DOI: 10.17803/1729-5920.2025.222.5.077-086

И. А. Ефремова
Саратовская государственная юридическая академия
г. Саратов, Российская Федерация

Криминологическая характеристика компьютерной преступности и новые методы ее предупреждения

Резюме. Компьютерные технологии активно совершенствуются, в связи с чем важнейшей задачей государства является соблюдение баланса между развитием технологий и защитой прав человека. Но в 2020–2023 гг. количество компьютерных преступлений увеличилось на треть, а сумма ущерба превысила 210 млрд руб., поэтому возникла необходимость внедрить новые методы их предупреждения. Преступления, предусмотренные главой 28 УК РФ, преимущественно совершены в городской местности; в одиночку; совершившие их лица не находились в состоянии алкогольного, наркотического или иного опьянения; не имели неснятых или непогашенных судимостей; совершили компьютерное преступление впервые. Новые методы предупреждения компьютерных преступлений практически не исследуются учеными и редко используются в превентивной деятельности, в то время как достижения в области искусственного интеллекта предлагают смену парадигмы, позволяя выработать и применять их. При этом не следует останавливаться на сегодняшних достижениях использования искусственного интеллекта в предупреждении компьютерных преступлений, нужно продолжать разрабатывать новые методы, поскольку искусственный интеллект способен работать в различных условиях, например при неполноте криминологических данных, неточной информации о предполагаемом месте совершения преступления.
Ключевые слова: преступления; компьютерные преступления; компьютерная информация; преступления в сфере компьютерной информации; предупреждение; методы предупреждения
Для цитирования: Ефремова И. А. Криминологическая характеристика компьютерной преступности и новые методы ее предупреждения. *Lex russica*. 2025. Т. 78. № 5. С. 77–86. DOI: 10.17803/1729-5920.2025.222.5.077-086

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-28-00312, https://rscf.ru/project/24-28-00312/.

Criminological Characterization of Computer Crime and New Methods of its Prevention

Irina A. Efremova
Saratov State Law Academy
Saratov, Russian Federation

Abstract. Computer technologies are actively developing. Due to this fact, the main task of the state is to maintain a balance between computer technologies and the protection of human rights. In 2020–2023, the number of computer crimes increased by a third, and the amount of damage exceeded 210 billion rubles. Thus, it is necessary to introduce new methods for their prevention. Crimes provided for by Chapter 28 of the Criminal Code of the Russian Federation are mainly committed in urban areas; alone; the persons who committed them were not in

a state of alcoholic, narcotic or other intoxication; had no unexpunged or outstanding convictions; committed a computer crime for the first time. New methods of preventing computer crime are hardly investigated by scientists and are rarely used in preventive activities, while advances in artificial intelligence offer a paradigm shift, allowing new methods to be developed and applied to prevent such crimes. At the same time, the current achievements of the use of artificial intelligence in the prevention of computer crimes should not be stopped, it is necessary to continue to develop new methods, since artificial intelligence is able to work in various conditions, for example, with incomplete criminological data, inaccurate information about the alleged place of the crime.
Keywords: crimes; computer crimes; computer information; computer information crimes; warning; warning methods
Cite as: Efremova IA. Criminological Characterization of Computer Crime and New Methods of its Prevention. *Lex russica*. 2025;78(5):77-86. (In Russ.). DOI: 10.17803/1729-5920.2025.222.5.077-086

Acknowledgements. The research was carried out with the support of the Russian Science Foundation grant No. 24-28-00312, URL: https://rscf.ru/project/24-28-00312/.

Введение

Компьютерные технологии активно развиваются, искусственный интеллект проникает во все сферы жизни, в связи с чем основными задачами государства выступают: соблюдение баланса между внедрением компьютерных технологий и защитой прав человека и гражданина, предупреждением преступности. Но в 2020–2023 гг. количество компьютерных преступлений увеличилось на треть, а сумма ущерба от них превысила 210 млрд руб.[1] Наиболее распространенные формы таких преступлений: вирусные атаки, фишинг, вишинг, кардинг, несанкционированное использование персональных данных граждан и т.д.[2] Указанное требует представления особенностей криминологической характеристики компьютерной преступности и выработки новых методов ее предупреждения[3].

Этим вопросам посвящены труды ряда ученых. Криминологическая характеристика компьютерной преступности раскрывалась Д. В. Добровольским, К. Н. Евдокимовым, Т. М. Лопатиной, Т. Л. Тропиной, Г. Ф. Шипулиным. Изучением методов предупреждения занимались А. И. Долгова, В. В. Лунеев. Давая криминологическую характеристику компьютерной преступности, исследователи использовали различные подходы, вследствие чего разнятся криминологические особенности и не вырабатываются новые методы предупреждения компьютерных преступлений, стремительно набирающих обороты.

Основная часть

Компьютерная преступность — наиболее обсуждаемый вид преступности, обладающий криминологическими особенностями. А. И. Долгова предлагала понимать под компьютерной преступностью совокупность уголовно-правовых деяний, где компьютерная информация — предмет преступных посягательств, а также преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация[4]. Другие ученые компьютерную преступность рассматривают в узком и широком смысле. Сторонник этого подхода К. Н. Евдокимов говорит о компьютерной преступности в узком смысле как о совокупности преступлений, где компьютерная информация — предмет преступления, средство и (или) орудие совершения общественно опасного деяния, в широком — как о противоправном социальном явлении, возникшем в ре-

[1] См.: В России с 2023 года ущерб от IT-преступлений превысил 210 млрд рублей // URL: https://tass.ru/obschestvo/20989539 (дата обращения: 10.06.2024).

[2] См.: *Ramadhoan M.*, *Amiruddin A., Ufran U.* Crime Prevention Through an Environmental Design Approach in Reducing Crime Rates in Indonesia // International Journal of Social Science Research and Review. 2024. No. 7. P. 177.

[3] См.: *Суходолов А. П.*, *Суходолов Я. А.*, *Колесникова А. В.* О необходимости совершенствования методологии современных криминологических исследований // Право и государство: теория и практика. 2022. № 8 (212). С. 125.

[4] См.: Криминология : учебник / под общ. ред. А. И. Долговой. 3-е изд., перераб. и доп. М., 2007. С. 735.

зультате использования компьютерных и иных информационных технологий в личных, корыстных и иных целях, что приводит к наступлению общественно опасных последствий[5]. Отдельными учеными компьютерная преступность сводится только к деяниям, предусмотренным главой 28 УК РФ «Преступления в сфере компьютерной информации».

Согласно данным Судебного департамента при Верховном Суде РФ за 2023 г., преступления, предусмотренные главой 28 УК РФ, преимущественно совершаются: в городской местности (удельный вес осужденных составляет 60,7 %); в одиночку (64,6 %; удельный вес лиц, совершающих уголовно наказуемые деяния рассматриваемой группы, 35,4 %); не в состоянии алкогольного, наркотического или иного опьянения (100 %); лицами, которые не имели неснятых или непогашенных судимостей (89,5 %); совершили компьютерное преступление впервые. Компьютерные преступления тщательно планируются. В соответствии с проанализированными материалами уголовных дел, в 5,1 % случаев виновные имеют психические отклонения, не исключающие вменяемость.

Большинство таких преступников — мужчины (71,5 %); в возрасте от 18 до 24 лет (42,3 %); 30–49 лет (35,7 %); граждане РФ (99,1 %); постоянные жители местности, в которой совершили общественно опасное посягательство (96,1 %); имеющие высшее образование (32,7 %), среднее профессиональное образование (41,4 %, при этом образование преимущественно техническое); не состоящие в официально зарегистрированном браке (51,2 %); не имеющие постоянного источника дохода (65,1 %).

Компьютерный преступник испытывает трудности в общении, его интересы сосредоточены в сфере компьютерных технологий, киберпространстве[6]. Виновные — незаурядные личности, способные быстро принимать неординарные решения; склонны к самоутверждению и повышению своего социального статуса в рамках группы окружающих людей[7]. Самоутверждение — неотъемлемая часть бытия, внутренняя потребность, присущая каждому человеку[8]. Находясь в обществе, он постоянно пытается утвердиться или самоутвердиться. Самоутверждение начинается с детских слов «Я сам!» и сопровождает человека до старости. Отсутствие мотивации к самоутверждению — скорее личностная патология, чем норма, а его утрата — знак жизненной капитуляции[9]. Лица, совершающие компьютерные преступления, реализуют данную потребность противоправным поведением. Среди компьютерных преступников значительное количество лиц положительно характеризовались по месту жительства и по месту работы[10]. Компьютерная преступность имеет высокотехнологический характер[11], поскольку виновными при совершении посягательств используются информационно-телекоммуникационные технологии.

В свою очередь, термин «метод» применяется для обозначения способов теоретического исследования или практического осуществления; способов действовать, поступать определенным

---

5 См.: *Евдокимов К. Н.* Противодействие компьютерной преступности: теория, законодательство, практика : дис. … канд. юрид. наук. М., 2021. С. 30.

6 См.: *Дремлюга Р. И.* Интернет-преступность : монография. Владивосток, 2008. С. 137 ; *Маслакова Е. А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты : дис. … канд. юрид. наук. Орел, 2008. С. 117–118 ; *Менжега М. М.* Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ : дис. … канд. юрид. наук. Саратов, 2005. С. 34 ; *Мещеряков В. А.* Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж, 2001. С. 105.

7 См.: *Евдокимов К. Н.* Указ. соч. С. 104.

8 См.: *Сурдин Г. В.* Потребность в самоутверждении как фактор развития личности // iPolytech Journal. 2012. № 2 (61). С. 34.

9 См.: *Лунеев В. В.* Мотивация преступного поведения. М., 1991. С. 239.

10 Если виновные были официально трудоустроены.

11 См.: Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ : монография / науч. ред. И. Г. Смирнова. М., 2016. С. 69–70 ; *Торбин Ю. Г.* Использование следователем информационных технологий при планировании расследования и производстве следственных действий // Использование специальных знаний в уголовном судопроизводстве : материалы Всерос. науч.-практ. конференции / редкол.: И. М. Колосова [и др.]. М., 2021. С. 111–119.

образом[12]; приема или системы приемов, совокупности определенных операций, направленных на решение конкретной задачи[13]. Первостепенно методы предупреждения преступлений базировались на интуиции и ограниченных криминологических данных, что приводило к использованию неэффективных превентивных методов. В СССР к методам предупреждения преступлений относили: общие меры; специальные меры, подразделяющиеся на процессуальные, непроцессуальные, экономические, технические, реабилитационные, организационные и др.[14] Ю. Ф. Гладырь отождествляет методы и меры предупреждения[15]. Но достижения в области искусственного интеллекта позволяют применять новые превентивные методы, в том числе к компьютерной преступности.

Искусственный интеллект — неотъемлемая составляющая современной жизни. С его помощью можно не только совершать преступления, но и успешно их предупреждать. Например, искусственный интеллект в состоянии распознать действия лиц, совершающих компьютерные преступления, создавая алгоритмы для анализа значительных объемов данных, образуемых в режиме реального времени, обнаруживая закономерности и отклонения, которые могут указывать на вероятную угрозу информационной безопасности. Интернет вещей отвечает за сбор данных, а искусственный интеллект — за их анализ. Он способствует принятию решений при незначительном участии человека. В частности, нейронные сети, робототехника, экспертные системы, обработка речи, планирование и машинное обучение устраняют трудоемкие операции, выполнявшиеся ранее вручную. Это позволяет сосредоточить усилия на более важном и повышает эффективность превентивной деятельности. Следовательно, искусственный интеллект, ставший краеугольным камнем действительности, коренным образом изменил превентивную деятельность правоохранительных органов.

Искусственный интеллект предоставляет значительное количество инструментов для расширения возможностей превентивной деятельности правоохранительных органов, позволяя им более плодотворно прогнозировать, выявлять и сдерживать преступное поведение. Например, анализируя криминологические данные компьютерных преступлений и выявляя их закономерности, он способен спрогнозировать, где и когда могут быть совершены обозначенные уголовно наказуемые деяния, что позволяет правоохранительным органам своевременно их предотвращать. Исследование, проведенное департаментом полиции Лос-Анджелеса (LAPD), показало, что их программа, используя алгоритмы искусственного интеллекта для прогнозирования очагов преступности, привела к сокращению числа краж со взломом на 33 % и насильственных преступлений в городе на 21 %[16]. Это можно применить и к компьютерным преступлениям, что положительно скажется на их предупреждении.

Правоохранительными органами в зарубежных государствах для предупреждения преступлений используются (использовались) такие программы и средства, как: интегрированная геолокационная платформа предиктивной аналитики (Великобритания, 2016 г. — н.в.); система анализа данных, основанная на разработках IBM и географической информационной системе Ersi (Канада, 2007 г. — н.в.); программа по созданию системы социального кредита (КНР, 2014–2020 гг.)[17]; многослойный персептрон с прямой связью (FFMLP)[18]; камеры видеонаблю-

---

[12] См.: *Ожегов С. И.*, *Шведова Н. Ю.* Толковый словарь русского языка : 72 500 слов и 7 500 фразеологических выражений. М. : Азъ, 1994. С. 245.

[13] См.: *Ефремова Т. Ф.* Новый словарь русского языка. Толково-словообразовательный : св. 136 000 словар. ст., ок. 250 000 семант. единиц. М. : Рус. яз., 2000. С. 521.

[14] См.: *Zeldes I.* Methods of Crime Prevention in the USSR // International Journal of Comparative and Applied Criminal Justice. 1978. No. 2. P. 32.

[15] См.: *Гладырь Ю. Ф.* Система предупреждения преступлений: история развития и современное состояние : дис. … канд. юрид. наук. М., 2006. С. 142.

[16] См.: *Mishra A.*, *Kahla L. Z.*, *Gayflor N.* Leveraging Artificial Intelligence for Crime Detection and Prevention // International Journal of Scientific Research in Engineering and Management. 2024. No. 8. P. 1.

[17] См.: *Суходолов А. П.*, *Бычкова А. М.* Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. С. 755.

[18] См.: *Kouziokas G.* Artificial Intelligence Based Crime Forecasting in Public Administration by Implementing a Feedforward Multilayer Perceptron // 16th International Conference on Artificial Intelligence and Law — VIII Workshop on Artificial Intelligence and the Complexity of Legal Systems (June 2017). P. 10.

дения замкнутого контура (CCTV), оснащенные системой распознавания лиц искусственным интеллектом, и т.д. Было обнаружено, что функционирование камер видеонаблюдения коррелировало со значительным сокращением количества криминальных инцидентов, но только на небольших территориях. Однако вскоре об установленном видеонаблюдении стало известно всем лицам, в том числе и тем, которые намеревались совершить общественно опасные посягательства, что вынудило их переместить свою преступную деятельность на иную территорию. Это подтверждается исследованиями, что необходимо учитывать при выработке мер предупреждения компьютерных преступлений.

Термин «искусственный интеллект» упоминается изыскателями наряду с такими понятиями, как «большие данные», «машинное обучение», «глубинное обучение» и «нейронные сети». Большие данные представляют собой потоки необработанной информации, обрабатываемые компьютеризированными системами путем их систематизации и упорядочивания. Большие данные в последнее время — один из наиболее популярных и востребованных методов анализа имеющейся информации. Они способствуют прогнозированию компьютерных преступлений; выявлению ранее неизвестных криминальных связей; быстрому получению сведений о компьютерных преступлениях; осуществлению ее анализа; преобразованию в строгую цифровую отчетность, что помогает выполнять моделирование совершаемого деяния, определять криминологические особенности личности преступника (пол, возраст, нервно-психическое здоровье, гражданство, семейное и социальное положение, образование, уровень дохода, занимаемая должность и т.д.), вид преступления, сферу его совершения. Поэтому их использование может положительно сказаться на предупреждении.

В последние несколько лет правоохранительные органы разных стран всё активнее задействуют большие данные в превентивной деятельности. Например, Агентство национальной безопасности США применяет технологии больших данных, чтобы предотвратить террористические акты. Другие государственные органы также используют их для предотвращения различных преступлений. В частности, полицейские Чикаго работают с собственной аналитической системой. У них имеется специальный алгоритм, направленный на формирование «круга риска», в который входят лица, имеющие высокую вероятность стать участниками вооруженного нападения или его жертвами. Данный алгоритм присваивает лицу так называемую оценку уязвимости с учетом его криминального прошлого (арестов, неправомерного применения оружия, принадлежности к различным преступным группировкам и т.д.). Разработчик указанной системы подчеркивает, что она анализирует криминальное прошлое человека, устанавливает криминогенные районы, время, когда районы наиболее опасны, что позволяет сфокусировать силы и средства правоохранительных органов (например, они могут установить камеры наблюдения, увеличить количество сотрудников для патрулирования в этом районе и т.д.). То есть использование этой системы помогает оптимизировать предупреждение преступности на объективной основе, понятной не только сотрудникам полиции, ученым-криминологам, но и представителям государственной и муниципальной власти страны[19]. Важность обозначенного превентивного метода обусловлена тем, что в связи с активным развитием компьютерных технологий необходимы современные методы прогнозирования, положительно сказывающиеся на предупреждении компьютерной преступности при наличии значительного количества данных, в отличие от традиционных методов. При этом некоторые из этих методов описывают только прошлую криминогенную ситуацию (метод регрессионного анализа, анализа зон риска и т.д.), что особенно актуально при переходе больших данных на big data 3.0, 4.0[20], поскольку их возможности в предупредительной деятельности расширились.

Существует метод предупреждения компьютерных преступлений, основанный на анализе больших данных, при котором предварительно обрабатывается и извлекается полезная информация из имеющихся текстовых данных. В сочетании с алгоритмом Apriori можно анали-

[19] См.: *Суходолов А. П.*, *Иванцов С. В.*, *Молчанова Т. В.*, *Спасенников Б. А.* Big data как современный криминологический метод изучения и измерений организованной преступности // Всероссийский криминологический журнал. 2019. № 5. С. 718.

[20] См.: *Aglyamova G.* Victimological Aspects of the Use of Artificial Intelligence in Crime Prevention // Juridical World. 2024. No. 1. P. 50.

зировать криминологические характеристики преступников и жертв компьютерных преступлений. Тем не менее совершенствовать методы предупреждения компьютерных преступлений следует не только с помощью искусственного интеллекта и различного рода цифровых технологий, но и за счет деятельности криминальных аналитиков. Криминальные аналитики хорошо зарекомендовали себя в ряде европейских государств и США. Их задачи — это внедрение новых инструментов предупреждения компьютерной преступности, активное использование различных аналитических расчетов и т.д. Необходимо понимать, что криминальные аналитики для этого должны обладать обширными знаниями в области программного обеспечения и компьютерных технологий, поэтому создание единого информационного пространства государством должно стать одной из приоритетных задач в процессе оснащения правоохранительных органов. Нужно исходить из того, что при реализации обозначенного необходимо наладить координацию и тесное взаимодействие между правоохранительными органами и иными органами государственной власти, общественными объединениями. Создание единого информационного пространства в мире требует развития и интеграции существующих информационно-аналитических ресурсов, информационных и телекоммуникационных систем, обеспечивающих установление тесного взаимодействия не только между самими органами государственной власти, но и с населением страны[21].

К новым методам предупреждения компьютерных преступлений можно отнести и использование алгоритма KNN, позволяющего точно спрогнозировать их уровень. Концептуальная схема системы прогнозирования уровня преступлений с использованием KNN выглядит следующим образом: несколько компонентов работают вместе для обеспечения точного прогнозирования уровня преступлений. Одним из компонентов является источник данных, представляющий собой набор данных для обучения и тестирования алгоритма KNN. Другие компоненты: предварительная обработка данных, обучение и тестирование данных, классификатор и оценка KNN. Особенности архитектуры системы прогнозирования уровня преступлений с применением алгоритма KNN делают ее масштабируемой, точной и эффективной. Точность зависит от качества и количества данных, используемых для алгоритма KNN. Но система ограничена доступностью высококачественных данных и вычислительной мощностью, необходимой для обработки значительного количества сведений. Поэтому рассмотренный метод предупреждения компьютерных преступлений требует значительного совершенствования, что скажется на результативности превентивной деятельности.

В качестве метода предупреждения компьютерных преступлений можно выделить метод корреляционного анализа[22], позволяющий установить причины и условия изучаемого вида общественно опасных посягательств и выработать предупредительные меры, поскольку сущность данного метода заключается в том, чтобы определить взаимосвязь изучаемого явления с результатами наблюдения, оценить ее и сделать выводы. Достоинства этого метода — простота расчета и определение явлений, которые в большей степени влияют на совершение преступлений, недостатки — значительное число наблюдений (по каждой переменной должно быть не менее 12). Мерой корреляции выступает коэффициент корреляции. В криминологических исследованиях компьютерных преступлений в большинстве случаев используется коэффициент корреляции Пирсона, но не используются в полном объеме коэффициенты корреляции Спирмена, Кендалла, Крамера.

Сегодня появились и закрепились на практике такие методы и специализированные инструменты, как, например, Data Mining (переводится как добыча данных, извлечение информации, раскопка данных, интеллектуальный анализ данных, поиск закономерностей, извлечение знаний, анализ шаблонов, «извлечение зерен знаний из гор данных»). Обозначенное предусмотрено для поиска в значительном количестве сведений неочевидных (сомнительных), объективных и важных (полезных) закономерностей для превентивной деятельности. Неочевидных — предпола-

[21] См.: *Ivliev P.*, *Prys I.*, *Burbina Yu*. The use of IT technologies in the prevention of crimes // BIO Web of Conferences. 2023. Vol. 65. No. 10. P. 1051.

[22] См.: *Козырев М. С.*, *Масликов В. А.* Применение корреляционного анализа при исследовании некоторых видов преступлений, совершаемых в Москве // Криминологический журнал Байкальского государственного университета экономики и права. 2016. № 1. С. 28.

гается, что найденные закономерности не обнаруживаются стандартными (классическими) методами обработки информации или экспертами. Объективных — проявившиеся закономерности должны полностью соответствовать действительности, в отличие от экспертного мнения, которое в значительной степени субъективное[23]. Полезных — это значит, что выводы имеют конкретное значение, и им можно найти практическое применение[24] в деятельности по предупреждению преступлений[25]. Это позволяет обнаружить реальные значения показателей общественно опасных деяний, что важно. Data Mining — мультидисциплинарная область, формирующаяся на базе таких наук, как прикладная статистика, распознавание образов, искусственный интеллект, теория баз данных и др. В криминологическом исследовании это процесс обнаружения сведений о ранее неизвестной преступности, практически полезных и доступных для интерпретации знаний, необходимых для принятия решений в деятельности по предупреждению преступлений.

Прогнозирование компьютерной преступности может осуществляться посредством системы, функционирующей на генетическом программировании, семантических концепциях и методах локального поиска для объединения социально-экономических данных, данных правоохранительных органов и другой информации, касающейся совершения компьютерных преступлений. Указанная система превосходит существующие системы с позиции точности прогнозирования, особенно когда наличествует значительное число данных. Она представляет собой модель прогнозирования преступности, имеющую перспективы развития. Потенциал обработки естественного языка (NLP) для предупреждения компьютерных преступлений также очевиден. Система использует естественный язык, алгоритмы обработки и модели машинного обучения, чтобы выявлять различные криминальные ситуации, включая атаки, сообщения, связанные с наркотиками, разжигание ненависти, вражды и оскорбительный контент[26]. Предлагаемая система может стать ценным инструментом для предупреждения компьютерных преступлений и повышения безопасности онлайн-пространства.

К прогнозирующей полицейской деятельности относится применение анализа данных, искусственного интеллекта и методов машинного обучения для определения компьютерных преступных действий до того, как они произойдут. Используя исторические данные о преступлениях, демографическую информацию и исходные данные в режиме реального времени, прогнозирующая полицейская деятельность направлена на обнаружение очагов преступности, оптимальное распределение полицейских ресурсов и в конечном итоге — предотвращение преступлений. Этот технологический подход получил распространение в правоохранительных органах по всему миру, поскольку они стремятся бороться с растущим уровнем компьютерной преступности при максимальном использовании ограниченных ресурсов.

С развитием технологий и науки о данных прогнозирующая полицейская деятельность стала более изощренной, используются сложные алгоритмы и большие наборы данных для выработки прогнозов и рекомендаций. Рост объема больших данных в сочетании с увеличением вычислительной мощности значительно расширил сферу применения и точность инструментов прогнозирования. Однако потенциальная чрезмерная полицейская деятельность и повышенный контроль за определенными сообществами и лицами могут привести к обвинениям в несправедливом обращении и дискриминации. Обеспечение прозрачности алгоритмов, регулярный аудит источников данных и вовлечение заинтересованных сторон сообщества в обсуждение политики — важные шаги на пути к более справедливой и успешной реализации поставленных задач.

В целях предупреждения компьютерных преступлений предлагается использование стратегий и методов SCP. Они ориентированы на обеспечение безопасности киберпространства. Тем не менее в большинстве случаев применяются лишь некоторые методы SCP, а также не все

[23] См.: Цифровая криминология: математические методы прогнозирования / А. П. Суходолов, С. В. Иванцов, Т. В. Молчанова [и др.]. Ч. 1 // Всероссийский криминологический журнал. 2018. № 2. С. 234.

[24] См.: Цифровая криминология: математические методы прогнозирования / А. П. Суходолов, С. В. Иванцов, Т. В. Молчанова [и др.]. Ч. 2 // Всероссийский криминологический журнал. 2018. № 3. С. 323.

[25] См.: *Fox V.* Introduction to Criminology. New Jersey, 1976.

[26] См.: *Al-Rummana G.* The Role of Big data Analysis in Increasing the Crime Prediction and Prevention Rates // Intelligent Data Analytics for Terror Threat Prediction. 2021. P. 209–220.

связи между методами SCP и возможностями сокращения компьютерных преступлений. Для того чтобы значительно повысить эффективность превентивной деятельности, необходимо использовать специальное оборудование. Для этого нужно формировать и развивать принципиально новые направления информационного и технического обеспечения следственной и оперативно-розыскной деятельности. Предупреждение компьютерных преступлений не должно быть исключительной прерогативой правоохранительных органов. Государственные структуры через средства массовой информации могут научить граждан грамотному реагированию на совершение в отношении них компьютерных преступлений. Национальным правительствам следует запустить рекламные кампании, чтобы помочь людям защитить себя от подобных преступлений. Простые меры безопасности, особенно среди молодежи, способны значительно снизить уровень преступности. Ввиду того что преступления в информационной среде набрали обороты в технически развитых западных странах, было бы нелогично использовать их опыт в борьбе с этим явлением.

Заключение

Преступления, предусмотренные главой 28 УК РФ, совершаются преимущественно в городской местности (удельный вес осужденных составляет 60,7 %); в одиночку (64,6 %; удельный вес лиц, виновных в уголовно наказуемых деяниях рассматриваемой группы, 35,4 %); не в состоянии алкогольного, наркотического или иного опьянения (100 %); лицами, которые не имели неснятых или непогашенных судимостей (89,5 %); совершили компьютерное преступление впервые. В большинстве случаев виновными являются мужчины (71,5 %); в возрасте от 18 до 24 лет (42,3 %), 30–49 лет (35,7 %); граждане РФ (99,1 %); постоянные жители местности, в которой они совершили общественно опасное посягательство (96,1 %); имеющие высшее образование (32,7 %); среднее профессиональное образование (41,4 %, при этом образование преимущественно техническое); не состоящие в официально зарегистрированном браке (51,2 %); не имеющие постоянного источника дохода (65,1 %).

Увеличение компьютерных преступлений требует внедрения новых методов их предупреждения. Но, к сожалению, сегодня новые методы предупреждения таких преступлений не исследуются учеными и редко применяются в превентивной деятельности, в то время как последние достижения в области искусственного интеллекта предлагают смену парадигмы, позволяя выработать и применять новые превентивные методы, например связанные с использованием искусственного интеллекта, больших данных и т.д. Вместе с тем не сто́ит останавливаться на обозначенных достижениях в данной сфере, необходимо продолжать разрабатывать методы, поскольку искусственный интеллект, ко всему указанному, способен работать в различных условиях, например при неполноте криминологических данных, неточной информации о предполагаемом месте совершения преступления. Представляется целесообразным совершенствовать методы предупреждения компьютерных преступлений не только с помощью искусственного интеллекта и цифровых технологий, но и за счет активного использования знаний, полученных благодаря криминальным аналитикам. Однако обозначенная тематика исследования требует дальнейших научных изысканий, поскольку компьютерная преступность постоянно развивается, приобретая новые формы, и с каждым разом причиняет всё больший ущерб объектам уголовно-правовой охраны. Кроме того, при создании новых методов предупреждения преступлений анализируемой группы на основе искусственного интеллекта должны учитываться опыт, знания, умения высококвалифицированных специалистов — субъектов превентивной деятельности.

СПИСОК ЛИТЕРАТУРЫ

Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации : дис. … канд. юрид. наук. Казань, 2017. 243 с.

Гладырь Ю. Ф. Система предупреждения преступлений: история развития и современное состояние : дис. … канд. юрид. наук. М., 2006. 159 с.

Козырев М. С., *Масликов В. А.* Применение корреляционного анализа при исследовании некоторых видов преступлений, совершаемых в Москве // Криминологический журнал Байкальского государственного университета экономики и права. 2016. № 1. С. 28–29.

Кравцов Д. А. Искусственный разум: предупреждение и прогнозирование преступности // Вестник Московского университета МВД России. 2018. № 3. С. 108–110.

Лунеев В. В. О криминолого-аналитическом и системном подходе к законотворчеству // Криминология: вчера, сегодня, завтра. 2014. № 4 (35). С. 14–25.

Суходолов А. П., Бычкова А. П. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. С. 753–766.

Суходолов А. П., Иванцов С. В., Молчанова Т. В., Спасенников Б. А. Big data как современный криминологический метод изучения и измерений организованной преступности // Всероссийский криминологический журнал. 2019. № 5. С. 718–726.

Суходолов А. П., Суходолов Я. А., Колесникова А. В. О необходимости совершенствования методологии современных криминологических исследований // Право и государство: теория и практика. 2022. № 8 (212). С. 125–133.

Утаров К. А. Математические методы в криминологии : дис. … канд. юрид. наук. М., 2004. 167 с.

Цифровая криминология: математические методы прогнозирования / А. П. Суходолов, С. В. Иванцов, Т. В. Молчанова [и др.] // Всероссийский криминологический журнал. 2018. № 2. С. 230–236 ; № 3. С. 323–329.

Aglyamova G. Victimological Aspects of the Use of Artificial Intelligence in Crime Prevention // Juridical World. 2024. No. 1. P. 50–55.

Aiello M. F. Policing through social networking: Testing the linkage between digital and physical police practices // The Police Journal. 2018. Vol. 91. Iss. 1. P. 89–97.

Al-Rummana G. The Role of Big data Analysis in Increasing the Crime Prediction and Prevention Rates // Intelligent Data Analytics for Terror Threat Prediction. 2021. P. 209–220.

Exploring the impact of how criminals interact with cyber-networks / T. Chikore, F. Nyabadza, Z. Chazuka [et al.] // A Mathematical Modeling Approach. 2024. No. 11. P. 10–23.

Fox V. Introduction to Criminology. New Jersey, 1976. 115 p.

Ivliev P., Ananyeva E., Prys I., Burbina Yu. The use of IT technologies in the prevention of crimes // BIO Web of Conferences. 2023. Vol. 65. No. 10. P. 1051–1061.

Kouziokas G. Artificial Intelligence Based Crime Forecasting in Public Administration by Implementing a Feedforward Multilayer Perceptron // 16th International Conference on Artificial Intelligence and Law — VIII Workshop on Artificial Intelligence and the Complexity of Legal Systems. June 2017. P. 10–22.

Mishra A., Kahla L. Z., Gayflor N. Leveraging Artificial Intelligence for Crime Detection and Prevention // International Journal of Scientific Research in Engineering and Management. 2024. No. 8. P. 1–6.

Ramadhoan M., Amiruddin A., Ufran U. Crime Prevention Through an Environmental Design Approach in Reducing Crime Rates in Indonesia // International Journal of Social Science Research and Review. 2024. No. 7. P. 177–195.

Zeldes I. Methods of Crime Prevention in the USSR // International Journal of Comparative and Applied Criminal Justice. 1978. No. 2. P. 32–33.

REFERENCES

Aglyamova G. Victimological Aspects of the Use of Artificial Intelligence in Crime Prevention. *Juridical World*. 2024;1:50-55.

Aiello MF. Policing through social networking: Testing the linkage between digital and physical police practices. *The Police Journal*. 2018;91(1):89-97.

Al-Rummana G. The Role of Big data Analysis in Increasing the Crime Prediction and Prevention Rates. In: Intelligent Data Analytics for Terror Threat Prediction. 2021. P. 209–220

Chikore T, Nyabadza F, Chazuka Z, Nyirenda-Kayuni M, Zhangazha M, Chukwudum Q, White J, Mhlabane F, Osman S, Ndlovu M, Mwaonanji J. Exploring the impact of how criminals interact with cyber-networks. *A Mathematical Modeling Approach*. 2024;11:10-23.

Fox V. Introduction to Criminology. New Jersey, 1976. 115 p.

Gaifutdinov RR. The concept and qualification of crimes against the security of computer information. Cand. Sci. (Law) Diss. Kazan; 2017. (In Russ.).

Gladyr YuF. Crime prevention system: development history and current state. Cand. Sci. (Law) Diss. Moscow; 2006. (In Russ.).

Ivliev P, Ananyeva E, Prys I., Burbina Yu. The use of IT technologies in the prevention of crimes // BIO Web of Conferences. 2023. Vol. 65. No. 10. P. 1051–1061.

Kouziokas G. Artificial Intelligence Based Crime Forecasting in Public Administration by Implementing a Feedforward Multilayer Perceptron. In: 16th International Conference on Artificial Intelligence and Law — VIII Workshop on Artificial Intelligence and the Complexity of Legal Systems. June 2017. P. 10–22

Kozyrev MS, Maslikov VA. The use of correlation analysis for the study of some crimes committed in moscow. *Russian Journal of Criminology*. 2016;1:28-29. (In Russ.).

Kravtsov DA. Artificial intelligence: crime prevention and prediction. *Vestnik of Moscow University of the Ministry of Internal Affairs of Russia*. 2018;3:108-110. (In Russ.).

Luneev VV. On criminal analytical and systematic approach to lawmaking. *Criminology: Yesterday, Today, Tomorrow*. 2014;4(35):14-25. (In Russ.).

Mishra A, Kahla LZ, Gayflor N. Leveraging Artificial Intelligence for Crime Detection and Prevention. *International Journal of Scientific Research in Engineering and Management.* 2024;8:1-6.

Ramadhoan M, Amiruddin A, Ufran U. Crime Prevention through an Environmental Design Approach in Reducing Crime Rates in Indonesia. *International Journal of Social Science Research and Review*. 2024;7:177-195.

Sukhodolov AP, Bychkova AP. Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution. *Russian Journal of Criminology*. 2018;6:753-766. (In Russ.).

Sukhodolov AP, Ivantsov SV, Molchanova TV, Spasennikov BA, Kaluzhina MA. Digital Criminology: Mathematical Methods of Prediction (Part 1). *Russian Journal of Criminology*. 2018;2:230-236. (In Russ.).

Sukhodolov AP, Ivantsov SV, Molchanova TV, Spasennikov BA, Kaluzhina MA. Digital Criminology: Mathematical Methods of Prediction (Part 2). *Russian Journal of Criminology*. 2018;3:323-329. (In Russ.).

Sukhodolov AP, Ivantsov SV, Molchanova TV, Spasennikov BA. Big Data as a Modern Criminological Method of Studying and Measuring Organized Crime. *Russian Journal of Criminology*. 2019;5:718-726. (In Russ.).

Sukhodolov AP, Sukhodolov YaA, Kolesnikova AV. On the Need to Improve the Methodology of Modern Criminological Research. *Law and State: The Theory and Practice*. 2022;8(212):125-133. (In Russ.).

Utarov KA. Mathematical methods in criminology. Cand. Sci. (Law) Diss. Moscow; 2004. (In Russ.).

Zeldes I. Methods of Crime Prevention in the USSR. *International Journal of Comparative and Applied Criminal Justice*. 1978;2:32-33.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Ефремова Ирина Алексеевна, доктор юридических наук, доцент, профессор кафедры уголовного и уголовно-исполнительного права, прокурорского надзора и криминологии Саратовской государственной юридической академии
д. 1, Вольская ул., г. Саратов 410056, Российская Федерация
efremova005@yandex.ru

INFORMATION ABOUT THE AUTHOR

Irina A. Efremova, Dr. Sci. (Law), Associate Professor, Professor, Department of Criminal and Penal Law, Prosecutorial Supervision and Criminology, Saratov State Law Academy, Saratov, Russian Federation
efremova005@yandex.ru

Материал поступил в редакцию 26 сентября 2024 г.
Статья получена после рецензирования 7 декабря 2024 г.
Принята к печати 15 апреля 2025 г.

Received 26.09.2024.
Revised 07.12.2024.
Accepted 15.04.2025.