ГОСУДАРСТВО И ПРАВО, 2023, № 2, с. 54–61
STATE AND LAW, 2023, No. 2, pp. 54–61

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ – СРЕДСТВО ИЛИ СПОСОБ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ?

© 2023 г. А. К. Жарова

Институт государства и права Российской академии наук, г. Москва

E-mail: anna_jarova@mail.ru

Поступила в редакцию 17.07.2022 г.

Аннотация. **Постановка проблемы.** Несмотря на пользу, которую получает общество от применения искусственного интеллекта (ИИ), его использование создает риски и угрозы, например, как средства совершения преступления. Определение понятия «искусственный интеллект» сводится к описанию совокупности отдельных информационных технологий, которые могут собирать и анализировать данные, а также имитировать когнитивную функцию человека. В научной литературе ведутся дискуссии о том, можно ли ИИ рассматривать как способ, предмет или средство совершения преступления. В статье доказывается, что ИИ нужно рассматривать как средство совершения преступления.
Цели и задачи исследования. Целью исследования являлся анализ возможностей использования ИИ в качестве средства совершения мошенничества в сфере компьютерной информации. В статье анализируются основные способы противоправных деяний, которые определены в ст. 159^6 УК РФ, судебная практика квалификации преступлений по ст. 159^6 УК РФ, положения Постановления Пленума Верховного Суда от 30 ноября 2017 г. № 48 (ред. от 29.06.2021 г.) «О судебной практике по делам о мошенничестве, присвоении и растрате». Смоделированы предполагаемые преступные деяния, которые могут быть квалифицированы по ст. 159^6 УК РФ, учитывающие способы совершения преступных деяний.

Ключевые слова: искусственный интеллект, мошенничество, средство совершения преступления, Уголовный кодекс РФ, модель преступления.

Цитирование: *Жарова А. К.* Искусственный интеллект – средство или способ совершения мошенничества в сфере компьютерной информации? // Государство и право. 2023. № 2. С. 54–61.

DOI: 10.31857/S102694520021177-5

ARTIFICIAL INTELLIGENCE – A MEANS OR METHOD OF COMMITTING FRAUD IN THE FIELD OF COMPUTER INFORMATION?

© 2023 A. K. Zharova

Institute of State and Law of the Russian Academy of Sciences, Moscow

E-mail: anna_jarova@mail.ru

Received 17.07.2022

Abstract. **Problem statement.** Despite the benefits that society receives from the use of artificial intelligence (AI), its use creates risks and threats, for example, as a means of committing a crime. The definition of "artificial intelligence" is reduced to the description of a set of individual information technologies that can collect and analyze data, as well as simulate human cognitive function. There are discussions in the scientific literature about whether and can be considered as a method, object or means of committing a crime. The article proves that it should be considered as a means of committing a crime.

Goals and objectives of the study. The purpose of the study was to analyze the possibilities of using AI as a means of committing fraud in the field of computer information. The article analyzes the main methods of illegal acts, which are defined in Article 159[6] of the Criminal Code of the Russian Federation, judicial practice of qualifying crimes under Article 159[6] of the Criminal Code of the Russian Federation, the provisions of the Resolution of the Plenum of the Supreme Court of November 30, 2017 No. 48 (ed. dated 29.06.2021) "On judicial practice in cases of fraud, embezzlement and embezzlement". The alleged criminal acts that can be qualified under art. 159[6] of the Criminal Code of the Russian Federation, taking into account the methods of committing criminal acts.

Key words: artificial intelligence, fraud, means of committing a crime, Criminal Code of the Russian Federation, crime model.

For citation: *Zharova, A.K (2023)*. Artificial intelligence – a means of method committing fraud in the field of computer information? // Gosudarstvo i pravo=State and Law, No. 2, pp. 54–61.

Введение

Тема признания искусственного интеллекта (ИИ) средством совершения противоправных деяний все больше привлекает ученых.

Понятие ИИ является собирательным и обобщает отдельные информационные технологии, которые могут обрабатывать и анализировать данные, а также имитировать когнитивную функцию человека. Алгоритмы ИИ могут содержать различные алгоритмы анализа данных, которые позволяют создавать цифровой профиль человека, определять тип используемого программного обеспечения и возможные его уязвимости, например алгоритмы машинного обучения на основе анализа данных создают прогнозные модели.

Российскими исследователями предпринимаются попытки систематизировать отдельные случаи наступления уголовной ответственности за ряд деяний, совершенных с применением ИИ[1]. Некоторые ученые предлагают в уголовном праве рассматривать ИИ как «предмет, способ или средство его совершения»[2].

В данной статье ИИ будет рассматриваться как средство совершения преступления, поскольку под способом совершения преступления понимается прием, образ действий или метод поведения лица во время совершения преступления[3]. ИИ не может быть отнесен ни к приему, ни образу действий или методу поведения лица, поскольку ИИ является программным обеспечением[4]. Под средствами совершения преступления понимают предметы, вещества, энергию и приспособления, свойства которых (физические, химические и иные) используются для совершения преступления[5].

ИИ как программное обеспечение, используемое для совершения преступления, позволяет рассматривать его в предметном, вещном качестве как средство совершения преступления. Однако признание ИИ предметом выглядит дискуссионным, поскольку это требует признания информации (программного обеспечения как совокупности информации) материальной.

По Гражданскому кодексу РФ программное обеспечение – это «представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения» (ст. 1261).

Таким образом, ИИ – это совокупность информации и запрограммированных информационных процессов.

Дискуссии о материальности информации ведутся до сих пор. Некоторыми авторами подчеркивается нематериальность информации[6], другие настаивают на том, что информация материальна, поскольку она может передаваться волновым способом, овеществляется в предметах и является

[1] См.: *Ефремова М.А., Лопатина Т.М.* Робототехника в уголовном законодательстве Российской Федерации // Росс. следователь. 2021. № 11. С. 55–58. DOI: 10.18572/1812-3783-2021-11-55-58; *Бегишев И.Р.* Международно-правовые основы регулирования искусственного интеллекта и робототехники // Междунар. публичное и частное право. 2021. № 1. С. 37–40. DOI: 10.18572/1812-3910-2021-1-37-40

[2] *Грачева Ю.В., Арямов А.А.* Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы росс. права. 2020. № 6. С. 169–178. DOI: 10.17803/1994-1471.2020.115.6.169–178

[3] См.: *Воеводкина К.М.* Обман в составе незаконного получения кредита по УК РФ: функция и значение // Росс. следователь. 2020. № 5. С. 37. DOI: 10.18572/1812-3783-2020-5-33-37; *Владыкина Т.А.* Изменение категории преступления // Уголовное право. 2018. № 5. С. 11–17.

[4] См.: *Жарова А.К.* Правовое обеспечение цифрового профилирования деятельности человека // Вестник Южно-Уральского гос. ун-та. Сер.: Право. 2020. Т. 20. № 2. С. 80–87.

[5] См.: Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. Г.А. Есакова. 9-е изд., перераб. и доп. М., 2021. С. 18.

[6] См.: *Синицын С.А.* Вещь как объект гражданских прав: возможные и должные критерии идентификации // Законодательство и экономика. 2016. № 11. С. 16; *Пучков В.О.* Информация – объект гражданского права? // Арбитражные споры. 2020. № 2. С. 138.

формализованным отражением объективной реальности в ее разнообразии форм распространения и изменчивости[7]. Мы придерживаемся позиции авторов, признающих материальность информации.

Применение ИИ в ИКТ-сфере в целях модификации информации, воздействия на информационные технологии (ИТ) позволяет совершать мошенничества. Однако квалификация таких преступлений, как мошенничество в сфере компьютерной информации, поднимает вопросы о составе преступления, определенного в ст. 159[6] УК РФ, для этого необходимо изучить возможные угрозы общественным отношениям при применении ИИ, оценить степень общественной опасности, риски и угрозы, возникающие при использовании ИИ.

Диспозиция нормы 159[6] УК РФ раскрывает мошенничество в сфере компьютерной информации как «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».

Мы имеем право поставить знак равенства между «функционированием средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» и «информационными технологиями», поскольку в соответствии с п. 2 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ (ред. от 30.12.2021 г.) «Об информации, информационных технологиях и о защите информации»[8] «информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов». Таким образом, функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей и есть информационные технологии. В связи с данным выводом мы можем сделать заключение, что в ст. 159[6] УК РФ речь идет о хищении чужого имущества или приобретении права на чужое имущество, реализованное технологическим способом в ИКТ-сфере.

Эту мысль подтверждает постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (ред. от 29.06.2021 г.) «О судебной практике по делам о мошенничестве, присвоении и растрате»[9] (далее – Постановление № 48), в котором под «вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него» (п. 20).

Ю.В. Грачева, С.В. Маликов, А.И. Чучаев считают, что такая форма хищения не может называться мошенничеством[10], поскольку в ст. 159[6] УК РФ «предусмотрен иной способ хищения, не совпадающий с мошенничеством». Однако с точки зрения теории уголовного права хищение может «совершаться открыто (грабеж), тайно (кража), путем обмана (мошенничество), с использованием насилия или угрозы насилия (грабеж, разбой)»[11]. Таким образом, мошенничество выступает одним из способов хищения имущества.

Некоторые авторы полагают, что объективная сторона данного преступления характеризуется таким способом его совершения, как «обман путем ввода, удаления, блокирования, модификации компьютерной информации...»[12]. Понимание совершения преступления через обман, несмотря на отсутствие этого способа совершения преступления в ст. 159[6] УК РФ, объяснимо, поскольку мошенничество как обман определено в ст. 159 Кодекса.

По мнению других авторов, «рассматриваемое преступление характеризуется незаконным изъятием чужого имущества путем вмешательства в функционирование компьютерной информации или информации телекоммуникационных сетей»[13]. Сложно согласиться с данным мнением, поскольку в диспозиции ст. 159[6] УК РФ отсутствует такой способ совершения преступления, как изъятие.

---

[7] См.: *Елин В.М.* Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 72.

[8] См.: СЗ РФ. 2006. № 31 (ч. I), ст. 3448.

[9] См.: Бюллетень Верховного Суда РФ. 2018. № 2.

[10] См.: *Грачева Ю.В., Маликов С.В., Чучаев А.И.* Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал ВШЭ. 2020. № 1. С. 188–210. DOI: 10.17323/2072-8166.2020.1.188.210

[11] Уголовное право России: учеб. для бакалавров / под ред. А.И. Плотникова. Оренбург, 2016. С. 96.

[12] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. Г.А. Есакова. 9-е изд., перераб. и доп. С. 102.

[13] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. Испр., доп., перераб. М., 2013. С. 127.

Такое противоречие в понимании способов совершения преступления свидетельствует о том, что диспозиция данной статьи является сложной для оценки технологических процессов и сформулирована неоднозначно. Так, с точки зрения В.М. Елина, диспозиция данной статьи заимствована из Европейской конвенции о киберпреступности[14], в связи с этим ее формулировка не соответствует в полной мере правилам и традициям уголовного законодательства Российской Федерации.

Общественная опасность деяний согласно ст. 159^6 УК РФ связана с реализацией преступниками информационных процессов, иными словами, с применением информационных технологий в ИКТ-сфере для достижения преступных целей.

Виновным может быть признан, например, пользователь информационных технологий или разработчик программного обеспечения – ИИ, программной среды, нейросети, которые позволяют достичь желаемого преступного результата – похитить чужое имущество или приобрести право на чужое имущество. Разработчик или программист такой информационной технологии может быть признан виновным только тогда, когда он, имея цель похищения имущества, создает программную разработку с функционалом, позволяющим внести изменения в функционирование ИТ.

Однако если программист дополнил функционал своей технологии вредоносными свойствами или определил ее целью нарушение работы критической информационной инфраструктуры, то потребуется дополнительная квалификация деяний по ст. 272, 273 или 274^1 УК РФ.

Преступные деяния, представленные в диспозиции ст. 159^6 УК РФ, нельзя отнести к классическому пониманию мошенничества, как оно представлено в ст. 159 УК РФ. В ст. 159^6 Кодекса отсутствуют такие деяния, как обман или злоупотребление доверием, например, они сформулированы в ст. 159^1, 159^2 («предоставление заведомо ложных и (или) недостоверных сведений»), ст. 159^5 УК РФ («хищение чужого имущества путем обмана»).

В соответствии с п. 1 Постановления № 48 в случае, если «способами хищения чужого имущества **при мошенничестве являются обман или злоупотребление доверием,** под воздействием которых владелец имущества или иное лицо передают имущество или право на него другому лицу либо не препятствуют изъятию этого имущества или приобретению права на него другим лицом, то квалификация преступлений должна осуществляться в соответствии со ст. ст. 158.1–159.5 УК РФ».

Можно сформулировать вывод, что отсутствие в ч. 1 ст. 159^6 УК РФ свидетельствует о том, что в ст. 158^1–159^5 Кодекса присутствуют способы совершения преступления – обман, злоупотребление доверием, которые отсутствуют в ст. 159^6, а также о том, что воздействие одних ИТ на другие ИТ не рассматривается в ст. 158^1–159^5 УК РФ в качестве средств совершения преступления, которые позволяют незаконно передать имущество или право на него другому лицу, либо не препятствовать изъятию этого имущества или приобретению права на него другим лицом.

Мошенничеству в сфере компьютерной информации посвящен п. 20 Постановления № 48, в соответствии с которым «мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статьям 272, 273 или 274.1 УК РФ».

Пленум Верховного Суда РФ правильно подчеркнул, что вмешательство в функционирование каких-либо ИТ является сугубо технологическим процессом. Вывод Пленума Верховного Суда РФ согласуется с пониманием функционирования ИТ как корректным выполнением функций, предусмотренных в ИТ.

В связи с отсутствием в ст. 159^6 УК РФ обмана как способа совершения преступления владелец имущества или иное лицо может и не знать, что его имущество незаконно передано другому лицу. А.А. Лаврушкина делает верный вывод, что состав ст. 159^6 УК РФ «представляет собой лишь форму хищения с использованием специфических средств, которые обозначены в диспозиции статьи»[15], поскольку мошенничество – это один из способов хищения.

Возможности ИИ немного шире, чем тех программных технологий, в которых не реализован алгоритм принятия решений на основе анализа данных. ИИ может также содержать алгоритм накопления знаний и самообучения на основе накопленной информации. В общих словах, эти алгоритмы позволяют определить условия, при удовлетворении которых будет запущено выполнение определенных программных действий и операций. Этими условиями могут быть образ конкретного человека, препятствие на дороге, повышение температуры, движение в комнате, зафиксированное датчиками, и др.

В научной литературе высказывается мысль, что «самообучаемая программа может причинять

[14] См.: *Елин В.М.* Указ. соч. С. 71.

[15] *Лаврушкина А.А.* Проблемы применения статьи 159.6 УК РФ с позиции теории и практики // Контентус. 2018. № 3 (68).

вред человеку и самостоятельно, не выступая орудием или средством совершения преступления». В качестве примера приводится случай «причинения смерти человеку беспилотным транспортным средством, которое во время испытания, передвигаясь в автономном режиме, не смогло или не пыталось вовремя затормозить, что привело к наезду на пешехода»[16]. Хотелось бы отметить ошибочность этой мысли, самообучаемая программа не может причинить вред человеку самостоятельно, нарушив заложенные в ней алгоритмы поведения. За совершенным преступлением стоит конкретный человек. В приведенном примере преступление могло случиться по вине разработчика, тестировщика или пользователя программной технологии. Вероятно, ситуация причинения смерти человеку беспилотным транспортным средством могла произойти потому, что программная технология была недостаточно протестирована, поскольку любая технология должна проходить этап тестирования, в котором выявляются ошибки в ее работе. Может быть, программист не предусмотрел и не реализовал алгоритм дополнительной проверки на наличие препятствий или распознавания образа человека, или не использовал при разработке надежные алгоритмы ИИ. Вероятна также ситуация, когда пользователь машины использовал ее не в той среде, для которой машина была протестирована.

Однако существуют ситуации, когда мы можем говорить об отсутствии вины разработчика программного обеспечения, например, если произошел удаленный доступ к технологии в связи с существующей в ней уязвимостью, вследствие чего машина вышла из-под контроля и был совершен наезд. Должны сразу оговориться, что уязвимости – это свойства любой технологии и борьба с ними заключается в их выявлении и программном решении.

В таких обстоятельствах необходимо определить, кто именно создал ту часть кода, которая позволила совершить противоправные деяния, поскольку сложный программный код зачастую разрабатывается группой специалистов[17]. Поиск ответа на этот вопрос – кто же является ответственным за произошедшие нарушения, непростой, особенно если программная технология создавалась на основании открытого программного кода. Эта сложность приводит некоторых авторов к мысли, что использование ИИ следует запретить[18]. Такое предложение является непродуманным, поскольку ИИ – одна из технологий, которая может на основании анализа данных принимать решение. Поэтому такой запрет приведет к ограничению использования ИИ. Для минимизации технологических рисков и угроз необходимо развивать стандартизацию ИИ, включая в стандарты требования к разработчикам и программистам разрабатывать или использовать алгоритмы, подтвердившие свою надежность, а также предусматривать обязательное тестирование разработанных технологий, особенно если их использование может нанести вред человеку.

Казалось бы, в качестве примера совершения преступления, совершенного при воздействии одних ИТ на другие ИТ, без осуществления обмана владельца имущества можно привести хищение имущества с использованием усиленной квалифицированной электронной подписи[19]. Например, когда неизвестный оформил усиленную квалифицированную электронную подпись (далее – УКЭП) за другого человека – Р.С., а затем «подарили» его московскую квартиру жителю Уфы. Эту электронную сделку зарегистрировали в Росреестре. О смене собственника пострадавший узнал лишь после того, как получил очередную квитанцию с неизвестной фамилией[20].

Можно привести другой пример преступных деяний, когда преступление совершалось в целях незаконного завладения чужими денежными средствами. Так, «группой лиц по предварительному сговору, используя электронно-цифровую подпись, изготавливались с целью сбыта и сбывались посредством систем дистанционного банковского обслуживания поддельные электронные платежные документы, обеспечивающие безналичные расчеты между юридическими лицами, т.е. совершались незаконные банковские операции, связанные с обналичиванием денежных средств. Данное преступление совершалось в том числе от имени ООО “ПРОМАЛЬЯНС”»[21].

Приведенные примеры из судебной практики показывают возможность реализации преступления в сфере компьютерной информации, без совершения обмана собственников имущества,

[16] *Мосечкин И.Н.* Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования. Киров, 2020.

[17] См.: *Жарова А.К.* Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55–61.

[18] См.: ООН хочет ввести мораторий на использование ИИ: зачем это нужно и к чему приведет? URL: https://hightech.fm/2021/09/16/moratorium-ai

[19] См.: Через электронную подпись крадут квартиры и бизнес: способы защититься. URL: https://pravo.ru/story/213752/

[20] См.: Информация по делу № 02-3237/2019. URL: https://mos-gorsud.ru/rs/babushki№skij/services/cases/civil/details/7ae9082f-aeec-49b9-9822-2bd1eae932e0?particip№ts=салтовский

[21] См.: Постановление Четвертого арбитражного апелляционного суда от 17.09.2015 г. URL: https://sudact.ru/arbitral/doc/ciAsAD5qaVd9/

поскольку они не знали о происходящих действиях. Однако эти примеры нельзя квалифицировать по ст. 159[6] УК РФ, поскольку в данных преступлениях не выполняется способ, сформулированный в Постановлении № 48, – «оказание незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети». В приведенных примерах не происходит незаконного воздействия на программное обеспечение УКЭП, а также не происходит перехвата ключа УКЭП, в связи с высоким уровнем криптографии. Преступники использовали пробелы в законодательстве об электронной подписи и оформляли на себя УКЭП, совершая подмену личности и получая ключ УКЭП.

В представленных примерах средством совершения преступления является ИТ – УКЭП, но происходят они при непосредственном участии человека, который обязан идентифицировать владельца сертификата УКЭП. В связи с этим квалификация данного преступления согласно ст. 159[6] УК РФ невозможна.

Зачастую суды квалифицируют преступные деяния, связанные с «умышленными действиями, с целью тайного хищения чужого имущества, с причинением значительного ущерба гражданину, посредством имеющегося у лица компьютера, с использованием ранее найденной банковской карты и мобильного телефона» по ст. 159[6] УК РФ. Такие преступления могли совершаться с использованием сети Интернет, услуги «мобильный банк», путем ввода данных карты, имитированной на имя пострадавшего, и списания денежных средств с лицевого счета потерпевшего[22].

В другом примере гражданин ХХ был признан виновным по ст. 159[6] УК РФ в том, «что он, используя принадлежащий потерпевшей мобильный телефон, а также сим-карту с абонентским номером, посредством направления СМС-сообщения по услуге денежных переводов, действуя умышленно, незаконно, перевел со счета банковской карты ПАО “Сбербанк России” принадлежащие ФИО денежные средства на счет банковской карты ПАО “Сбербанк России”, зарегистрированной на имя ХХ, тем самым похитив денежные средства»[23].

В приведенных примерах происходит хищение денежных средств посредством реализации различных схем использования ИТ, например «путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана преступник воспользовался телефоном потерпевшего, подключенным к услуге “мобильный банк”, авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.)».

Однако для таких случаев в Постановлении № 48 дано разъяснение, что преступление должно квалифицироваться как кража, «если виновным **не было оказано незаконного воздействия на программное обеспечение** серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом **изменение данных о состоянии банковского счета** и (или) о движении денежных средств, происшедшее **в результате использования виновным учетных данных потерпевшего**, не может признаваться таким воздействием».

Таким образом, в Постановлении № 48 Пленума Верховного Суда РФ выделены следующие признаки преступления, описанные в ст. 159[6] УК РФ: 1) отсутствие обмана; 2) незаконное воздействие на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети; 3) хищение чужого имущества или приобретение права на чужое имущество.

Можно предположить, что преступлением, удовлетворяющим этим признакам, будет, например, использование уязвимости, связанной с недостатками проверки вводимых данных в целях хищения имущества.

ФСТЭК России в Банке данных угроз безопасности информации[24] описал эту уязвимость и известные способы ее эксплуатации[25]. Уязвимости данного типа связаны с ошибками, позволяющими нарушителю осуществить несанкционированное внедрение кода в различные элементы, используемые в составе веб-приложений: веб-страницы; запросы; заголовки; команды; сообщения; электронные документы, которые позволяют нарушителю получить несанкционированный доступ к запрашиваемому элементу веб-приложения.

Таким образом, можно представить следующую модель преступления, удовлетворяющего вышеуказанным признакам: злоумышленник, воспользовавшись уязвимостью проверки вводимых данных, получил доступ к сохраненным в браузере паролям, например к паролю от входа в банковское приложение, а далее похитил денежные средства. В таком примере изменение данных о состоянии банковского счета, происшедшее в результате использования виновным учетных данных пострадавшего, происходит в связи с незаконным воздействием на программное

[22] См.: Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-417/2017 | Мошенничество в сфере компьютерной информации. URL: https://sud-praktika.ru/precede№t/548118.html

[23] Приговор суда по ч. 2 ст. 159.6 УК РФ № 1-336/2017 | Мошенничество в сфере компьютерной информации. URL: https://sud-praktika.ru/precede№t/414374.html

[24] См.: Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/webvul№s

[25] См.: там же.

обеспечение компьютера – браузер и незаконным собиранием информации, хранимой в нем.

В общем случае уязвимости, связанные с недостатками контроля доступа и защиты данных, могут быть использованы нарушителем с помощью специально сформированного запроса или путем перехвата трафика.

Можно также предложить сценарий, когда в качестве средства осуществления преступления будет выступать ИИ. Поскольку на данный момент времени судебная практика по уголовным делам, в которых ИИ является средством совершения преступлений, еще не сложилась, смоделируем предполагаемые преступные деяния, которые могут быть квалифицированы по ст. 159^6 УК РФ. Так, допустим, ИИ, включающий алгоритм машинного обучения, за счет проникновения в информационные системы пользователя, собирает всю информацию об активности конкретного человека в сети Интернет, распознавая его среди множества других пользователей, анализирует ее и передает злоумышленнику, который, используя эту информацию, совершает хищение имущества пользователя.

Рассуждая о вредоносности ИИ, можно представить следующие сценарии его реализации. Первый – это самостоятельное объединение ИИ в нейросеть, которая самостоятельно (например, на основе алгоритмов машинного обучения выбирает модель поведения) и определяет себе цель, учитывая особенности активности каждого человека в ИКТ-сфере, против которого она совершает противоправные действия. Однако в настоящее время математический инструментарий ИИ не может реализовать такой сценарий.

Второй сценарий – использование определенной технологии ИИ, не объединенной в нейросеть, как средства совершения преступлений. Сегодня ИИ применяется в области больших неструктурированных данных, разнообразных операций. Функционирование ИИ определяется логикой его разработчика. ИИ уже сейчас может найти уязвимости ИТ, преодолеть некоторые защиты и внести изменения в установленное на компьютере программное обеспечение. Однако ИИ не может самостоятельно определять свою цель функционирования и действует по заложенному разработчиком алгоритму. В связи с этим мы можем, учитывая различные обстоятельства, признать разработчика ИИ преступником.

Третий сценарий – это объединение ИИ в нейросеть с логической бомбой, которая сработает при наступлении заложенных в нее условий. После этого нейросеть может осуществить вредоносные действия. Для закладки логической бомбы могут использоваться уязвимости ИТ, которые сопровождают любую ИТ, либо может быть произведена закладка в аппаратно-программное решение.

Например, в 2018 г. IBM представила общественности вредоносное программное обеспечение DeepLocker, использующее технологии ИИ. DeepLocker не был обнаружен средствами безопасности, включая средства антивирусного ядра и вредоносных программных сред. Благодаря встроенному условию запуска DeepLocker сопровождал процесс видеоконференции до тех пор, пока не распознал лицо цели[26]. Для распознавания цели DeepLocker был оснащен арсеналом средств распознавания геолокации, лица и голоса человека, анализа данных о человеке, собранных из открытых источников. Ключом срабатывания данного вируса являлось изображение лица конкретного человека.

Заключение

Мошенничество выступает одним из способов хищения имущества. В ст. 159^6 УК РФ отсутствуют такие деяния, как обман или злоупотребление доверием, и хищение имущества должно быть реализовано аппаратно-программным или программным способом в ИКТ-сфере.

В связи с возможностями применения ИИ как средства совершения преступления необходима проработка отдельного правового регулирования применения ИИ в различных областях жизнедеятельности человека. На данном этапе развития математического инструментария и программирования ИИ – это одно из технологических решений, которое может выполнять когнитивные функции человека, но не может задавать самостоятельно свои цели. Однако дальнейшее технологическое развитие может привести к переходу ИИ на новый уровень с постановкой перед собой новых целей и их реализации. В связи с этим необходимо обращать внимание на стандартизацию технологий ИИ, определение надежных алгоритмов ИИ и борьбу с уязвимостями, присущими ИИ.

СПИСОК ЛИТЕРАТУРЫ

1. *Бегишев И.Р.* Международно-правовые основы регулирования искусственного интеллекта и робототехники // Междунар. публичное и частное право. 2021. № 1. С. 37–40. DOI: 10.18572/1812-3910-2021-1-37-40
2. *Владыкина Т.А.* Изменение категории преступления // Уголовное право. 2018. № 5. С. 11–17.
3. *Воеводкина К.М.* Обман в составе незаконного получения кредита по УК РФ: функция и значение // Росс. следователь. 2020. № 5. С. 37. DOI: 10.18572/1812-3783-2020-5-33-37

[26] См.: Почему DeepLocker AI лучше других вредоносных ПО. URL: https://www.make-i№fo.com/deeplocker-ai-malware/

4. *Грачева Ю.В., Арямов А.А.* Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы росс. права. 2020. № 6. С. 169–178. DOI: 10.17803/1994-1471.2020.115.6.169-178

5. *Грачева Ю.В., Маликов С.В., Чучаев А.И.* Предупреждение девиаций в цифровом мире уголовно-правовыми средствами // Право. Журнал ВШЭ. 2020. № 1. С. 188–210. DOI: 10.17323/2072-8166.2020.1.188.210

6. *Елин В.М.* Мошенничество в сфере компьютерной информации как новый состав преступления // Бизнес-информатика. 2013. № 2 (24). С. 71, 72.

7. *Ефремова М.А., Лопатина Т.М.* Робототехника в уголовном законодательстве Российской Федерации // Росс. следователь. 2021. № 11. С. 55–58. DOI: 10.18572/1812-3783-2021-11-55-58

8. *Жарова А.К.* Вопросы обеспечения безопасности цифрового профиля человека // Юрист. 2020. № 3. С. 55–61.

9. *Жарова А.К.* Правовое обеспечение цифрового профилирования деятельности человека // Вестник Южно-Уральского гос. ун-та. Сер.: Право. 2020. Т. 20. № 2. С. 80–87.

10. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. Г.А. Есакова. 9-е изд., перераб. и доп. М., 2021. С. 18, 102.

11. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А.И. Чучаева. Испр., доп., перераб. М., 2013. С. 127.

12. *Лаврушкина А.А.* Проблемы применения статьи 159.6 УК РФ с позиции теории и практики // Контентус. 2018. № 3 (68).

13. *Мосечкин И.Н.* Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования. Киров, 2020.

14. *Пучков В.О.* Информация – объект гражданского права? // Арбитражные споры. 2020. № 2. С. 138.

15. *Синицын С.А.* Вещь как объект гражданских прав: возможные и должные критерии идентификации // Законодательство и экономика. 2016. № 11. С. 16.

16. Уголовное право России: учеб. для бакалавров / под ред. А.И. Плотникова. Оренбург, 2016. С. 96.

REFERENCES

1. *Begishev I.R.* International legal bases of regulation of artificial intelligence and robotics // International Public and Private Law. 2021. No. 1. P. 37–40. DOI: 10.18572/1812-3910-2021-1-37-40 (in Russ.).

2. *Vladykina T.A.* Changing the category of crime // Criminal Law. 2018. No. 5. P. 11–17 (in Russ.).

3. *Voevodkina K.M.* Deception as part of the illegal receipt of a loan under the Criminal Code of the Russian Federation: function and meaning // Russ. investigator. 2020. No. 5. P. 37. DOI: 10.18572/1812-3783-2020-5-33-37 (in Russ.).

4. *Gracheva Yu. V., Aryamov A.A.* Robotization and artificial intelligence: criminal law risks in the field of public security // Actual problems of Russ. law. 2020. No. 6. P. 169–178. DOI: 10.17803/1994-1471.2020.115.6.169-178 (in Russ.).

5. *Gracheva Yu. V., Malikov S.V., Chuchaev A.I.* Prevention of deviations in the digital world by criminal legal means // Law. HSE Journal. 2020. No. 1. P. 188–210. DOI: 10.17323/2072-8166.2020.1.188.210 (in Russ.).

6. *Elin V.M.* Fraud in the field of computer information as a new crime // Business Informatics. 2013. No. 2 (24). P. 71, 72 (in Russ.).

7. *Efremova M.A., Lopatina T.M.* Robotics in the criminal legislation of the Russian Federation // Riss. investigator. 2021. No. 11. P. 55–58. DOI: 10.18572/1812-3783-2021-11-55-58 (in Russ.).

8. *Zharova A.K.* Issues of ensuring the security of a digital profile of a person // Lawyer. 2020. No. 3. P. 55–61 (in Russ.).

9. *Zharova A.K.* Legal support of digital profiling of human activity // Herald of the South Ural State University. Ser.: Law. 2020. Vol. 20. No. 2. P. 80–87 (in Russ.).

10. Commentary to the Criminal Code of the Russian Federation (article by article) / ed. by G.A. Esakov. 9th ed., reprint and add. M., 2021. P. 18, 102 (in Russ.).

11. Commentary to the Criminal Code of the Russian Federation (article by article) / ed. by A.I. Chuchaev. Corrected, supplemented, revised. M., 2013. P. 127 (in Russ.).

12. *Lavrushkina A.A.* Problems of application of Article 159.6 of the Criminal Code of the Russian Federation from the standpoint of theory and practice // Contentus. 2018. No. 3 (68) (in Russ.).

13. *Mosechkin I.N.* Artificial intelligence in criminal law: prospects for improving protection and regulation. Kirov, 2020 (in Russ.).

14. *Puchkov V.O.* Information – an object of civil law? // Arbitration disputes. 2020. No. 2. P. 138 (in Russ.).

15. *Sinitsyn S.A.* A thing as an object of civil rights: possible and proper identification criteria // Legislation and Economics. 2016. No. 11. P. 16 (in Russ.).

16. Criminal Law of Russia: textbook for bachelors / ed. by A.I. Plotnikov. Orenburg, 2016. P. 96 (in Russ.).

Сведения об авторе

ЖАРОВА Анна Константиновна –
доктор юридических наук, доцент, старший научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10
ORCID: 0000-0002-2981-3369

Authors' information

ZHAROVA Anna K. –
Doctor of Law, Associate Professor, Senior Researcher, Institute of State and Law of the Russian Academy of Sciences; 10 Znamenka str., 119019 Moscow, Russia