



Научно-практический электронный журнал

# **МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА**



Выпуск №5 (том 3)  
(октябрь, 2019)



Международный научно-практический  
электронный журнал «МОЯ  
ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА»

Сайт: <http://mpcareer.ru>

ISSN 2658-7998

УДК 001

ББК 94

И72

## **Международный научно-практический электронный журнал «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА». Выпуск №5 (том 3) (октябрь, 2019)**

Сборник содержит научные статьи отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Информация об опубликованных статьях предоставляется в систему Российского индекса научного цитирования (РИНЦ) и размещена на платформе научной электронной библиотеки (eLIBRARY.RU). Лицензионный договор № 284-07/2019 от 30 июля 2019 г.

Миссия научно-практического электронного журнала «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает представителей экспертного сообщества, докторов, преподавателей, научных сотрудников, бакалавров, магистрантов, аспирантов и иных лиц, интересующихся вопросами, освещаемыми в журнале.

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание статей ответственность несут авторы статей. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

© ООО «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА»

© Коллектив авторов



УДК 004.8

**Воробьев Р.А.**

студент 4 курса бакалавриата

Казанский Государственный Энергетический университет

Научный руководитель: **Зарипова Р.С.**

Кандидат технических наук, доцент

Казанский Государственный Энергетический университет

## ОПАСНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

**Аннотация:** Применение искусственного интеллекта в различных сферах жизни человека приобретает всю большую актуальность. Однако повсеместное внедрение и общедоступность создания систем искусственного интеллекта предоставляют опасность для всего человечества. Данное исследование показало, что опасности исходят не от самой системы искусственного интеллекта, а от человека, который её применяет. Результатом исследования является понимание реальных опасностей, которые несёт за собой злонамеренное использование систем искусственного интеллекта.

**Ключевые слова:** Искусственный интеллект, опасность, нейронная сеть, «фейк», преступление.

**Annotation:** The use of artificial intelligence in various areas of human life is becoming increasingly important. However, the widespread adoption and accessibility of the creation of artificial intelligence systems pose a danger to all mankind. This research showed that the dangers do not come from the artificial intelligence system itself, but from the person who uses it. The result of the study is an understanding of the real dangers that the malicious use of artificial intelligence systems entails.

**Keywords:** Artificial Intelligence, danger, neural network, fake, crime.

Многие десятилетия фильмы, книги и видеоигры готовили нас к восстанию машин под управлением искусственного интеллекта, ведущего к почти полному



истреблению человеческого рода. К сожалению или к счастью, пока что мы далеки от представленного в них понятия искусственного интеллекта. Но мы с каждым годом всё ближе к его созданию. Доступные на текущий момент представители систем машинного интеллекта не способны к автономной жизнедеятельности, поэтому сами по себе опасности не представляют, однако в качестве инструмента злоумышленников способны принести множество проблем.

Для начала необходимо понять, что собой представляет современный искусственный интеллект. Согласно [1], под искусственным интеллектом следует понимать свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека; науку и технологию создания интеллектуальных машин, особенно интеллектуальных компьютерных программ. С каждым годом открываются новые и совершенствуются старые подходы к созданию систем искусственного разума. Более известен подход, при котором электронно-вычислительная машина познаёт окружающий её мир, либо определённую предметную область при помощи нейронной сети, совершая ошибки и учась на них.

Основные принципы, управляющие рациональной частью мышления, ещё до нашей эры сформулировал Аристотель. А первая компьютерная модель нейронной сети была разработана в начале 40-х годов XX века. Пик популярности пришёлся на период 70-80-х годов прошлого века. К сожалению не все в научном сообществе разделяли всеобщий энтузиазм, да и технологии того времени были далеки от современных. Совокупность данных факторов порождала новые проблемы быстрее, чем удавалось решить старые. Интерес общественности к технологиям нейронных сетей поубавился и на время нейронные сети ушли в тень. Но в 00-е года XXI века нейронные сети снова заявили о себе: решена проблема попадания в локальный минимум, создаются алгоритмы глубокого обучения [2].

Нейронные сети сегодня переживают своё второе рождение. Только ленивый не слышал об их существовании. Спектр их применения огромен: от



школьных проектов [3] до медицины. Повсеместное внедрение систем искусственного интеллекта, взаимодействующих с окружающим миром посредством нейронных сетей, делает жизнь миллионов людей лучше, помогает в развитии различных сфер жизни человечества. Например, нейронная сеть помогает людям выявить рак, посредством распознавания новообразований на изображении [4]. А так же производители встраивают системы машинного интеллекта в камеры новейших смартфонов для лучшего качества изображения и более качественного распознавания человека в кадре [5].

Однако системы искусственного интеллекта могут принести и огромный вред. Естественно, что на данный момент они не способны самостоятельно выстраивать логические цепочки и имитировать полноценное человеческое сознание, однако, выступая в качестве высококласного орудия в руках злоумышленников, способны причинить немало проблем. Об этом заявил профессор Междисциплинарного центра биоэтики Йельского университета США Венделл Валлах [6]. С помощью обученных нейронных сетей уже создаются: системы для замены лиц на изображениях и видео; системы для распознавания речи, позволяющие, перехватывая звук с микрофона устройства, анализировать его и передавать в виде текста преступникам; программы чтения по губам, которые легко можно использовать для шпионажа за целью, находящейся на большом расстоянии; приложения для создания изображений несуществующих людей возможно использовать для подмены информации в базе данных полиции и вышестоящих органов, либо для финансовых махинаций; системы изменения голоса, предоставляющие имитацию любого голоса; системы для наложения фальшивой мимики на существующие видеофрагменты. Использование вместе последних двух систем даёт возможность создания фальшивых видео роликов с любым человеком на планете, говорящим то, что выгодно злоумышленникам. Масштаб применения таких систем от локальных мошеннических схем до международных преступлений. И это лишь известные примеры злонамеренного применения систем искусственного интеллекта, а сколько ещё создается, разрабатывается?



Где сила, там и сопротивление. Для предотвращения преступлений, совершаемых при помощи систем искусственного интеллекта крупные IT-гиганты либо сами программное обеспечение, способное в будущем помочь распознать подделку, либо создают, а затем выкладывают в открытый доступ качественный набор данных, для создания данной программы другими компаниями в будущем. Как, например, компания Google, создавшая базу данных из нескольких тысяч deepfake-видео для борьбы с deepfake (поддельные видео, в которых искусственный интеллект используется для того, чтобы изменить лицо, или для редактирования речи говорящего на видео) [7].

На данный момент большую часть deepfake контента возможно вычислить, как говорится, на глазок, но уже сейчас существуют экземпляры, которые выглядят настолько реалистично, что обычный человек не сможет распознать подделку. Производительные мощности нашего времени не позволяют создавать и обучать системы искусственного интеллекта, выдающие идеальный результат, за пару дней, однако через пару лет технологии шагнут далеко вперед и нам будут доступны невиданные ранее мощности, а, следовательно, количество преступлений, осуществленных при помощи подобных систем, возрастет. Поэтому разработка программного обеспечения, способного распознать фальшивое изображение, видеозапись или аудиозапись, и другие созданные при помощи системы искусственного интеллекта, является одной из первоочередных задач для любого государства. С помощью подобной системы разведывательные службы соседних стран, террористические организации способны с лёгкостью посеять панику внутри государства, развязать гражданскую войну, начать третью мировую войну. Поэтому создание программного обеспечения для распознавания «фейков» должно быть одной из важнейших задач для всего мирового сообщества.

Повсеместное внедрение искусственного интеллекта помогает человеку в большинстве сфер его жизни. Однако, вследствие этого доступность создания и использования искусственного интеллекта создает немало опасностей. Хотя текущая стадия развития искусственного интеллекта и далека от того, что мы



видим в произведениях поп-культуры, но опасности искусственного интеллекта более чем реальны. Только сами опасности таятся не в искусственном интеллекте, а в людях, что создают и используют его в своих корыстных целях. Поэтому необходимо совместными усилиями всего мирового сообщества разрабатывать и совершенствовать программы для противодействия злоумышленникам.

### Список литературы

1. Искусственный интеллект [Электронный ресурс] – URL: [https://ru.wikipedia.org/wiki/Искусственный\\_интеллект](https://ru.wikipedia.org/wiki/Искусственный_интеллект)
2. Горбачевская Е. Н., Краснов С. С. История развития нейронных сетей / Е. Н. Горбачевская, С. С. Краснов // Вестник Волжского университета им. В.Н. Татищева. – 2015, № 1(23). – С. 52-56.
3. Пырнова О.А. Технологии искусственного интеллекта в образовании / О.А. Пырнова, Р.С. Зарипова / Russian Journal of Education and Psychology. – 2019. – Т. 10. – №3. – С. 41-44.
4. Coudray N., Ocampo P.S., Sakellaropoulos T., Narula N., Snuderl M., Fenyo D., Moreira A.I., Razavian N., Tsirigos A. Classification and mutation prediction from non-small cell lung cancer histopathology images using deep learning // Nature medicine. – 2018, Vol. 24.-P. 1559-1567.
5. В США назвали «главную опасность искусственного интеллекта» [Электронный ресурс] – URL: <https://www.mk.ru/science/2019/05/27/v-ssha-nazvali-glavnuyu-opasnost-iskusstvennogo-intellekta.html>
6. Пырнова О.А. Искусственный интеллект в камерах смартфонов / О.А. Пырнова, Р.С. Зарипова / Информационные технологии в строительных, социальных и экономических системах. – 2019. – № 1 (15). – С. 82-84.
7. Google makes deepfakes to fight deepfakes [Электронный ресурс] – URL: <https://www.bbc.com/news/technology-49837927>



|                                                                                                                                                                                                                                                          |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ТЕХНОЛОГИИ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ:<br>ВОЗМОЖНОСТИ И ПРЕПЯТСТВИЯ ПРИМЕНЕНИЯ<br>Скворцов К.А.                                                                                                                                                | 183 |
| УПРАВЛЕНИЕ ЗАПАСАМИ МАТЕРИАЛОВ И КОМПЛЕКТУЮЩИХ НА<br>СКЛАДЕ АВТОМОБИЛЬНОГО СЕРВИСНОГО ЦЕНТРА<br>Москова А.Р.                                                                                                                                             | 187 |
| ОПАСНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА<br>Воробьев Р.А.                                                                                                                                                                                                     | 192 |
| ИСПОЛЬЗОВАНИЕ НЕЧЕТКОГО КОГНИТИВНОГО МОДЕЛИРОВАНИЯ<br>ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>ИНФОРМАЦИОННЫХ ПОРТАЛОВ РЕГИОНАЛЬНЫХ ОРГАНОВ<br>ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ<br>Лексиков Е.В., Яковенко А.Н.                                         | 197 |
| БУДУЩИЕ СПЕЦИАЛИСТЫ НАПРАВЛЕНИЯ ПОДГОТОВКИ<br>«ОРГАНИЗАЦИЯ РАБОТЫ С МОЛОДЁЖЬЮ» В РАМКАХ УСВОЕНИЯ<br>ОБЩЕСТВОМ НОВЫХ ПРОФЕССИЙ (НА ПРИМЕРЕ СТУДЕНТОВ<br>ИНСТИТУТА СОЦИАЛЬНЫХ КОММУНИКАЦИЙ УДМУРТСКОГО<br>ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА)<br>Жевлакова Ю.С. | 208 |
| РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ЭФФЕКТИВНОСТИ<br>ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ<br>НА ПРЕДПРИЯТИИ<br>Лексиков Е.В., Канева М.И., Фроликова М.Ю.                                                                                              | 215 |
| ОСОБЕННОСТИ МАШИННОГО ОБУЧЕНИЯ И РАСПОЗНОВАНИЯ<br>ОБРАЗОВ<br>Сулейманов М.М., Красильников Б.В.                                                                                                                                                          | 224 |
| ПРИНЦИП ОПТИМАЛЬНОГО ДЕЙСТВИЯ<br>Никитин В.В.                                                                                                                                                                                                            | 229 |
| РАЗРАБОТКА МЕТОДИКИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ<br>ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ<br>Лексиков Е.В., Фроликова М.Ю., Канева М.И.                                                                                                                 | 238 |
| ОСОБЕННОСТИ РАБОТЫ РОБОТА КОНТРОЛЛЕРА НА ОСНОВЕ<br>ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ<br>Филиппова Л.Б., Лысов Д.А.                                                                                                                                              | 246 |
| ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ<br>Воргунова В.Р.                                                                                                                                                                                                | 251 |
| АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ В ОБЛАСТИ ОЦЕНКИ<br>РИСКОВ БЕЗОПАСНОСТИ ПДН В ИСПДН<br>Маланин А.И., Иванова М.И., Лысов Д.А.                                                                                                                            | 258 |
| РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ<br>СИСТЕМЫ УЧЕТА ПРЕСС-ФОРМ ПРЕДПРИЯТИЯ<br>Ледрова А.М.                                                                                                                                                     | 264 |
| РАЗРАБОТКА ПРОГРАММНОГО МОДУЛЯ УЧЕТА КАДРОВ В РАМКАХ<br>РЕГИОНАЛЬНОГО ПОДРАЗДЕЛЕНИЯ ООО «ТАТАВТОМАТИЗАЦИЯ»<br>Каримова Н.Ф.                                                                                                                              | 267 |
| РАЗРАБОТКА СИСТЕМЫ ОХРАНЫ И КОНТРОЛЯ ОБЪЕКТА В<br>КОНЦЕПЦИИ УМНОГО ДОМА<br>Чайко А.А.                                                                                                                                                                    | 271 |
|                                                                                                                                                                                                                                                          |     |