные примеры.

Анализ сетевого трафика. Анализ сетевого трафика позволяет своевременно обнаруживать и предотвращать деятельность злоумышленников во внутренних сетях. Чаще всего это задача классификации трафика в реальном времени, в которой алгоритм машинного обучения выполняет роль системы обнаружения и предотвращения вторжений (Intrusion Detection System, Intrusion Prevention System) [30].

WAF (Web Application Firewall). Распространенность веб-приложений, а также их уязвимость, ставит вопрос о защите. В данной задаче алгоритм МО обучается обнаруживать и предотвращать атаки на веб-приложения. Данная задача классификации хорошо решается рекуррентными нейронными сетями [28] и автокодировщиками [32].

Анализ исходного кода. В данной задаче алгоритмы машинного обучения могут применяться в качестве аналогов статических анализаторов кода для выявлений уязвимостей ПО на стадиях разработки. Это задача классификации. Здесь применяются архитектуры рекуррентных нейронных сетей и модели типа Transformer [33].

Фаззинг (Fuzzing). Фаззинг– это один из способов тестирования ПО, при котором на вход приложения подаются данные, способные привести к неправильному функционированию приложения. Для эффективного фаззинга приложений исследователи применяют рекуррентные и генеративные нейронные сети [29].

SQL-инъекции. SQL-инъекции являются распространённой уязвимостью приложений, использующих базы данных. Важной задачей является своевременно детектирование SQL-атак, поэтому многие исследователи занимаются данной задачей [35]. Генеративные нейронные сети могут быть применены для генерации новых примеров SQL-инъекций [34].

Фильтрация фишинговых сообщений. Фишинг является распространённым видом интернет-мошенничества. Нейронные сети и другие методы машинного обучения хорошо подходят в качестве инструмента фильтрации фишинговых атак. В данной задаче широко исследуется применение следующих алгоритмов: деревья принятия решений (decisiontrees), случайные леса (randomforest), автокодировщики (autoencoders), SVM [31].

4. Проблемы кибербезопасности в искусственном интеллекте

Проблемы технологии методов синтеза изображения (дипфейков).

Технология дипфейков стала серьезным оружием. Например, создание поддельных политических, порнографических и видео с различным содержанием является серьезной угрозой информационной безопасности.

По всему миру принимаются различные меры для пресечения таких видов угроз: введение ответственности за публикацию подобного контента, разработка нормативных актов для решения проблем при использовании технологий.

Возникает вопрос об ответственности не только за распространение данного контента, но и о правах собственности на такого рода произведение. Автор программного обеспечения не всегда знает о конечном продукте, поэтому необходимо определиться с интеллектуальными правами преступников и жертв.

Проблема непонимания и недоверия к технологии искусственного интеллекта. По мнению кандидата юридических наук Романа Дремлюга, в наше время многие не понимают технологию искусственного интел-

лекта [27]. Одно из заблуждений – работа всей системы искусственного интеллекта зависит от программиста, а значит ответственность несет создатель системы. Программист же способен исключить лишь некоторые риски. Неверное суждение об ответственности программиста ведет к неверной оценке возможностей интеллекта. Сегодня искусственный интеллект охватывает все большие области нашей жизнедеятельности, его работу уже можно наблюдать в судебной деятельности, в экспериментах с постановкой медицинского диагноза.

Киберпреступления в сфере финансовых услуг. Развитие банковских продуктов и услуг не стоят на месте. Большинство из них можно получить в любом месте и в любое время, необходимо лишь иметь под рукой компьютер или смартфон и доступ в интернет. Однако, мошенники развиваются быстрее, чем системы безопасности, и безопасность предоставления таких услуг также не успевает за развитием услуг. Для обеспечения безопасности в оказании банковских услуг онлайн необходимо повышать ответственность и наделять финансовые организации дополнительными полномочиями.

Проблема потерь рабочих мест. Все чаще возникают вопросы о необходимости сотрудников в тех направлениях трудовой деятельности, где их возможно заменить роботизированными машинами. Действительно, технологический процесс быстро и успешно развивается: машины, позволяющие производить вычисления без ошибок и с высокой скоростью, электронные системы отслеживания и мониторинга и многое другое. Согласно прогнозамк2030 году промышленный сектор может сократить несколько миллионов сотрудников, их рабочие места займут роботизированные системы. Но не нужно думать, что с приходом роботов и искусственного интеллекта наступит безработица. Благодаря совершенствованию и роботизации рабочих процессов возрастет потребность в высококвалифицированных рабочих местах. Однако, последствия от роботизации производств в разных странах могут отличаться. Страны, в которых зависимость от низкоквалифицированных работников выше, сильнее пострадают от роботизации.

5. Применение машинного обучения в кибербезопасности

В работах [36 – 40] представлены многочисленные примеры использования машинного обучения и искусственного интеллекта в кибербезопасности.

Классификация данных по конфиденциальности. Соблюдение законов и защита конфиденциальности данных – одна из основных задач, стоящих перед организациями. Классификация помогает отделить данные, позволяющие произвести идентификацию пользователей, от неидентифицирующих данных.

Профили безопасности на основе поведения пользователей. Разработка моделей на основе поведения пользователей в системе может позволить совершенствовать систему безопасности в организации. Такие модели позволяют зафиксировать действия злоумышленника путем анализа изменений его поведения в системе. Создание профилей пользователей на основе их поведения может стать базой для предиктивной модели угрозы.

Профили безопасности на основе данных о работе системы. Проанализировав работу компьютерного рабочего места пользователя, также возможно составить профиль безопасности по следующим признакам: загрузка центрального процессора, оперативной памяти, интернет-канала. Их чрезмерная активность может означать наличие в системе вредоносного кода.

Блокировка ботов на основе поведения. Действия ботов могут парализовать работу веб-сайтов, что негативно скажется на работе организации в целом. Системы с применением машинного обучения позволяют не только определять активных ботов, но и произвести их блокировку. Основываясь на поведении злоумышленника, алгоритм сформирует прогнозную модель и превентивно заблокирует даже новых злоумышленников с похожей активностью.

6. Вклад искусственного интеллекта в решение проблем кибербезопасности

Разговаривая о современных способах использования машинного обучения и искусственного интеллекта в области информационной безопасности, нельзя не сказать о ряде проблем в этой сфере. Применение технологий искусственного интеллекта в процессах, которые хорошо нам известны, может оказаться очень полезным для их улучшения.

Человеческий фактор и эффективность ручного труда. Существенная часть уязвимостей кибербезопасности заключена в человеческом факторе. Компьютерная без-

опасность не перестает совершенствоваться и становиться сложнее. Применяемые инструменты помогают искать и устранять проблемы при модификациях и обновлениях систем. Оценка надежности выполнения работ вручную – достаточно ресурсозатратная задача, тогда как использование интеллектуальной автоматизации позволяет оперативно обнаруживать проблемы и получать анализ по их устранению.Одни и те же действия для решения проблемы невозможно каждый раз выполнить одинаково, тем более в постоянно меняющейся среде. Производить индивидуальные настройки устройств, обновлять и исправлять данные настройки, – достаточно трудоемкая задача. При этом вид и характер угроз непрерывно изменяется. Время реагирование человека на такие угрозы резко снижается, особенно при возникновении нештатных ситуаций. Системы же, основанные на искусственном интеллекте, работают с минимальными задержками.

Скорость реагирования на угрозу. Оперативность при возникновении угрозы – важнейший показатель эффективности обеспечения безопасности. Технологии позволяют автоматизировать кибератаки, что ускоряет процесс перехода от поиска и использования уязвимостей в системах и развертыванию. Одним из примеров таких угроз являются шифровальщики LockBit. Реакции человека зачастую недостаточно для предотвращения угрозы, несмотря на то, что отлично известно о типе атаки. Многим специалистам по безопасности приходится заниматься устранением последствий, а не предотвращением атак. Дополнительная проблема заключается в необнаруженных атаках.Технологии помогают специалистам сформировать отчеты, для упрощения обработки данных и принятия решений, а также предоставить рекомендации для уменьшения ущерба предотвращения новых атак.

Прогнозирование угроз. Определить и подготовить прогноз для новых угроз еще один фактор, оказывающий влияние на время реагирования на атаку. Программы на основе машинного обучения позволяют не только распознавать атаку, определяя схожие черты по ранее обнаруженным, но и облегчают прогнозирование таких угроз и сокращают время реагирования, благодаря работе с базой известных угроз.

Кадры. Поиск квалифицированного специалиста с требуемыми знаниями и навыками является систематической проблемой. Оплата труда такого специалиста, а также его обучение и повышение квалификации требует серьезного финансирования. Внедрение систем искусственного интеллекта позволяет существенно сократить расходы на содержание специалистов.

Адаптируемость. В сравнении с другими проблемами,проблема адаптируемости не лежит на поверхности, но может принести значительный ущерб безопасности.Сотрудники могут не обладать знаниями в работе с некоторыми методами, инструментами, либо правилами, принятыми в конкретной организации, что может привести к неэффективности выполнения работы команды в целом. Выполнение даже простой задачи может существенно затянуться. На внедрение всего нового требуется время. Для решения этой проблемы могут помочь алгоритмы машинного обучения.

7. Заключение

Защита компьютерных систем от компьютерных атак является одним из основных вопросов национальной и международной безопасности. На сегодняшний день информационная безопасность подвержена определенным трудностям: это и большие потоки событий, и снижение экспертизы, и отсутствие достаточного количества обученного персонала. Наблюдается огромный рост атак, независимо от принимаемых усилий по защите систем, что объясняет высокую значимость применения современных методик по защите информационных систем от такого вида атак. Одной из самых востребованных методик является машинное обучение. Пока для принятия решения невозможен полный отказ от участия человека, однако, существует множество разработанных моделей, которые позволяют определять новые угрозы и выявлять аномалии. Использование методов машинного обучения в сфере информационной безопасности является одним из самым перспективных способов для обеспечения защиты современных информационных систем.

В настоящей статье описана краткая история развития искусственного интеллекта в кибербезопасности, проведены исследования различных методов машинного обучения и искусственного интеллекта, показано, что искусственный интеллект и машинное обучение играют значительную роль в защите информационных систем, рассмотрено практическое применение искусственного интел-

лекта в области информационной безопасности, наиболее значимые современные научно-исследовательские задачи и некоторые примеры проблем, связанных с искусственным интеллектом в области информационной безопасности, приведены примеры использования машинного обучения в кибербезопасности, уделено внимание вкладу искусственного интеллекта в решение проблем кибербезопасности и его роли в области информационной безопасности. Дальнейшее направление исследования заключается в том, чтобы рассмотреть классы различных наборов данных, методы выявления аномалий, определить достоинства и недостаткиалгоритмов машинного обучения, выработать универсальный подходк разработке моделей, обобщить и опубликовать результаты.

Литература

1. Choi Y., Liu P., Shang Z., Wang H., Wang Z., Zhang L., Zhou J., Zou Q. Using Deep Learning to Solve Computer Security Challenges: A Survey, arXiv preprint arXiv:1912.05721, 2020.

2. Dhir N., Hoeltgebaum H., Adams N., Briers M., Burke A., Jones P. Prospective Artificial Intelligence Approaches for Active Cyber Defence, arXiv preprint arXiv:2104.09981, 2021.

3. Указ Президента Российской Федерации № 646 (2016). Доступен по ссылке: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. Доктрина информационной безопасности Российской Федерации.

4. Yavanoglu O., Aydos M. A review on cyber security datasets for machine learning algorithms. IEEE International Conference on Big Data (Big Data), 2017.

5. Dua S., Du X. Data mining and machine learning in cybersecurity. CRC press, 2016.

6. Symantec Corporation. Symantec Web Application Firewall. OWASP TOP 10 2017 COVERAGE. Available at: https://docs.broadcom.com/doc/web-application-firewall-owasp-top-10-2017-coverage-en. The Ten Most Critical Web Application Security Risks, 2017.

7. Mnih V., Kavukcuoglu K., Silver D., Rusu A.A., Veness J., Bellemare M.G., Graves A., Riedmiller M., Fidjeland A.K., Ostrovski G., Petersen S., Beattie Ch., Sadik A., Antonoglou I., King H., Kumaran Dh., Wierstra D, Legg Sh. & Hassabis D. Human-level control through deep reinforcement learning. J. Nature, 2015, V. 518. pp. 529–533.

8. Silver D., Huang A., Maddison C.J., Guez A., Sifre L., Driessche G., Schrittwieser J., Antonoglou I., Panneershelvam V., Lanctot M., Dieleman S., Grewe D., Nham J., Kalchbrenner N., Sutskever I., Lillicrap T., Leach M., Kavukcuoglu K., Graepel Th. & Hassabis D. Mastering the game of Go with deep neural networks and tree search, J. Nature, 2016, V. 529, pp. 484–489.

9. Kaspersky. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее. Доступен по ссылке: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity.

10. Meshram A., Haas C. Anomaly detection in industrial networks using machine learning: a roadmap. Machine Learning for Cyber Physical Systems, 2017, pp. 65–72.

11. Feily M., Alireza S., Sureswaran R. A survey of botnet and botnet detection. Emerging Security Information, Systems and Technologies, 2009.

12. Salem M.B., Hershkop S., Stolfo S.J. A survey of insider attack detection research, Insider Attack and Cyber Security, 2008, pp. 69-90.

13. Van Der Malsburg C. Frank Rosenblatt: Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms, J. Springer, 1984, pp. 245–248.

14. Goodfellow I., Bengio Y., Courville A. Deep Learning, The MIT Press, 2016.

15. Albon C. Machine Learning with Python Cookbook Practical Solutions from Preprocessing to Deep Learning, O'Reilly Media, Inc., 2018, 366 p.

16. Watt J., Borhani R., Katsaggelos A.K. Machine Learning Refined Foundations, Algorithms, and Applications, Cambridge University Press, 2020, 301 p.

17. Goldblum M., Tsipras D., Xie C., Chen X., Schwarzschild A., Song D., Madry A., Li B., Goldstein T. Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. CoRR abs, 2020.

18. Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.

19. Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.

20. Чио К., Фримэн Д. Машинное обучение и безопасность, ДМКПресс, 2020, 388 с.

21. Neethu B. Adaptive Intrusion Detection Using Machine Learning, International Journal of Computer Science and Network Security, 2013, pp. 118-124.

22. Kozik R., Choras M., Renk R., Hołubowicz W. A Proposal of Algorithm for Web Applications Cyber Attack Detection, J. Springer, 2014.

23. Rashid T. Make Your Own Neural Network, CreateSpace Independent Publishing Platform, 2016, 222 p.

24. Bhuyan M., Bhattacharyya K., Kalita J. Towards Generating Real-life Datasets for Network Intrusion Detection, IJ Network Security, 2015, pp. 683-701.

25. Kato K., Klyuev V. An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine, IJICR, 2014, pp. 464-471.

26. Glassner A. Deep Learning, The Imaginary Institute, 2018.

27. Дремлюга Р.И. Основы национального регулирования применения искусственного интеллекта: опыт Сингапура, Азиатско-Тихоокеанский регион: экономика, политика, право, 2022, с. 214–224.

28. IŞiker B., SoGukpinar I. Machine Learning Based Web Application Firewall, 2021 2nd International Informatics and Software Engineering Conference (IISEC), 2021, pp. 1-6.

29. Zhu X. et al. Defuzz: Deep learning guided directed fuzzing, arXiv preprint arXiv:2010.12149, 2020.

30. Alkasassbeh M., Almseidin M. Machine learning methods for network intrusion detection, arXiv preprint arXiv:1809.02610, 2018.

31. Shahrivari V., Darabi M., Izadi M. Phishing detection using machine learning techniques, arXiv preprint arXiv:2009.11116, 2020.

32. Vartouni A., Kashi S., Teshnehlab M. An anomaly detection method to detect web attacks using Stacked Auto-Encoder, 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018, pp. 131-134.

33. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1-6.

34. Lu D. et al. A GAN-based Method for Generating SQL Injection Attack Samples, 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2022, pp. 1827-1833.

35. Latchoumi T., Reddy M., Balamurugan K. Applied machine learning predictive analytics to SQL injection attack detection and prevention, European Journal of Molecular & Clinical Medicine., 2020.

36. Асяев Г.Д., Соколов А.Н. Обнаружение вторжений на основе анализа аномального поведения локальной сети с использованием алгоритмов машинного обучения с учителем, Вестник УрФО. Безопасность в Информационной Сфере, 2020, с. 77-83.

37. Соколов А.Н., Алабугин С.К., Пятницкий И.А. Применение методов одноклассовой классификации для обнаружения вторжений, Вестник УрФО. Безопасность в Информационной Сфере, 2018, с. 43-48.

38. Алабугин С.К., Соколов А.Н., Пятницкий И.А. Применение рекуррентных и сверточных нейронных сетей для выявления аномалий технологического процесса, Вестник УрФО. Безопасность в Информационной Сфере, 2019, с. 60-65.

39. Асяев Г.Д., Соколов А.Н. Модели предиктивной защиты информации автоматизированной системы управления водоснабжением на основе временных рядов с использованием технологий машинного обучения, Вестник УрФО. Безопасность в Информационной Сфере, 2021, с. 39-45.

40. Фельдман Е.В. Ручай А.Н., Чербаджи Д.Ю. Модель выявления аномальных банковских транзакций на основе машинного обучения, Вестник УрФО. Безопасность в Информационной Сфере, 2021, с. 27-35.

References

1. Choi Y., Liu P., Shang Z., Wang H., Wang Z., Zhang L., Zhou J., Zou Q. Using Deep Learning to Solve Computer Security Challenges: A Survey, arXiv preprint arXiv:1912.05721, 2020.

2. Dhir N., Hoeltgebaum H., Adams N., Briers M., Burke A., Jones P. Prospective Artificial Intelligence Approaches for Active Cyber Defence, arXiv preprint arXiv:2104.09981, 2021.

3. Ukaz Prezidenta Rossiyskoy Federatsii № 646 (2016). Dostupen po ssylke: http://static.kremlin.ru/media/acts/files/0001201612060002.pdf. Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii.

4. Yavanoglu O., Aydos M. A review on cyber security datasets for machine learning algorithms. IEEE International Conference on Big Data (Big Data), 2017.

5. Dua S., Du X. Data mining and machine learning in cybersecurity. CRC press, 2016.

6. Symantec Corporation. Symantec Web Application Firewall. OWASP TOP 10 2017 COVERAGE.

Available at: https://docs.broadcom.com/doc/web-application-firewall-owasp-top-10-2017-coverage-en. The Ten Most Critical Web Application Security Risks, 2017.

7. Mnih V., Kavukcuoglu K., Silver D., Rusu A.A., Veness J., Bellemare M.G., Graves A., Riedmiller M., Fidjeland A.K., Ostrovski G., Petersen S., Beattie Ch., Sadik A., Antonoglou I., King H., Kumaran Dh., Wierstra D, Legg Sh. & Hassabis D. Human-level control through deep reinforcement learning. J. Nature, 2015, V. 518. pp. 529–533.

8. Silver D., Huang A., Maddison C.J., Guez A., Sifre L., Driessche G., Schrittwieser J., Antonoglou I., Panneershelvam V., Lanctot M., Dieleman S., Grewe D., Nham J., Kalchbrenner N., Sutskever I., Lillicrap T., Leach M., Kavukcuoglu K., Graepel Th. & Hassabis D. Mastering the game of Go with deep neural networks and tree search, J. Nature, 2016, V. 529, pp. 484–489.

9. Kasperskiy. Iskusstvennyy intellekt i mashinnoye obucheniye v oblasti kiberbezopasnosti – prognoz na budushcheye. Dostupen po ssylke: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity.

10. Meshram A., Haas C. Anomaly detection in industrial networks using machine learning: a roadmap. Machine Learning for Cyber Physical Systems, 2017, pp. 65–72.

11. Feily M., Alireza S., Sureswaran R. A survey of botnet and botnet detection. Emerging Security Information, Systems and Technologies, 2009.

12. Salem M.B., Hershkop S., Stolfo S.J. A survey of insider attack detection research, Insider Attack and Cyber Security, 2008, pp. 69-90.

13. Van Der Malsburg C. Frank Rosenblatt: Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms, J. Springer, 1984, pp. 245–248.

14. Goodfellow I., Bengio Y., Courville A. Deep Learning, The MIT Press, 2016.

15. Albon C. Machine Learning with Python Cookbook Practical Solutions from Preprocessing to Deep Learning, O'Reilly Media, Inc., 2018, 366 p.

16. Watt J., Borhani R., Katsaggelos A.K. Machine Learning Refined Foundations, Algorithms, and Applications, Cambridge University Press, 2020, 301 p.

17. Goldblum M., Tsipras D., Xie C., Chen X., Schwarzschild A., Song D., Madry A., Li B., Goldstein T. Dataset Security for Machine Learning: Data Poisoning, Backdoor Attacks, and Defenses. CoRR abs, 2020.

18. Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.

19. Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.

20. Chio K., Frimen D. Mashinnoye obucheniye i bezopasnost', DMKPress, 2020, 388 c.

21. Neethu B. Adaptive Intrusion Detection Using Machine Learning, International Journal of Computer Science and Network Security, 2013, pp. 118-124.

22. Kozik R., Choras M., Renk R., Hołubowicz W. A Proposal of Algorithm for Web Applications Cyber Attack Detection, J. Springer, 2014.

23. Rashid T. Make Your Own Neural Network, CreateSpace Independent Publishing Platform, 2016, 222 p.

24. Bhuyan M., Bhattacharyya K., Kalita J. Towards Generating Real-life Datasets for Network Intrusion Detection, IJ Network Security, 2015, pp. 683-701.

25. Kato K., Klyuev V. An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine, IJICR, 2014, pp. 464-471.

26. Glassner A. Deep Learning, The Imaginary Institute, 2018.

27. Dremlyuga R.I. Osnovy natsional'nogo regulirovaniya primeneniya iskusstvennogo intellekta: opyt Singapura, Aziatsko-Tikhookeanskiy region: ekonomika, politika, pravo, 2022, s. 214–224.

28. IŞiker B., SoGukpinar I. Machine Learning Based Web Application Firewall, 2021 2nd International Informatics and Software Engineering Conference (IISEC), 2021, pp. 1-6.

29. Zhu X. et al. Defuzz: Deep learning guided directed fuzzing, arXiv preprint arXiv:2010.12149, 2020.

30. Alkasassbeh M., Almseidin M. Machine learning methods for network intrusion detection, arXiv preprint arXiv:1809.02610, 2018.

31. Shahrivari V., Darabi M., Izadi M. Phishing detection using machine learning techniques, arXiv preprint arXiv:2009.11116, 2020.

32. Vartouni A., Kashi S., Teshnehlab M. An anomaly detection method to detect web attacks using Stacked Auto-Encoder, 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS), 2018, pp. 131-134.

33. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1-6.

34. Lu D. et al. A GAN-based Method for Generating SQL Injection Attack Samples, 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2022, pp. 1827-1833.

35. Latchoumi T., Reddy M., Balamurugan K. Applied machine learning predictive analytics to SQL injection attack detection and prevention, European Journal of Molecular & Clinical Medicine., 2020.

36. Asyayev G.D, Sokolov A.N., Obnaruzheniye vtorzheniy na osnove analiza anomal'nogo povedeniya lokal'noy seti s ispol'zovaniyem algoritmov mashinnogo obucheniya s uchitelem, Vestnik UrFO. Bezopasnost' v Informatsionnoy Sfere, 2020, c.77-83

37. Sokolov A.N., Alabugin S.K., Pyatnitskiy I.A. Primeneniye metodov odnoklassovoy klassifikatsii dlya obnaruzheniya vtorzheniy, Vestnik UrFO. Bezopasnost' v Informatsionnoy Sfere, 2018, c. 43-48.

38. Alabugin S.K., Sokolov A.N., Pyatnitskiy I.A. Primeneniere kurrentnyx i svertochnyx nejronnyx setej dlya vyyavleniya anomalij texnologicheskogo processa, Vestnik UrFO. Bezopasnost v Informacionnoj Sfere, 2019, c. 60-65.

39. Asyaev G.D., Sokolov A.N. Modeli prediktivnoj zashhity informacii avtomatizirovannoj sistemy upravleniya vodosnabzheniem na osnove vremennyx ryadov s ispolzovaniemtexnologijmashinnogoobuch eniya, Vestnik UrFO. Bezopasnost v Informacionnoj Sfere, 2021, c. 39-45.

40. Feldman E.V., Ruchay A.N., Cherbadzhi D.Yu. Model vyyavleniya anomalnyx bankovskix tranzakcij na osnove mashinnogo obucheniya, Vestnik UrFO. Bezopasnost v Informacionnoj Sfere, 2021, c. 27-35.

РУЧАЙ Алексей Николаевич, кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет. Россия, 454001, Челябинск, ул. Братьев Кашириных, 129.; доцент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. Ленина, 76. E-mail: ran@csu.ru

ТОКАРЕВ Игорь Вячеславович, аспирант (соискатель) математического факультета, Челябинский государственный университет. Россия, 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: tokarev_i_v@mail.ru

ГРИБАЧЁВ Антон Сергеевич, аспирант (соискатель) математического факультета, Челябинский государственный университет. Россия, 454001, Челябинск, ул. Братьев Кашириных, 129. E-mail: a.gribachev@yandex.ru

RUCHAY Alexey Nikolaevich, PhD in Physics and Mathematics, Associate Professor, Head of the Department of Computer Security and Applied Algebra, Chelyabinsk State University. Russia, 454001, Chelyabinsk, st. Brothers Kashirin, 129.; Associate Professor, Department of Information Security, South Ural State University (National Research University). Russia, 454080, Chelyabinsk, Lenin Ave., 76. E-mail: ran@csu.ru

TOKAREV Igor Vyacheslavovich, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. Russia, 454001, Chelyabinsk, st. Brothers Kashirin, 129. E-mail: tokarev_i_v@mail.ru

GRIBACHEV Anton Sergeevich, PhD candidate of the Faculty of Mathematics, Chelyabinsk State University. Russia, 454001, Chelyabinsk, st. Brothers Kashirin, 129. E-mail: a.gribachev@yandex.ru