Юлия Игоревна КАРАВАЕВА,
ученый секретарь Ученого совета Вологодского института права и экономики Федеральной службы исполнения наказаний (ВИПЭ ФСИН России), кандидат социологических наук
jy@mail.ru
160002, Россия, г. Вологда, ул. Щетинина, д. 2

Современные цифровые технологии и проблема обеспечения прав человека

Аннотация. *В статье рассматривается уровень доверия к искусственному интеллекту в условиях стремительного цифрового развития и внедрения самообучающихся технологий. Оперативно развивающиеся гаджеты формируют у человека новый цифровой аватар, изменяя не только личные привычки, но и подход к информационной безопасности.*

Анализ проводится на основе существующих исследований, статистических данных и официальных отчетов. В частности, используются данные из исследований Mediascope о поведении пользователей в Интернете и доклады МВД России о преступлениях в киберпространстве.

Согласно данным Mediascope, россияне проводят в Интернете в среднем 3,5 часа в день, при этом значительная доля времени отводится на развлекательный контент. В результате наблюдается увеличение числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий — на 16,4 % за период с января по август 2024 г. Также отмечается удвоение случаев киберпреступности за последние пять лет.

Постоянный рост киберпреступности ставит под сомнение степень доверия к технологиям искусственного интеллекта. Необходимость стандартизации и защиты данных становится актуальной задачей национального уровня. Президент России В. В. Путин подчеркнул важность внедрения технологий ИИ для повышения уровня безопасности и снижения ущерба от киберугроз.

Ключевые слова: *искусственный интеллект, доверие, информационно-телекоммуникационные технологии, киберпреступность, дипфейк, антифейковые технологии, квантовая криптография*

DOI: 10.17803/2311-5998.2025.133.9.170-176

Julia I. KARAVAEVA,
Academic Secretary of the Academic Council,
Vologda Institute of Law and Economics
of the Federal Penitentiary Service of Russia,
Cand. Sci. (Sociology)
jy@mail.ru
2, ul. Shchetinin, Vologda, Russia, 160002

Modern digital technologies and the problem of ensuring human rights

Abstract. *This article examines the level of trust in artificial intelligence in the context of rapid digital development and the implementation of self-learning technologies. The rapidly evolving gadgets are creating a new digital avatar for individuals, altering not only personal habits but also approaches to information security.*

The analysis is based on existing research, statistical data, and official reports. In particular, data from Mediascope studies on user behavior on the internet and reports from the Ministry of Internal Affairs of Russia on cybercrime are utilized.

According to Mediascope data, Russians spend an average of 3.5 hours per day online, with a significant portion of that time devoted to entertainment content. As a result, there has been an increase in the number of crimes committed using information and telecommunications technologies—by 16.4% from January to August 2024. Additionally, a doubling of cybercrime incidents over the past five years has been noted.

The constant rise in cybercrime raises questions about the level of trust in artificial intelligence technologies. The need for standardization and data protection has become an urgent national issue. Russian President V.V. Putin emphasized the importance of implementing AI technologies to enhance security levels and mitigate damage from cyber threats.

Keywords: *artificial intelligence, trust, information and telecommunications technologies, cybercrime, deepfake, anti-fake technologies, quantum cryptography*

Актуальность проблемы

Мы живем в век опережающего развития технологий, самообучающихся гаджетов. Нельзя сказать, что цифровое развитие — это тенденция только последних лет, нет, это длительный пролонгированный процесс[1]. Например, в СССР пред-

[1] *Нагорных Р. В.* Публично-правовые основы инновационного развития государственной и муниципальной службы в современной России // Юридическое образование и наука.

почтение было отдано производственной сфере применения компьютерных технологий. Ставка делалась на создание автоматизированных систем управления промышленным производством, станков с числовым программным управлением, а также на организацию вычислительных центров коллективного пользования для сбора и анализа разнообразной информации[2].

Но именно за последние 15—20 лет цифровая трансформация вошла в нашу повседневную, бытовую жизнь. Используемые нами девайсы создают наш цифровой аватар, накапливают статистику персональных запросов, просмотров, времени, проведенного на том или ином ресурсе. Переформулируя русскую пословицу «Скажи мне, кто твой друг, и я скажу — кто ты?» на современный лад, можно сказать: «Ты — то, что ты смотришь. Скажи мне, кто твои друзья, на кого ты подписан в Сети, и я скажу каков твой социальный профиль».

По данным исследования Mediascope «Человек в смартфоне» за период с января по август 2024 г., россияне проводят в интернете в среднем 3,5 часа в день[3]. Данное время человек затрачивает на видео, мессенджеры, соцсети, игры, маркетплейсы. Обратим внимание, что среди перечисленных ресурсов не указаны сайты для самообразования, данное время не является рабочим, продуктивным, экономически полезным. Фактически 4 часа — это среднее окно развлекательного контента.

В этот период человек расслабляется, бдительность ослабевает, он настроен на отдых. Даркнет[4] и мошенники пользуются данным фактором. Например, злоумышленники используют рекламу в поисковых системах, фишинговые сайты могут занять верхние позиции при поиске, рабочие ссылки могут подменяться на вредоносные. По данным из доклада В. А. Колокольцева, представленного в ходе заседания Общественного совета при МВД России, в январе — августе 2024 г. зарегистрировано 500,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 16,4 % больше, чем за тот же период 2023 г.[5]

Тенденция к увеличению числа киберпреступлений в России и мире

Активное развитие киберпреступность получила в период пандемии, за последние 5 лет число противоправных деяний в киберпространстве увеличилось более чем вдвое. Сегодня их доля в общем массиве остается значительной и

2022. № 1. С. 26—30.

2 *Самохвалов В. М., Сизых И. С.* Особенности и задачи развития информационных технологии в СССР // Актуальные проблемы авиации и космонавтики. 2022. Т. 3. С. 676—678

3 URL: https://mediascope.net/news/2654610/ и URL: https://mediascope.net/upload/iblock/a88/93gub0nnuaudd6zkn9gc5g2zijv1t2pb/человек%20в%20смартфоне_mediascope.pdf (дата обращения: 12.11.2024).

4 Цифровой мир : терминологический словарь-справочник в определениях официальных документов / И. Р. Бегишев, И. Р. Альмухамедова, А. К. Арюков [и др.]. М. : Проспект, 2024.

5 URL: https://rg.ru/2024/09/25/policiia-v-seti.html (дата обращения: 12.11.2024).

составляет около 40 %, т.е. это почти каждое второе преступление. А по тяжким и особо тяжким составам этот показатель уже приблизился к 60 %. Пострадавшими от незаконных действий в цифровой сфере становятся и физические, и юридические лица, в том числе государственные структуры.

В связи с укрупнением масштабов бедствия логично возникает вопрос о стандартизации, защите данных прав и конкретизации обязанностей[6].

Собственно, данная потребность определена как приоритетная на самом высшем уровне. Задача по созданию системы эффективного противодействия таким деяниям и снижению ущерба от них включена в национальные цели развития страны, определенные Президентом РФ В. В. Путиным. Выступая на международной онлайн-конференции Artificial Intelligence Journey (AI Journey), он заявил, что в ближайшие 10 лет предстоит повсеместно внедрить технологии искусственного интеллекта и анализа больших данных.

В настоящее время в России основные стратегии, затрагивающие сферу развития искусственного интеллекта, изложены в Указах Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»[7] и от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года[8].

Отметим, что внимание данному вопросу уделено и на международном уровне. Так, в принятой резолюции 79/1 Генеральной Ассамблеи ООН от 22.09.2024 зафиксирована задача 5 — усилить международное регулирование в отношении искусственного интеллекта на благо человечества[9].

В то же время признание цифровой трансформации общества, стремление регламентировать данную сферу не в полной мере обеспечивают абсолютное соблюдение прав человека[10]. Напомним об одиозном случае, произошедшем в Гонконге. В начале 2024 г. одна из крупнейших корпораций потеряла 26 млн долларов, так как один из сотрудников был обманут с помощью технологии дипфейк (deepfake)[11]. Введенный в заблуждение сотрудник работал в финансовом отделе и обладал полномочиями на принятие решений, соответственно, мы можем сделать вывод, что специалист имел достаточный уровень образования, опыта, но и с учетом имеющегося бэкграунда все же был обманут. По данным гонконгской полиции все участники видео-конференц-связи были фэйковыми, сгенерированы с помощью цифровых технологий на основе фото и видео реальных персон из открытых источников.

---

[6] *Саргсян А. А.* Перспективы цифровизации назначения и исполнения уголовного наказания // Пенитенциарная наука. 2022. Т. 16. № 2 (58). С. 146—152.

[7] URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 12.11.2024).

[8] URL: http://www.kremlin.ru/events/president/news/73986 (дата обращения: 12.11.2024).

[9] URL: https://documents.un.org/doc/undoc/gen/n24/272/24/pdf/n2427224.pdf (дата обращения: 12.11.2024).

[10] *Воробьев С. М., Мельникова О. В., Ивлиев П. В.* Цифровая трансформация современного российского государства: актуальные вопросы правовой регламентации // Пенитенциарная наука. 2022. Т. 16. № 1 (57). С. 8—18.

[11] Российская газета. 04.02.2024. URL: https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-milliony-dollarov-u-krupnejshej-korporacii.html.

На пути от доверия к скепсису

Описанная выше мошенническая схема строится на чувстве доверия сотрудника руководству, партнерам, средствам связи и своим органам восприятия. Этот пример подводит нас к обозначенной в заголовке проблематике — вопросу о степени доверия к искусственному интеллекту. Выше было отмечено, что искусственный интеллект, цифровые технологии — это не спринтерская, а марафонская дистанция со стартом в более глубоком прошлом, чем 15—20 лет назад. Первоначально цифровизация была априори положительной — она облегчала труд. Доверие к искусственному интеллекту строится на исторических примерах успеха в производстве, медицине. Накопленный положительный опыт и его потенциал способствуют доверию девайсам связи и коммуникаций. К положительному образу (имиджу) цифровизации приплюсовывается положительная характеристика элитарности. Доступ к возможностям цифровизации имели высокообразованные люди, имеющие более высокий уровень жизни, более высокий социальный статус.

Сегодня же с помощью новых технологий совершаются трансграничные преступления. Различные программные устройства обеспечивают анонимность преступника. Сегодня для совершения противоправного действия весьма важно иметь доступ к уникальным персональным характеристикам потенциального потерпевшего. Изображение внешности человека, его голос, интонацию и т.д. возможно сгенерировать (к примеру, с использованием reface technology).

Выводы и предложения

Необходимо отметить, что отдельные запреты и ситуативные блокировки не будут систематически эффективны. Необходима синергия образования, науки, бизнеса, государства для обеспечения прав человека[12].

Мы не можем сегодня запретить ребенку пользоваться гаджетами, мы должны научить его быть технологичным, продвинутым, подкованным.

Начать надо хотя бы с себя и уделять время на прочтение пользовательского соглашения не 1,5—2 секунды, которые достаточны только для отлистывания до кнопки «ок». Нужны соответствующие образовательные программы, треки в региональных вузах. Наука продолжит разрабатывать антифейковые технологии. Нормотворцы продолжат совершенствовать законодательную базу. Уже есть страны, такие как Саудовская Аравия, Бахрейн, Объединенные Арабские Эмираты, где предусмотрена и регламентирована уголовная ответственность за киберпреступления.

В Саудовской Аравии уголовная ответственность за киберпреступления установлена Законом о преступлениях в области информационных технологий 2007 г.

[12] *Некрасов В. Н.* 10 условий успешной трансформации уголовного права в эпоху инновационных перемен. Условие 1 // Ius Publicum et Privatum. 2023. № 3 (23). С. 156—165.

В Объединенных Арабских Эмиратах уголовная ответственность за киберпреступления[13] предусмотрена Федеральным законом № 34 2021 г. «О борьбе со слухами и киберпреступлениями». Закон определяет широкий спектр киберпреступлений, включая несанкционированный доступ к системам и кражу данных, а также более серьезные преступления, такие как онлайн-травля, распространение дезинформации, эксплуатация несовершеннолетних с помощью цифровых средств и электронное мошенничество. Наказания зависят от характера и тяжести преступления и могут включать лишение лицензии, штрафы, тюремное заключение и депортацию.

Несомненно, будет развиваться и преступность. Наше доверие к цифровизации может смениться абсолютным скепсисом. Но в любом случае можно сказать, что цифровизация и развитие искусственного интеллекта тяготеют к расширению и распространению, имеют больше преимуществ, чем недостатков, являются фактором прогресса и развития. А законодательная база по объективным причинам (одна процедура согласования и соблюдение принципа «не навреди») пока не успевает за технологическим прогрессом. Между тем понимание необходимости совершенствования указанных мер защиты присутствует на самых высоких уровнях.

В данных рассуждениях об эволюции доверия к технологиям сто́ит напомнить о разработке и создании квантового компьютера, от которого зависит национальная безопасность. Так, в интервью «Российской газете» Р. Р. Юнусов, один из создателей отечественных квантовых технологий и сооснователь Российского квантового центра в Сколково, говорит, что квантовая криптография может оставить изощренных хакеров без работы[14].

Сегодня Россия накапливает собственные разработки, и отмечу, что этому даже способствует умение устоять в условиях многочисленных международных санкций. Два года назад, когда российские ученые лишились возможности работать на зарубежных цифровых площадках и платформах, когда на все сферы экономики, науки, бизнеса оказывалось беспрецедентное давление, был заложен фундамент сегодняшнего рывка вперед, развития собственных наработок.

Хочется верить, что нас ждет безопасное высокотехнологичное будущее, а сегодняшние примеры ошибок искусственного интеллекта, когда система распознавания лиц Amazon определила 28 конгрессменов США как преступников, останется в далеком прошлом.

Еще один громкий пример ошибки искусственного интеллекта, когда ярославский ученый-гидролог Александр Цветков 10 месяцев провел в СИЗО из-за ошибки системы распознавания лиц в Домодедовском аэропорту, которая показала 55 % совпадение внешности с фотороботом преступника — убийцы. Конечно, можно сказать, что масштабные достижения не обходятся без единичных ошибок (есть даже поговорка: «Лес рубят — щепки летят»). Но, если подобные громкие ошибки и их резонанс могут затронуть каждого из нас, любого гражданина, думаю,

[13] *Волеводз А. Г., Цыплакова А. Д.* Уголовная ответственность юридических лиц в Объединенных Арабских Эмиратах и Королевстве Саудовская Аравия: сравнение материальных и процессуальных аспектов // Российский следователь. 2024. № 3. С. 51—56.

[14] URL: https://rg.ru/2023/01/10/igry-v-kubity.html (дата обращения: 23.11.2024).

что вопрос должен быть рассмотрен особо тщательно. Уверена, что уровень доверия к искусственному интеллекту будет зависеть от развития законодательства и антифейковых технологий и будет расти пропорционально уменьшению подобных ошибок и сокращению числа киберпреступлений.

БИБЛИОГРАФИЯ

1. *Волеводз А. Г., Цыплакова А. Д.* Уголовная ответственность юридических лиц в Объединенных Арабских Эмиратах и Королевстве Саудовская Аравия: сравнение материальных и процессуальных аспектов // Российский следователь. — 2024. — № 3. — С. 51—56.
2. *Воробьев С. М., Мельникова О. В.*, *Ивлиев П. В.* Цифровая трансформация современного российского государства: актуальные вопросы правовой регламентации // Пенитенциарная наука. — 2022. — Т. 16. — № 1 (57). — С. 8—18.
3. *Нагорных Р. В.* Публично-правовые основы инновационного развития государственной и муниципальной службы в современной России // Юридическое образование и наука. — 2022. — № 1. — С. 26—30.
4. *Некрасов В. Н.* 10 условий успешной трансформации уголовного права в эпоху инновационных перемен. Условие 1 // Ius Publicum et Privatum. — 2023. — № 3 (23). — С. 156—165.
5. *Самохвалов В. М., Сизых И. С.* Особенности и задачи развития информационных технологии в СССР // Актуальные проблемы авиации и космонавтики. — 2022. — Т. 3. — С. 676—678.
6. *Саргсян А. А.* Перспективы цифровизации назначения и исполнения уголовного наказания // Пенитенциарная наука. — 2022. — Т. 16. — № 2 (58). — С. 146—152.
7. Цифровой мир : терминологический словарь-справочник в определениях официальных документов / И. Р. Бегишев, И. Р. Альмухамедова, А. К. Арюков [и др.]. — М. : Проспект, 2024. — 672 с.