

А. К. Жарова<sup>1</sup><sup>1</sup> Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия

## Интеллектуальные системы распознавания образов и смысла в системе предупреждения правонарушений, совершаемых с использованием Сети

Жарова Анна Константиновна, доктор юридических наук, доцент, Финансовый университет при Правительстве Российской Федерации

E-mail: anna\_jarova@mail.ru

ORCID ID: <https://orcid.org/0000-0002-2981-3369>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56964137900>

Web of Science Researcher ID: <https://www.webofscience.com/wos/author/record/H-4012-2015>

eLIBRARY SPIN-код: 2240-1467

### Аннотация

**Цель:** исследование проблем правового регулирования интеллектуальных систем распознавания образов и смысла в системе предупреждения и пресечения правонарушений, совершаемых с использованием информационно-телекоммуникационной сети.

**Методы:** диалектический подход к познанию социальных явлений, позволяющий проанализировать их в историческом развитии и функционировании в контексте совокупности объективных и субъективных факторов, который определил выбор следующих методов исследования: формально-юридический, сравнительно-правовой, правового моделирования, теории множеств, теории графов.

**Результаты:** предупреждение правонарушений включает формы профилактики и процессуальные формы предупреждения правонарушений. Объединяет эти два множества форм принятие мер по устранению обстоятельств, способствующих совершению правонарушений. Однако выявление причин и условий, способствующих совершению правонарушений, не входит в множество процессуальных форм предупреждения правонарушений. Процессуальные формы направлены на предотвращение конкретных видов правонарушений, в то время как профилактика в какой-то мере использует методы предиктивной аналитики, предполагая возможность наступления негативного антисоциального события и используя различные организационные, технологические и правовые инструменты и меры. Следовательно, прогнозирование преступных действий является одним из этапов предупреждения правонарушений, осуществляемых с использованием методов предиктивной аналитики данных, оставленных человеком. Точность вычислений, проводимых искусственным интеллектом (ИИ), с каждым годом увеличивается, в связи с чем растет и точность полученных вероятностей и прогнозов.

**Научная новизна:** в статье проведено междисциплинарное исследование проблемы предотвращения негативных социальных отклонений, происходящих с использованием информационно-телекоммуникационной сети, путем организации взаимодействия провайдеров хостинга, использующих интеллектуальные системы распознавания образов и смысла и правоохранительных органов. Установлено, что применение ИИ правоохранительными органами и их взаимодействие с провайдерами хостинга позволяют не только выявить противоправный и общественно опасный контент, но и оценить вероятность совершения преступления конкретным человеком. Применение ИИ провайдерами хостинга позволит обеспечить профилактику противоправных действий, выявить стадию формирования преступного умысла, выраженного в размещенной им информации, и тем самым минимизировать возможность перерастания умысла в реальность преступных действий.

**Практическая значимость:** основные положения и выводы статьи могут быть использованы в научной, педагогической и правоприменительной деятельности при рассмотрении вопросов, связанных с правовым регулированием алгоритмов ИИ, возможности их применения в целях предупреждения и пресечения правонарушений, совершаемых с использованием информационно-телекоммуникационной сети.

### Ключевые слова:

уголовное право и криминология, предупреждение, пресечение и прогнозирование преступности, искусственный интеллект, интеллектуальные системы распознавания, сеть, хостинг, провайдер

### Финансирование

Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Статья находится в открытом доступе в соответствии с Creative Commons Attribution Non-Commercial License (<https://creativecommons.org/licenses/by-nc/4.0/>), предусматривающем некоммерческое использование, распространение и воспроизводство на любом носителе при условии упоминания оригинала статьи.

---

**Как цитировать статью:** Жарова, А. К. (2024). Интеллектуальные системы распознавания образов и смысла в системе предупреждения правонарушений, совершаемых с использованием Сети. *Russian Journal of Economics and Law*, 18(2), 469–480. <https://doi.org/10.21202/2782-2923.2024.2.469-480>

---

### Scientific article

A. K. Zharova<sup>1</sup>

<sup>1</sup> *Financial University under the Government of the Russian Federation, Moscow, Russia*

## Intellectual systems of pattern and meaning recognition in the system of prevention of crimes committed using the Internet

Anna K. Zharova, Dr. Sci. (Law), Associate Professor, Финансовый университет при Правительстве Российской Федерации  
E-mail: [anna\\_jarova@mail.ru](mailto:anna_jarova@mail.ru)  
ORCID ID: <https://orcid.org/0000-0002-2981-3369>  
Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=56964137900>  
Web of Science Researcher ID: <https://www.webofscience.com/wos/author/record/H-4012-2015>  
eLIBRARY SPIN-код: 2240-1467

### Abstract

**Objective:** to study the issues of legal regulation of intellectual systems for pattern and meaning recognition as part of the system to prevent and suppress offenses committed using information and telecommunication network.

**Methods:** dialectical approach to the cognition of social phenomena, which allows analyzing them in their historical development and functioning in the context of objective and subjective factors, which determined the choice of the following research methods: formal-legal, comparative-legal, legal modeling, set theory, graph theory.

**Results:** prevention of offenses includes prophylaxis and procedural forms of prevention of offenses. These two sets of forms share measures to eliminate the circumstances that contribute to the commission of offenses. However, the set of procedural forms of prevention does not include identification of causes and conditions contributing to the commission of offenses. Procedural forms aim at preventing specific types of offenses, while prevention to some extent uses the methods of predictive analytics, assuming the possibility of a negative antisocial event and using various organizational, technological and legal tools and measures. Consequently, prediction of criminal actions is one of the stages of prevention of offenses carried out using predictive analytics of data left by a person. The accuracy of calculations carried out by artificial intelligence (AI) is increasing every year; hence, the accuracy of the obtained probabilities and forecasts is also increasing.

**Scientific novelty:** the article presents an interdisciplinary study of preventing negative social deviations occurring with the use of information and telecommunication network by means of interaction between the hosting providers, using intelligent systems of pattern and meaning recognition, and law enforcement agencies. It was established that the application of AI by law enforcement agencies and their interaction with hosting providers allows not only to identify illegal and socially dangerous content, but also to assess the probability of committing a crime by a particular person. Application of AI by hosting providers allows preventing illegal actions. This can be done by revealing the stage of criminal intent expressed in the information posted by a potential offender, thus minimizing the possibility of the intent outgrowth into real criminal actions.

**Practical significance:** the main provisions and conclusions of the article can be used in scientific, pedagogical and law enforcement activities when considering issues related to the legal regulation of AI algorithms, the possibility of their application in order to prevent and suppress offenses committed with the use of information and telecommunications network.

### Keywords:

criminal law and criminology, crime prevention, suppression and forecasting, artificial intelligence, intelligent recognition systems, network, hosting, provider

### Financial support

The article was prepared based on the results of research carried out at the expense of budgetary funds under the state assignment to Financial University.

The article is in Open Access in compliance with Creative Commons Attribution Non-Commercial License (<https://creativecommons.org/licenses/by-nc/4.0/>), stipulating non-commercial use, distribution and reproduction on any media, on condition of mentioning the article original.

**For citation:** Zharova, A. K. (2024). Intellectual systems of pattern and meaning recognition in the system of prevention of crimes committed using the Internet. *Russian Journal of Economics and Law*, 18(2), 469–480. (In Russ.). <https://doi.org/10.21202/2782-2923.2024.2.469-480>

## Введение

Интернет является не только коммуникационной средой, но и технологией, с использованием которой совершаются противоправные действия. Несмотря на то, что Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и правоохранительные органы занимаются защитой прав и свобод человека, количество правонарушений, совершаемых с использованием Сети, не становится значительно меньше. Все социальные институты могут столкнуться с правонарушениями, происходящими с использованием Сети, результатом которых зачастую являются серьезные негативные последствия как для отдельных лиц, так и для общества в целом.

Предотвращение таких социальных отклонений, происходящих с использованием Сети, возможно путем организации взаимодействия провайдеров хостинга, использующих интеллектуальные системы распознавания образов и смысла (далее – ИИ), и правоохранительных органов. ИИ позволяет распознать стадии преступления, намерение совершить противоправные действия, а взаимодействие с правоохранительными органами – минимизировать риск перехода в следующие стадии преступления.

В связи с этим в статье поставлена задача дать ответ на вопросы, могут ли провайдеры хостинга быть отнесены к субъектам предупреждения преступности или к лицам, участвующим в профилактике преступлений, а также может ли искусственный интеллект распознать в Сети стадии совершения преступлений.

Для поиска ответа на поставленную задачу были применены следующие методы: моделирования условий, теории множеств, теории графов, а также анализа, сравнения и синтеза.

## Результаты исследования

### Предупреждение и профилактика правонарушений. Общее и отличия

Под правонарушением понимается «преступление или административное правонарушение, представляющее собой противоправное деяние (действие, бездействие), влекущее уголовную или административную ответственность»<sup>1</sup>. В законодательстве и научном сообществе для описания системы объективных и субъективных предпосылок преодоления правонарушений используются понятия «профилактика правонарушений, преступности» и «предупреждение правонарушений, преступлений». Например, в Руководящих принципах

<sup>1</sup> Об основах системы профилактики правонарушений в Российской Федерации. № 182-ФЗ от 23.06.2016. (2016). Собрание законодательства Российской Федерации, 26 (ч. I), ст. 3851.

Организации Объединенных Наций для предупреждения преступности среди несовершеннолетних (Эр-Риядские руководящие принципы, 1990 г.).

УК РФ оперирует понятием «предупреждение преступлений»<sup>2</sup>, МВД России – понятиями «профилактика правонарушений»<sup>3</sup>, «предупреждение преступлений»<sup>4</sup>. В соответствии с Методическими рекомендациями по организации в Федеральной службе судебных приставов работы по предупреждению преступлений<sup>5</sup> «предупреждение преступлений имеет как процессуальные формы, т. е. предусмотренные Уголовно-процессуальным кодексом Российской Федерации, – внесение дознавателем в порядке ч. 2 ст. 158 УПК РФ в соответствующую организацию или соответствующему должностному лицу представления о принятии мер по устранению обстоятельств, способствующих совершению преступления или других нарушений закона, так и иные формы профилактики (проведение разъяснительной работы среди населения, выступления в образовательных учреждениях, трудовых коллективах, в средствах массовой информации по вопросам предупреждения преступлений; публикация материалов в печати, в информационной сети Интернет и т. п.)»<sup>6</sup>.

В соответствии с Федеральным законом «Об основах системы профилактики правонарушений в Российской Федерации» под понятием «профилактика правонарушений» понимается «совокупность мер социального, правового, организационного, информационного и иного характера, направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений или антиобщественного поведения»<sup>7</sup>. В соответствии с тем же законом лицами, участвующими в профилактике правонарушений, являются «граждане, общественные объединения и иные организации, оказывающие помощь (содействие) субъектам профилактики правонарушений в рамках реализации своих прав в сфере профилактики правонарушений в соответствии с Федеральным законом «Об основах системы профилактики правонарушений в Российской Федерации» и другими федеральными законами»<sup>8</sup>.

В научной литературе представлены различные точки зрения на понятия «профилактика правонарушений, преступлений» и «предупреждение правонарушений, преступлений». Так, А. А. Савченко считает, что предупреждение преступлений включает в себя различные меры и действия, направленные на ограничение возможности совершения преступлений, охрану общества в целом и индивида в частности. Она пишет: «...профилактика преступлений сводится к своевременному обнаружению и искоренению предпосылок. Соответственно, предупреждение преступлений должно носить общий характер, а профилактика – более индивидуальный» (Савченко, 2010). Другие авторы считают, что профилактика, предотвращение и пресечение преступлений являются этапами предупреждения преступлений (Малков, 2014)<sup>9</sup> или что профилактика и предупреждение правонарушений – это этапы концепции предотвращения правонарушений<sup>10</sup>.

Наша точка зрения, что формы профилактики правонарушений и процессуальные формы предупреждения преступлений являются подмножеством множества предупреждения правонарушений. Это разные понятия, которые в целом направлены на предотвращение антиобщественных и негативных явлений. Анализ законодательства и Методических рекомендаций по организации в Федеральной службе судебных приставов работы по предупреждению преступлений позволяет представить следующую схему множества «Предупреждение правонарушений» (рис. 1).

В виде графа связи между подмножествами можно представить следующим образом (рис. 2).

<sup>2</sup> Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996. (1996). Собрание законодательства Российской Федерации, 25, ст. 2954.

<sup>3</sup> Приказ Министерства внутренних дел России № 715 от 29.09.2022. (Документ опубликован не был).

<sup>4</sup> Указ Президента РФ № 306 от 11.03.2003 (в ред. от 07.12.2016). (2003). Собрание законодательства Российской Федерации, 12, ст. 1099.

<sup>5</sup> Письмо ФССП России № 00043/16/83207-BB от 07.09.2016, утв. ФССП России 02.09.2016 № 0004/11. (2016). Бюллетень Федеральной службы судебных приставов, 10.

<sup>6</sup> Там же.

<sup>7</sup> Об основах системы профилактики правонарушений в Российской Федерации. № 182-ФЗ от 23.06.2016. (2016). Собрание законодательства Российской Федерации, 26 (ч. I), ст. 3851.

<sup>8</sup> Там же.

<sup>9</sup> Рясков, Д. А. (2014). Предупреждение преступлений: лекция по теме № 7. Ставропольский филиал Краснодарского университета. [https://ставф.крд.мвд.рф/upload/site122/document\\_file/Lekciya\\_7\(7\).pdf](https://ставф.крд.мвд.рф/upload/site122/document_file/Lekciya_7(7).pdf)

<sup>10</sup> Филиппова, Е. О. (2019). Предупреждение преступности: учебное пособие. Оренбург: Оренбургский гос. ун-т.



Рис. 1. Множество «Предупреждение правонарушений»

Fig. 1. Scheme of the “Crime prevention” set



Рис. 2. Граф «Формы предупреждения правонарушений»

Fig. 2. “Forms of crime prevention” graph

Подмножество «Формы профилактики» пересекается с подмножеством «Процессуальные формы» в части «принятия мер по устранению обстоятельств, способствующих совершению преступления или других нарушений закона»<sup>11</sup>, что образует их общую часть, принадлежащую двум подмножествам. Иными словами, общей частью двух подмножеств является множество действий, направленных на устранение обстоятельств, способствующих совершению правонарушения.

Однако нужно отметить, что подмножество «Формы профилактики» предусматривает действие «выявление причин и условий, способствующих совершению правонарушений», которое не входит в подмножество «Процессуальные формы». Тем самым можно сделать вывод, что представление вносится, когда уже установлен факт правонарушения или обстоятельств, облегчающих его совершение.

<sup>11</sup> Письмо ФССП России № 00043/16/83207-BB от 07.09.2016, утв. ФССП России 02.09.2016 № 0004/11. (2016). Бюллетень Федеральной службы судебных приставов, 10.



В таком случае для моделирования условий применения форм профилактики правонарушений и процессуальных форм предупреждения правонарушений определим, что наступлением правонарушения является «1», отсутствием правонарушения – «0».

Для применения форм профилактики правонарушений вероятность возникновения антиобщественного или негативного события должна быть отлична от нуля, но не близка к единице. Иными словами, профилактика правонарушения возможна, когда эксперты фиксируют и наблюдают признаки возникновения антиобщественных событий, могут оценить риски и угрозы развития этих событий и спрогнозировать их динамику, а также имеются предпосылки для их реализации. Например, профилактика возможна в случаях пандемии, преступности, правонарушений.

Процессуальные формы предупреждения правонарушений так же, как и профилактика правонарушений, означают совокупность мер и действий, направленных на предупреждение антиобщественного события, но в случае, когда вероятность возникновения такого события близка к единице. Иными словами, когда событие из множества негативных событий формализуется в конкретное событие. Например, предупреждение теракта может включать в себя оперативные мероприятия правоохранительных органов для предотвращения его совершения.

Таким образом, отличие между формой профилактики правонарушений и процессуальной формой предупреждения правонарушений заключается в том, что профилактика нацелена на предотвращение предпосылок, приводящих к возникновению антисоциальных событий, тогда как процессуальные формы предупреждения нацелены на предотвращение конкретного антисоциального события.

### **Могут ли провайдеры хостинга быть отнесены к субъектам предупреждения преступности или к лицам, участвующим в профилактике правонарушений**

Анализ правовых актов позволяет сделать вывод, что предупреждение преступлений имеет процессуальные формы и формы профилактики. Причем процессуальные формы предупреждения правонарушений могут использовать субъекты, имеющие определенный круг задач и обладающие определенными правами и обязанностями, а также компетенциями в области криминологии. Например, к субъектам предупреждения экономической преступности относятся конкретные государственные структуры, обладающие компетенциями и полномочиями в данной области.

Провайдеры хостинга обладают совокупностью прав и обязанностей в области предоставления услуг хранения информации третьих лиц в Сети, предоставления доступа к ней и использования технологических мощностей для осуществления этих действий. Круг задач, прав и обязанностей провайдеров хостинга не входит в область криминологии. Хотя в случаях, предусмотренных законодательством, провайдеры хостинга обязаны взаимодействовать с Роскомнадзором и уполномоченными органами обеспечения безопасности, в том числе национальной безопасности.

Однако, как мы видели, Федеральным законом «Об основах системы профилактики правонарушений в Российской Федерации» предусмотрена такая форма профилактики предупреждения правонарушений, как «выявление и устранение причин и условий, способствующих совершению правонарушений»<sup>12</sup>, т. е. для случая, когда правонарушение еще не установлено. В то же время провайдеры хостинга обладают технологическими мощностями, которые позволяют выявлять и в определенных случаях устранять причины и условия, способствующие совершению правонарушений. Например, в случае распространения вредоносной информации в Сети провайдеры хостинга могут путем мониторинга информации выявить ее и заблокировать к ней доступ.

Исходя из положений ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», мы можем сделать вывод, что если определенные аспекты деятельности юридических лиц, например провайдеров хостинга, которые могут быть связаны с профилактикой правонарушений путем содействия работе иных структур по предупреждению правонарушений, то они могут быть отнесены к лицам, участвующим в профилактике правонарушений.

<sup>12</sup> Об основах системы профилактики правонарушений в Российской Федерации. № 182-ФЗ от 23.06.2016. (2016). Собрание законодательства Российской Федерации, 26 (ч. I), ст. 3851.

Таким образом, с точки зрения законодательства провайдеров хостинга можно отнести к лицам, участвующим в профилактике правонарушений, но нельзя – к субъектам предупреждения правонарушений. Поскольку провайдер хостинга не обладает определенными правами и обязанностями, не имеет определенный круг задач и не обладает определенной компетенцией в области криминологии.

В то же время такие лица, участвующие в профилактике правонарушений, могут претендовать на правовую, финансовую, административную, материально-техническую помощь со стороны государства<sup>13</sup>.

Участие провайдеров хостинга в системе профилактики преступности будет эффективным, поскольку они могут предоставить правоохранительным органам доступ к информации, сохраненной на их серверах, для расследования преступлений и их предотвращения. В более широком контексте признание провайдеров хостинга субъектами профилактики преступности может быть полезным для повышения безопасности в Сети.

Исходя из задач, которые стоят перед лицами, участвующими в профилактике правонарушений, перед интернет-провайдерами должны быть поставлены задачи выявления вредного содержания и общественно опасных действий в Сети, например, посредством применения ИИ, анализа больших данных.

### **ИИ в системе предупреждения правонарушений**

Все чаще мы встречаем примеры применения систем ИИ в различных областях экономики и общественных отношений. В Указе Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» определена одна из целей развития искусственного интеллекта в Российской Федерации – это «обеспечение национальной безопасности и правопорядка» (п. 23)<sup>14</sup>.

Возможности ИИ могли бы служить инструментом выявления точек напряженности в Сети (Филипова, Коротеев, 2023), а объединение ИИ и уполномоченных органов в области обеспечения общественной безопасности как комбинации взаимодействия позволило бы не только получить смысловой анализ таких признаков преступного деяния, как противоправность, общественная опасность, содержащаяся в размещенной информации (Громова, Петренко, 2023), оценить реальность намерений человека совершить противоправные действия, но и вовремя отреагировать уполномоченным органам в области обеспечения общественной безопасности и тем самым предотвратить правонарушения.

ИИ – это «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека»<sup>15</sup>. В комплекс технологических решений входят информационно-коммуникационная инфраструктура, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке больших данных и поиску решений (п. 5 пп. «а»)<sup>16</sup>.

Поскольку ИИ может выявлять нездоровую активность в любых информационных системах, его использование провайдерами хостинга позволит предупредить правонарушение. Такой нездоровой активностью могут быть подготовка к преступлению, намерение совершить преступление, и в этих случаях ИИ может вычислить вероятность совершения преступления, построить причинно-следственные связи развития событий и передать эту информацию правоохранительным органам. Например, такая информационная модель взаимодействия могла предотвратить совершение преступлений, информацию о планировании которых преступники выкладывали в Сеть задолго до его реализации<sup>17, 18</sup>. После совершения преступления следственные органы исследуют страницы преступника в социальных сетях, выявляют и блокируют такую информацию.

В соответствии с ч. 4 ст. 12 Федерального закона «О полиции» к обязанностям полиции отнесено «выявление лиц, имеющих намерение совершить преступление»<sup>19</sup>. Понятие «намерение совершить преступление»

<sup>13</sup> Там же.

<sup>14</sup> Указ Президента РФ № 490 от 10.10.2019. (2019). Собрание законодательства Российской Федерации, 41, ст. 5700.

<sup>15</sup> Там же.

<sup>16</sup> Там же.

<sup>17</sup> Андреева, В. (2021, 11 мая). «Хочу, чтобы признали себя рабами»: найден блог предполагаемого стрелка из Казани. Пятый канал. <https://www.5-tv.ru/news/342735/hocu-ctoby-priznali-seba-rabami-najden-blog-predpolagaemogo-strelka-izkazani/>

<sup>18</sup> (2012, 7 ноября). Юрист, расстрелявший коллегу, опубликовал манифест о ненависти к человечеству. Телеканал «Россия». <https://smotrim.ru/article/2001510>

<sup>19</sup> О полиции. № 3-ФЗ от 07.02.2011. (2011). Собрание законодательства Российской Федерации, 7, ст. 900.

включает оценку вероятности совершения уголовно наказуемых действий, что, в свою очередь, является прогнозированием.

В зарубежной научной литературе обсуждается возможность использования ИИ в целях прогнозирования преступлений (Navalgund & Priyadharshini, 2018)<sup>20</sup> и уделяется внимание проблеме использования ИИ для предсказательной аналитики и предотвращения преступлений. В российском научном пространстве исследований, посвященных этой тематике, меньше (Расторопов, 2020; Сretenцев, Волкова, 2021) и основное внимание в них уделено применению ИИ на этапе расследования преступления (Sukhodolov & Bychkova, 2018). Например, программе «Конструктор места происшествия», системам моделирования различных следственных действий (Смушкин, 2023; Яшин, 2022). Но эти отечественные системы не решают проблему прогнозирования преступления, хотя еще в 2008 г. авторы предлагали использовать методы предиктивной аналитики в целях принятия обоснованных управленческих решений (Горбенко, Мамасуев, 2008).

Актуальность проблемы применения ИИ подтверждает поставленная в Ведомственной программе цифровой трансформации МВД России на 2022–2024 гг.<sup>21</sup> задача ликвидации имеющихся отставаний по вопросам применения технологий ИИ.

Несмотря на то, что в зарубежных исследованиях имеются результаты прогнозирования преступления, закономерен вопрос о том, можно ли прогнозировать совершение преступления. Иными словами, имеются ли у преступления те параметры или признаки, которые подлежат вероятностной оценке.

### Прогнозирование преступления

В криминологическом исследовании может быть выявлено, что определенные социальные, экономические, демографические или географические факторы связаны с повышенной вероятностью совершения преступлений в определенном районе или сообществе. Эти данные затем могут использоваться для создания моделей предиктивной аналитики. Задачи криминологического прогнозирования включают прогнозирование «преступности, личности преступника, факторы (причины и условия) преступности, последствия преступности, меры борьбы с преступностью»<sup>22</sup>. Причем преступность рассматривается на трех уровнях интерпретации: свойства преступности как массового явления, свойства преступника, признаки преступного деяния.

Рассмотрим вопрос признаков преступного деяния, который является одним из ключевых в области использования ИИ для прогнозирования преступлений. Ученые пытаются выявить параметры и признаки, связанные с совершением преступлений, для того чтобы определить вероятностную оценку.

Если подходить к оценке преступления как преступного деяния, то построение системы установленных причинно-следственных связей и закономерностей, сопровождающих преступные деяния, позволит дать оценку состояния и вероятного направления его развития. Принимая во внимание, что преступление является конкретным юридическим фактом, он должен обладать определенными закономерностями и признаками, подлежащими оценке.

Т. Н. Долгих считает, что в теории уголовного права, несмотря на сформулированное понятие преступления, вопрос о перечне признаков преступления является дискуссионным, поскольку УК РФ не определяет понятие и виды признаков преступления (Долгих, 2023). С учетом анализа определения, сформулированного в ч. 1 ст. 14 УК РФ, выделяются следующие признаки преступления как деяния: общественная опасность, противоправность, виновность, наказуемость. Эти признаки присущи уже совершенному деянию, у которого в связи с его реальностью можно определить и оценить вышеобозначенные признаки.

ИИ можно доверить оценку только двух признаков: общественной опасности и противоправности. Два других признака – наказуемость и виновность – должны быть оценены только человеком, ИИ в этом случае может дать только рекомендацию, окончательное решение должно принимать уполномоченное лицо.

Например, для получения ответа, является ли смысловая конструкция в Интернете общественно опасной и содержит ли она признаки противоправности, интеллектуальной системе необходимо оценить не только

<sup>20</sup> Westermann, H., Joyce, M., & Dupont, B. (2019). Artificial Intelligence in the Context of Crime and Criminal Justice. Academia. [https://www.academia.edu/40999602/Artificial\\_Intelligence\\_in\\_the\\_Context\\_of\\_Crime\\_and\\_Criminal\\_Justice](https://www.academia.edu/40999602/Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice)

<sup>21</sup> Распоряжение МВД России № 1/37 от 11.01.2022. СПС «КонсультантПлюс». (Документ опубликован не был.)

<sup>22</sup> Комиссаров, В. С., Крылова, Н. Е., Тяжкова, И. М. (ред.) (2012). Уголовное право Российской Федерации. Общая часть: учебник для вузов. Москва: Статут.



смысл текста, но и все связанные с размещением этого текста события, например, провести анализ всей информации, которая размещена на странице социальной сети преступника, его социальных связей, поскольку одна и та же информация может носить различную окраску в зависимости от контекста. Например, словосочетание «я тебя убью» может быть как выражением любви, так и угрозой совершения убийства. Для оценки реальности угрозы интеллектуальные системы должны проанализировать множество данных, оставленных человеком, разместившим текст, – его цифровые следы и цифровые тени (Жарова и др., 2022). В этом случае получаемый результат работы интеллектуальной системы будет отвечать требованию смыслового толкования обстоятельств криминальной ситуации в неразрывной связи со всеми сведениями по делу (Халиков, 2021).

Хотя в целях объективности необходимо отметить, что не существует абсолютно точных технологий и возможны ошибки в оценке данных. Ошибки в оценке данных могут возникать из-за различных факторов, включая неполные данные, недостаточную контекстуальную информацию или проблемы с алгоритмами анализа. Но задача ИИ – не принять решение за уполномоченное лицо, а передать результат своей работы – вероятностную оценку опасности, противоправности и реальности намерений человека, полученную на основе совокупности цифровых данных, уполномоченным органам в области обеспечения безопасности.

Фактически оценка ИИ признаков деяния позволит ответить, можно ли отнести это деяние к преступлению. В случае прогнозирования развития событий необходимо проанализировать совокупность данных, оставленных человеком в Сети. Прогнозирование вероятности совершения преступлений конкретным человеком происходит на основе анализа его криминогенных качеств (Антонян, Аминов, 2019)<sup>23</sup>. В этом случае ИИ анализирует существующие отношения, действия, совершаемые человеком. Результаты работы таких математических моделей уже представлены общественному обсуждению (Завьялов, 2021)<sup>24</sup>.

Таким образом, вопрос отнесения параметров и признаков, которые могут быть подвергнуты вероятностной оценке в контексте прогнозирования преступлений, остается сложным и часто вызывает споры в научном сообществе.

### Оценка ИИ стадий преступления

Возможным этапом оценки преступных деяний является оценка стадий совершения преступлений. С. В. Расторопов считает, что «преступные действия достаточно предсказуемы и прогнозируемы, необходимо лишь правоохранительным органам найти в больших объемах данных эти закономерности» (Расторопов, 2020).

Такой анализ может помочь правоохранительным органам эффективнее предотвращать правонарушения и бороться с преступностью, а также улучшить стратегии противодействия преступлениям.

Для анализа больших данных в целях выявления в них преступных действий можно использовать различные методы машинного обучения, анализа текстов, образов и другие технологии, чтобы выявлять закономерности и предсказывать действия человека. Анализ больших данных может позволить оценить преступные действия на предмет их соответствия стадиям преступления: приготовлению, покушению и оконченому действию. В этом случае ИИ должен оценить вероятность перерастания одной стадии преступления в другую, выявить сопровождающие преступные действия события и явления, распознать их, сравнить полученные данные с другими данными, построить причинно-следственную связь и предотвратить переход стадий преступления в последующие стадии (Жарова, 2022). Хотя оценка стадий возможна не для любых преступлений. Специалисты в области уголовного права считают, что стадии преступлений возможны только для умышленных преступлений<sup>25</sup>. В таком случае закономерен вопрос: может ли ИИ выявить преступный умысел в размещенной информации. Иными словами, может ли ИИ построить вероятностную модель перерастания преступного умысла в совершение преступных действий определенным человеком?

Преступный умысел как отражение преступных намерений может быть выражен посредством телодвижения, слов, символов, фото- и видеоматериалов. Современные возможности ИИ позволяют оценить всю связанную с человеком информацию и выявить, например, в Сети предварительную преступную деятельность.

<sup>23</sup> Малков, В. Д. (2006). Криминология: учебник для вузов (2-е изд., перераб. и доп.). Москва: Юстицинформ.

<sup>24</sup> Cisco Secure Endpoint (AMP for Endpoints). CISCO. [https://www.cisco.com/c/en\\_hk/products/security/amp-for-endpoints/index.html](https://www.cisco.com/c/en_hk/products/security/amp-for-endpoints/index.html)

<sup>25</sup> Парог, А. И. (отв. ред.). (2011). Комментарий к Уголовному кодексу Российской Федерации (постатейный) (7-е изд., перераб. и доп.). Москва: Проспект.

Необходимо оговориться, что, хотя большая часть российских специалистов уголовного права не относят формирование преступного умысла к стадиям преступления (Андрусенко и др., 2012), есть и те, кто считает это нулевой стадией подготовки преступления (Ситникова, 2015; Баев, 2017).

В зарубежной научной литературе ученые представляют результаты своих работ, связанные с выявлением ИИ преступных намерений, умысла по результатам проведенного анализа пользовательского контента на платформах социальных сетей (Vokolo et al., 2023). В проведенном авторами статьи эксперименте использование методов машинного обучения позволило понять и проанализировать настроения пользователей в социальной сети, связанные с возможными преступными действиями. ИИ достаточно точно определил преступные намерения, отраженные в пользовательском контенте, что позволило правоохранительным органам усилить свои упреждающие меры.

Обсуждая возможность предотвращения преступлений, мы должны исходить из того, что распознавание ИИ преступного умысла, выраженного в информации, размещенной в Сети, позволит оценить вероятность перерастания умысла в реальность преступных действий и заблаговременно отправить эту информацию уполномоченным органам в области обеспечения безопасности. Тем самым риск развития преступных действий будет минимизирован, а правоохранительные органы примут соответствующие профилактические меры.

## Заключение

Таким образом, можно сделать вывод, что предупреждение правонарушений содержит формы профилактики и процессуальные формы предупреждения правонарушений. Объединяет эти два подмножества форм принятие мер по устранению обстоятельств, способствующих совершению преступления или других нарушений закона. Однако нужно отметить, что выявление причин и условий, способствующих совершению правонарушений, не входит в подмножество процессуальных форм предупреждения правонарушений.

Процессуальные формы направлены на предотвращение конкретных видов правонарушений, в то время как профилактика в какой-то мере применяет методы предиктивной аналитики, предполагая возможность наступления негативного антисоциального события и используя различные организационные, технологические и правовые инструменты и меры.

Таким образом, прогнозирование преступных действий – это один из этапов предупреждения правонарушений, осуществляемый с использованием методов предиктивной аналитики данных, оставленных человеком. Точность вычислений, проводимых ИИ, с каждым годом увеличивается, в связи с чем растет и точность полученных вероятностей и прогнозов.

Применение ИИ уполномоченными органами охраны правопорядка, их взаимодействие с провайдерами хостинга позволяют не только выявить противоправный и общественно опасный контент, но и оценить вероятность совершения преступления конкретным человеком. Применение ИИ провайдерами хостинга позволит обеспечить профилактику противоправных действий, выявить стадию формирования преступного умысла, выраженного в размещенной им информации, и тем самым минимизировать возможность перерастания умысла в реальность преступных действий.

## Список литературы

Андрусенко, С. П., Голованова, Н. А., Гравина, А. А. (2012). *Международно-правовые стандарты в уголовной юстиции Российской Федерации*: научно-практическое пособие. Москва: ИЗиСП, Анкил.

Антонян, Е. А., Аминов, И. И. (2019). Блокчейн-технологии в противодействии кибертерроризму. *Актуальные проблемы российского права*, 6(103), 167–177. <https://doi.org/10.17803/1994-1471.2019.103.6.167-177>

Баев, О. Я. (2017). Криминалистические методики в реализации доказывания по уголовным делам и совершенствование основ их конструирования. *Законы России: опыт, анализ, практика*, 5, 21–29.

Горбенко, А. О., Мамасуев, А. В. (2008). Применение аналитических систем при принятии управленческих решений в органах внутренних дел (аналитические системы OLAP). *Вестник Академии экономической безопасности МВД России*, 4, 96–99. EDN: NEFKRP.

Громова, Е. А., Петренко, С. А. (2023). Квантовое право: начало. *Journal of Digital Technologies and Law*, 1(1), 62–88. <https://doi.org/10.21202/jdtl.2023.3>

- Долгих, Т. Н. (2024). Признаки преступления в теории уголовного права. *СПС КонсультантПлюс*.
- Жарова, А. К. (2022). Необходимо ли ужесточение требований об обязательном общем мониторинге информации провайдером хостинга? *Труды по интеллектуальной собственности*, 41(2), 21–29. <https://doi.org/10.17323/tis.2022.14439>
- Жарова, А. К., Елин, В. М., Минбалева, А. В. (2022). *Парадигма цифрового профилирования деятельности человека: риски, угрозы, преступления*. Москва: ООО «Русайнс». EDN: DNKVPR.
- Завьялов, И. А. (2021). Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений. *Вестник Московского университета МВД России*, 3, 228–236. EDN: MWOJZD.
- Малков, В. Д. (2014). Предупреждение и профилактика преступлений и иных правонарушений в системе борьбы с преступностью. *Вестник МГЛУ*, 25(711), 78–88.
- Расторопов, С. В. (2020). Использование искусственного интеллекта для предупреждения и выявления преступлений (мировой опыт). *Международное публичное и частное право*, 5, 40–43. EDN: QPDQHX. DOI: <https://doi.org/10.18572/1812-3910-2020-5-40-43>
- Савченко, А. А. (2010). Соотношение понятий профилактики преступлений и предупреждения преступлений в современной юридической доктрине. *Современное право*, 3, 112–114. EDN: MTWGEL.
- Ситникова, А. И. (2015). Глава «Неоконченное преступление» УК РФ и ее законодательно-текстологическое обоснование. *Lex russica*, 11, 83–95. <https://doi.org/10.17803/1729-5920.2015.108.11.083-095>
- Смушкин, А. Б. (2023). Экосистема предварительного расследования. *Актуальные проблемы российского права*, 18(7), 143–158. <https://doi.org/10.17803/1994-1471.2023.152.7.143-158>
- Сретенцев, Д. Н., Волкова, В. Р. (2021). Перспективы внедрения систем искусственного интеллекта в сферу расследования преступлений. *Российский следователь*, 11, 38–42. EDN: HLNQDU.
- Суходолов, А. П., Бычкова, А. М. (2018). Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции. *Всероссийский криминологический журнал*, 12(6), 753–766. [https://doi.org/10.17150/2500-4255.2018.12\(6\).753-766](https://doi.org/10.17150/2500-4255.2018.12(6).753-766)
- Филипова, И. А., Коротеев, В. Д. (2023). Будущее искусственного интеллекта: объект или субъект права? *Journal of Digital Technologies and Law*, 1(2), 359–386. <https://doi.org/10.21202/jdtl.2023.15>
- Халиков, А. Н. (2021). Герменевтические проблемы истолкования криминалистической информации при расследовании уголовных дел. *Российский следователь*, 2, 19–23.
- Яшин, А. А. (2022). Виртуальные технологии в расследовании преступлений: перспективные направления и возможности использования. *Адвокатская практика*, 6, 23–26.
- Bokolo, B. G., Onyehanere, P., Ogegbene-Ise, E., Olufemi, I., & Tettey, J. N. A. (2024). Leveraging Machine Learning for Crime Intent Detection in Social Media Posts. In F. Zhao, D. Miao (Eds.), *AI-generated Content. AIGC 2023. Communications in Computer and Information Science* (Vol. 1946, pp. 224–236). Singapore: Springer. [https://doi.org/10.1007/978-981-99-7587-7\\_19](https://doi.org/10.1007/978-981-99-7587-7_19)
- Navalgund, U. V., & Priyadharshini, K. (2018, December). Crime Intention Detection System Using Deep Learning. In *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)* (pp. 1–6). <https://doi.org/10.1109/iccsdet.2018.8821168>

## References

- Andrusenko, S. P., Golovanova, N. A., & Gravina, A. A. (2012). *International-legal standards in criminal justice of the Russian Federation: scientific and practical tutorial*. Moscow: IZISP, Ankil. (In Russ.).
- Antonyan, E. A., & Aminov, I. I. (2019). Blockchain technologies in countering cyberterrorism. *Actual Problems of Russian Law*, 6(103), 167–177. (In Russ.). <https://doi.org/10.17803/1994-1471.2019.103.6.167-177>
- Baev, O. Ya. (2017). Forensic Techniques in the Implementation of Proof in Criminal Cases and Improve the Basics of its Design. *Laws of Russia: Experience, Analysis, Practice*, 5, 21–29. (In Russ.).
- Bokolo, B. G., Onyehanere, P., Ogegbene-Ise, E., Olufemi, I., & Tettey, J. N. A. (2024). Leveraging Machine Learning for Crime Intent Detection in Social Media Posts. In F. Zhao, D. Miao (Eds.), *AI-generated Content. AIGC 2023. Communications in Computer and Information Science* (Vol. 1946, pp. 224–236). Singapore: Springer. [https://doi.org/10.1007/978-981-99-7587-7\\_19](https://doi.org/10.1007/978-981-99-7587-7_19)
- Dolgikh, T. N. (2024). Signs of crime in the theory of criminal law. *ConsultantPlus*. (In Russ.).
- Filipova, I. A., & Koroteev, V. D. (2023). Future of the Artificial Intelligence: Object of Law or Legal Personality? *Journal of Digital Technologies and Law*, 1(2), 359–386. (In Russ.). <https://doi.org/10.21202/jdtl.2023.15>
- Горбенко, А. О., & Мамасуев, А. В. (2008). The use of analytical systems in making managerial decisions in internal affairs bodies (OLAP analytical systems). *Bulletin of the Academy of Economic Security of the Ministry of Internal Affairs of Russia*, 4, 96–99.
- Gromova, E. A., & Petrenko, S. A. (2023). Quantum law: the beginning. *Journal of Digital Technologies and Law*, 1(1), 62–88. (In Russ.). <https://doi.org/10.21202/jdtl.2023.3>
- Khalikov, A. N. (2021). Hermeneutical problems of interpretation of forensic information in the investigation of criminal cases. *Russian Investigator*, 2, 19–23. (In Russ.).

- Malkov, V. D. (2014). The prevention of crime and other offences in the system of combating crime. *Bulletin of Moscow State Linguistic University*, 25(711), 78–88. (In Russ.).
- Navalgund, U. V., & Priyadharshini, K. (2018, December). Crime Intention Detection System Using Deep Learning. In *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)* (pp. 1–6). <https://doi.org/10.1109/iccsdet.2018.8821168>
- Rastoropov, S. V. (2020). The use of artificial intelligence for crime prevention and identification (the world experience). *International Public and Private Law*, 5, 40–43. (In Russ.). <https://doi.org/10.18572/1812-3910-2020-5-40-43>
- Savchenko, A. A. (2010). Correlation between the notions of crime prophylactics and crime prevention in the modern legal doctrine. *Modern law*, 3, 112–114. (In Russ.).
- Sitnikova, A. I. (2015). Chapter “Uncompleted crime (inchoate crime)” of the CC RF and its legislative and textual justification. *Lex russica*, 11, 83–95. (In Russ.). <https://doi.org/10.17803/1729-5920.2015.108.11.083-095>
- Smushkin, A. B. (2023). Ecosystem of preliminary investigation. *Actual Problems of Russian Law*, 18(7), 143–158. (In Russ.). <https://doi.org/10.17803/1994-1471.2023.152.7.143-158>
- Sretensev, D. N., & Volkova V. R. (2021). Prospects for the introduction of artificial intelligence systems in crime investigation. *Russian Investigator*, 11, 38–42. (In Russ.).
- Sukhodolov, A. P., & Bychkova, A. M. (2018). Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution. *Russian Journal of Criminology*, 12(6), 753–766. (In Russ.). [https://doi.org/10.17150/2500-4255.2018.12\(6\).753-766](https://doi.org/10.17150/2500-4255.2018.12(6).753-766)
- Yashin, A. A. (2022). Virtual technologies in the investigation of crimes: promising directions and possibilities of use. *Law Practice*, 6, 23–26. (In Russ.).
- Zavyalov, I. A. (2021) Foreign experience of using artificial intelligence in solving crimes. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 3, 228–236. (In Russ.).
- Zharova, A. K. (2022). Is it necessary to tighten the requirements for mandatory general monitoring of information by hosting providers? *Works on Intellectual Property*, 41(2), 21–29. (In Russ.). <https://doi.org/10.17323/tis.2022.14439>
- Zharova, A. K., Elin, V. M., & Minbaleev, A. V. (2022). *The paradigm of digital profiling of human activity: risks, threats, crimes*. Moscow: Rusains Limited Liability Company. (In Russ.).
- 

## Вклад автора

Автор подтверждает, что полностью отвечает за все аспекты представленной работы.

## Author's contribution

The author confirms sole responsibility for all aspects of the work.

## Конфликт интересов / Conflict of Interest

Автором не заявлен / No conflict of interest is declared by the author

## История статьи / Article history

Дата поступления / Received 02.04.2024

Дата одобрения после рецензирования / Date of approval after reviewing 12.05.2024

Дата принятия в печать / Accepted 20.05.2024