Рисунок 3 – Функциональная модель «Как будет» - обучение персонала

Таким образом в результате внедрения виртуального тренажера будет расширен функционал отдела кадров и отдела обучения, повысит пропускную способность и уменьшит рабочие часы некоторых специалистов.

Окатов Д.А., Минеева Т.А.

Технологии искусственного интеллекта в информационной безопасности

*Северный (Арктический) федеральный университет имени М. В. Ломоносова
(Россия, Архангельск)*

doi: 10.18411/lj-06-2021-67

Аннотация

Данная статья посвящена изучению технологии искусственный интеллект и его применение в информационных системах с целью обеспечения безопасности данных и защиты информации.

Ключевые слова: информационная безопасность, искусственный интеллект, информация, платформы обнаружения атак.

Abstract

This article is devoted to the study of artificial intelligence technology and its application in information systems in order to ensure data security and information protection.

Keywords: information security, artificial intelligence, information, attack detection platforms.

С развитием компьютерных систем информационная безопасность занимает важное место в современном мире. Технологии искусственного интеллекта широко применяются в информационных системах с целью защиты информационных систем от несанкционированного доступа.

Информация - любые сведения, принимаемые и передаваемые, сохраняемые различными источниками [4].

С развитием компьютерных технологий и программного обеспечения появляется необходимость в защите информации от перехвата злоумышленниками, её утечки по информационным каналам. Решением данной проблемы является применение технологий искусственного интеллекта в сфере информационной безопасности.

Искусственный интеллект – свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека [3].

В настоящее время все больше устройств нуждаются в защите информации от перехвата злоумышленниками. Мошеннические организации стали применять искусственный интеллект для незаконного присваивания информации, поэтому организации по защите информации внедряют платформы и системы для предотвращения атак, в основе которых лежат технологии искусственного интеллекта.

Рисунок 1 – Системы и платформы обнаружения атак

- EDR - Endpoint Detection and Response - платформы обнаружения атак на рабочих станциях, серверах, любых компьютерных устройствах (конечных точках) и оперативного реагирования на них. На основе базы знаний, накопленной со множества устройств, данные платформы обнаруживают, определяют вид и тип угрозы и самостоятельно реагируют на неё.
- NDR - Network Detection and Response - устройства и аналитические платформы, которые обнаруживают атаки на сетевом уровне и позволяют оперативно на них реагировать. На основе базы знаний и статистики, данные платформы выявляют угрозы в сетевом трафике и автоматически реагируют на них.
- UEBA - User and Entity Behavior Analytics - системы поведенческого анализа пользователей и информационных сущностей. Данные системы детектируют необычное поведение и используют его для обнаружения внутренних и внешних угроз.
- TIP - Threat Intelligence Platform - платформы раннего детектирования угроз и реагирования на них, действующие на основе большого количества различных данных и индикаторов компрометации.

Применение искусственного интеллекта позволяет повысить результативность выявления неизвестных угроз на ранних этапах.

- 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, искусственный интеллект помогает не только проводить анализ, но и автоматически реагировать надлежащим образом на выявленные угрозы.
- Средства защиты приложений - Application Security - системы, позволяющие определять угрозы безопасности прикладных приложений. Данные системы осуществляют автоматический сбор информации об уязвимостях, атаках и заражениях, доступной в открытых источниках и запускает сценарий защитных действий, таких как сканирование на уязвимости, изменение правил защиты для веб-приложений, выявление угроз и изменения рисков модели [1].

Технологии искусственного интеллекта активно применяются в антивирусных программах, файерволах. К ним относятся продукты Лаборатории Касперского, компании ESET, а также во встроенном защитнике операционной системы Windows «Windows Defender».

Благодаря внедрению данных систем и платформ с искусственным интеллектом, уровень обнаружения угроз значительно повышается, сокращается время реакции и совершенствуются способы определения реальных попыток нарушения периметра безопасности.

Технологии искусственного интеллекта помогают не только предотвращать атаки мошенников на информационные системы, но и защищать данные благодаря системам аутентификации и разделения деятельности пользователей по ролям.

В большинстве случаев вход в систему осуществляется через логин и пароль, что является самым популярным методом защиты информации, но не самым надежным. С развитием технологий искусственного интеллекта данный метод защиты информации не является преградой для злоумышленников. Поэтому прибегают к биометрической аутентификации. Данный метод значительно безопаснее, поскольку используются уникальные данные человека: отпечаток пальца, радужная оболочка глаза, геометрия руки, лица, голос.

Рисунок 2 – Биометрическая аутентификация по отпечатку пальца

Перехват информации может происходить без ведома пользователей, так как её передача происходит через множество информационных каналов. Данная ситуация происходит при удаленном подключении к различным системам. Для предотвращения перехвата используется динамическая среда аутентификации.

Системы искусственного интеллекта создают глобальную среду аутентификации в режиме реального времени, которая изменяет привилегии доступа в соответствии с местоположением или сетью, используя многофакторную аутентификацию, включающую в себя сбор данных и анализ поведения пользователя в приложении, устройстве или сети при удаленном доступе к данным.

На основе проведенных исследований рассмотрены технологии искусственного интеллекта в информационной безопасности с целью предотвращения атак злоумышленниками и защиты от перехвата данных. Искусственный интеллект вносит заметный вклад в борьбу с современными информационными угрозами, а также внедрение технологий искусственного интеллекта в информационной безопасности сокращает время выявления проблем и реагирования на инциденты.

1. AntiMalware [Электронный ресурс] / Искусственный интеллект в информационной безопасности – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security, свободный (Дата обращения: 11.03.2021)
2. Информатика // Большая российская энциклопедия / Кравец С. Л. — М.: ОАО «Научное издательство «Большая Российская Энциклопедия», 2008. — Т. 11. Изучение плазмы - Исламский фронт спасения. — С. 481—484. — 767 с.
3. Habr [Электронный ресурс] / Искусственный интеллект трансформирует информационную безопасность, но не стоит ждать мгновенных перемен – Режим доступа: https://habr.com/ru/company/vps_house/blog/344664/, свободный (Дата обращения: 02.04.2021)
4. Investments Academic [Электронный ресурс] / Информация – Режим доступа: <https://investments.academic.ru/1012/Информация>, свободный (Дата обращения: 04.04.2021)
5. Афанасьева, Д.В. Применение искусственного интеллекта в обеспечении безопасности данных [Текст] / Д.В. Афанасьева // Известия ТулГУ. Технические науки. – 2020. – Выпуск 2. – С. 151 – 154.

Панченко (Морозова) Н.В., Шаханова Р.Д.

Исследование уровня инфляции с помощью множественного регрессионного анализа

*Северо-Кавказская государственная академия
(Россия, Черкесск)*

doi: 10.18411/lj-06-2021-68

Аннотация

В статье определена тема исследования, её актуальность, объект, предмет и цель исследования. А также проведен множественный регрессионный анализ.

Ключевые слова: уровень инфляции, прогнозирование, множественный регрессионный анализ.

Abstract

The article defines the research topic, its relevance, object, subject and purpose of the research. A multiple regression analysis was also performed.

Keyword: inflation rate, forecasting, multiple regression analysis.