 DOI 10.17150/2411-6122.2025.2.42-48 ISSN 2411-6122

Научная статья
УДК 343.9
EDN DQDSAD
DOI 10.17150/2411-6122.2025.2.42-48

От нейронных сетей к нейропреступности

Д.В. Жмуров
Байкальский государственный университет, г. Иркутск, Российская Федерация, zdevraz@ya.ru

Аннотация. В статье исследуется феномен нейропреступности, зарождающийся на стыке высоких технологий и криминальной активности. Нейропреступность определяется как новая форма преступлений, связанная с использованием нейротехнологий для противозаконных целей. В работе проведена классификация нейропреступлений, включающая в себя пять основных категорий: компрометация нейроустройств, нарушение нейроприватности, дискредитация когнитивной автономии, создание нейроопасного контента и использование нейротехнологий для совершения общеуголовных преступлений. Каждая из категорий анализируется с акцентом на современные и в большей степени потенциальные угрозы. Особое внимание уделено условиям, при которых нейропреступность может стать реальной угрозой для общества. Автор предлагает обратить внимание на необходимость заранее разработанных мер безопасности, регулирующих рамок и этических стандартов, необходимых для предотвращения криминального распространения этих опасных технологий.

Ключевые слова: нейропреступность, нейропреступление, нейротехнологии, криминологическая футурология, преступность будущего.

Для цитирования: Жмуров Д.В. От нейронных сетей к нейропреступности / Д.В. Жмуров. — DOI 10.17150/2411-6122.2025.2.42-48. — EDN DQDSAD // Сибирские уголовно-процессуальные и криминалистические чтения. — 2025. — № 2. — С. 42–48.

Original article

From Neural Networks to Neurocrime

D.V. Zhmurov
Baikal State University, Irkutsk, the Russian Federation, zdevraz@ya.ru

Abstract. The author examines the phenomenon of neurocrime emerging at the crossroads of high tech and criminal activities. Neurocrime is defined as a new form of crime connected with the use of neuro-technologies for illegal purposes. The article contains a classification of neurocrimes, broken into five key categories: compromising neurodevices, violation of neuroprivacy, discrediting cognitive autonomy, creation of neurohazardous content and the use of neurotechnologies to commit common crimes. Each of these categories is analyzed from the standpoint of current and, to a greater degree, potential threats. Special attention is paid to the conditions under which neurocrime could pose a real danger to society. The author suggests that safety measures should be worked out in advance to regulate the boundaries and ethical standards necessary to prevent a spread of the criminal use of these dangerous technologies.

Keywords: neurocrime, neurotechnology, criminological futurology, crimes of the future.

For citation: Zhmurov D.V. From Neural Networks to Neurocrime. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2025, no 2, pp. 42–48. (In Russian). EDN: DQDSAD. DOI: 10.17150/2411-6122.2025.2.42-48.

Тот, кто не смотрит в будущее, рискует оказаться в прошлом. Криминологические знания позволяют предвидеть и прогнозировать перспективные состояния преступности. На этом фоне природа технологических процессов от которых человечество уже не сможет отказаться ставит перед исследователем самые разнообразные гипотезы. И одной из таких является идея *нейропреступности*, отражающая риски ее возникновения и стремительного развития. Именно этому феномену посвящена настоящая статья.

Мысль о существовании нейропреступности давно просматривается в научно-фантастической и футурологической литературе. Но пока это общие наброски, иллюстрации романистов к описанию возможного будущего. Писатели увлечены им и почти все как один указывают на высокий шанс масштабирования нейротехнологий. Это и выгрузка наиболее ценных образцов сознания в «Гамбите девятихвостого лиса» Юн Ха Ли; и массовая послеродовая имплантация стеков, т.е. специальных устройств, записывающих воспоминания («Видоизмененный углерод» Ричарда Моргана); или появление нейрометодик благодаря которым возможно выявление пассивных психопатов с целью коррекции их поведения в «Квантовой ночи» Роберта Сойера, а также многое другое. На страницах романов-утопий, рассказов-предупреждений или предсказаний затрагивается тема настоящей работы. Думается, что часть этой «придуманной» терминологии рано или поздно перейдет в научную парадигматику.

Тема использования нейротехнологий для совершения преступлений затрагивается в произведении «Интонатор» Ольги Верея. Сюжетные перипетии романа повествуют о жертвах нейроатак, которые «успевают добровольно переписать на преступника свое имущество, передать секретную информацию или выполнить какое-либо указание…» без видимых следов воздействия и каких-либо воспоминаний.

Применение нейроимплантов, вживляемых правопослушным гражданам для использования их в качестве наемных убийц сюжетно затронуто в научно-фантастическом триллере «В чужой шкуре» (реж. Брэндон Кроненберг, 2020 г.).

Тема «контроля сознания» настолько пришлась по вкусу современным создателям контента, что она фигурирует повсеместно: от «спекулятивной фантастики» до многочисленных видеоигр.

Вместе с тем, нейротехнологии, несмотря на их фантастичность, уже стали обыденным явлением. Wimagine, Telepathy от Neuralink, BrainGate от Cyberkinetics, очувствление протезов от «Моторики», ДВФУ или Сколтеха [1] и многое другое — являют собой воплощенную реальность. Тысячи людей пользуются этими изобретениями. И применение это приветствуется с чрезвычайным энтузиазмом. Специалисты определяют *нейротехнологии* как *совокупность способов, которые направлены на изучение и понимание того, как функционирует человеческий мозг в совокупности с индивидуальным сознанием* [2].

 DOI 10.17150/2411-6122.2025.2.42-48 ISSN 2411-6122

Логично предположить, что одним из направлений цифровизации преступности станет расширение криминального использования обозначенных выше технологий. Задача современной криминологии заключается в оценке этих рисков и их возможных последствий.

Итак, гипотетическую нейропреступность целесообразно определить, как *совокупность уголовно-наказуемых деяний, совершенных с использованием технологий, взаимодействующих с центральной нервной системой (головным мозгом) в рамках мониторирования или модуляции нервной активности*.

Этот термин уже упоминался в ряде источников [3] и на отдельных научных конференциях[1] [4]. М. Йенка и П. Хазелагер определяют нейропреступность как одну из форм распространения компьютерных преступлений на нейронные устройства. При этом основное внимание авторы уделяют «нейрохакингу» цель которого — незаконный доступ и манипулирование нейронной информацией [5].

Схожие идеи высказывают некоторые отечественные эксперты, утверждая о гипотетической возможности подмены памяти и имплантации мыслей (убеждений) [6]. Вместе с тем, целесообразность использования супертехнологий, в условиях существующих пропагандистских инструментов и наработанной практики манипулирования сознанием, вызывает некоторые сомнения.

Несмотря на это, перспективы совершения нейропреступлений вполне реальны. Последние можно определить как *неправомерное воздействие на центральную нервную систему (головной мозг) человека с использованием технологий обеспечивающих мониторинг, модификацию или управление нервной деятельностью*.

В отличие от традиционных преступлений, нейропреступления воздействуют на весьма сложные и уязвимые аспекты человеческой природы — восприятие, мышление и волю.

Укажем некоторые перспективные формы подобных деяний:

– ***компрометация нейроустройств*** — действия, направленные на злонамеренное вмешательство в работу нейротехнологического оборудования или систем, с которыми оно взаимодействует.

Их цель — дискредитация реципиента (носителя инвазивных или внешних устройств), причинение ему физического и психического вреда. Данная сфера преступной активности тесно связана с разработками в области нейроимплантации, нейропротезирования и нейроинтерфейсов.

Так, нейроимплантация предполагает вживление специфических устройств в мозг носителя для лечения различных заболеваний или улучшения функциональности организма. Импланты стимулируют определенные области мозга для лечения депрессии, эпилепсии, облегчения мочеиспускания, терапии болевого синдрома и проч.[2] Преступники могут попытаться дистанционно получить доступ к таким модулям и менять режимы их работы, что приведет к непредсказуемым последствиям

[1] Rise of neurotechnology. Defend against neurocrime(s) before it's too late // Bocconi University. Angelo Sraffa Department of Legal Studies. September 2017. URL: https://ius.unibocconi.eu/events/rise-neurotechnology-defend-against-neurocrimes-its-too-late (дата обращения 16.01.2025).

[2] Виды патологии, в комплексе лечения которой применяют нейромодуляцию и абляции // Национальный медицинский исследовательский центр психиатрии и неврологии им. В.М. Бехтерева. URL: https://clck.ru/3FmQ2j (дата обращения 16.01.2025).

для здоровья носителя. Популярными могут стать практики компрометации двигательных протезов, созданных для сознательного управления движениями (отказ в управлении, неправомерное управление). В ряде случаев их несанкционированный контроль окажется вполне способным вызвать убийство реципиента, путем целенаправленной деструктивной активности искусственной части тела.

Спектр нарушений, связанных с дискредитацией нейроустройств, может быть достаточно широк: от лишения слуха и зрения (выведение из строя кохлеарных и ретинальных имплантов) вплоть до стимуляции нестандартного поведения в рамках которого носитель может причинить вред себе или окружающим. Эти деяния могут именоваться «принудительной нейростимуляцией», «нейрохакингом» и проч.;

– ***нарушение нейроприватности***, которая понимается как право на неприкосновенность нейроданных и подразумевает вмешательство в активность центральной нервной системы и головного мозга без санкционированного контроля (мониторинга). Эта идея связана с защитой сведений, собранных из интерфейсов «мозг-компьютер» и иных систем, обрабатывающих нейронную информацию (в частности, нейротрекеров).

Например, крупные технологические корпорации, включая Meta[3] и Apple, вкладывают значительные ресурсы в разработку технологий для декодирования человеческих мыслей. Подобные инновации обладают не только революционным потенциалом для медицинской практики, но могут представлять угрозу конфиденциальности. В 2022 г. Apple получила патент на технологию AirPods, использующую ЭЭГ для анализа биосигналов и электрической активности мозга пользователя. Между тем, Meta поддерживает исследовательскую группу, создающую методы дистанционного обнаружения и считывания нейроактивности[4].

В будущем преступления, связанные со взломом нейрохранилищ, могут стать серьезной угрозой. Те нейрохранилища, что окажутся способны консолидировать данные о мыслительных процессах, воспоминаниях и предпочтениях людей, станут новой целью для киберпреступников. Похищенные сведения как нельзя лучше подойдут для шантажа или вымогательств; подделки личностных профилей; их продажи организациям или корпорациям и т.п. Не исключено, что возникнет проблема нейрокомпьютерного шпионажа, заключающегося в тайном наблюдении за мыслями и когнитивными процессами человека. Например, считывание мыслей сотрудника компании для облечения доступа к коммерческой тайне;

– ***дискредитация когнитивной автономии*** — понятие, связанное со способностью отдельных нейропреступлений подрывать или негативно влиять на возможность принятия человеком независимых и осознанных решений.

Современные авторы подчеркивают, что использование нейронных устройств в киберпреступных целях угрожает не только физической безопасности пользователей, но влияет на поведение и даже самоидентификацию [7].

Очевидно, что дискредитация когнитивной автономии путем использования

[3] Деятельность корпорации Meta признана в России экстремистской и запрещена.

[4] Нейроприватность: защитите свои мысли от технологического вторжения // Security Lab : офиц. сайт. URL: https://www.securitylab.ru/news/548196.php (дата обращения 16.01.2025).

 DOI 10.17150/2411-6122.2025.2.42-48 ISSN 2411-6122

нейроустройств является относительно новой и сложной темой. Она касается неэтичного или незаконного вмешательства в мыслительные процессы индивида при помощи соответствующих технологий. Уместно перечислить некоторые из возможных инцидентов:

• осуществление нейроманипуляций (использование технологий для изменения мыслей, мотивации, восприятия или поведения человека без его согласия). Не исключено, что когнитивные протезы, которые сегодня остаются научной фантастикой, в будущем смогут использоваться для управления поведением;

• формирование нейроконфабуляций (внедрение фальшивых воспоминаний с помощью средств нейропроекции);

• амнезиагенез (стирание воспоминаний, например, жертвы о совершенном преступлении);

• когнитивное клонирование (копирование или передача когнитивных процессов личности без согласия оригинального субъекта);

• изоляция сознания (применение технологий, которые интернируют или подавляют сознание человека, нарушая его самовосприятие и автономию);

• нейротаргетинг (использование данных мозговой активности для воздействия на потребительское поведение людей, а в более деструктивном плане — создание зависимостей или управление предпочтениями значительных масс населения);

– ***создание нейроопасного контента***, т.е. информационных продуктов, используемых для контроля или нанесения вреда другому человека посредством нейротехнологического вмешательства.

Появление нейроопасных вредоносных программ (нейровирусов, нейротроянов и далее по аналогии) — вопрос недалекого будущего. Это программные решения, воздействующие на когнитивные функции или психическое состояние человека, целью которых является сбор нейроданных, нарушение работы нейроинтерфейсов и имплантируемого оборудования, удаленный контроль за ними;

– ***использование нейротехнологий при совершении общеуголовных преступлений.*** Многие из подобных инцидентов уже стали повседневностью. Например, фишинг и вымогательство с использованием ChatGPT, который пишет вполне правдоподобные тексты для целей шантажа, а генеративные модели создают эротические дипфейки за удаление которых жертвам предлагается заплатить [8]. Мошенники активно используют возможности искусственного интеллекта для создания фальшивых аудиосообщений в мессенджерах и социальных сетях. Эксперты компании McAfee отметили, что для фабрикации голоса достаточно всего трех секунд аудиозаписи. Специалисты из Роскачества уточнили, что для этих целей хватает 20-секундной записи разговора [9].

Несмотря на все вышесказанное, эра нейропреступности еще не наступила. Для этого необходимо сочетание нескольких важных условий, среди которых:

а) становление *нейронета* как массовой социальной практики, т.е. начало взаимодействия во всемирной паутине на принципах нейрокоммуникации. По прогнозам экспертов нейронет заменит собою Web 3.0 приблизительно в 2030–2040 гг.[5];

б) *диффузия нейротехнологий*, означающая, что человечество должно

[5] Нейронет // Википедия. URL: https://ru.wikipedia.org/wiki/Нейронет (дата обращения 04.10.24).

пройти определенный путь от начального этапа разработки до их превращения в предметы массового потребления с относительно невысокой себестоимостью;

в) *интеграция нейротехнологий* в повседневную жизнь предполагает расширение их массового использования. Это включает в себя адаптацию человеко-машинных интерфейсов (HMI) для решения обыденных задач, таких как управление медиаустройствами или кухонным оборудованием;

г) продолжение процессов *массового накопления данных*, включая сведения о поведении людей и различного рода конфиденциальной информации;

д) *возникновение затруднений* при осуществлении традиционных криминальных практик (ввиду цифровой оптимизации правоохранительной системы), что станет дополнительным стимулом обратиться к разработке и криминальному использованию нейротехнологий и ИИ.

В течение нескольких десятилетий развитие технологий значительно изменит человеческое общество, и одно из возможных направлений этого процесса — переход к нейропреступности. Несмотря на интерес к этой теме, мы не готовы эволюционировать до новой формы преступного поведения, основанного на нейротехнологиях. Пока эти перемены не произошли, ученые имеют возможность подготовиться и рассмотреть этические, правовые и социальные последствия, которые принесет с собой это неотвратимое будущее.

Список использованной литературы

1. 8 проектов в сфере нейротехнологий и их значение для будущего медицины / Ю. Матвиенко, М. Лебедев, Д. Клеева, Г. Согоян // РБК-Тренды. — URL: https://trends.rbc.ru/trends/industry/66c6fa5a9a794758aab077c7.

2. Бабак Р.С. Нейротехнологии и искусственный интеллект простым языком / Р.С. Бабак, Д.И. Вагин // Scientia Potentia Est. — 2022. — № 1. — С. 1–4.

3. Ienca M. Neuroprivacy, Neurosecurity and Brain-Hacking: Emerging Issues in Neural Engineering / M. Ienca. — DOI 10.24894/BF.2015.08015 // Bioethica Forum. — 2015. Vol. 8. — P. 51–53.

4. Стенограмма круглого стола «Международный опыт использования цифровых технологий в борьбе с киберпреступностью», состоявшегося 6 апреля 2019 г. в рамках московского юридического форума / Т.В. Редникова, А.В. Серебренникова, М.В. Лебедев, И.М. Ацкевич. — DOI 10.31085/2310-8681-2020-1-207-153-176. — EDN JZGZRF // Союз криминалистов и криминологов. — 2020. — № 1. — С. 153–176.

5. Ienca M. Hacking the Brain: Brain — Computer Interfacing Technology and the Ethics of Neurosecurity / M. Ienca, P. Haselager. — DOI 10.1007/s10676-016-9398-9 // Ethics and Information Technology. — 2016. — No. 18. — P. 117–129.

6. Студнев Г. Нужно ли защищать наши мысли от ИИ и нейротехнологий? / Г. Студнев // Сириус. — 2023. — 25 мая. — URL: https://siriusmag.ru/articles/1311-kak-zasitit-nasi-mysli-ot-vmesatelstva-izvne/.

7. Корр А. Этические риски китайской технологии «управления мозгом» / А. Корр // The Epoch Times. — URL: https://kurl.ru/LemaP.

8. Агазода Р. Как нейросети влияют на убийц, жертв и расследователей / Р. Агазода // Tproger. — URL: https://tproger.ru/articles/kak-nejroseti-vliyayut-na-ubijc-zhertv-i-rassledovatelej.

9. Ганжа А. ОтпетыеМошенникИИ / А. Ганжа // Коммерсант. — 2024. — URL: https://www.kommersant.ru/doc/6616414.1.

References

1. Matvienko Yu., Lebedev M., Kleeva D, Sogoyan G. Eight Projects in the Sphere of Neurotechnologies and their Significance for the Future of Medicine. *RBK-Trends*. Available at: https://trends.rbc.ru/trends/industry/66c6fa5a9a794758aab077c7. (In Russian).

2. Babak R.S., Vagin D.I. Neurotechnologies and Artificial Intelligence in Simple Words. *Scientia Potentia Est*, 2022, no. 1, pp. 1–4. (In Russian).

3. Ienca M. Neuroprivacy, Neurosecurity and Brain-Hacking: Emerging Issues in Neural Engineering. *Bioethica Foruma*, 2015, vol. 8, pp. 51–53. DOI: 10.24894/BF.2015.08015.

4. Rednikova T.V., Serebrennikova A.V., Lebedev M.V., Matskevich I.M. Transcript of the Round Table "International Experience in the Use of Digital Technologies in the Fight Against Cybercrime", Held on April 6, 2019 in the Framework of the Moscow Legal Forum (Moscow State Law University Named After O. E. Kutafin (MSAL). *Soyuz kriminalistov i kriminologov = The Union of Criminalists and Criminologists*, 2020, no. 1, pp. 153–176. (In Russian). EDN: JZGZRF. DOI: 10.31085/2310-8681-2020-1-207-153-176.

5. Ienca M., Haselager P. Hacking the Brain: Brain — Computer Interfacing Technology and the Ethics of Neurosecurity. *Ethics and Information Technology*, 2016, no. 18, pp. 117–129. DOI: 10.1007/s10676-016-9398-9.

6. Studnev G. Do we Need to Protect our Thoughts from AI and Neurotechnologies? *Sirius*, 2023, May 25. Available at: https://siriusmag.ru/articles/1311-kak-zasitit-nasi-mysli-ot-vmesatelstva-izvne/. (In Russian).

7. Korr A. Ethical Risks of the Chinese Technology of "Brain Management". *The Epoch Time*. Available at: https://kurl.ru/LemaP. (In Russian).

9. Agazoda R. How Neuronetwords Influence Murderers, Victims and Investigators. *Tproger*. Available at: https://tproger.ru/articles/kak-nejroseti-vliyayut-na-ubijc-zhertv-i-rassledovatelej. (In Russian).

10. Ganzha A. Dirty Rotten AI Scoundrels. *Kommersant*, 2024. Available at: https://www.kommersant.ru/doc/6616414. (In Russian).

Информация об авторе

Жмуров Дмитрий Витальевич — кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии, Институт юстиции, Байкальский государственный университет, Иркутск, Российская Федерация, https://orcid.org/0000-0003-0493-265X, SPIN-код: 3644-6102, Scopus Author ID: 35770006500, Researcher ID: ABH-8471-2020.

Author Information

Zhmurov, Dmitriy V. — Ph.D. in Law, Ass. Professor, Department of Criminal Law and Criminology, Institute of Justice, Baikal State University, Irkutsk, the Russian Federation, https://orcid.org/0000-0003-0493-265X, SPIN-код: 3644-6102, Scopus Author ID: 35770006500, Researcher ID: ABH-8471-2020.

Поступила в редакцию / Received 16.01.2025

Одобрена после рецензирования / Approved after reviewing 30.01.2025

Принята к публикации / Accepted 21.05.2025

Дата онлайн-размещения / Available online 26.06.2025