ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ В ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Ангапов В.Д.[1], Бобров А.В.[2], Тимонин В.А.[3], Вишняков А.С.[4]

[1]Ангапов Василий Данилович – старший системный архитектор, Digital IQ, г. Москва;
[2]Бобров Андрей Владимирович – ведущий системный инженер, EPAM Systems, г. Анталья, Турция;
[3]Тимонин Вадим Андреевич – системный инженер, Digital IQ, г. Казань;
[4]Вишняков Александр Сергеевич - старший архитектор, Digital IQ, г. Лакония, Соединенные Штаты Америки

Аннотация: *в современном мире активно интегрируются различные информационные технологии, вместе с чем повышаются и риски информационной безопасности. Цель представленной статьи заключается в анализе основных вопросов относительно обеспечения информационной безопасности информационных систем на основе использования интеллектуальных технологий. Научная ценность работы состоит в предпринимаемой попытке систематизации знаний относительно использования технологий машинного обучения при решении задач по обеспечению защиты данных в различных информационных системах. Статья имеет практическую значимость, заключающуюся в возможности использования представленных материалов с целью интеграции уже существующих и реализации новых эффективных методов машинного обучения для защиты информационных систем.*

Ключевые слова: *информационная система, машинное обучение, защита информации, искусственный интеллект.*

THE USE OF MACHINE LEARNING TECHNOLOGIES IN THE PROTECTION OF INFORMATION SYSTEMS

Angapov V.D.[1], Bobrov A.V.[2], Timonin V.A.[3], Vishnyakov A.S.[4]

[1]Angapov Vasily Danilovich – senior system architect, DIGITAL IQ, MOSCOW;
[2]Bobrov Andrey Vladimirovich – leading system engineer, EPAM SYSTEMS, ANTALYA, TÜRKIYE;
[3]Vadim Andreevich Timonin – systems engineer, DIGITAL IQ, KAZAN;
[4]Vishnyakov Alexander Sergeevich - senior architect, DIGITAL IQ, LACONIA, USA

Abstract: *in the modern world, various information technologies are being actively integrated, along with which the information security risks are also increasing. The purpose of the presented article is to analyze the main issues regarding the information security of information systems based on the use of intelligent technologies. The scientific value of the work consists in an attempt to systematize knowledge about the use of machine learning technologies in solving data protection problems in various information systems. The article has practical significance, which consists in the possibility of using the presented materials in order to integrate existing and implement new effective machine learning methods for the protection of information systems.*

Keywords: *information system, machine learning, information security, artificial intelligence.*

УДК 004.056.53

Информационные технологии (далее – ИТ) и информационные системы (далее – ИС), в частности, становятся неотъемлемой частью как в бытовых, так и профессиональных сферах жизнедеятельности современного человека. Устойчивые тенденции, связанные с их развитием и интеграцией, вызваны возможностью качественного изменения и повышения эффективности функционирования различных бизнес-процессов. В связи с этим практически каждое современное предприятие и организация направляют существенные инвестиции в сторону создания новых и интеграции уже существующих информационных технологий в своей деятельности [1].

Внедрение ИТ подразумевает отказ от бумажного документооборота и полного перехода на электронную форму ведения документации, хранения, передачи и использования информации. Несмотря на ряд объективных преимуществ, наблюдаемых при использовании инновационных технологий, появляются новые угрозы, связанные с обеспечением информационной безопасности (далее – ИБ). Так, актуализируется увеличение числа информационных атак, угроз и иных противоправных действий, направленных с целью хищения и фальсификации электронных данных. В связи с этим актуализируются вопросы и задачи, связанные

обеспечением информационной безопасности и должного уровня защиты данных в структуре современных предприятий и организаций, использующих различные ИС [2].

Задачи по обеспечению защиты информационных систем подразумевают необходимость проведения анализа большого объема данных в короткие сроки. Классические инструменты обеспечения информационной безопасности не способны предоставить такие возможности, в связи с чем появляется необходимость перехода на инновационные решения и инструменты. Одними из них являются интеллектуальные технологии, предоставляющие возможность анализировать большие объемы данных в режиме реального времени. Так, для возможности эффективного обеспечения защиты ИС необходимо использовать различные технологии искусственного интеллекта (далее – ИИ) и машинного обучения.

Машинное обучение (machine learning, ML) может использоваться для обнаружения аномального поведения в реальном времени, что представляет защиту информационных систем от активных атак. Автоматизация и соблюдение нормативов безопасности посредством ИИ упрощает процесс контроля безопасности ИС и способствует повышению надежности продуктов. Это, в свою очередь, имеет на сегодняшний день критически-важное значение в контексте постоянно возрастающих угроз информационной безопасности. Помимо этого, использование интеллектуальных технологий наблюдается и при решении других задач, основной целью которых является защита различных информационных систем. Так, на рис. 1 представлены основные направления использования технологии ИИ и машинного обучения при обеспечении безопасной работы программного обеспечения [3].

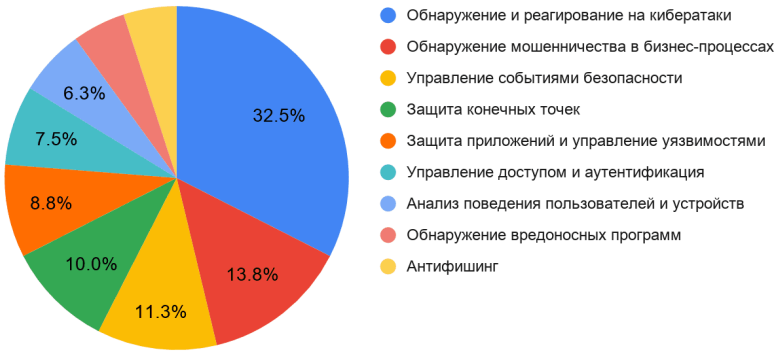

Рис. 1. Применение технологии ИИ в безопасной разработке ПО.

Искусственный интеллект также помогает в предсказании потенциальных угроз на основе анализа больших объемов, данных и паттернов поведения злоумышленников. Системы ML способны выявлять новые виды угроз, которые могли бы остаться незамеченными при традиционных методах анализа. Это позволяет ответственным работникам за обеспечение информационной безопасности быстро реагировать на изменяющиеся угрозы и адаптировать свои стратегии безопасности.

Одной из ключевых возможностей использования интеллектуальных технологий является обеспечение непрерывного определения угроз в информационной системе предприятия. Машинное обучение также может помочь в автоматизации процессов тестирования безопасности, включая сканирование уязвимостей. На рис. 2 представлен один из возможных алгоритмов решения задачи по обнаружению и идентификации угрозы ИБ в ИС предприятия. Это может улучшить эффективность выявления уязвимостей и сократить время, затрачиваемое на поиск и устранение проблем [4].

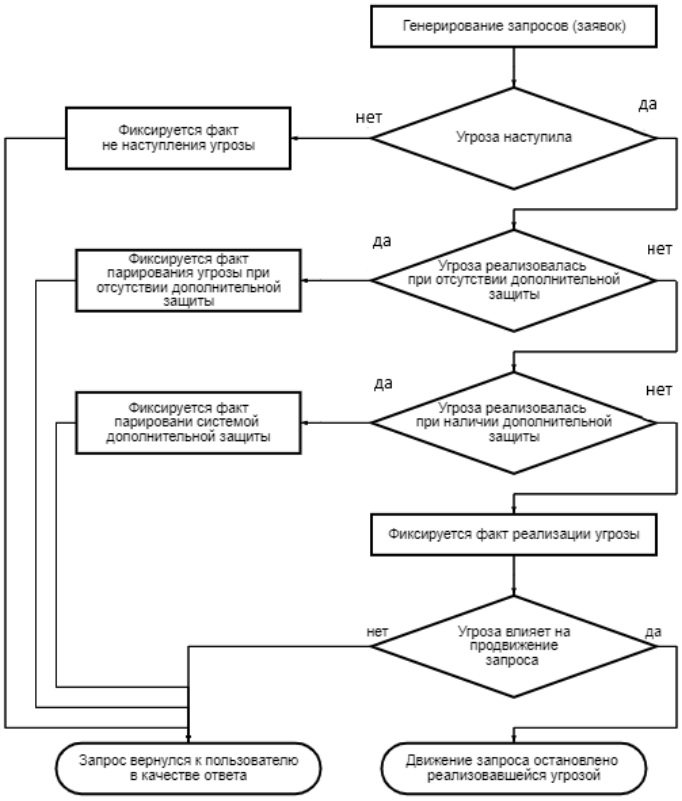

Рис. 2. Алгоритм универсальной модели определения угрозы.

Так, технологии машинного обучения имеют огромный потенциал в области защиты информационных систем. Они позволяют анализировать большие объемы данных и выявлять скрытые угрозы, которые могут быть незаметны для человека. Модели машинного обучения способны обучаться на основе большого количества исторических данных и выявлять аномалии с подозрительными активностями, что, в свою очередь, позволяет предотвратить наступление потенциальных атак и минимизировать ущерб для информационных систем [5].

Одним из основных преимуществ использования технологий ML в защите ИС является способность обнаруживать и идентифицировать новые и ранее неизвестные угрозы. Традиционные методы анализа данных могут быть неэффективными в случае появления новых видов атак, поскольку их работа основана на уже известных сигнатурах и шаблонах. В то время как алгоритмы машинного обучения могут обнаружить необычную или нехарактерную активность, которая может быть связана с неизвестными угрозами. Это позволяет оперативно реагировать на новые виды атак и разрабатывать соответствующие методы обнаружения и защиты.

На сегодняшний день существует множество уже готовых к использованию интеллектуальных инструментов, основанных на машинном обучении, для решения задач по защите информационных систем. Каждое из них может использоваться для решения совершенно различных задач ИБ:

- сканирования на уязвимости;
- мониторинга угроз в режиме реального времени;
- когнитивные решения, предназначенные для оценки новостей и актуальной информации из мира ИБ с целью формирования перечня новых угроз безопасности, и множество иных [6].

Далее представлены некоторые из наиболее эффективных инструментов машинного обучения, использование которых может стать актуальным средством по обеспечению защиты информационных систем современных предприятий:

- IBM Watson for Cyber Security. Эта система использует машинное обучение и когнитивные технологии для обнаружения и предотвращения кибератак. Решение анализирует большие объемы данных, включая логи, доклады о безопасности и новости о киберпреступности, чтобы обнаружить возникновение новых угроз в мире ИТ и предупредить о них;
- FireEye Malware Protection System. Данный инструмент использует алгоритмы машинного обучения для обнаружения и защиты от вирусов, троянов и вредоносного программного обеспечения. Он анализирует поведение программ и сетевой активности, чтобы идентифицировать и блокировать потенциально опасные угрозы;
- Darktrace Enterprise Immune System. Эта система использует технологии искусственного интеллекта и машинного обучения для обнаружения и защиты от угроз на ранних стадиях. Она учится отслеживать нор-

мальное поведение внутри информационной сети и сигнализировать о подозрительных активностях, таких как несанкционированный доступ или аномальный трафик данных;

- McAfee Advanced Threat Defense. Данная система использует алгоритмы машинного обучения для обнаружения и предотвращения сложных и хитрых угроз. Система анализирует поведение файлов и программ, чтобы идентифицировать потенциально вредоносные коды и блокировать их до того, как они причинят ущерб;

- Cybereason Endpoint Protection Platform. Эта платформа использует машинное обучение для обнаружения и блокировки вредоносных программ и неизвестных угроз. Она анализирует тысячи событий и сигналов, чтобы идентифицировать аномалии и потенциальные атаки, а затем принимает меры для их предотвращения и восстановления информационной системы [7].

Важно отметить, что это только некоторые из инструментов, основанных на машинном обучении, для защиты информационных систем. Существует множество других продуктов и решений, каждое из которых обладает своими уникальными функциями и возможностями.

При этом все программные инструменты в рассматриваемой области можно разделить следующие виды:

- системы предотвращения вторжений (IPS) на основе машинного обучения, которые могут обнаружить и заблокировать вредоносное программное обеспечение, даже если оно еще не известно специалистам ИБ;

- системы управления доступом (IAM) на основе машинного обучения, которые могут отслеживать поведение пользователей и выявлять подозрительную активность, которая может быть признаком угрозы или атаки;

- системы анализа данных на основе машинного обучения, которые могут выявлять аномалии в поведении ИС, указывающие на проблему информационной безопасности.

Итак, технологии машинного обучения предоставляют множество возможностей и преимуществ для повышения эффективности защиты информационных систем:

- во-первых, ML позволяет автоматизировать задачи, которые ранее выполнялись вручную. Например, ML может использоваться для анализа больших массивов данных, выявления аномальных событий и предотвращения вторжений. Это позволяет освободить персонал предприятия для выполнения более сложных и в то же время актуальных задач, таких как разработка новых методов защиты от потенциальных угроз ИБ;

- во-вторых, технологии машинного обучения позволяют адаптировать защиту ИС к меняющимся угрозам. ML-системы могут учиться на новых данных и адаптировать свои модели обнаружения угроз в соответствии с новыми тенденциями. Это помогает обеспечить более эффективную защиту от постоянно развивающихся угроз и вести непрерывный мониторинг уязвимостей информационной системы;

- в-третьих, ML позволяет персоналу принимать более обоснованные решения. ML-системы могут предоставлять персоналу информацию и рекомендации, которые помогают ему лучше понимать угрозы и принимать более обоснованные решения применительно к защите ИС.

Важными аспектами рассматриваемого направления являются риски и ограничения использования машинного обучения. В первую очередь необходимо отметить то, что для обучения таких систем информационной безопасности необходимо использование большого объема данных. При этом данные могут быть недоступны или содержать недостоверную информацию. Это, в свою очередь, способно привести к нарушениям в работе систем защиты данных, а также качества и эффективности при решении задач.

Другим ограничением является недостаток объяснимости интеллектуальных технологий. Средства, реализованные на основе машинного обучения, способны выполнять точные прогнозы, однако их решения остаются «черными ящиками», которые трудно объяснить человеку. В контексте рассматриваемого направления это может привести к значительным проблемам так как для принятия соответствующих мер по защите необходимо полное понимание причин и способов обнаружения атак. Для возможности решения данной проблемы на сегодняшний день начинает набирать популярность использование специального программного обеспечения, способного интерпретировать принятия решений искусственным интеллектом на язык человека. Примером подобного решения является продукт AVSOFT ATHENA.

Самая главная проблема заключается в недостаточной объективности алгоритмов машинного обучения. Рассматриваемые технологии могут быть предвзятыми, что в конечном итоге приводит к ложным срабатываниям или получению неправильных представлений о рисках. Так, к примеру, модель защиты информации на основе машинного обучения может ошибочно классифицировать обычные действия пользователя как подозрительные, основывая свое решение на предвзятых данных. Ложные срабатывания, в свою очередь, приводят к ненужным тревогам и перегрузке систем информационной безопасности. Для повышения точности работы в системе информационной безопасности могут использоваться сразу несколько интеллектуальных инструментов. Преимуществом такого варианта работы станет независимость и получение наиболее объективных решений.

Таким образом, основной целью представленной статьи являлось выполнение анализа относительно вопросов использования технологий машинного обучения в защите информационных систем. В рамках текущей работы определена актуальность развития информационных технологий и, как следствие, вопросов информационной безопасности. Определено, что одним из наиболее эффективных инструментов для обеспечения безопасности современных ИС являются интеллектуальные технологии. Представлены основные преимущества использования машинного обучения для решения данных задач, классификация программных

инструментов и реальные примеры, использование которых необходимо современным предприятиям и организациям для обеспечения должного уровня защиты информационных систем.

В заключение необходимо отметить, что технологии машинного обучения играют важную роль в обеспечении безопасности информационных систем. Одним из основных преимуществ таких технологий является их способность обнаруживать и предотвращать новые и ранее неизвестные виды атак. Кроме того, технологии машинного обучения способствуют автоматизации процесса обнаружения и реагирования на угрозы. Это позволяет повысить оперативность реагирования на инциденты ИБ и повысить эффективность принятия решений. Такие системы также способны обучаться на основе новых данных, улучшая свою производительность и адаптируясь к изменяющимся тенденциям в области информационной безопасности [8].

Список литературы / References

1. *Худхейр А.Р., Заргарян Е.В., Заргарян Ю.А.* Модели машинного обучения и глубокого обучения для электронной информационной безопасности в мобильных сетях // Известия ЮФУ. Технические науки. 2022. №3 (227). С. 211-222.
2. *Козин И.С., Рощин А.А.* Метод обеспечения безопасности информации при ее обработке в информационной системе на основе машинного обучения // Техника средств связи. 2019. №4 (148). С. 70-82.
3. *Ковцур М.М., Кириллов Д.И., Михайлова А.В., Потемкин П.А.* Разработка методики внедрения машинного обучения для повышения информационной безопасности web-приложения // Техника средств связи. 2020. №4 (152). С. 74-86.
4. *Артюшкина Е.С., Андирякова О.О., Тюрина Д.А*. Использование методов машинного обучения при анализе сетевого трафика и вредоносного программного обеспечения // Индустриальная экономика. 2023. №4. С. 12-15.
5. *Ожиганова М.И., Куртаметов Э.С*. Применение машинного обучения в защите веб-приложений // NBI-technologies. 2020. №2. С. 16-20.
6. *Щербаков А.Е.* Исследование применения искусственного интеллекта и машинного обучения в области кибербезопасности: техники обнаружения аномалий и предотвращения угроз // Вестник науки. 2023. №7 (64). С. 151-156.
7. *Власенко А.В., Дзьобан П.И., Жук Р.В.* Обзор инструментов машинного обучения и их применения в области кибербезопасности // Прикаспийский журнал: управление и высокие технологии. 2020. №1 (49). С. 144-155.
8. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды ИСП РАН. 2022. №5. С. 111-126.
9.