УДК 004.896

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ РЕШЕНИЯ ГЛОБАЛЬНОЙ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННОМ МИРЕ

Д. И. Муравицкий[1)], А. Д. Петрович[2)]

[1)] *магистр, преподаватель-стажёр, Белорусский государственный университет, экономический факультет, г. Минск, Беларусь, e-mail: muravickijd@gmail.com*
[2)] *магистр, преподаватель-стажёр, Белорусский государственный университет, экономический факультет, г. Минск, Беларусь, e-mail: am.lina.petrovich@gmail.com*

Технический прогресс и, в частности, развитие мощных компьютерных систем хранения и обработки информации многократно повысили роль информации в современном мире. В связи с чем, возникла острая необходимость в защите как персональных данных, так и секретной информации организации. Особую роль в обеспечении безопасности информации играет динамично развивающиеся технологии искусственного интеллекта. Востребованность данной технологии обусловлена способностью обрабатывать большое количество событий, автоматизировать действия аналитиков и обеспечивать оперативное реагирование на возникшие угрозы.

Ключевые слова: защита информации; информационная безопасность; технологии искусственного интеллекта.

ARTIFICIAL INTELLIGENCE AS A TOOL FOR SOLVING THE GLOBAL PROBLEM OF INFORMATION PROTECTION IN THE MODERN WORLD

D. I. Muravitsky[1)], A. D. Petrovich[2)]

[1)] *Master's Degree, Trainee Teacher, Belarusian State University, Faculty of Economics, Minsk, Belarus, e-mail: muravickijd@gmail.com*
[2)] *Master's Degree, Trainee Teacher, Belarusian State University, Faculty of Economics, Minsk, Belarus, e-mail: am.lina.petrovich@gmail.com*

Technological progress and, in particular, the development of powerful computer systems for storing and processing information have greatly increased the role of information in the modern world. In this connection, there is an urgent need to protect both personal data and classified information of the organization. Dynamically developing artificial intelligence technologies play a special role in ensuring information security. The demand for this technology is due to its ability to process a large number of events, automate the actions of analysts and ensure a prompt response to emerging threats.

Keywords: information protection; information security; artificial intelligence technologies.

Стремительное развитие информационных технологий в современном мире превратили информацию в важнейший ресурс развития экономики. На сегодняшний день все больше появляются отрасли, которые почти полностью состоят только из информации [3], а вместе с тем особую популярность получили системы хранения и обработки данных, где процесс хранения от персональных данных до секретной информации организации играет значительную роль.

Ввиду этого, наиважнейшей проблемой современного мира является защита информации и информационная безопасность. Под термином «информационная безопасность» подразумевают защиту информации от преднамеренных или случайных воздействий искусственного или естественного характера, чреватых нанесением информации неисправимых повреждений, тем самым причинив владельцам или пользователям информации ущерб [1]. С целью предотвращения хищения или повреждения информации злоумышленниками, предприятия разрабатывают ряд мероприятий и технических средств, применяющихся на всех этапах работы с информацией. Важно так же учитывать, что защищать от ущерба необходимо и оборудование, на котором храниться информация, а также каналы связи.

Специалистами выдвинуты три главных свойства, по которым можно судить о степени защищённости информации:

– целостность представляет собой обеспечение достоверности и корректного отображения охраняемых данных; Обработка данных должна происходить без сбоев, а пользователи не должны сталкиваться с различными непредвиденными модификациями, сбоями в работе программного обеспечения;

– конфиденциальность означает, что доступной для просмотра и редактирования информация становится только для авторизированных пользователей системы защиты;

– доступность предполагает наличие доступа к защищённой информации для всех авторизированных в системе пользователей [5].

Нарушение даже одного из свойств защитной информации достаточно, чтобы использование системы стало бессмысленным.

В целях обеспечения защиты информации предприятия:

– разрабатывают внутреннюю документацию, в которой регламентируются свод правил работы с компьютерной техникой и корпоративной информацией;

– проводят внутренние инструктажи и периодические проверки персонала;

– инициируют подписание дополнительных соглашений к трудовым договорам, в которых обозначается ответственность за разглашение или использование в личных целях корпоративной информации;

– распределяют ответственность среди нескольких должностных лиц, в целях предотвращения скопления важных массивов информации в распоряжении одного лица;

– помещают копирование информации под ключ, чтобы предотвратить неконтролируемое распространение или уничтожение корпоративной информации;

– разрабатывают и корректируют план восстановления системы на случай возникновение непредвиденных неполадок [2].

Особую роль в безопасности информации играет динамично развивающиеся технологии искусственного интеллекта (ИИ). Использование новейших технологий на базе ИИ обусловлено, в первую очередь, необходимость немедленного реагирования при возникновении уязвимости в системе защиты информации, а во-вторых, снижением человеческого фактора при реагировании на кибер-атаки. Например, непосредственно перед нанесением урона системе, злоумышленники реализуют «отвлекающий манёвр», активируя DDoS-атаку или сетевое сканирование, что отвлекает сотрудников от нанесения скрытой более крупной кибер-атаки [4]. В связи с данным фактором, всё большее число организаций прибегают к использованию искусственного интеллекта для обеспечения защиты персональных и корпоративных данных. В связи с их способностью обрабатывать огромные массивы данных, автоматизировать рабочий процесс специалистов, а также обеспечивать оперативное реагирование на возникшие угрозы. Вышеизложенное позволяет выделить третий фактор преимущества использования технологий ИИ в обеспечении информационной безопасности предприятия – использование злоумышленниками технологий искусственного интеллекта, следовательно, целесообразно использовать симметричные по уровню технологичности меры.

Библиографические ссылки

1. *Батаева И. П.* Защита информации и информационная безопасность // Труды Международного симпозиума «Надежность и качество». 2012. С. 1–4.

2. *Грачёва Е. А.* Информационная безопасность // The Newman in Foreign policy. 2020. № 54. С. 57–59.

3. *Козачок В. И., Власова С. А.* Информация и её значение в процессе развития современного общества // Гуманитарные, социально-экономические и общественные науки. 2014. С. 102–124.

4. *Шананин В. А.* Применение систем искусственного интеллекта в защите информации // Инновации и инвестиции. 2022. № 11. С. 201–205.

5. *Яшина А. М.* Современные способы защиты информации и информационная безопасность // Труды Международного симпозиума «Надежность и качество». 2018. № 2. С. 104–106.