DOI 10.37882/2223-2966.2023.8-2.28

ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ

APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS TO ENSURE INFORMATION PROTECTION

A. Poluyan
E. Tseligorova
V. Galushka
N. Kodatsky

Summary. Intelligent information security methods are approaches based on the use of artificial intelligence (AI) and machine learning to increase the level of information protection and combat cyber threats. With the development of technology and the use of computers in various fields, data is one of the most valuable resources. Loss of data can lead to serious consequences and adversely affect the work of organizations and individuals. The use of AI technologies can help improve each of these aspects of information security. One of the most popular AI technologies in the field of information security is machine learning [1]. In the context of information security, this technology can be used to detect anomalies in network traffic, monitor protection systems, classify and filter malware, etc. Despite the fact that the use of AI in information security requires large amounts of data and powerful computing resources, the correct use of AI technologies can significantly increase the level of protection of information systems and data [2].

Keywords: artificial intelligence, information. security, network traffic, protection systems, machine learning.

Полуян Анна Юрьевна
Кандидат технических наук, доцент,
Донской государственный технический университет (Ростов-на-Дону)
orfiki@rambler.ru
Целигорова Елена Николаевна
Кандидат технических наук, доцент,
Донской государственный технический университет (Ростов-на-Дону)
eceligorova@donstu.ru
Галушка Василий Викторович
Кандидат технических наук, доцент,
Донской государственный технический университет (Ростов-на-Дону)
vgalushka@donstu.ru
Кодацкий Никита Максимович
Донской государственный технический университет (Ростов-на-Дону)

Аннотация. Интеллектуальные методы информационной безопасности — это подходы, основанные на использовании искусственного интеллекта (ИИ) и машинного обучения для повышения уровня защиты информации и борьбы с киберугрозами. С развитием технологий и использованием компьютеров в различных сферах, данные являются одним из наиболее ценных ресурсов. Потеря данных может привести к серьезным последствиям и негативно повлиять на работу организаций и частных лиц. Использование ИИ-технологий может помочь улучшить каждый из этих аспектов информационной безопасности. Одна из самых популярных технологий ИИ в области информационной безопасности — машинное обучение [1]. В контексте информационной безопасности, данная технология может использоваться для обнаружения аномалий в сетевом трафике, мониторинга систем защиты, классификации и фильтрации вредоносных программ и т.д. Несмотря на то, что использование ИИ в информационной безопасности требует больших объемов данных и мощных вычислительных ресурсов, правильное применение ИИ-технологий может существенно повысить уровень защиты информационных систем и данных [2].

Ключевые слова: искусственный интеллект, информация. безопасность, сетевой трафик, системы защиты, машинное обучение.

Искусственный интеллект является мощным инструментом для обеспечения безопасности цифровых систем [2]. Среди методов использования ИИ в информационной безопасности выделяются такие, как машинное обучение, глубокое обучение, нейронные сети, анализ данных и др.

Самым распространенным приемом прикладного применения ИИ в области информационной безопасности является мониторинг угроз. Многие системы мониторинга используют алгоритмы машинного обучения и нейронные сети для обнаружения угроз и аномалий в работе сети. Это позволяет быстро реагировать на возможные атаки и предотвращать сложные кибератаки до того, как они нанесут серьезный ущерб. Такие системы используют алгоритмы машинного обучения для построения моделей поведения злоумышленников, что позволяет более эффективно блокировать подозрительный трафик и отделять его от нормального.

Осуществление мониторинга безопасности на основе искусственного интеллекта можно разбить на следующие действия:

1. сбор данных: система собирает данные о действиях пользователей, событиях в системе, трафике

в сети и других параметрах, связанных с безопасностью;
2. обработка данных: полученные данные анализируются с помощью методов и технологий ИИ, таких как машинное обучение, нейронные сети и другие. Анализ может проводиться как в режиме реального времени, так и по результатам накопления данных;
3. выявление угроз: на основе анализа данных система определяет потенциальные угрозы безопасности, например, аномальные поведения пользователей, попытки несанкционированного доступа и т.д.;
4. реакция на угрозы: в зависимости от типа выявленных угроз, система может автоматически принимать меры для предотвращения атак или уведомлять операторов о возможной угрозе.

Такую последовательность действий можно реализовать с использованием языка python, который предоставляет множество возможностей для написания сетей искусственного интеллекта. Рассмотрим шаги алгоритма:

1. Импортируем необходимые библиотеки для анализа данных

```
import pandas as pd
import numpy as np
```

2. Загружаем данные о действиях пользователей в системе

```
data = pd.read_csv('user_actions.csv')
```

3. Преобразуем данные в формат, пригодный для анализа машинным обучением

```
X = data.drop(columns=['user_id', 'action_type'])
y = data['action_type']
```

4. Обучаем модель машинного обучения на исторических данных

```
from sklearn.ensemble import RandomForestClassifier
clf = RandomForestClassifier()
clf.fit(X, y)
```

5. Получаем данные о текущих действиях пользователей и предсказываем вероятность аномального поведения

```
current_data = pd.read_csv('current_user_actions.csv')
predictions = clf.predict_proba(current_data.drop(columns=['user_id']))
```

6. Анализируем результаты предсказаний и принимаем меры по предотвращению атак

```
if any(predictions[:, 1] > 0.9):
 send_alert_email('Detected abnormal user behavior')
 block_user_account()
else:
save_to_database(current_data)
```

Таким отразим, загружаем данные о действиях пользователей из файла, преобразуем их в формат, пригодный для машинного обучения, обучаем модель и используем ее для анализа текущих действий пользователей. Если модель выявляет аномальное поведение, то отправляется уведомление на почту и блокируем аккаунт пользователя. В противном случае, сохраняются данные в базу данных.

Использование интеллектуальных методов обнаружение вредоносного кода также является важной задачей в сфере информационной безопасности. В этой области ИИ используется для создания более точных и разнообразных моделей классификации вредоносных программ и анализа сигнатур вредоносных программ [2].

Более того, информация, содержащаяся в логах, также может быть использована для выявления угроз и определения наличия подозрительной активности. Использование методов машинного обучения и анализа данных позволяет быстро и точно обрабатывать большие объемы логов и выявлять скрытые угрозы. Однако, важно помнить, что методы ИИ не являются универсальными решениями и требуют глубокого понимания проблемы, а также экспертизы и оценки специалистов в области информационной безопасности.

Различные приложения ИИ применяются во многих областях информационной безопасности.

Одна из наиболее распространенных сфер — это защита персональных данных. Обработка больших объемов персональной информации требует высокого уровня конфиденциальности. Для этого ИИ используется для создания алгоритмов шифрования и дешифрования информации, а также для определения подозрительной активности и предотвращения утечек данных [1–2]. Использование алгоритмов шифрования на основе ИИ позволяет создать более сложные и надежные алгоритмы, которые сложнее поддаются перебору. Кроме того, ИИ может использоваться для мониторинга сетевого трафика и обнаружения подозрительной активности. Например, ИИ может определять, когда пользователь пытается получить доступ к данным, к которым он не имеет разрешения, или когда происходит необычный запрос на сервер. Если ИИ обнаруживает такую подозрительную активность, он может автоматически заблокировать доступ к данным и уведомить администратора о возможной попытке несанкционированного доступа.

Создание алгоритмов шифрования и мониторинга сетевой активности на основе ИИ помогает защитить персональные данные клиентов от несанкционированного доступа и утечек. Но зачастую безопасность информационных систем зависит не только от технических

решений, но и от культуры безопасности компании и обученности ее сотрудников.

Приведем примеры использования ИИ-технологий для защиты информации в организациях.

1. В облачных системах, которые становятся все более популярными среди пользователей, с помощью ИИ можно обнаруживать и предотвращать кибератаки, а также анализировать поведение злоумышленников в защищенных облачных системах [3]. К примеру, компания использует облачную платформу для хранения и обработки своих данных. Чтобы защитить данные от кибератак и других угроз, компания может использовать ИИ-технологии для обнаружения аномалий в сетевом трафике и анализа поведения злоумышленников. Например, ИИ может мониторить входящие и исходящие запросы на сервер, чтобы выявлять необычные паттерны трафика, которые могут указывать на попытку кибератаки или другую подозрительную активность. Если ИИ обнаруживает аномалию, он может автоматически блокировать доступ к серверу и отправлять уведомление администратору об угрозе. Кроме того, ИИ может использоваться для анализа поведения злоумышленников в защищенных облачных системах. Например, ИИ может анализировать лог-файлы, чтобы выявлять типичные особенности действий злоумышленников, такие как время их активности, использование определенных программ и т.д. На основе этого анализа, ИИ может создавать профили злоумышленников и использовать эти данные для обнаружения подозрительной активности и предотвращения кибератак.

Использование ИИ поможет защитить данные компании от потенциальных угроз. Однако, важно понимать, что безопасность облачных систем зависит не только от технических решений, но и от политик безопасности компании и обученности сотрудников в области информационной безопасности.

2. В финансовой сфере, где конфиденциальность и безопасность транзакций являются критически важными, применение ИИ может обеспечить дополнительный уровень защиты. ИИ можно использовать для определения подозрительных операций и фиксации аномалий в финансовых транзакциях [2–4]. Допустим, банк использует ИИ-алгоритмы для мониторинга финансовых операций. Алгоритмы ИИ могут анализировать проводимые транзакции и определять необычные паттерны, которые могут указывать на мошеннические операции или другую подозрительную активность. Например, ИИ может автоматически анализировать транзакции клиентов и выявлять переводы в незнакомые страны, необычно большие транзакции или несколько транзакций с разных устройств в краткое время. Если ИИ обнаруживает подозрительную активность, он может отправить уведомление контрольному центру банка, который затем может проанализировать транзакцию более детально и принять решение о блокировке операции или связаться с владельцем счета для проверки подлинности операции. Кроме того, ИИ может использоваться для создания алгоритмов предотвращения мошенничества. Например, ИИ может анализировать данные клиента и его историю операций, чтобы определить, какие операции скорее всего будут нормальными для этого клиента. Если ИИ обнаруживает необычную операцию, он может отправить уведомление контрольному центру для дополнительной проверки.

Такое использование ИИ может помогает банкам защитить своих клиентов от потенциальных мошеннических операций и других видов финансовых преступлений. Однако, важно понимать, что ИИ должен использоваться в сочетании с другими методами безопасности, такими как обучение персонала и использование аутентификации двухфакторной аутентификации, необходимой для авторизации транзакций.

3. Банковские операции также могут быть эффективнее обеспечены за счет применения различных приложений ИИ. Для этого ИИ используется для обнаружения мошеннических операций, а также для создания алгоритмов выявления сомнительной активности счетов [2-5]. Например, банк использует ИИ-алгоритмы для мониторинга транзакций на банковских счетах. Эти алгоритмы могут определять необычные сценарии использования счетов и обнаруживать мошеннические операции или другую подозрительную активность. ИИ может автоматически анализировать паттерны использования счетов и выявлять переводы в незнакомые страны или необычно большие транзакции. Если ИИ обнаруживает подозрительную активность, он может отправить уведомление контрольному центру банка, который затем может проанализировать транзакцию более детально и принять решение о блокировке операции или связаться с владельцем счета для проверки подлинности операции. Кроме того, ИИ также может использоваться для создания алгоритмов предотвращения мошенничества. Например, анализировать данные клиента и его историю операций, чтобы определить, какие операции скорее всего будут нормальными для этого клиента. Если будет обнаружена неприсущая операцию, он может от-

править уведомление контрольному центру для дополнительной проверки.

Использование ИИ для обнаружения мошенничества и создания алгоритмов выявления подозрительной активности помогает банкам защитить своих клиентов от потенциальных мошеннических операций и других видов финансовых преступлений. Однако, важно понимать, что ИИ должен использоваться в сочетании с другими методами безопасности, такими как обучение персонала и использование аутентификации двухфакторной аутентификации, необходимой для авторизации транзакций.

4. Электронная коммерция также становится все более популярной, и ее безопасность играет ключевую роль в успешной работе интернет-магазинов и других электронных площадок [2]. В данном контексте, применение ИИ может обеспечить защиту от кибератак и утечек данных, а также помочь в создании индивидуальных предложений и рекомендаций для пользователей на основе анализа их поведения [2]. Алгоритмы ИИ могут анализировать данные о покупках, предпочтениях и поведении клиентов, чтобы создавать индивидуальные предложения и рекомендации для каждого пользователя. ИИ может использоваться для обеспечения безопасности электронных платежей и защиты от кибератак. Например, ИИ может мониторить транзакции и выявлять необычные паттерны транзакций, которые могут указывать на мошенническую активность. Если ИИ обнаруживает подозрительную операцию, он может блокировать транзакцию и отправлять уведомление администратору сайта для проверки.

Персонализация электронной коммерции с использованием ИИ поможет в обеспечении безопасности интернет-магазина. Это поспособствует привлечению клиентов и защищать их данные от потенциальных угроз. Однако, важно понимать, что ИИ должен использоваться в сочетании с другими методами безопасности, такими как использование SSL-шифрования и двухфакторной аутентификации для обеспечения максимальной защиты данных пользователей.

Системы информационной безопасности на основе ИИ имеют множество преимуществ, таких как повышение эффективности, автоматизация процессов, уменьшение затрат и увеличение скорости реакции на угрозы. Однако, их использование может также привести к ряду серьезных недостатков и рисков.

Один из главных преимуществ — это возможность повысить эффективность защиты данных и оперативно реагировать на угрозы. Функции ИИ, такие как машинное обучение и анализ больших объемов данных, позволяют быстро выявлять уязвимости в системах и предотвращать кибератаки [6-8]. Автоматизация процессов и использование ИИ также может уменьшить затраты на информационную безопасность. Большинство задач по обеспечению безопасности могут быть выполнены алгоритмами ИИ без необходимости найма дополнительных сотрудников. Системы ИИ могут быстро реагировать на изменяющуюся угрозу и предотвращать возможные атаки до того, как они нанесут серьезный ущерб.

Однако, использование ИИ в информационной безопасности также связано с рисками и недостатками. Один из основных рисков — это потенциальная угроза конфиденциальности. Алгоритмы ИИ могут обрабатывать большие объемы данных, включая личную информацию пользователей, что может привести к утечкам данных и нарушению конфиденциальности. Кроме того, ошибки в алгоритмах ИИ являются еще одним серьезным недостатком этой технологии в информационной безопасности. Ошибочный анализ данных или неверное определение угрозы может привести к созданию ложных срабатываний и сбоям в работе систем безопасности [7–10]. Возможность злоупотребления ИИ также является риском для безопасности. Злоумышленники могут использовать ИИ для создания более сложных и запутанных кибератак, что усложняет процесс их выявления и предотвращения.

Таким образом, использование ИИ в информационной безопасности имеет как преимущества, так и недостатки, и требует глубокого понимания технологии и экспертизы специалистов в области информационной безопасности. Однако, при правильном подходе, ИИ может значительно повысить защиту данных и обеспечить эффективность работы сети.

Заключение

Выработка стратегий использования ИИ в информационной безопасности должна происходить на основе оценки эффективности. Стратегия должна определять цели, задачи и ожидаемые результаты, а также методы и технологии, которые будут использоваться для достижения поставленных целей. Машинное обучение, например, может быть быстро настроено для работы с новыми данными, однако требует больших объемов информации для обучения. Нейронные сети могут создавать более точные модели поведения злоумышленников, но их настройка может быть сложной и требовательной к вычислительным ресурсам. Анализ данных позволяет создавать детальные анализы информации, но для этого требуются квалифицированные специалисты. Но при выборе метода следует учитывать не только его преимущества, но и недостатки и риски, связанные с его использованием. Таким образом, методы ИИ в ин-

формационной безопасности могут быть использованы для предотвращения кибератак, обеспечения защиты персональных данных, анализа пользовательской активности и других задач. При этом необходимо учитывать как преимущества, так и недостатки этих технологий и находить решения, которые будут обеспечивать высокую безопасность при минимальном вмешательстве в личную жизнь пользователей. Важным преимуществом использования ИИ в информационной безопасности является возможность автоматизации процессов, что позволяет оперативно реагировать на угрозы и защищать цифровые системы. Поэтому необходимо постоянно совершенствовать технологии ИИ и находить баланс между безопасностью и защитой личных данных.

ЛИТЕРАТУРА

1. Клод Т. Машинное обучение и кибербезопасность — изд. Омега-Л, 2020. — 350 с.
2. Домминг Р. Искусственный интеллект и информационная безопасность — изд. Питер, 2019. — 400 с.
3. Burkov A. The Hundred-Page Machine Learning Book — изд. MIT Press, 2018. — 500 с.
4. Francois C. Deep Learning with Python — изд. Manning Publications, 2017. — 384 с.
5. Deitel P. Python for Artificial Intelligence, Big Data, and Cloud Computing –изд. Pearson, 2019. — 600 с.
6. Уильям С. Безопасность компьютерных систем. Программирование защиты — изд. Питер, 2005. — 560 с.
7. Goodfellow I., Bengio Y., и Courville A. Deep Learning Network — изд. MIT Press, 2016. — 800 с.
8. Aggarwal C. Neural Networks and Deep Learning — изд. Springer, 2018. — 360 с.
9. Geron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow — изд. Packt Publishing, 2018. — 800 с.
10. Richard S. Sutton и Andrew G. Barto. Reinforcement Learning: An Introduction — изд. Packt Publishing, 2017. — 216 с.