ОЦЕНКА АКТУАЛЬНОСТИ И ЭФФЕКТИВНОСТИ ИНТЕГРАЦИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СЕГМЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ASSESSMENT OF THE RELEVANCE AND EFFECTIVENESS OF THE INTEGRATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN THE INFORMATION SECURITY SEGMENT

Авторы: *Попов Валентин Геннадьевич (МТУСИ)*
Галиаскаров Денис Фидарисович (МТУСИ)
Болябкин Михаил Владимирович (МТУСИ)

Аннотация: *Основной целью данной работы является изучение актуальности использования интеллектуальных средств в работе систем информационной безопасности. В статье изучаются основные сведения, актуальность и эффективность интеграции интеллектуальных средств в задачах защиты информации. Работа производится посредством применения теоретических и эмпирических методов исследования. Новизна представленной работы заключается в обобщении и систематизации знаний, касающихся актуальности вопросов интеграции технологий искусственного интеллекта в задачах информационной безопасности. Для наиболее полного раскрытия темы и получения достоверных данных автором используются научные материалы отечественных и зарубежных источников.*

Ключевые слова: *информационная безопасность, искусственный интеллект, информационные системы, атака, информация, защита.*

Annotation: *The main purpose of this work is to study the relevance of the use of intelligent tools in the work of information security systems. The article examines the basic information, relevance and effectiveness of the integration of intelligent tools in the tasks of information security. The work is carried out by applying theoretical and empirical research methods. The novelty of the presented work lies in the generalization and systematization of knowledge concerning the relevance of the issues of integration of artificial intelligence technologies in information security problems. For the most complete disclosure of the topic and obtaining reliable data, the author uses scientific materials from domestic and foreign sources.*

Keywords: *information security, artificial intelligence, information systems, attack, information, protection.*

В современном мире непрерывно и с невероятно высокой скоростью увеличивается число информационных архивов, переводов денежных средств и коммуникаций в цифровую форму, в результате чего был создан самостоятельный вид актива, называемый информацией. Равносильно иным ценностям, информация подвержена нападению со стороны различных хакерских и мошеннических атак. В совокупности данных факторов на сегодняшний день существует ряд рисков, относящихся к

области информационной безопасности [1].

Одними из наиболее актуальных технологий, активно разрабатывающимися и тестируемых в задачах информационной безопасности на современных предприятиях, являются интеллектуальные средства. Одной из основных технологий, относящихся к сфере ИТ, а также имеющих колоссальное влияние во многих процессах, происходящих в современном мире, является искусственный интеллект. Актуальность использования искусственного интеллекта (ИИ) как никогда высока в современном мире. Именно посредством данных технологий на сегодняшний день решаются одни из самых крупных и сложно-вычислимых задач. Искусственный интеллект находит применение не только при решении математических и иных инженерных задач для принятия оптимальных решений, данная технология успешно применяется в сфере защиты информации [2].

Интеграция искусственного интеллекта в системы информационной безопасности является достаточно новым и малоизученным на сегодняшний день направлением. Данный фактор связан с тем, что сами по себе интеллектуальные средства находятся в стадии развития, исходя из чего и смежные с данной технологией направления также нуждаются в более детальном и глубоком изучении и анализе.

Необходимо отметить, что ключевой технологией, на базе которой основывается искусственный интеллект, которая также определяет актуальность его использования, является возможность к «самообучению» и использованию накопленных данных с целью прогнозирования будущего. Основной отличительной особенностью в ИИ относительно обычных цифровых решений является то, что при выполнении задач искусственный интеллект не основывается на логических схемах, заданных ранее программистами, а самостоятельно производит настройку комплексных механизмов для принятия решений, основываясь на тех данных и задачах, которые были изначально поставлены программистами [3].

Одним из новых направлений развития искусственного интеллекта при решении задач информационной безопасности является интеграция искусственных нейронных сетей. Нейронные сети, имеющие аналогичное по смыслу названия искусственные нейронные сети (ИНС) или нейросети, выступают в качестве математической модели, которая имеет программную и аппаратную реализацию. ИНС выстраиваются на

принципиальной базе биологических сетей, а именно по принципу сетей нервных клеток живых существ.

На рис. 1 представлена схема простой нейронной сети [3]:

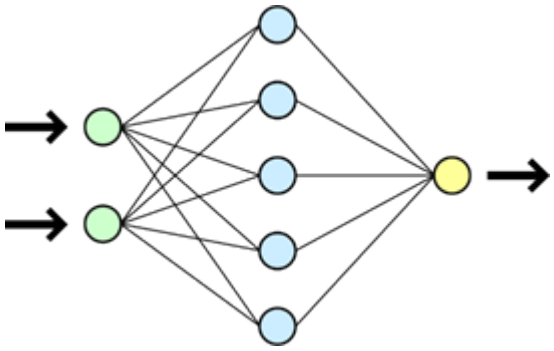

Рис. 1. Схема простой нейросети. Зеленые – входные нейроны; голубые – скрытые нейроны; желтые – выходной нейрон

В математическом интерпретировании искусственный нейрон представляется в виде нелинейной функции. Под w характеризуются связи, посредством которых сигналы от одних нейронов поступают во входные сигналы других нейронов. Каждый из ИНС нейрон включает в себя единственный выход, называющийся синапсом. Необходимо отметить, что каждый выход нейрона связан (или может быть связан) с неограниченным числом выходов других нейронов (рис. 2). Для понимания запишем следующую математическую модель искусственного нейрона [4]:

$$y = f(\sum_{i=1}^{n}(w_i \cdot x_i + b_i)), \quad (1)$$

где w_i – представляют веса соответствующих входов;

x_i – представляют сигналы на входах нейрона;

b_i – представляют вход и вес нейрона смещения.

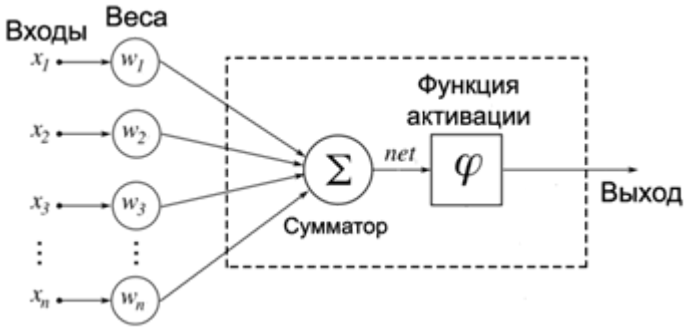

Рис. 2. Схема искусственного нейрона

Современные предприятия, которые внедряют технологии искусственного интеллекта и, в частности, ИНС в системы информационной безопасности, получают колоссальные результаты, выражающиеся в повышении эффективности обнаружения атак на информационные ресурсы. На рис. 3 представлено распределение продуктов ИБ с применением технологий ИИ [4]:

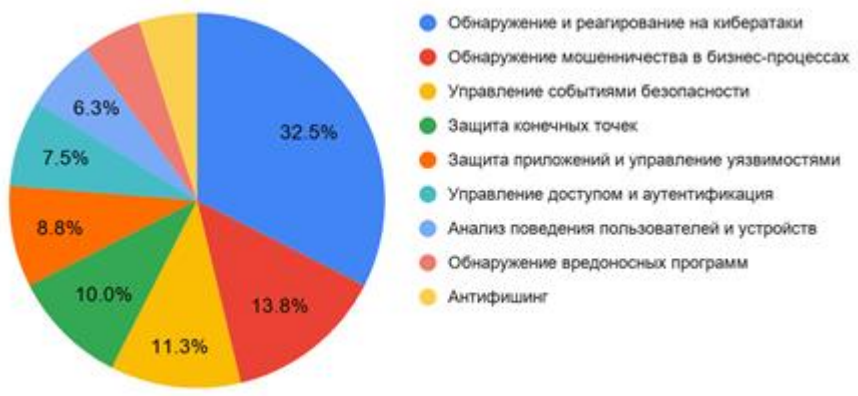

Рис. 3. Распределение продуктов с применением технологий ИИ

Большинство компаний, активно использующие ИНС с целью повышения эффективности работы систем защиты информации подтверждают, что интеллектуальные технологии повышают эффективность в расследовании инцидентов, уменьшение времени реакции на угрозы, повышают эффективность управления персоналом и др. Также многими представителями компаний подтверждается факт сокращения количества ложных срабатываний в результате интеграции нейронных сетей в системы информационной безопасности.

Таким образом, искусственный интеллект и, в частности, ИНС являются наукой и технологией создания интеллектуальных машин, подавляющее большинство которых являются интеллектуальными компьютерными программами. Технологии ИИ в широком смысле подразумевают программное обеспечение, имеющее возможность к выполнению задач посредством использования когнитивных способностей человека, к примеру, распознавание речи, интерпретация визуальных образов, анализ логических операций, создание моделей будущего на основе накопленных данных и др., что является наиболее эффективным инструментом в решении задач информационной безопасности на современных предприятиях [5].

Технологии искусственного интеллекта являются одними из самых инновационных и прорывных достижений науки на сегодняшний день. Данные средства повсеместно внедряются практически во всех сферах жизнедеятельности современного человека, начиная от бытовых, и заканчивая профессиональными. В данной работе были более подробно изучены вопросы, касающиеся актуальности использования интеллектуальных средств в задачах информационной безопасности.

Литература

1. Балановская А.В. Анализ современного состояния угроз информационной безопасности предприятий // Информационная безопасность регионов. 2015.
2. Сырецкий Г.А. Искусственный интеллект и производственная безопасность: настоящее и будущее // Интерэкспо Гео-Сибирь. 2016.
3. Dubina I. V., Slavyanov A. S. Artificial intelligence as a tool to improve the effectiveness and sustainability of the business // Economics and business: theory and practice. 2019.
4. Афанасьева Д.В., Применение искусственного интеллекта в обеспечении безопасности данных // Известия ТулГУ. Технические науки. 2020.
5. Larin S. N., Elizarova M. I., Sokolov N. A. Analysis of the development of the world market of high-tech products on the example of artificial intelligence technologies // Economics and business: theory and practice. 2019.

Literature

1. Balanovskaja A.V. Analiz sovremennogo sostojanija ugroz in-formacionnoj bezopasnosti predprijatij // Informacionnaja bezopas-nost' regionov. 2015.

2. Syreckij G.A. Iskusstvennyj intellekt i proizvodstvennaja bezopasnost': nastojashhee i budushhee // Interjekspo Geo-Sibir'. 2016.

3. Dubina I. V., Slavyanov A. S. Artificial intelligence as a tool to improve the effectiveness and sustainability of the business // Economics and business: theory and practice. 2019.

4. Afanas'eva D.V., Primenenie iskusstvennogo intellekta v obespechenii bezopasnosti dannyh // Izvestija TulGU. Tehnicheskie nauki. 2020.

5. Larin S. N., Elizarova M. I., Sokolov N. A. Analysis of the devel-opment of the world market of high-tech products on the example of artificial intelligence technologies // Economics and business: theory and practice. 2019.