Регулярный мониторинг не только позволяет контролировать уровень усвоения учащимися финансовой грамоты, но и корректировать недостатки и вовремя восполнять пробелы в знаниях и умениях учащихся.

Таким образом, необходимо подчеркнуть важность целенаправленного создания педагогически продуманной образовательной среды, которая сама превращается в фактор формирования финансовой грамотности.

### Список использованных источников

1. Финансовая грамотность. Исследования. [Электронный ресурс]. URL: https://www.nbrb.by/today/finliteracy/research (дата обращения: 05.10.2022)

УДК 004.89

**Е.Ф. Васнева**
Нижегородский государственный университет им. Н.И. Лобачевского
Нижний Новгород, Россия

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ

***Аннотация.*** *В статье представлен краткий обзор реализации искусственного интеллекта для обеспечения кибербезопасности с использованием определенных технологий и дана оценка перспектив расширения возможностей кибербезопасности за счет усиления механизма защиты.*

**E.F. Vasneva**
Nizhny Novgorod State University N.I. Lobachevsky
Nizhny Novgorod, Russia

## ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

***Abstract.*** *The article provides a brief overview of the implementation of artificial intelligence to ensure cybersecurity using certain technologies and assesses the prospects for expanding cybersecurity capabilities by strengthening the protection mechanism.*

Интеллектуальные технологии могут помочь защититься от сложных киберустройств, при этом уровень вредоносных программ и кибероружия растет с каждым годом. Использование методов

искусственного интеллекта (далее – ИИ) и наукоемких инструментов будет иметь жизненно важное значение в новых наступательных методах, таких как полностью автоматизированные реакции на атаки в сетях.

Быстрое реагирование на обстоятельства в Интернете требует использования ИИ. Многими данными необходимо управлять очень быстро, чтобы объяснять и интерпретировать действия в киберпространстве и принимать необходимые решения. Тем не менее, машины с обычными, фиксированными алгоритмами проблематично построить для успешной защиты от кибератак, поскольку постоянно возникают новые проблемы.

ИИ можно рассматривать как аспект интеллекта и создание интеллектуальных устройств, как технологию, которая предлагает решение для преодоления сложных проблем [1].

Является ли ИИ будущим кибербезопасности? Промышленные предприятия и компании частного сектора уже внедрили программы ИИ, поскольку он может легко экономить ресурсы и время, просматривая стандартизированные данные и всесторонне считывая и изучая неструктурированные данные, цифры, речевые шаблоны и предложения. Но во всем есть слабые места. Хакеры пытаются выяснить, как получить доступ к машинам, проскальзывая через уязвимости, о существовании которых мы и не подозреваем. ИИ может обнаружить те маленькие признаки, которые в противном случае остались бы незамеченными, и остановить хакерскую группу на начальном этапе. Хакеры всегда будут исследовать слабые места в системе, включая ИИ. ИИ управляется человеком и, следовательно, все еще может быть побежден. По мере того, как хакеры приспосабливаются к системам ИИ, программистам придется применять новые защитные меры [2].

Является ли ИИ преимуществом или проблемой для цифровой безопасности? С одной стороны, современная инфраструктура управления информацией ценна, поскольку она облегчает оценку, изучение и понимание киберпреступности специалистами по безопасности. Это укрепляет стратегии цифрового управления, которые компании используют для борьбы с киберпреступностью и помогают обеспечить безопасность бизнеса и клиентов. С другой стороны, ИИ может быть очень ресурсоемким. Фактически, это также может служить грозным оружием в арсенале компьютерных преступников, которое использует технологии для улучшения и усиления кибератак. Дебаты вокруг ИИ не представляли собой ничего особенного с точки зрения информационной безопасности.

Информация лежит в самом центре тенденций в области кибербезопасности. Но что может быть лучше для анализа информации, чем использование компьютерных систем, которые могут думать за наносекунды, а затем выполнять задачи, которые заняли бы у людей значительно больше времени? ИИ быстро становится предметом особого внимания в сообществе компьютерной безопасности.

Использование ИИ может даже помочь расширить перспективы существующих решений для обеспечения кибербезопасности, а также перестроить способ создания новых. Когда сети станут более широкими и сложными, ИИ станет огромным стимулом для обеспечения безопасности предприятия. Проще говоря, растущая сложность сетей выходит за рамки того, что люди могут сделать самостоятельно.

Существует множество способов, с помощью которых системы ИИ могут обеспечить устойчивость операций по обеспечению кибербезопасности. Некоторые из этих функций включают в себя разработку точных методов входа в систему на основе биометрических паролей, обнаружение рисков и подозрительной активности с помощью прогностического анализа, улучшение мышления и интерпретации посредством естественного распознавания речи, обеспечение идентификации и соединения по требованию. При существующих преимуществах использования ИИ в обеспечении безопасности, не стоит забывать про риски. Одна из больших трудностей в применении ИИ в информационной защите заключается в том, что это требует больше времени и средств, чем традиционные решения для защиты компьютеров. Отчасти это связано с тем, что технологии защиты информации, основанные на фреймворках ИИ, стоят недешево. Тем не менее, существуют новые технологии, которые делают технологии киберзащиты ИИ более экономически эффективными для бизнеса. Гораздо проще выбрать жизнеспособные меры защиты информации, чем сталкиваться со штрафами, задержками и другими расходами, связанными с жестокими кибератаками.

Применение ИИ в информационной защите создает новые проблемы для физической защиты. Несмотря на важность использования технологий ИИ для выявления вредоносных угроз и борьбы с ними, кибератаки могут также использовать инструменты ИИ для прогрессивных поведенческих атак. Отчасти это связано с тем, что доступ к передовым технологиям ИИ, помимо стратегий машинного обучения, расширяется по мере снижения затрат на производство и применение этих разработок. Компьютерные злоумышленники смогут

быстрее и с меньшими затратами создавать все более сложные и эффективные вредоносные приложения. Сочетание переменных факторов создает угрозу злоупотреблений со стороны киберпреступников.

Опасность для информационной безопасности состоит в том, что нейронные сети в программе ИИ можно ввести в заблуждение. Как следствие, нейронные сети ошибочно идентифицируют или ложно представляют артефакты из-за намеренно измененных входных данных. К счастью, риски, связанные с ИИ, активно изучаются для минимизации слабых мест.

Очевидно, что только благодаря использованию подходов ИИ можно было эффективно преодолеть еще больше проблем кибербезопасности. При принятии решений необходимо всестороннее использование информации, а помощь в принятии обоснованных решений является одной из нерешенных проблем кибербезопасности. В секторе ИИ было разработано большое разнообразие подходов для разрешения сложных ситуаций, в которых задействован человеческий интеллект. Большинство из этих стратегий достигли зрелой стадии, когда доступны конкретные алгоритмы, основанные на этих подходах [3]. Рассмотрим их далее.

Нейронные сети включают в себя возможность параллельного распределенного обучения и принятия решений. Рабочая частота является их наиболее определяющей характеристикой. Они идеально подходят для идентификации моделей обучения, группировки, компиляции ответов на угрозы, использования методов ИИ в киберзащите и т.д. Были разработаны планы по обнаружению DDoS-атак, идентификации программных червей, фильтрации спама, анализу вредоносных программ и судебной экспертизе. Быстрая мобильность, независимо от того, реализована ли она в аппаратном обеспечении или используется в наборах графических микросхем, обуславливает важность глубокого обучения в области компьютерной безопасности. Инновация нейронных сетей: когнитивные сети третьего поколения – стремительное машинное обучение, которые более эффективно имитируют искусственные нейроны и которые предлагают более широкие возможности для применения.

Наиболее часто применяемые методы ИИ, безусловно, являются специализированными программами. Это технология поиска решений проблем, поднятых либо заказчиком, либо определенной технологией в определенной области. Это может быть использовано специально для оказания помощи в принятии решений, например, в области медицинского обслуживания, банковского дела или виртуальных

миров. Существуют различные методы оптимизации для решения сложных задач размером от крошечных аналитических медицинских диагнозов до высокоразвитых гибридных систем. Схема экспертизы включает в себя базу знаний, которая содержит специализированный анализ конкретной области применения. Оболочка ИИ должна быть подтверждена программным обеспечением (далее – ПО) базы знаний и может быть расширена с помощью программ интерактивных запросов и других программ, которые могут использоваться в квалифицированных гибридных «двигателях».

Интеллектуальные агенты – компоненты ПО вычислительного интеллекта с некоторыми функциями интеллектуального действия, которые делают их особенными – реактивными. Они могут обладать способностью к подготовке, организации и оценке. В сообществе разработчиков ПО действительно существует понятие программных агентов, в котором они рассматриваются как артефакты, которые, по крайней мере, активно используют сетевой язык агента. Интеллектуальные агенты использовались для защиты от DDoS-атак, и были описаны симуляции, в которых можно эффективно защитить агентов сотрудничества от этих атак.

Вычислительные подходы для получения новых идей, новых способностей и инновационных способов координации текущих знаний требуют компьютерного обучения. Задачи обучения широко варьируются от базового параметрического обучения до сложных типов абстрактного обучения, таких как изучение концепций, изучение грамматики, юзабилити и поведенческое обучение. Первоначально интеллектуальный анализ данных был получен из неконтролируемого обучения ИИ. В целом неконтролируемое обучение может быть функцией самоорганизующихся нейронных сетей. Параллельные нейронные сети используются для вывода в параллельном оборудовании с особым классом методов обучения. Эти методологии обучения определяются эволюционным алгоритмом и нейронными сетями.

Изучение, разработка и внедрение подходов ИИ к кибербезопасности приведет к способности различать ближайшие цели и долгосрочные перспективы. Многочисленные подходы ИИ могут быть использованы для обеспечения кибербезопасности, а неотложные проблемы кибербезопасности требуют более разумных решений.

В условиях, когда киберугрозы растут в геометрической прогрессии, нельзя игнорировать сложные стратегии кибербезопасности. Новейшие технологии в области понимания, интерпретации и управления информацией, особенно в области

компьютерного обучения, значительно улучшат возможности систем в области кибербезопасности.

## Список использованных источников

1. Искусственный интеллект и безопасность: проблемы, заблуждения, реальность и будущее. – [Электронный ресурс]. – URL: https://clck.ru/32N7YN (дата обращения: 08.10.2022).
2. Sadiku, M.N.O., Fagbohungbe, O.I., & Musa, S.M. Artificial Intelligence in Cyber Security. – [Электронный ресурс]. – URL: https://clck.ru/32N7kA (дата обращения: 10.10.2022).
3. Tyugu, E. Artificial intelligence in cyber defense. – [Электронный ресурс]. – URL: https://clck.ru/32N86z (дата обращения: 12.10.2022).

УДК 665.6.

**К.В. Вишневский, А.В. Дернович**
Белорусский государственный технологический университет
Минск, Беларусь

# ИНЖИНИРИНГОВЫЕ УСЛУГИ ПО ПРОЕКТИРОВАНИЮ ОЧИСТНЫХ СООРУЖЕНИЙ (ОС) НЕФТЕСОДЕРЖАЩИХ И ХИМИЧЕСКИ ЗАГРЯЗНЕННЫХ СТОКОВ НЕФТЕПЕРЕРАБАТЫВАЮЩИХ (НПЗ) И НЕФТЕХИМИЧЕСКИХ ЗАВОДОВ (НХЗ). СОВРЕМЕННЫЕ ТЕНДЕНЦИИ И ПОДХОДЫ

***Аннотация.*** *В настоящее время перед нефтеперерабатывающей и нефтехимической отраслью остро стоит проблема очистки производственных сточных вод. Основной причиной создавшегося положения является несоответствие эффективности очистки существующих ОС требованиям времени. В настоящее время подобными инжиниринговыми услугами планируют заниматься создаваемые производственно-сервисные центры ряда производственных компаний и холдингов РФ.*

**K.V. Vishnevsky, A.V. Dernovich**
Belarusian State Technological University
Minsk, Belarus

# ENGINEERING SERVICES FOR THE DESIGN OF PURIFICATION FACILITIES (PF) OF OIL-CONTAINING AND