Секция «40.16 Биоэтика и прикладная этика»

# Рост киберпреступности как угроза частной жизни современного человека

**Научный руководитель – Оренбург Михаил Юльевич**

***Воробьева Виктория Александровна***
*Студент (бакалавр)*
Московский государственный университет имени М.В.Ломоносова, Философский факультет, Москва, Россия
*E-mail: sheld008@mail.ru*

Технологии ИИ становятся всё более распространёнными, что вынуждает правительство РФ принимать активные меры по разработке, улучшению и внедрению их в разные сферы. Так, в рамках федерального проекта «Искусственный интеллект», утверждённого в 2021 г. для реализации Национальной стратегии, предполагается использование 24,1 млрд руб. из бюджетного финансирования и 5,1 млрд руб. из внебюджетного финансирования [9]. Возрастает и количество людей, которые не только слышали об ИИ, но и способны объяснить, что это такое. Согласно данным ВЦИОМа количество последних увеличилось на 18% за период с 2021 года по 2024 год [2].

Однако неуклонно растёт и количество киберпреступлений, т.е. преступлений, связанных с компьютерными техническими средствами [5, с. 163]. Согласно краткой характеристике состояния преступности в Российской Федерации за январь – декабрь 2024 года от МВД РФ, было зарегистрировано 765,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 13,1% больше, чем в аналогичном периоде прошлого года (с 34,8% в январе-декабре 2023 года до 40,0%) [6]. Важную роль в этом процессе играет появление новых технологий, направленных на генерацию медиаконтента.

Целью данного исследования является рассмотрение сочетания биометрии и дипфейков в качестве потенциальной угрозы цифровой безопасности. Для достижения цели были поставлены следующие задачи: перечислить ряд факторов, сочетание которых делает новые технологии небезопасными; рассмотреть конкретный пример нарушения утечки персональных данных; поставить ряд вопросов, связанных с безопасностью в киберпространстве.

В качестве материалов исследования были использованы публикации, размещённые на портале Cyberleninka, данные всероссийского центра изучения общественного мнения (ВЦИОМ), национального портала в сфере искусственного интеллекта, а также новостных изданий. В работе были использованы такие общенаучные методы, как анализ и синтез.

Росту киберпреступности способствует ряд факторов. Первым является курс РФ на цифровизацию, в рамках которого осуществляется сбор биометрии, при явной недостаточности мер, принятых в рамках цифровой безопасности. Это приводит к опасениям по поводу утечки биометрических данных, которые только усугубляются за счет особо громких случаев, например, утечка примерно 27,8 млн записей и 23 ГБ данных из базы данных южнокорейской компании Suprema в 2019 г. Периодические спекуляции о возможности несанкционированного доступа к персональным данным с портала «Госуслуги», накладываются на вызывая боязнь данных инициатив [8]. Подтверждением возможности подобных случаев служат различные телеграмм-каналы, которые за небольшую плату предлагают поиск информации о любом человеке. Так на данный момент возможно узнать ФИО, полную дату рождения, адреса проживания как человека, так и его родственников. По данным ВЦИОМа 23% и 41% опрошенных опасаются и скорее опасаются утечки персональных данных [10].

Вторым – пробелы в компьютерной грамотности населения. По данным аналитического центра НАФИ индекс цифровой грамотности граждан РФ достиг высокой отметки в 71 п.п. (по сравнению с показателями 2018 года равным 52 п.п.), но уже третий год не увеличивается [4]. Из-за этого не все граждане РФ имеют возможность отличить сгенерированное изображение от настоящего. В то время как на данный момент существует множество различных бесплатных нейросетей, способных «оживить» фотографии, сгенерировать голос и использовать его по усмотрению пользователя, создать видео с каким-либо человеком и т.д. Однако, есть и другая сторона вопроса: захотят ли люди как-либо проверить информацию, прежде чем верить ей?

Третьим – недостаточная гибкость отечественной правовой системы, основанной не на прецеденте, а также не высокая скорость реагирования на развитие новых технологий. Так, четкое определение дипфейка в действующем законодательстве РФ до сих пор отсутствует [1, с. 27]. Ряд авторов, таких как Бодров Н.Ф., Лебедева А.К. и др. указывают на отставание Российского законодательства от темпов научно-технического развития [6]. Так, биометрия регулируется Федеральным законом от 29.12.2022 №572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», при том, что Тинькофф Банк начал осуществлять сбор биометрических данных уже в 2018 году [7].

Данные факторы открывают широкий простор как для мошеннических действий, так и для кибербуллинга. Печальным примером подобно стала ситуация с 16-летней школьницей из Уфы. Из-за ссоры в чате игры, житель Новгородской области начал травлю, которая длилась несколько месяцев и вышла за пределы интернет-пространства. Он использовал фотографии девушки для создания фейкового телеграм-канала с откровенно жестоким контентом, порочащим её честь и достоинство, а также завладел её персональными данными, которые использовал для увеличения масштабов травли. Кроме того, ему стали известны данные родителей жертвы, её младшей сестры и одноклассников, которым он также направлял сообщения с призывами к суициду, угрозами физической расправы и сгенерированным неприемлемым контентом. Травле подверглись даже те, кто пытался заступиться за девушку, поскольку их личные данные тоже были скомпрометированы. При этом, неизвестно, какими источниками информации пользовался злоумышленник [3].

В данной ситуации преступника смогли привлечь за доведение до самоубийства, поскольку его сообщения содержали явный к этому призыв. Однако какой масштаб подобное деяние могло бы принять, будь у него ещё и биометрия жертвы? В подобном случае вероятно, как минимум, возможность взять кредит на имя жертвы или генерация более правдоподобного неприемлемого материала. Причём в наиболее уязвимом положении при подобных обстоятельствах окажутся подростки и пожилые люди. Ничто не помешает кому-либо сгенерировать порочащий честь ребёнка контент и разослать его знакомым и друзьям, что успеет нанести непоправимый вред репутации. При этом последствия для формирования подрастающей личности могут быть достаточно серьёзными. В случае с пожилыми людьми, стресс от ситуации может причинить серьёзный вред их здоровью.

В связи с этим встаёт целый ряд проблем: как оценить нанесённый ущерб, если он не столько материальный, сколько моральный? По каким статьям судить преступника? Какое место в отечественной правовой системе должны занять нормы, регулирующие отношения в области генерации видео-, фото- и аудиофайлов? Как усилить меры безопасности хранения биометрических данных?

Разумеется, в зависимости от последствий, могут быть применены такие статьи УК РФ, как ст. 110 – доведение до самоубийства, ст. 128 – клевета, ст. 163 – вымогательство, ст.

282 – возбуждение ненависти либо вражды, а равно унижение человеческого достоинства и др.. Действует ряд федеральных законов, регламентирующих биометрию (№572-ФЗ) и отношения, связанные с обработкой персональных данных (№152-ФЗ), а также статья 272 УК РФ «Неправомерный доступ к компьютерной информации», этого явно недостаточно, поскольку технические средства не всегда позволяют отследить причину утечки персональных данных, которая может привести к необратимой потере репутации жертвы кибернасилия. Соответственно перед законодательством РФ ставится задача разработки новых НПА и совершенствования технологий, которую ещё предстоит решить.

**Источники и литература**


1) Бодров Н.Ф., Лебедева А.К. — Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. – 2023. – № 11. С. 26 –38.
2) Доверие к ИИ // ВЦИОМ. Новости URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/doverie-k-ii (дата обращения: 15.02.2026).
3) Житель Новгородской области пытался довести школьницу до самоубийства из-за чата // Автономная некоммерческая организация «ТВ-Новости» URL: https://russian.rt.com/russia/news/1428487-dovedenie-samoubiistvo-shkolnica (дата обращения: 15.02.2026).
4) Индекс цифровой грамотности-2024: цифровая грамотность россиян не растет третий год подряд // Аналитический центр НАФИ URL: https://nafi.ru/analytics/indeks-tsifrovoy-gramotnosti-2024-tsifrovaya-gramotnost-rossiyan-ne-rastet-tretiy-god-podryad-/ (дата обращения: 13.02.2026).
5) Кочкина Эльвира Леонидовна Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. №3 (17). С. 162 – 169.
6) Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2024 года // Официальный сайт Министерства внутренних дел Российской Федерации URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 15.02.2026).
7) Тинькофф Банк приступил к сбору биометрических данных по всей России // ТБанк URL: https://www.tbank.ru/about/news/31102018-tinkoff-bank-biometry-aggregation/ (дата обращения: 15.02.2026)
8) Утекла огромная база биометрической информации // InfoWatch URL: https://www.infowatch.ru/analytics/utechki-informatsii/utekla-ogromnaya-baza-biometricheskoy-informatsii (дата обращения: 15.02.2026).
9) Федеральный проект «Искусственный интеллект» // Национальный портал в сфере искусственного интеллекта URL: https://ai.gov.ru/national-strategy/ (дата обращения: 15.02.2026).
10) Цифровая самооборона // ВЦИОМ. Новости URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/cifrovaja-samooborona (дата обращения: 16.02.2026).