Научная статья
УДК 343.85
DOI: 10.37973/VESTNIKKUI-2024-57-8

УГОЛОВНО-ПРАВОВОЙ АСПЕКТ ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И ПРИЕМОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Елена Владимировна Зотина,
Казанский юридический институт МВД России, Казань, Россия,
ezotina@mail.ru

Аннотация

Введение: в статье рассматриваются некоторые особенности уголовно-правового предупреждения мошеннических действий, совершаемых с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии.

Обзор литературы: изучены труды М.М. Бабаева, И.Р. Бегишева, Р.И. Дремлюги, М.А. Ефремовой, С.И. Иванцова, Ю.Е. Пудовочкина, Е.А. Русскевича, Н.Ю. Скрипченко, С.Н. Титова и других ученых, посвященные вопросам превентивной криминализации и ужесточения уголовной ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий.

Материалы и методы: методологическая основа исследования представлена совокупностью общенаучных и специальных методов научного познания, среди которых диалектический метод, формально-юридический и системно-структурный методы, а также контент-анализ. Эмпирической основой исследования послужили документы стратегического планирования; федеральное законодательство, затрагивающее исследуемую тему; а также материалы публикаций, представленных в открытых источниках (средствах массовой информации).

Результаты исследования: автор статьи приходит к выводу, что уголовно-правовое предупреждение мошенничества с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии – неотъемлемая часть общей уголовно-правовой политики законодателя, направленной на обеспечение надлежащей охраны информационной безопасности. Рассматриваются позиции ученых о перспективах криминализации информационно-телекоммуникационных технологий и технологий искусственного интеллекта при совершении мошеннических действий. Автор статьи полагает нецелесообразным введение квалифицирующего признака «с использованием информационно-телекоммуникационных технологий» в составы преступлений о мошенничестве, в то время как применяемые технологии искусственного интеллекта способствуют криминальной трансформации социоинженерных атак, повышают степень общественной опасности, делая их более массовыми и при этом персонифицированными, что обусловливает целесообразность криминализации данных технологий при совершении преступного посягательства.

Обсуждение и заключение: предлагается внесение изменений в уголовное законодательство в части дополнения модели дифференциации уголовной ответственности новым квалифицирующим признаком – «совершение преступления с использованием технологий искусственного интеллекта». Автор предлагает ввести данный квалифицирующий признак в ст. 159, 159^3, 159^6 Уголовного кодекса Российской Федерации, а также дополнить перечень отягчающих обстоятельств, установленный ст. 63 Уголовного кодекса Российской Федерации, новым обстоятельством – «совершение преступления с использованием технологий искусственного интеллекта».

Ключевые слова: мошенничество; информационно-телекоммуникационные технологии; социальная инженерия; предупреждение, дифференциация уголовной ответственности

Для цитирования: Зотина Е.В. Уголовно-правовой аспект предупреждения мошенничества с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 3 (57). С. 73 – 82. DOI: 10.37973/VESTNIKKUI-2024-57-8

Scientific article
UDC 343.85
DOI: 10.37973/VESTNIKKUI-2024-57-8

CRIMINAL ASPECT OF PUBLIC TELECOMMUNICATIONS NETWORKS CRIME AND SOCIAL ENGINEERING PREVENTION

Elena Vladimirovna Zotina,
the Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, Russia,
ezotina@mail.ru

Abstract

Introduction: the author discusses certain features of public telecommunications networks and social engineering crimes.

Literature review: the author studied the works of M.M. Babaev, I.R. Begishev, R.I. Dremlyuga, M.A. Efremova, S.I. Ivantsov, Y.E. Pudovochkin, E.A. Russkevich, N.Y. Skripchenko, S.N. Titov and others on preventive criminalization and increasing criminal liability for public telecommunications networks crimes.

Materials and Methods: general and specific methods of scientific conception (dialectical, legal, system and structure methods and content analysis) formed the methodology of the study. Strategic planning documents, federal laws dealing with the subject under study, as well as publications in public domain (Mass media) were empirical research.

Results: the author concludes that criminal prevention of these types of crimes is an integral part of the common criminal policy of the legislature aimed at the proper protection of information security. The author also considers scientific positions of the perspectives on the criminalization of information and telecommunications technologies and AI technologies used in fraud. The author believes it is inappropriate to introduce a qualifying characteristic "with the use of public telecommunications" to the crimes of fraud while applied artificial intelligence technologies contribute to the criminal transformation of social engineering attacks, increases the threat to society making them more massive yet personalized which makes it appropriate to criminalize these technologies in the commission of criminal offences.

Discussion and Conclusions: it is proposed to amend the criminal legislation in terms of additions to the differentiation model of criminal responsibility with a new qualifying element "committing a crime using artificial intelligence technology". The author suggests to introduce the element to Articles 159, 159^3, 159^6 of the Criminal Code of the Russian Federation, as well as to add "committing a crime using artificial intelligence technology" to the list of aggravating circumstances established by Article 63 of the Code.

Keywords: fraud; information and telecommunication technologies; social engineering; prevention, differentiation of criminal liability

For citation: Zotina E.V. Criminal Aspect of Public Telecommunications Networks Crime and Social Engineering Prevention. Bulletin of the Kazan Law Institute of MIA of Russia. 2024;15(3):73-82. (In Russ.). DOI: 10.37973/VESTNIKKUI-2024-57-8

Введение

Предупреждение преступности – это комплекс мер, оказывающих воздействие на ее причинный комплекс, выявление преступников и оказание на них предупредительного, исправительного воздействия.

Значимую роль в системе мер предупреждения преступности играют нормы уголовного права; предупреждение преступлений в качестве задачи закреплено в ст. 2 Уголовного кодекса Российской Федерации (УК РФ)[1]. Эффективное предупреждение преступлений должно начинаться с реализации государством уголовно-правовой политики, направленной на оказание действенного предупредительного эффекта. Представляется, что указанное особенно актуально в современных условиях интенсивно развивающихся новых технологий, которые могут быть использованы и уже начинают использоваться в преступных целях. В связи с этим система уголовно-правовых мер должна быть ориентирована не только на реализацию карательно-репрессивной функции,

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 12.06.2024) // Собрание законодательства Российской Федерации. 1996. 17 июня. № 25. Ст. 2954; Собрание законодательства Российской Федерации. 2024. 1 января. № 1 (ч. 1). Ст. 22.

но и на предупреждение совершения новых преступлений. Как справедливо отмечает профессор С.И. Иванцов, «уголовное право является той отраслью законодательства, в которой государственная политика предупреждения преступности находит наиболее полное выражение» [1, с. 3].

Согласно данным ГИАЦ МВД России, в настоящее время каждое третье преступление совершается с использованием информационно-телекоммуникационных технологий[1]. В этой сфере в 2023 году зарегистрировано на 29,7% больше уголовно наказуемых деяний, чем в январе-декабре 2022 года[2]. Существенная доля преступлений с использованием информационно-телекоммуникационных технологий приходится на хищения (мошенничества и кражи). Все большее распространение при совершении данных преступлений получают приемы криминальной социальной инженерии. Задействуются и технологии искусственного интеллекта, в частности, дипфейки для подделки голоса и изображения физических лиц, чат-боты для генерации фишинговых писем. По сравнению с 2022 годом, в 2023 году количество видеодипфейков увеличилось в три раза, аудиодипфейков – почти в восемь раз. Экспертное сообщество прогнозирует еще более широкое распространение дипфейков в ближайшие годы[3]. При этом нормативно-правовое регулирование данных технологий требует своего совершенствования с целью минимизации и исключения криминологических рисков, связанных с противоправным использованием нейросети. В связи с этим вопросы предупреждения мошеннических действий, совершаемых с использованием информационно-телекоммуникационных технологий (в том числе технологий искусственного интеллекта) и приемов социальной инженерии, при помощи уголовно-правовых мер остаются актуальными и требующими научной проработки и дискуссии.

Обзор литературы

Уголовно-правовые и криминологические особенности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, а также вопросы предупреждения данных преступлений рассматривали И.Р. Бегишев, Г.Р. Григорян, Р.И. Дремлюга, К.Н. Евдокимов, С.В. Иванцов, С.Я. Лебедев, Н.В. Летелкин, Д.А. Овсюков, В.С. Овчинский, А.Л. Осипенко, А.П. Перетолчин, А.В. Петрянин, М.А. Простосердов, Д.В. Пучков, Э.Л. Сидоренко, В.Г. Степанов-Егиянц, М.В. Талан, М.Д. Фролов, З.И. Хисамова, И.Р. Шикула, П.С. Яни и другие исследователи.

Материалы и методы

Эмпирическую основу исследования составили документы стратегического планирования; федеральное законодательство, затрагивающее исследуемую сферу; сведения о состоянии преступности, публикуемые ГИАЦ МВД России; постановления Пленума Верховного Суда Российской Федерации; публикации в СМИ. При подготовке статьи использованы общенаучные (анализ, синтез, индукция, дедукция, сравнение, наблюдение, описание, обобщение) и частнонаучные (формально-юридический, системно-структурный, контент-анализ) методы познания. Формально-юридический и системно-структурный методы использованы при изучении нормативного материала и толковании норм уголовного закона. Метод контент-анализа публикаций в СМИ применялся при анализе информации, представленной в открытых источниках.

Результаты исследования

Идея о превентивной функции уголовного закона приобретает особую актуальность в контексте динамично развивающихся процессов цифровизации и информационной глобализации общества, когда стремительное развитие новых технологий способствует трансформации преступности, придавая ей все более высокотехнологичный характер; при этом существующие уголовно-правовые запреты не всегда соответствуют этим изменениям и, соответственно, не содержат механизмов, призванных не допустить массовой криминализации лиц, вовлеченных в «цифровую преступность». Так, например, профессора Ю.Е. Пудовочкин и М.М. Бабаев указывают, что современные изменения законодательства определяют специфику текущей (трансформированной) уголовной политики: «использование уголовного закона для позитивного урегулирования общественных отношений, признание не только реально существующих, но и потенциально возможных деяний общественно опасными и уголовно наказуемыми, поддержка политического курса и забота об «улучшении» граждан» [2, с. 118]. По их мнению, разумная идея совмещения воздания и предупреждения приобрела такую конфигурацию, при которой довлеющей стала идея именно предупреждения преступлений [2]. Идея превентивной криминализации приобретает все большую поддержку среди правоведов. Выражая

[1] Состояние преступности в России за январь-декабрь 2023 года // ГИАЦ МВД России. URL: file:///C:/Users/%D0%95%D0%BB%D0%B5%D0%BD%D0%B0/Downloads/Sbornik_dlya_UOS.pdf (дата обращения: 08.04.2024).

[2] Там же.

[3] XII Петербургский международный юридический форум. URL: https://legalforum.info/news/54-rossijan-schitajut-chto-regulirovat-dipfejki-neobhodimo-na-zakonodatelnom-urovne/ (дата обращения: 01.08.2024).

солидарность с данной позицией, считаем, что современная уголовно-правовая доктрина в условиях трансформации права должна быть направлена не только на сдерживание, минимизацию, ликвидацию уже существующих криминальных проявлений, но и минимально возможных, потенциальных угроз, создающих угрозу национальным интересам и безопасности страны. К числу подобных угроз, несомненно, следует отнести преступления, совершаемые с использованием информационно-телекоммуникационных технологий, а также их модификации, связанные с активизацией криминального потенциала технологий искусственного интеллекта, которые получают активное распространение.

Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, – это одна из основных задач уголовно-правовой политики современного законодателя.

Ученые справедливо отмечают, что требуется реализация комплекса правовых мер предупреждения преступности, направленных на обеспечение надлежащей уголовно-правовой охраны информационной безопасности. Так, по мнению отечественных исследователей, давно назрела необходимость как пересмотра отечественного уголовного законодательства, так и принятия международного нормативного акта, направленного на уголовно-правовую охрану общественных отношений, связанных с обеспечением информационной безопасности, искусственного интеллекта; принятия единых правил и норм в противодействии цифровой преступности и бесконтрольному обороту виртуальных активов. И.Р. Бегишев обоснованно указывает, что принятие Российской Федерацией Концепции развития регулирования отношений в сфере технологий искусственного интеллекта до 2030 года, наряду с Национальной стратегией развития искусственного интеллекта до 2030 года, «стало признанием российским обществом и правительством серьезных вызовов и угроз, которые возникли и продолжают расти с развитием технологий искусственного интеллекта и робототехники, что ставит важную задачу перед правовой системой в целом и уголовным правом в частности» [3]. 27 июля 2021 года Россия внесла в Спецкомитет ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях российский проект первого в истории универсального договора по борьбе с киберпреступностью. Данный проект был подготовлен при участии Генеральной прокуратуры Российской Федерации, Министерства иностранных дел Российской Федерации и учитывает современные вызовы и угрозы в сфере международной информационной безопасности, вводит новые составы преступлений, совершаемых с использованием информационно-телекоммуникационных (распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и др.). Также проект расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов[1]. Однако информация, имеющаяся в СМИ, дает основание утверждать, что не все предложения Российской Федерации вошли в итоговый проект[2].

К предупредительной деятельности, связанной с назначением уголовного наказания, относятся вопросы криминализации и декриминализации деяний.

Криминализация технологий искусственного интеллекта, используемых при совершении преступных посягательств, в том числе и мошеннических действий, находится в поле внимания зарубежных и отечественных исследователей. Дискуссия по поводу данной проблемы ведется как на крупнейших правовых площадках и научных конференциях, так и в научной периодике. Особое внимание приобретает вопрос правового регулирования дипфейков в связи с увеличением фактов совершения мошеннических действий с использованием данной технологии. На XII Петербургском международном юридическом форуме, состоявшемся в июне 2024 года в г. Санкт-Петербурге, вопрос об установлении ответственности за дипфейки стал одним из самых обсуждаемых и актуальных. Кроме того, заместитель Председателя Государственной Думы Федерального Собрания Российской Федерации Ирина Яровая отметила, что «сегодня нужно ввести дополнительный квалифицирующий признак, устанавливающий ответственность за само формирование рассылки через так называемые бот-чаты для достижения противоправного результата. Сам характер такого преступления имеет более вы-

[1] Россия внесла в специальный комитет ООН проект конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях // Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=63983506 (дата обращения: 20.01.2024).

[2] URL: https://www.kommersant.ru/doc/6452715 (дата обращения: 20.01.2024).

сокую степень общественной опасности, более серьезные общественно опасные последствия»[1]. Указанное имеет прямое отношение к рассылке фишинговых писем.

Опыт зарубежных стран свидетельствует, что некоторые государства идут по пути криминализации технологий искусственного интеллекта. В Китае с января 2023 года действуют «Положения об управлении глубоким синтезом информационных сервисов в Интернете». Они требуют у поставщиков услуг по созданию контента и пользователей маркировать контент, подвергнутый манипуляциям любого типа. «Положения» также содержат запрет на фейковые новости. Особое внимание уделяется рискам неправомерного использования технологии дипфейк и попыткам регулировать ее использование с помощью специального законодательства [4]. В штате Теннеси США подписан закон (ELVIS ACT – «Закон Элвиса»), направленный на защиту интересов прав музыкантов и авторов песен от потенциальной опасности искусственного интеллекта. В Германии предлагается внесение изменений в уголовное законодательство, предусматривающих ответственность за создание и распространение искусственно сгенерированного медиаконтента без согласия изображенного лица.

Анализ отечественной научной литературы дает основание утверждать, что в отношении криминализации информационно-телекоммуникационных технологий, технологий искусственного интеллекта высказываются мнения о введении дополнительных квалифицирующих признаков в ряд статей УК РФ и о дополнении перечня отягчающих обстоятельств, установленного ст. 63 УК РФ, соответствующим пунктом, связанным с упоминанием искусственного интеллекта. Рассмотрим некоторые научные позиции.

Еще в 2021 году Р.И. Дремлюга высказал мнение о необходимости дополнения модели дифференциации уголовно-правовой ответственности новым квалифицирующим признаком «совершенное посредством систем искусственного интеллекта» в рамках статей Главы 28 «Преступления в сфере компьютерной информации» УК РФ. Кроме этого, он предложил дополнить перечень отягчающих обстоятельств новым пунктом «с»: «совершение преступления посредством систем искусственного интеллекта» [5]. Д.А. Овсюков предлагает ввести дополнительные квалифицирующие признаки «сопряженное с передачей компьютерной информации в информационно-телекоммуникационных сетях (включая сеть «Интернет»)» и «сопряженное с размещением компьютерной информации в информационно-телекоммуникационных сетях (включая сеть «Интернет»)» в ч. 2 и 3 соответственно ст. 159 УК РФ [6]. М.А. Ефремова, Е.А. Русскевич указывают, что совершение обманного преступления с использованием дипфейков свидетельствует о значительном увеличении общественной опасности совершаемого деяния и данное обстоятельство не учтено в российском законодательстве в полной мере. Кроме того, по их мнению, «инструментальная роль» технологии в механизме преступного посягательства ставит под сомнение мысль о необходимости принятия каких-либо специальных мер по самостоятельной криминализации дипфейков [7]. Таким образом, криминализировать следует не саму технологию, а ее криминальное использование при совершении того или иного преступного посягательства. Следовательно, необходимо дополнить отечественную модель дифференциации уголовной ответственности новым квалифицирующим признаком – «совершение преступления с использованием технологии дипфейк» [7]. С.Н. Титов высказывает аналогичную позицию в отношении криминализации информационно-телекоммуникационных технологий и выступает за введение соответствующего квалифицирующего признака в статьи УК РФ: по его мнению, использование данных технологий должно влечь более строгую ответственность в тех случаях, когда оно существенно облегчает совершение преступления, ведет к расширению числа получателей деструктивной информации или незаконных товаров и веществ и в перспективе способно увеличить число совершаемых преступлений. Он формулирует содержание квалифицирующего признака в отношении преступлений, совершаемых против интеллектуальной собственности с использованием информационных технологий, следующим образом: «Деяние, совершенное с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», либо с использованием систем искусственного интеллекта» [8, с. 158]. Выражая согласие с указанными позициями исследователей, мы считаем, что вопрос возможной криминализации информационно-телекоммуникационных технологий и технологий искусственного интеллекта должен решаться исключительно в рамках совершения преступных посягательств с их использованием. Автономная криминализация технологий не имеет смысла, так как это всего лишь инструмент, который мо-

[1] XII Петербургский международный юридический форум. URL: https://legalforum.info/news/rol-iskusstvennogo-intellekta-v-protivodejstvii-propagande-radikalnoj-ekstremistskoj-i-terroristicheskoj-dejatelnosti/ (дата обращения: 01.08.2024).

жет использоваться как в благих, так и преступных целях.

Грешнова Н.А., В.Н. Ситник, рассуждая о возможности установления уголовной ответственности за использование дипфейков, приходят к выводу о необходимости дополнения перечня отягчающих обстоятельств, предусмотренных ст. 63 УК РФ, новым пунктом – «использование цифровых технологий» [9].

Проанализировав существующие в научной литературе позиции о возможности криминализации деяний, сопряженных с использованием информационно-телекоммуникационных технологий, сформулируем ряд выводов.

Во-первых, обращение к тексту действующего уголовного закона дает основание утверждать, что законодатель уже включил квалифицирующий признак «с использованием информационно-телекоммуникационных сетей» в некоторые статьи УК РФ, например, ч. 2 ст. 110, ч. 3 ст. 110^1, ч. 2 ст. 110^2, ч. 2 ст. 230, ч. 2 ст. 245 УК РФ и другие. При этом необходимо отметить, что данный квалифицирующий признак не учтен в составах преступлений против собственности. По справедливому замечанию С.Н. Титова, данный квалифицирующий признак упоминается в составах преступлений, связанных с распространением, передачей информации, призывам к осуществлению действий. Ученый указывает, что «значение информационных технологий заключается в облегчении такой коммуникации, ее ускорении, если требуется, в расширении аудитории. Воспользовавшись такими возможностями, преступник с большей легкостью способен осуществить преступный замысел, что говорит об увеличении его разрушительной силы в отношении объекта преступления, а значит, об увеличении опасности совершаемого деяния» [8, с.154].

Следует рассмотреть вопрос о возможной криминализации информационно-телекоммуникационных технологий при совершении мошеннических действий в расширительном толковании – в каком направлении необходимо рассмотреть ужесточение ответственности, то есть пойти по пути дифференциации или индивидуализации уголовного наказания?

Существующая в научном мире дискуссия по данному вопросу свидетельствует о двух важнейших методах реализации уголовной политики: дифференциации и индивидуализации наказания.

Дифференциация уголовного наказания осуществляется через признаки состава преступления, и введение квалифицирующего признака в состав преступления – это способ дифференциации законодателем уголовной ответственности. Признаки, составляющие основу квалифицированного состава преступления, характеризуют совершенное преступное деяние как обладающее более высокой степенью общественной опасности по сравнению с преступлением, предусмотренным основным составом. В соответствии с этим за совершение такого преступления предусмотрена более строгая санкция.

Поскольку дифференциация уголовного наказания относится к правотворческому методу реализации уголовной политики, она отражает суть преступного деяния, общественную опасность, лежащую в основе криминализации. По мнению профессора А.В. Шеслера, квалифицирующие либо привилегированные признаки определенного состава преступления являются типичными и криминообразующими именно для конкретного вида преступления [10, с. 125].

Индивидуализация уголовного наказания – это средство смягчения или утяжеления наказания, реализуемое правоприменителем. Отягчающие и смягчающие обстоятельства характерны для многих видов преступлений и влияют на снижение или повышение общественной опасности преступного посягательства, но не на ее наличие как свойства преступления.

При этом одни и те же формулировки могут подразумевать под собой как квалифицирующие признаки определенного состава преступления, так и отягчающие обстоятельства, например, «совершение преступления в составе группы лиц, группы лиц по предварительному сговору, организованной группы или преступного сообщества (преступной организации)». Являясь квалифицирующим признаком, данная формулировка подчеркивает типичность совершения преступления именно группой лиц по предварительному сговору или организованной группой. Так, мошенничество с использованием информационно-телекоммуникационных технологий достаточно часто совершается именно организованными преступными формированиями с устойчивыми связями внутри группы, сплоченностью, распределением ролей и т.п.

Возвращаясь к вопросу об указании использования информационно-телекоммуникационных технологий в качестве квалифицирующего признака в общем и специальных составах о мошенничестве, полагаем это не всегда целесообразным. В то же время, по нашему мнению, идея криминализации технологий искусственного интеллекта (как разновидности информационно-телекоммуникационных технологий) при совершении мошенничества заслуживает внимания и научной дискуссии.

Имеющаяся судебно-следственная практика подтверждает, что значительная часть мошенничеств совершается в настоящее время с использованием информационно-телекоммуникационных технологий (в том числе и технологий искусственного интеллекта). Данные технологии используются преступниками как на стадии подготовки к совершению преступления (речь идет о сборе конфиденциальной информации о потенциальных жертвах, рекрутинге участников преступных схем – «курьерах» и «дропперах», подготовке криминальных планов-сценариев), так и на стадии совершения преступного посягательства. Применение информационно-телекоммуникационных технологий, особенно технологий искусственного интеллекта, способствует анонимизации преступников, трансграничности, придает криминальным атакам массовый и в то же время персонифицированный характер за счет возможности копирования особенностей аудиовизуальных индивидуальных особенностей поведения человека посредством использования дипфейков и имитации индивидуально-стилистических особенностей письменной речи в результате генерирования чат-ботами текстовых сообщений.

При этом использование информационно-телекоммуникационных технологий не всегда повышает характер и степень общественной опасности мошенничества, совершаемого с их использованием, а именно повышенная степень общественной опасности преступного деяния является основанием для его криминализации [11, с. 89]. Следует отметить, что использование информационно-телекоммуникационных технологий может быть квалифицирующим признаком лишь в том случае, когда оно носит высокотехнологичный характер и способствует более быстрому, легкому, массовому, но в то же время персонифицированному, анонимному совершению преступного посягательства и причиняет или способно причинить вред больший, чем без использования подобных технологий. Введение данного квалифицирующего признака способно вызвать сложности в квалификации деяния и, соответственно, назначении наказания, призванного достичь целей уголовного закона. Так, например, использование только аналоговой телефонии (относящейся к информационно-телекоммуникационным технологиям) при совершении мошеннических действий, без подключения сети Интернет и иных информационно-телекоммуникационных технологий, вряд ли может свидетельствовать о повышении степени общественной опасности деяния. Мы согласны с позицией профессора Н.Ю. Скрипченко, указывающей, что «тотальность и мультивариативность использования информационно-телпекоммуникационных сетей в преступной деятельности актуализирует вопрос определения границ, в рамках которых задействованность коммуникационных резервов соответствующих технологий будет образовывать механизм преступного деяния» [12, с. 210]. По справедливому замечанию Н.Ю. Скрипченко, в своем постановлении от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» Пленум Верховного Суда Российской Федерации фактически перевел отдельные виды вспомогательного применения соответствующих технологий в инструментальные [12]. Речь идет о пункте 20: «Преступление квалифицируется как совершенное с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», независимо от стадии совершения преступления, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети.»[1]. Полагаем, указанное в полной мере относится и к случаям совершения мошенничества с использованием информационно-телекоммуникационных технологий, когда использование того или иного вида информационно-телекоммуникационных технологий не всегда приводит к повышению общественной опасности посягательства; соответственно, не всегда должно учитываться в качестве квалифицирующего признака.

Что же касается технологий искусственного интеллекта, то их применение, по нашему мнению, способно существенно повысить характер и степень общественной опасности преступного посягательства, так как криминальная трансформация мошеннических действий, совершаемых с использованием дипфейков, чат-ботов, свидетельствует, что число подобных посягательств увеличивается, а применяемые технологии являются высокотехнологичными, активно развивающимися и минимизируют возможность идентификации потенциальной жертвой ложного

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 // Российская газета. 2022. 28 декабря.

скрипта или социоинженерной атаки, повышают степень доверия жертвы к преступнику за счет генерирования искусственного контента, имеющего максимальное количество индивидуализирующих признаков.

Отметим, что в России настоящее время уже имеются законодательные проекты, направленные на криминализацию дипфейков. Так, например, в Государственной Думе Российской Федерации разработан законопроект об уголовной ответственности за использование искусственного интеллекта в преступных целях. Предлагается внести изменения в статьи 128 «Клевета», 158 «Кража», 159 «Мошенничество», 163 «Вымогательство» и 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием» УК РФ, добавив в них новый квалифицирующий признак «совершение преступления с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, равно с использованием биометрических персональных данных потерпевшего или иного лица»[1]. Подобное представляется нам не совсем верным, так технологии искусственного интеллекта не ограничиваются только дипфейками и более уместным с юридико-технической точки зрения является упоминание технологий искусственного интеллекта.

В дополнение к вышеизложенному полагаем, заслуживает внимания точка зрения о необходимости выделения использования технологий искусственного интеллекта в качестве обстоятельства, отягчающего наказание, для других видов преступлений, например, вовлечения несовершеннолетнего в совершение преступления (ст. 150 УК РФ), незаконного получения кредита (ст. 176 УК РФ) или других. В данном случае речь идет не о дифференциации, а индивидуализации уголовного наказания.

Обсуждение и заключение

Подводя итоги изложенному, приходим к выводу, что в целях минимизации, нейтрализации и превенции криминальной угрозы использования технологий искусственного интеллекта, а также в связи с увеличением фактов использования преступниками криминогенных возможностей нейросети необходимо дополнить отечественную модель дифференциации уголовной ответственности новым квалифицирующим признаком – «совершение преступления с использованием технологий искусственного интеллекта». Представляется целесообразным включение данного квалифицирующего признака в ч. 3 ст. 159, 159^3, 159^6 Уголовного кодекса Российской Федерации. В целях обеспечения единообразного применения судами норм уголовного закона и устранения терминологической неопределенности юридико-технического характера предлагаем дополнить постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» пунктом 32.1 следующего содержания: «Для целей статей ст. 159, 159^3, 159^6 УК РФ под технологиями искусственного интеллекта следует понимать комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений».

В целях достижения цели общей превенции противоправного использования технологий искусственного интеллекта нормами уголовного закона предлагаем дополнить перечень отягчающих обстоятельств, предусмотренных ст. 63 Уголовного кодекса Российской Федерации, новым обстоятельством – «совершение преступления с использованием технологий искусственного интеллекта».

СПИСОК ИСТОЧНИКОВ

1. Иванцов С.И. Уголовно-правовые аспекты предупреждения современной преступности // Актуальные вопросы обеспечения общественной безопасности и противодействия преступности в Крымском федеральном округе: материалы Всероссийской научно-практ. конференции 16 июня 2016 г. / под общ. ред. С.А. Буткевича. Краснодар: Краснодарский университет МВД России, 2016. С. 3 – 8.

2. Пудовочкин Ю.Е., Бабаев М.М. Современное нормотворчество как основа формирования новой теории криминализации // Lex russica. 2023. Т. 76. № 1. С. 110 – 125. DOI: 10.17803/1729-5920.2023.194.1.110-125

[1] Разработан законопроект об уголовной ответственности за «дипфейки» // Российская газета. 2024. 28 мая.

3. Бегишев И.Р. Уголовно-правовая охрана общественных отношений, связанных с робототехникой: дис. … д-ра юрид. наук: 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Казань, 2022. 506 с.
4. Виноградов В.А., Кузнецова Д.В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. Том 17. № 2. С. 215–240. DOI:10.17323/2072-8166.2024.2.215.240
5. Дремлюга Р.И. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 3. С. 153 – 165.
6. Овсюков Д.А. Корыстные преступления против собственности, совершаемые с использованием информационно-телекоммуникационных сетей: вопросы квалификации: автореф. дис. … канд. юрид. наук: 5.1.4 – Уголовно-правовые науки. Москва, 2023. 34 с.
7. Ефремова М.А., Русскевич Е.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 2 (56). С. 97 – 105. DOI: 10.37973/VESTNIKKUI-2024-56-13
8. Титов С.Н. Может ли использование информационных технологий быть квалифицирующим признаком преступлений против интеллектуальной собственности? // Вестник Санкт-Петербургского университета МВД России. 2024. № 1 (101). С. 151–159; doi: 10.35750/2071-8284-2024-1-151-159
9. Грешнова Н.А., Ситник В.Н. Обеспечение общественного интереса в условиях цифровизации: проблемы уголовного законодательства в России (на примере технологии дипфейк (deepfake)) // Вестник Саратовской государственной юридической академии. 2022. № 5 (148). С. 182 – 189.
10. Шеслер А.В. Дифференциация и индивидуализация уголовного наказания как методы реализации уголовно-правовой политики // Вестник Кузбасского института. 2018. № 3 (36). С. 123 – 128.
11. Прозументов Л.М. Основание криминализации (декриминализации) деяний // Вестник Томского государственного университета. Право. 2014. № 4 (14). С. 81 – 91.
12. Скрипченко Н.Ю. Использование информационно-телекоммуникационных сетей в криминальных целях: нормативный учет и перспективы расширения уголовно-правового значения // Вестник РУДН. Серия Юридические науки. 2024. Т. 28. № 1. С. 196 – 214.

REFERENCES

1. Ivancov S.I. Ugolovno-pravovye aspekty preduprezhdeniya sovremennoj prestupnosti // Aktual'nye voprosy obespecheniya obshchestvennoj bezopasnosti i protivodejstviya prestupnosti v Krymskom federal'nom okruge: materialy Vserossijskoj nauchno-prakt. konferencii 16 iyunya 2016 g. / pod obshch. red. S.A. Butkevicha. Krasnodar: Krasnodarskij universitet MVD Rossii, 2016. S. 3 – 8.
2. Pudovochkin YU.E., Babaev M.M. Sovremennoe normotvorchestvo kak osnova formirovaniya novoj teorii kriminalizacii // Lex russica. 2023. T. 76. № 1. S. 110 – 125. DOI: 10.17803/1729-5920.2023.194.1.110-125
3. Begishev I.R. Ugolovno-pravovaya ohrana obshchestvennyh otnoshenij, svyazannyh s robototekhnikoj: dis. … d-ra yurid. nauk: 12.00.08 – Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo. Kazan', 2022. 506 s.
4. Vinogradov V.A., Kuznecova D.V. Zarubezhnyj opyt pravovogo regulirovaniya tekhnologii «dipfejk» // Pravo. ZHurnal Vysshej shkoly ekonomiki. 2024. Tom 17. № 2. S. 215–240. DOI:10.17323/2072-8166.2024.2.215.240
5. Dremlyuga R.I. Ispol'zovanie iskusstvennogo intellekta v prestupnyh celyah: ugolovno-pravovaya harakteristika // Aziatsko-Tihookeanskij region: ekonomika, politika, pravo. 2021. № 3. S. 153 – 165.
6. Ovsyukov D.A. Korystnye prestupleniya protiv sobstvennosti, sovershaemye s ispol'zovaniem informacionno-telekommunikacionnyh setej: voprosy kvalifikacii: avtoref. dis. … kand. yurid. nauk: 5.1.4 – Ugolovno-pravovye nauki. Moskva, 2023. 34 s.
7. Efremova M.A., Russkevich E.A. Dipfejk (deepfake) i ugolovnyj zakon // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2024. T. 15. № 2 (56). S. 97 – 105. DOI: 10.37973/VESTNIKKUI-2024-56-13
8. Titov S.N. Mozhet li ispol'zovanie informacionnyh tekhnologij byt' kvalificiruyushchim priznakom prestuplenij protiv intellektual'noj sobstvennosti? // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2024. № 1 (101). S. 151–159; doi: 10.35750/2071-8284-2024-1-151-159

9. Greshnova N.A., Sitnik V.N. Obespechenie obshchestvennogo interesa v usloviyah cifrovizacii: problemy ugolovnogo zakonodatel'stva v Rossii (na primere tekhnologii dipfejk (deepfake)) // Vestnik Saratovskoj gosudarstvennoj yuridicheskoj akademii. 2022. № 5 (148). S. 182 – 189.
10. SHesler A.V. Differenciaciya i individualizaciya ugolovnogo nakazaniya kak metody realizacii ugolovno-pravovoj politiki // Vestnik Kuzbasskogo instituta. 2018. № 3 (36). S. 123 – 128.
11. Prozumentov L.M. Osnovanie kriminalizacii (dekriminalizacii) deyanij // Vestnik Tomskogo gosudarstvennogo universiteta. Pravo. 2014. № 4 (14). S. 81 – 91.
12. Skripchenko N.YU. Ispol'zovanie informacionno-telekommunikacionnyh setej v kriminal'nyh celyah: normativnyj uchet i perspektivy rasshireniya ugolovno-pravovogo znacheniya // Vestnik RUDN. Seriya YUridicheskie nauki. 2024. T. 28. № 1. S. 196 – 214.

Информация об авторе:
Зотина Елена Владимировна, начальник редакционно-издательского отделения Казанского юридического института МВД России, ezotina@mail.ru
Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Zotina Elena V., Head of Editorial and Publishing Department, the Kazan Law Institute of the Ministry of Internal Affairs of Russia, ezotina@mail.ru
The author has read and approved the final version of the manuscript.

Статья получена: 20.04.2024.
Статья принята к публикации: 25.09.2024.
Статья опубликована онлайн: 25.09.2024.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.