Yugay Lyudmila Yurievna
Yuridik fanlar bo'yicha falsafa doktori (PhD), O'zbekiston Respublikasi IIV Akademiyasi
Oliy o'quv yurtidan keyingi ta'lim fakulteti doktoranti
E-manzil: yugai.lyudmila@mail.ru

BIOMETRIK TEXNOLOGIYALARDAN FOYDALANGAN HOLDA FIRIBGARLIKNING MOHIYATI: XATARLAR VA OLDINI OLISH CHORALARI

Yugay Lyudmila Yurievna
Doctor of Philosophy (PhD) in legal sciences, doctorate of the Faculty of Postgraduate Education of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan,
E-mail: yugai.lyudmila@mail.ru

FRAUD WITH BIOMETRIC AUTHENTICATION: ESSENCE, RISKS AND COUNTERMEASURES

Югай Людмила Юрьевна
Доктор философии (PhD) по юридическим наукам, докторант Факультета послевузовского образования Академии МВД Республики Узбекистан,
Эл-почта: yugai.lyudmila@mail.ru

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ: СУЩНОСТЬ, РИСКИ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

В XXI веке цифровые технологии распространили свое влияние на многие аспекты жизни: в социальной сфере, экономике, предпринимательстве, государственном управлении и в городском хозяйстве. Успешно реализуется система цифровых баз, внедрены биометрические документы, в действующий АПК «Безопасный город» внедряются биометрические технологии, в частности системы распознавания лиц; фото и видео с цифровых камер находят свое применение в правоохранительной деятельности.

Основной задачей биометрии является идентификация и верификация лица. В условиях современной пандемии остро стоит вопрос удалённой идентификации личности при помощи биометрических методов. Это удобно, безопасно и экономично.

На сегодняшний день во всем мире, в том числе и в нашей стране, инновационные биометрические подходы активно внедряются в банковскую, нотариальную сферы, в правоохранительную деятельность, системы контроля управления доступом и т.д. На сегодняшний день

предусмотрены проекты по внедрению биометрических технологий, таких как систем распознания лиц (Face-ID) и голосовой верификации личности, внедрение Единой биометрической системы[1].

При этом, необходимо отметить, что около 26% всех наиболее распространённых биометрических проектов в мире внедрены в банковской сфере, причем их география очень обширна – Канада, США, Мексика, Коста-Рика, Гватемала, Нидерланды, Великобритания, Франция, Китай, Индия, Япония, Южная Корея, Сингапур, Катар, Пакистан, Кувейт, ЮАР и другие страны[2].

Необходимо отметить, что достаточно широкий сегмент охвата биометрическими технологиями сфер жизнедеятельности общества создаёт серьёзные риски и угрозы при недостаточно ответственном отношении к сохранности указанных персональных данных.

На сегодняшний день биометрические параметры человека похищаются и создаются при помощи подручных средств, нейронных сетей, искусственного интеллекта, а также технологии машинного обучения.

В 2019 г. Facebook совместно Microsoft, Массачусетским технологическим институтом, Калифорнийским университетом в Беркли, Оксфордским университетом и другими исследовательскими организациями объявил конкурс по созданию и технологиям выявления дипфейков (DeepFake Detection Challenge).

Дипфейки (DeepFake – «глубокая подделка») – это технология создания искусственным интеллектом цифрового двойника реальной личности. Нейросеть по пикселям собирает ролик на основе готовых изображений. Например, изучает тысячи фотографий отдельного лица и создает видео. Данный цифровой двойник может иметь лицо, голос реального человека, присущие ему жесты и мимику.

Кроме того по данным CNN, Агентство перспективных оборонных исследовательских проектов (DAPRA) при Министерстве обороны США сотрудничает с крупнейшими исследовательскими учреждениями страны, чтобы выявить дипфейки.

В феврале 2021 г. МВД России объявило конкурс на разработку программы, позволяющей обнаружить дипфейк. Причем создаваемая система должна выявлять подделку не после обнаружения, а во время просмотра или прослушивания данных файлов.

Вышеуказанные технологии могут быть использованы для компрометации политических деятелей, создания порнографических видео с участием известных актеров или других публичных персон, получения финансовой прибыли и многого другого. Специалисты признают, что на данный момент обнаружение DeepFake чрезвычайно сложно.

В январе 2021 г. Народная прокуратура Шанхая обвинила двух жителей Китая, которые при помощи дипфейков с 2018 г. обманывали налоговую службу. Они покупали фотографии людей на «чёрном онлайн-рынке», «оживляли» с помощью дипфейк-приложений и проходили

проверку систем распознавания. Мошенники оформляли на несуществующих людей компании-пустышки и выдавали поддельные налоговые накладные. За два года мошенники подделали накладные на сумму свыше 76 млн долларов.

В начале сентября 2021 года в социальных сетях появилось видео под заголовком «Важное заявление от Олега Тинькова». На нем человек, похожий на Олега Тинькова, обещает подарить 50%-ный бонус к любой сумме вложения. Авторы подделки смогли воспроизвести «моргание» у фейкового Тинькова. В 2020 году отсутствие моргания считалось одним из признаков, позволяющих выявить deepfake. При переходе по ссылкам рядом с дипфейком, просят оставить оставить персональные данные.

Например, в октябре 2019 г. в Калифорнии запретили использовать различные голосовые, текстовые и визуальные фейки в предвыборной гонке. Подобные позиции на запрет дипфейков высказывались в Великобритании и Канаде.

В ближайшем будущем использование данной технологии обязательно будет регулироваться по всему миру. М.А. Желудков считает, что необходимо создание особой системы цифровых и правовых форм защиты от технологии дипфейк[3].

С.В. Баженовым, В.Е. Дивольдом, А.А. Морозовым, Д.В. Поповым, Д.М. Сафроновым, А.В. Серовым была разработана Концепция национальной системы биометрической идентификации личности, которая определяет принципы Национальной системы биометрической идентификации личности, вопросы информационной безопасности и защиты персональных данных[4].

Полагаем, что целесообразна разработка подобного документа в Республике Узбекистан, поскольку необходим основополагающий нормативный акт, который будет определять принципиальные понятия, задачи и регламент оборота биометрических данных. Также считаем необходимым, разработку и принятие Закона «О государственной биометрической регистрации», который на законодательном уровне будет регламентировать использование общегражданских и специальных биометрических баз данных.

С появлением биометрии преступникам становится проще совершить мошеннические операции с применением технологии дипфейка, например при получении кредита. Подмена видео- и фотоданных при получении кредита или продажи недвижимости создает реальную опасность для личности, которая даже не подозревает, что по его идентификационным данным совершается преступление

Официальных статистических данных по данному способу совершения преступлений не ведется.

Рост числа преступлений в сети «Интернет», в т.ч. мошеннических действий, напрямую зависит от появления новых технологических

способов обмана и введение в заблуждение граждан независимо от их интеллектуального уровня или социального положения[5].

Киберпреступники заинтересованы в разработке, постоянном совершенствовании и внедрении инновационных высокотехнологичных подходов для осуществления кражи биометрических данных или их фальсификации с целью для совершения преступлений. Если дипфейки первого поколения выявляются с вероятностью 100%, то в случае второго поколения данные показатели составляют от 15 до 30%.

Ущерб от данной категории преступлений более существенный по сравнению с традиционными видами преступлений. Последствия от них могут быть экономическими, политическими, репутационными, моральными и т.д. В связи с этим, необходимо своевременно принимать соответствующие меры.

Подводя итог, необходимо отметить, что мерами по противодействию мошенничества с использованием биометрии являются следующие:

– при использовании ЕБС биометрический идентификатор не должен быть определен в качестве основного, он должен быть альтернативным. Помимо биометрического идентификатора целесообразно подтверждение другими видами идентификаторов либо сочетание нескольких видов биометрических параметров для идентификации личности;

– финансирование и проведение масштабных научных исследований по выявлению Deepfake;

– обеспечение технических и организационных систем безопасности;

– совершенствование нормативно-правовой базы в сфере оборота биометрических данных и соблюдение регламента обеспечения их безопасности (разработка Концепции национальной системы биометрической идентификации личности и др.).

Библиографические ссылки:

1 Постановление Президента Республики Узбекистан № ПП–4996 «О мерах по созданию условий для ускоренного внедрения технологий искусственного интеллекта» от 17 февраля 2021 г. // Национальная база данных законодательства, 18.02.2021 г., № 07/21/4996/0127, 29.07.2021 г., № 07/21/5199/0721.

2 Подрез А. Биометрические технологии и перспективы их использования в финансовой сфере // Банкаўскі веснік, ЛІСТАПАД 2018. – С. 61–66.

3 Желудков М.А. Изучение влияния новых цифровых технологий на детерминацию мошеннических действий (технология DeepFake) // Развитие наук антикриминального цикла в свете глобальных современных вызовов обществу: Сборник трудов по материалам всероссийской заочной научно-практической конференции с международным участием (Саратов, 16

октября 2020 г.) / Под общ. Ред. А.Г. Блинова, Е.В. Кобзевой. – ФГБОУ ВО «Саратовская государственная юридическая академия», 2021. – С. 262–270.

4 Баженов С.В., Дивольд В.Е., Морозов А.А., Попов Д.В., Сафронов Д.М., Серов А.В. Создание Концепции национальной системы биометрической идентификации личности // Труды Академии управления МВД России. – 2020. – № 2 (54) – С. 41–53.

5 Желудков М.А. Изучение влияния новых цифровых технологий на детерминацию мошеннических действий (технология Deep Fake) // Развитие наук антикриминального цикла в свете глобальных современных вызовов обществу: Сборник трудов по материалам всероссийской заочной научно-практической конференции с международным участием (Саратов, 16 октября 2020 г.) / Под общ. Ред. А.Г. Блинова, Е.В. Кобзевой. – ФГБОУ ВО «Саратовская государственная юридическая академия», 2021. – С. 262–270.

6. Расулев, А.К. Компьютерные преступления: уголовно-правовые и криминологические аспекты / А.К. Расулев. – Ташкент, 2006. – 27 с.

7. Расулев, Абдулазиз. "Информационная безопасность в условиях пандемии коронавируса." Review of law sciences 2 (2020).

8. Турсунов, Ахтам Соломович, and Абдулазиз Каримович Расулев. "УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ МЕРЫ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ." Вопросы криминологии, криминалистики и судебной экспертизы 2 (2019): 40-44.