УДК 004.8

РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

[1]Скрыпников А.В., [1]Денисенко В.В., [2]Хитров Е.Г., [1]Савченко И.И., [1]Евтеева К.С.

[1]ФГБОУ ВО «Воронежский государственный университет инженерных технологий», Воронеж, e-mail: mr.saranov@mail.ru;

[2] ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого», Санкт-Петербург, e-mail: yegorkhitrov@gmail.com

Кибербезопасность – быстро развивающаяся область, требующая постоянного усовершенствования благодаря заметному продвижению в облачных сетях и веб-технологиях, онлайн-банкинге, социальных сетях, мобильной среды окружающей, смарт-сетки и прочих. На данный момент в большинстве случаев информационная безопасность является реактивной. Методы машинного обучения могут быть применены во многих сферах науки. Их отличительные свойства – масштабируемость, адаптивность, потенциал. Именно поэтому есть возможность моментально адаптироваться под новые и ранее неизвестные вызовы. Машинным обучением является класс методов ИИ (искусственного интеллекта), характерной чертой данных методов считается не обычное прямой решение поставленной задачи, а обучение в процессе поиска и применения решений сходных задач во множественном количестве. Создание таких машинных методов требует использования средств статистики математической, численных методов, теории вероятности и графов, прочих техник работы с цифровыми данными. Проанализированы типы программных решений, платформ и устройств информационной безопасности с использованием искусственного интеллекта для автоматизированного реагирования на сетевые и локальные угрозы, также на поведение пользователей и различных информационных сущностей. Показана необходимость применения машинного обучения в сфере кибербезопасности.

Ключевые слова: машинное обучение, искусственный интеллект, кибербезопасность, данные, исследование, информационная безопасность

SOLVING PROBLEMS OF INFORMATION SECURITY WITH THE USE OF ARTIFICIAL INTELLIGENCE

[1]Skrypnikov A.V., [1]Denisenko V.V., [2]Khitrov E.G., [1]Savchenko I.I., [1]Evteeva K.S.

[1]Voronezh State University of Engineering Technologies, Voronezh, e-mail: mr.saranov@mail.ru;

[2]St. Petersburg Polytechnic University of Peter the Great, St. Petersburg, e-mail: yegorkhitrov@gmail.com

Cybersecurity is a fairly rapidly developing area that requires constant improvement due to the noticeable advancement in cloud networks and web technologies, online banking, social networks, mobile environment, smart grids and others. Machine learning methods can be applied in many areas of science. Their distinctive properties are scalability, adaptability, potential. That is why it is possible to instantly adapt to new and previously unknown challenges. Machine learning is a class of AI (artificial intelligence) methods, a characteristic feature of these methods is not the usual direct solution of the problem, but learning in the process of finding and applying solutions to similar problems in a plurality. The creation of such machine methods requires the use of mathematical statistics, numerical methods, probability theory and graphs, and other techniques for working with digital data. The types of software solutions, platforms and information security devices using artificial intelligence for automated response to network and local threats, as well as to the behavior of users and various information entities are analyzed.

Keywords: machine learning, artificial Intelligence, cybersecurity, data, research, information security

К сожалению, приходится констатировать, что информационная безопасность на данный момент в большинстве случаев является реактивной. Только после того, как произошло какое-либо чрезвычайное происшествие, связанное с воровством данных, финансов, выведением из строя техники, начинается реакция и борьба с последствиями. Эффективность систем безопасности и защиты напрямую зависит от того, как быстро специалисты будут извещены о том, что была произведена атака.

Одной из современных тенденций киберпреступности является создание вредоносных доменов, используемых для атак не больше одного-двух раз. Внесение их в черный список не поможет защититься, поскольку домены будут появляться со скоростью, сходной с геометрической прогрессией. Решить эту проблему может помочь машинное обучение. Машинное обучение – это метод, основанный на анализе данных, автоматизирующий построение аналитических моделей; является направлением исследований в области искусственного интеллекта, основанным на идее возможности создания систем, способных учиться на наборах данных, выявлять закономерности и принимать решения с минимальным вмешательством человека.

Антивирусные программы и приложения, которые используют сигнатуры для обнаружения вирусов, также подвержены постоянным атакам. Ежедневно происходит

обнаружение миллиардов вредоносных записей, которые не успевают нанести какой-либо вред, так как они моментально уничтожаются.

Традиционные методы обнаружения вредоносных программ позволяют отследить записи, которые ранее уже были успешно использованы хакерами. Машинные методы в этом плане предпочтительнее, так как они способны выявить такие записи, которые еще ни разу себя не проявляли, но содержат вирусы [1].

Исследование направлено на анализ возможностей и условий применения методов машинного обучения в перспективных системах комплексной защиты информации и изучение технических решений, использующих модели и алгоритмы машинного обучения.

Материалы и методы исследования

Исследование базируется на принципах разработки эффективных систем управления рисками информационной безопасности и накопленном личном опыте в области администрирования информационных систем и обеспечения требований информационной безопасности.

Результаты исследования и их обсуждение

Для того чтобы машинные методы успешно справлялись со своей задачей, необходимо на вход модели либо алгоритма подать множество входных данных, на них модель пройдет обучение. После того, как модель пройдет обучение, появится возможность добавлять входные данные, в которых модель сможет находить искомое [2].

Основными ключевыми элементами машинного метода обучения считаются:

1. Датасет. Большое количество вводимых данных. Для того чтобы модель могла успешно распознавать что-либо, нужно подавать на вход немалое количество данных, в этом случае используется датасет. К датасету относятся сетевые потоки, почтовые сообщения, логи, интернет-трафик и сведения об активности пользователей. Для получения наиболее точного результата предсказания и обнаружения вредоносных записей, датасет должен содержать огромное количество данных, которые должны быть самыми разнообразными. Для обнаружения спама требуются сотни тысяч, миллионы сообщений, которые необходимо тщательно проанализировать. Для предсказания действий пользователя необходимо тщательно отслеживать его деятельность в интернете в течение нескольких недель. Для обнаружения доменов, несущих вред, необходимо изучить сотни миллиардов, триллионы DNS-запросов. Эффективность методов машинного обучения напрямую зависит от качества датасета. Если использовать датасеты ненадлежащего качества, имеющие некорректные данные, то даже идеальная модель машинного обучения не в силах будет помочь в решении задачи.

2. Признаки. Именно их ищут в датасетах. К ним относятся: доменное имя, длительность сетевой сессии, электронный адрес отправителя, IP-адрес, используемый протокол, время суток и прочее. В зависимости от поставленной задачи может быть обнаружено больше сотни различных признаков. К примеру, некоторые системы защиты конечных устройств содержат 400 и более признаков.

3. Алгоритмы-модели. Чтобы найти искомое в датасетах по определенным признакам, можно подобрать разные способы, которые зависят от задаваемых параметров. Верный выбор модели либо алгоритма – это некий баланс между быстротой работы, аккуратными предсказаниям и сложностью модели. Именно поэтому приходится довольно часто экспериментировать с моделями до тех пор, пока среди них не обнаружится более подходящая для решения конкретной поставленной задачи.

Универсальный алгоритм, применяемый методами машинного обучения, не был обнаружен, несмотря на то, что известны попытки признать таковой нейронную сеть. Для разных задач должны применяться разные модели. Обычно их делят по типу обучения или по функции. К примеру:

1. По типу обучения: с учителем, без него, с подкреплением.

2. По функции: регрессия, нейросети, дерево решения, кластеризация, байесовские [3].

Классическое машинное обучение может применяться в случаях, когда в наличии есть простые данные и вполне конкретные признаки. Одним из примеров может служить блокировка кредитной карты после того, как с нее сняли наличные за границей; это достаточно простой случай. Обычно все платежные и прочие операции с картой производились в домашнем регионе, алгоритм работал по четко заведенному порядку. Далее неожиданно происходит операция за границей, а при этом банк не предупрежден о том, что клиент покинул пределы страны и планирует пользоваться картой за рубежом. При помощи классического машинного обучения эта задача решается моментально.

Примерно 75% классических алгоритмов – это обучение с учителем. Рабо-

та производится с маркированными либо уже размеченными данными. Это подразумевает, что модели необходимо сообщать, где спам, а где его нет, где присутствует мошенничество, а где его нет; где DDoS, а где его нет. После прохождения обучения с учителем можно научиться с легкостью выделять и классифицировать новые данные. При этом в них просто выделить нечто аномальное. Классические алгоритмы помогают увидеть загрузку какого- либо вредоносного кода, ранее не известного, обнаружить спам- и фишинговые атаки, автоматически созданные вредоносные домены. Наиболее популярными алгоритмами можно назвать регрессию и классификацию. Благодаря регрессии можно получить предсказание значения, а классификация предскажет категорию.

Чтобы предсказать, когда именно начнется рост атак вредоносных записей и кодов, нужно использовать регрессию, а если необходимо разобраться, каких атак предвидится больше, требуется классификация. Из этих типов алгоритмов каждый может быть подразделен на множество алгоритмов машинного обучения с учителем. Таким образом можно предсказать атаку вредоносного программного обеспечения или заблокировать подозрительный HTTP-трафик.

Но бывает так, что данные входные не размечены. Например, в один момент происходит четырехкратная попытка войти в аккаунт под одной и той же учетной записью, что фиксируется системой защиты. Политика конфиденциальности предусматривает только три попытки входа. Следовательно, происходит атака. Для обнаружения множества попыток попадания в систему машинное обучение не требуется.

Второй пример. Если одна и та же учетная запись в течение одних суток подвергается попыткам проникновения из разных географических точек, можно говорить о вредоносной атаке. Но можно и не говорить об этом, ведь человек, являющийся пользователем, может просто отправиться в командировку и заходить в рабочую программу в разных отелях разных стран, каждый раз создавая новую сессию. Именно такие сценарии ошибочно признаются банками мошенничеством. Чтобы обнаружить этот вид активной деятельности, методы машинного обучения также не нужны.

Но при попытке доступа к учетной записи из необычного места, которое не входит в базу системы безопасности и, следовательно, его невозможно распознать как неправомерный вход, методы машинного обучения обязательно понадобятся. Используется обучение без учителя, а также один из алгоритмов, который называется кластеризацией. Ее возможность объединять схожие события в кластеры может пригодиться в данном случае. Нестандартное место входа – это сигнал для признания его аномалией и подозрения на вредоносность события. Это вполне может сигнализировать о попытке украсть учетные записи. Кластеризация без учителя – менее точный метод, чем алгоритм с учителем. В попытках разобраться может выясниться интересная деталь: пользователь, к примеру, подключает к своей учетной записи определенное приложение, которое имеет доступ к защищенным данным, облачному хранилищу, а затем забывает об этом. Автоматическое подключение такого приложения может регистрироваться из любого места планеты.

Рассмотрим пример, где обучение без учителя отлично сработает. Это обнаружение утечки информационных данных либо саботаж администратора. Нет возможности утверждать, где находится грань между нормальным и аномальным количеством удаляемых из облака либо скачанных по локальной сети файлов на один компьютер. При этом есть возможность сравнивать между собой обнаруженный признак у различных пользователей и групп пользователей, создавая их объединение в кластеры, выявляя при этом аномальное и нормальное поведение [1].

К примеру, в один день пользователи способны загрузить в сеть Интернет примерно 100 Мбит данных; но тут же какой-либо из пользователей загружает более 10 гигабайт. Эту явную аномалию можно обнаружить и без методов машинного обучения. Но можно ими воспользоваться для того, чтобы объединить некоторые признаки. К ним относятся: протокол, дата, время суток, тип данных, их объем, адрес получателя. Таким образом можно определить и отделить выгрузку дистрибутива обновленной версии приложения для удаленных офисов от воровства данных.

Один из видов машинного обучения без учителя – нейросети. Они в последнее время невероятно быстро набирают популярность. Применяются там, где датасеты достаточно сложны, либо тяжело выделяются признаки, которые выбирают модель в датасете. Основная идея нейросети – ее внутренние слои имеют безграничную возможность выполнять свои собственные суждения о том, что представляет важность в датасете и что необходимо извлечь из него в процессе машинного обучения. Все примеры, приведенные выше, могут быть обнаружены нейронными сетями. Однако чаще всего их используют для наиболее сложных

сценариев. К ним относятся: борьба с угрозами для биометрии, распознание фальшивых документов и файлов, распознание текстов по безопасности и прочие. У нейросетей существует серьезный недостаток – полное отсутствие обратной связи. Именно поэтому нет возможности объяснить, по какой причине из входных данных получается именно этот результат.

На данном этапе можно выделить несколько областей кибербезопасности, где применяется машинное обучение и искусственный интеллект (ИИ):

1. UEBA (User and Entity Behavior Analytics) – система проводит анализ поведения пользователей и различных информационных сущностей, что позволяет обнаруживать случаи нестандартного поведения и использовать их для детектирования внутренних и внешних угроз, применяя шаблоны (паттерны) угроз.

2. TIP (Threat Intelligence Platform) – платформы раннего детектирования угроз и реагирования на них. Применение методов машинного обучения повышает эффективность обнаружения неизвестных угроз на ранних этапах.

3. EDR (Endpoint Detection and Response) – система обнаружения атак оперативного реагирования на любых компьютерных устройствах. Продукты данного типа могут обнаруживать вредоносные программы, автоматически классифицировать угрозы и самостоятельно реагировать на них.

4. SIEM (Security Information and Event Management) – мониторинг систем в реальном времени, анализ безопасности системы на основе информации, поступающий от сетевых устройств, приложений и сервисов.

5. NDR (Network Detection and Response) – устройства и аналитические платформы обнаруживают атаки на сетевом уровне и оперативно реагируют на них. ИИ использует накопленную статистику и базу знаний об угрозах.

6. SOAR (Security Orchestration and Automated Response) – системы, позволяющие выявлять угрозы информационной безопасности и автоматизировать реагирование на инциденты. В решениях данного типа, в отличие от SIEM-систем, ИИ помогает не только проводить анализ, но и автоматически реагировать надлежащим образом на выявленные угрозы.

7. Средства защиты приложений (Application Security) – системы, позволяющие определять угрозы безопасности прикладных приложений, управлять дальнейшим циклом мониторинга и устранения таких угроз.

8. Антифрод (Antifraud) – платформы, работающие в режиме реального времени. Обнаруживают угрозы в бизнес-процессах и мошеннические операции. ИИ используется для определения отклонений от установленных бизнес-процессов, что позволяет быстро выявить возможное финансовое преступление или уязвимость процессов. Применение ИИ в таких системах особенно актуально, так как позволяет быстро адаптироваться к изменению логики и различных метрик бизнес-процессов, а также использовать лучшие практики в индустрии.

На данный момент самыми популярными направлениями применения ИИ в кибербезопасности можно считать обнаружение и реагирование на кибератаки – 33 % от всех продуктов и обнаружение мошенничества в бизнес-процессах – 11 %. Специалисты крупнейших IT-компаний также отмечают тот факт, что применение продуктов с использованием ИИ сокращает количество ложных срабатываний, повышает эффективность обнаружения и скорость реакции на угрозы, а также помогает в расследовании инцидентов [4, 5].

Существует целый перечень проблем информационной безопасности. Среди них можно выделить огромнейшие потоки событий, снижение качества экспертиз, а также глобальную нехватку персонала. Несмотря на постоянно обновляющийся список предпринимаемых мер, число атак растет ежедневно, ежечасно. На данный момент примерный период необнаружения угроз равен 200 дням. Это отличный результат быстрой работы защитных средств, используемых для защиты данных.

Кроме того, не следует думать, что машинное обучение – единственно правильная методика поведения в области кибербезопасности. Первым неприятным моментом является то, что разработан целый класс атак на машинное обучение, которые направлены на датасеты и на алгоритмы, что может привести к пропущенным атакам, неверным решениям, ложным срабатываниям. Ко второй неприятности относится то, что мошенники постоянно совершенствуют свои методы и также применяют машинное обучение в своей деятельности – это и создание программ, наносящих вред, и анализ поведения пользователей, а также фишинг, обход систем защиты, разработка сборщиков персональных данных (ботов), подмена личности и так далее. В противовес мошенникам, умеющим пользоваться методами машинного обучения, можно использовать только искусственный интеллект. И именно поэтому применение машинного обучения в кибербезопасности – необходимость, ведь

без него современная система информационной безопасности может просто прекратить свое существование [6, 7].

Заключение

Сегодня еще не достигнут тот уровень безопасности, при котором можно абсолютно и полностью отказаться от участия человека при принятии решений в области информационной безопасности.

Многие модели, разработанные современными учеными, способны детектировать новейшие угрозы, подозрительные действия и аномалии, они могут ответить на вопросы «что произошло?» и «почему это произошло?». Но, к сожалению, еще нет возможности предсказывать будущее в кибербезопасности, помимо некоторых узких сфер. Именно поэтому вопрос «что произойдет?» пока остается без ответа. И тем более пока нет ответа на вопрос «что я должен сделать?».

В течение последних 6 лет на рынке информационной безопасности было выявлено и зафиксировано более 220 поглощений, которые напрямую связаны с искусственным интеллектом. На сегодняшний день это направление вошло в пятерку наиболее распространенных сделок, а многие игроки рынка кибербезопасности (помимо отечественных) активно инвестируют в технологии машинного обучения, которые затем интегрируют в свои продукты [5].

К сожалению, конечный потребитель все еще не может достаточно активно пользоваться всеми преимуществами, которые дает искусственный интеллект, так как у него нет правильно обработанных датасетов, квалифицированных аналитиков, способных самостоятельно применять существующие модели анализа либо разработать свои [5].

Для того чтобы успешно пользоваться моделями машинного обучения, нужно четко понимать, что из себя представляет эта технология. Это требуется еще и для того, чтобы искать новые решения или эксплуатировать готовые.

Список литературы

1. Годин В.В., Корнеев И.К. Управление информационными процессами: 17-модульная программа для менеджеров «Управление развитием организации». Модуль 17. М.: ИНФРА-М, 2000. 512 с.

2. Голицына О.Л., Максимов Н.В., Попов И.И. Информационные системы: учебное пособие. ЭБС ЗНАНИУМ. 2-е изд. М.: Форум: НИЦ ИНФРА-М, 2014. 448 с.

3. Федотова Е.Л. Информационные технологии и системы: учебное пособие. М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. 352 с.

4. Skrypnikov A.V., Kozlov V.G., Denisenko V.V., Saranov I.A., Kuznetsova E.D., Savchenko I.I. Information security as the basis of digital economy. Advances in Economics, Business and Management Research. Proceedings of the Russian Conference on Digital Economy and Knowledge Management (RuDEcK 2020). 2020. P. 149–153.

5. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы. 2-е изд., испр. и доп. М.: ФИЗМАТЛИТ, 2010. 471 с.

6. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX: учебное пособие. СПб.: БХВ-Петербург, 2014. 635 с.

7. Гупал В.М. Математические методы анализа дискретных структур генетического кода. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2015. 334 с.