Научная статья
УДК 343.98

Киберпреступления, совершаемые несовершеннолетними: причины, способы, профилактика

Илона Анатольевна Макаренко, доктор юридических наук, профессор

Уфимский университет науки и технологий
Уфа (450076, ул. Заки Валиди, д. 32), Российская Федерация
ilona475@mail.ru
https://orcid.org/0009-0003-4853-6736

Аннотация:
Введение. *Современный этап развития общества характеризуется повсеместным использованием информационных технологий во всех сферах деятельности. Не стала исключением и преступная деятельность, анонимность которой в настоящее время довольно просто обеспечить с помощью различных технических средств. Широкая распространенность киберпреступлений и отчасти шаблонность их совершения способствуют вовлечению в незаконную деятельность несовершеннолетних, что ставит под угрозу не только дальнейшее становление их как личности, формирование и закрепление в сознании негативных социальных установок, но и расширяет круг правонарушителей, оказывая деструктивное воздействие на состояние общества. Особое внимание в статье уделяется причинам совершения киберпреступлений несовершеннолетними правонарушителями и наиболее распространенным способам реализации ими преступных действий. Отмечается необходимость дальнейших исследований закономерностей криминальных деяний в этой сфере, формулирования предложений по их раскрытию и расследованию, осуществления комплекса профилактических мер.*
Методы. *При подготовке статьи использовались соответствующие поставленной цели научные методы – анализ, обобщение, классификация, моделирование.*
Результаты. *В работе раскрыты актуальные на данный момент причины совершения несовершеннолетними преступлений в области информационно-телекоммуникационных технологий, учитывая которые, необходимо предпринять комплекс мер в целях профилактики противоправного поведения данной категории граждан, показана необходимость дальнейшей разработки методики расследования этого вида преступных деяний. Отмечено, что необходим комплекс мер для профилактики рассматриваемых преступлений – внесение изменений в законодательство, объяснение уголовно-правового запрета (для развенчания ореола высокопрофессионального хакера, способного управлять информационными технологиями или цифровой вселенной), общественный и родительский контроль за действиями подростков в социальных сетях и др.*

Ключевые слова:
киберпреступления, компьютерные преступления, несовершеннолетний правонарушитель, способы совершения киберпреступлений, меры профилактики

Для цитирования:
Макаренко И. А. Киберпреступления, совершаемые несовершеннолетними: причины, способы, профилактика // Вестник Санкт-Петербургского университета МВД России. 2025. № 3 (107). С. 136–141.

Статья поступила в редакцию 25.06.2025; одобрена после рецензирования 29.08.2025; принята к публикации 25.09.2025.

Original article

Cybercrime committed by minors: causes, methods, prevention

Ilona A. Makarenko, Doc. Sci. (Jurid.), Professor

Ufa University of Science and Technology
32, Zaki Validi str., Ufa, 450076, Russian Federation
ilona475@mail.ru
https://orcid.org/0009-0003-4853-6736

Abstract:
Introduction. *The current stage of societal development is characterised by the widespread use of information technology in all areas of activity. Criminal activity has not been exempt from this process, as its anonymity can now be easily ensured through various technical means. Due to the widespread occurrence of cybercrimes and their often standardised modus operandi, minors are increasingly involved in illegal activities. This poses a threat not only to their ongoing personal maturation and the development of negative social orientations in their minds, but also expands*

Keywords:
cybercrime, computer crime, minor offender, methods of committing cybercrime, preventive measures.

ISSN 2949-1150 (online)
2071-8284 (print)

the scope of individuals engaged in criminal conduct causing detrimental effects on the state of society. The author pays particular attention to the reasons why minors commit cybercrimes as well as to the most common methods they use to carry out their criminal activities. The author points out the need for further work concerning criminal schemes in this area, developing proposals for their detection and investigation, and implementing a set of preventative measures.

Methods. *The preparation of this article involved the application of scientific methods relevant to the research's purpose, including analysis, generalisation, classification and modelling.*

Results. *The research reveals the current reasons for committing crimes in the field of information and telecommunications technologies by minors. Taking these reasons into account, it is necessary to take a set of measures to prevent unlawful behaviour by this group of citizens. The research also demonstrates the need for further development of methods for investigating this type of criminal activity. The author stresses the importance of a comprehensive set of measures for preventing crimes in question, such as amending legislation, explaining criminal law prohibitions (for debunking the myth of highly professional hackers capable of controlling information technologies or the digital universe), public and parental monitoring of teenagers' activities on social media, etc.*

For citation:
Makarenko I. A. Cybercrime committed by minors: causes, methods, prevention // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 3 (107). P. 136–141.

The article was submitted June 25, 2025; approved after reviewing August 29, 2025; accepted for publication September 25, 2025.

Введение

Сегодня мы уже не можем представить себе существования без использования информационных технологий, которыми пользуемся повсеместно во всех сферах деятельности. Однако приходится констатировать, что интернет и различные технические средства используются не всегда во благо. В условиях растущей зависимости общества от информационных технологий пропорционально растут угрозы компьютерных атак, краж цифровых данных, кибертерроризма и т. п. При этом большинство киберпреступлений носит международный характер, а на катастрофичность их последствий западные ученые указывали более 20 лет назад, описывая как случайные, так и преднамеренные инциденты информационной безопасности, показывая различие между традиционными угрозами и новыми опасностями, исходящими от киберпреступников [1, с. 28].

Только в России в январе–мае 2025 года зарегистрировано 308,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 1,3 % больше, чем за аналогичный период прошлого года[1]. При этом с каждым годом растет количество таких преступлений, совершенных несовершеннолетними или при их соучастии. Аналогичная тенденция активного вовлечения несовершеннолетних в киберпреступность отмечается и учеными, что обусловлено такими привлекательными особенностями интернета, как обеспечение анонимности действий, возможность нейтрализации средств защиты информационной безопасности, сокрытие следов преступной деятельности и пр. [2, с. 144].

Исследование причин совершения несовершеннолетними преступлений с использованием компьютерных технологий, безусловно, является одним из звеньев формирования криминалистической характеристики указанных преступлений, совершаемых этой категорией лиц, выдвижения версий при расследовании преступлений, справедливого наказания виновных в совершении преступлений и главное – своевременного принятия превентивных мер. Несовершеннолетние – будущее нашего общества, и от того, насколько их противоправные действия будут своевременно пресекаться, раскрываться и наказываться, зависит распространение киберпреступлений в будущем.

Методы

При подготовке статьи использовались соответствующие поставленной цели научные методы – анализ научной литературы, статистической информации, обобщение имеющихся разработок в исследуемой области, классификация способов совершения преступлений с использованием информационно-телекоммуникационных технологий, моделирование возможных последствий от рассматриваемых преступных деяний и способов их предотвращения.

Результаты

В. Н. Карагодин отмечает, что «именно подростки приобретают достаточные умения по использованию в различных целях цифровых технологий. Бесконтрольное ознакомление с компьютерной информацией у ряда подростков усиливает желание, хоть временно оторваться от повседневности, представляющейся им скучной и неинтересной. Будничным занятиям они предпочитают общение на привлекательные темы с малоизвестными людьми, ознакомление

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - май 2025 года // Министерство внутренних дел Российской Федерации : [официальный сайт]. URL: https://мвд.рф/reports/item/66517593 (дата обращения: 10.07.2025).

с информацией о возможности нарушения установленных запретов, в том числе и влекущих уголовное наказание» [3, с. 82]. По существу, современные подростки уже с раннего детства погружены в виртуальное пространство, причем многие не просто пользуются гаджетами для развлечения и решения примитивных задач, а глубоко погружены в возможности использования программного обеспечения, в создание самих программ – и не всегда законных. Мы согласны с учеными [4, с. 175; 5, с. 2], которые считают, что раннее знакомство с электронными устройствами и цифровыми сервисами, возможность самостоятельно действовать в цифровом пространстве становятся факторами для формирования личности несовершеннолетнего киберпреступника.

В связи с этим задача изучения личности несовершеннолетнего преступника продолжает оставаться актуальной. Кроме обстоятельств, подлежащих доказыванию в соответствии со ст. 73 Уголовно-процессуального кодекса Российской Федерации[2] (далее – УПК РФ), в отношении несовершеннолетнего существуют дополнительные, перечисленные в ст. 421 УПК РФ: возраст, число, месяц и год рождения; условия жизни и воспитания несовершеннолетнего, уровень психического развития и иные особенности его личности; влияние на несовершеннолетнего старших по возрасту лиц. Изучая личность несовершеннолетнего, совершающего преступления с использованием информационных технологий, важной представляется информация о его практических навыках и умениях в использовании компьютерных технологий. Безусловно, имеет значение умысел подростка и понимание совершаемых действий как преступных. Нередко их используют вслепую либо внушают, что совершаемые ими действия не являются противозаконными, более того, совершив их, он докажет свои способности хакера, что принесет известность и уважение среди сверстников.

Современные подростки во многом отличаются от своих сверстников, живших ранее. Социально-экономическое развитие общества не могло не отразиться на их формировании, равно как и повсеместное внедрение интернета в их жизнь. Живое общение чаще стало заменяться виртуальным, а контроль родителей за тем, с кем и о чем общается ребенок, максимально снижен. Родители чаще всего заняты на работе либо решают личные проблемы. Слабый контроль за детьми объясняется также тем, что взрослое поколение в меньшей степени осведомлено о возможностях компьютерных технологий и пользуются компьютером исключительно как средством обмена данными, просмотра новостей, набора текста или для компьютерных игр. В связи с этим родители часто не обладают необходимым комплексом знаний, чтобы разобраться в тонкостях использования ребенком информационно-телекоммуникационных сетей и технологий. Соответственно, бесконтрольность влечет за собой свободу действий и возможность несовершеннолетним совершать противоправные действия, в т. ч. связанные с использованием информационных технологий.

Кроме объективных факторов, способствующих изменению личностных характеристик современных несовершеннолетних, сохраняются и субъективные факторы, характеризующие подростковый возраст и основанные на физиологических его особенностях. Склонность подростков к принятию необдуманных решений, желание самоутвердиться, повышенная восприимчивость к стороннему влиянию – все эти обстоятельства всегда способствовали вовлечению подростков в преступную деятельность, эти обстоятельства и в настоящее время играют ключевую роль в вовлечении несовершеннолетних в совершение киберпреступлений. Кроме того, возможность быстро заработать деньги и оставаться обезличенным еще более обостряет желание совершать противозаконные действия. Психологические факторы совершения подростками преступлений по большому счету со временем не меняются. Детям свойственно любопытство и желание испытать новые ощущения, проверить свои способности, приобрести опыт, при этом испытать чувство гордости и своей значимости. Уверенность, что они останутся безнаказанными, а их действия не причинят никому серьезных последствий, только сильнее мотивирует к совершению преступлений.

Можно отметить, что причины, по которым несовершеннолетние все чаще совершают преступления в сфере информационных технологий, весьма разнообразны и обусловлены как социально-экономическими, так и психологическими факторами.

Низкая осведомленность о последствиях неправомерных действий также является одной из причин необдуманных действий несовершеннолетних, а наблюдая за успешными действиями друзей или знакомых, подростки с удовольствием им подражают ради самовыражения и самоутверждения среди сверстников. Несовершеннолетние убеждены, что идентифицировать их в виртуальном пространстве невозможно, что они остаются анонимными и поэтому уверены, что правоохранительные органы не смогут обнаружить следы их действий и доказать причастность к ним.

С сожалением необходимо признать, что в некотором роде уверенность подростков в безнаказанности подтверждается и статистическими данными. Из 308 тыс. совершенных с января по май 2025 года преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, раскрыто только 82 893 преступления – меньше трети[3].

---

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 07.06.2025) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2001. № 52. (ч. I). Ст. 4921.

[3] URL: https://мвд.рф/reports/item/66517593 (дата обращения: 10.07.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

К наиболее распространенным незаконным действиям несовершеннолетних в области информационных технологий, по мнению П. Г. Смагина, можно отнести:

1. Получение неправомерного доступа к охраняемой законом информации. Например, взлом баз данных или систем хранения конфиденциальной информации, включая личные и финансовые сведения пользователей.

2. Взлом аккаунтов в социальных сетях. Это может включать похищение персональных данных, личной информации или использование взломанных страниц для распространения спама, фишинга и другой противоправной деятельности.

3. Совершение кибератак. Речь идет о воздействии на серверы веб-ресурсов либо информационные системы с целью их блокировки, модификации данных или нанесения вреда владельцам.

4. Создание, использование и распространение вредоносных программ. Это одна из наиболее опасных сфер, т. к. такие действия способны причинить ущерб как частным лицам, так и организациям.

5. Нарушение авторских, смежных, изобретательских и патентных прав. Незаконное использование чужой интеллектуальной собственности, впоследствии распространяемой, например, на торрент-трекерах, причиняет существенный вред правообладателям.

6. Публикация оправдывающей терроризм или экстремизм информации. Подростки могут размещать подобные материалы на своих страницах в социальных сетях, зачастую не осознавая всех юридических последствий таких действий.

7. Несанкционированный доступ к игровым ресурсам. Попытки взломать игровые аккаунты для получения виртуальных ценностей или преимущества в игре становятся все более частым явлением.

8. Кибертравля. Преследование и унижение сверстников в интернете становится одним из самых серьезных социальных вызовов для образовательных учреждений и родителей [6, с. 4]. При этом случаи кибербуллинга среди несовершеннолетних становятся распространяются все шире, а подростки в подобных инцидентах играют двойную роль – как преступников, так и жертв [7, с. 763]. И именно дети чаще, чем взрослые, участвуют в кибербуллинге [8, с. 20].

Чтобы доказать причастность лица к совершению преступления одним из перечисленных способов, необходимо обладать цифровой грамотностью, знать закономерности осуществления преступных действий и способы фиксации следов преступления. Поэтому в настоящее время необходимы новые исследования в области расследования преступлений с использованием информационно-телекоммуникационных технологий.

Необходимо отметить, что в литературе все чаще встречается анализ закономерностей преступной деятельности в рассматриваемой сфере. Например, глубокие исследования проводятся З. И. Харисовой, которой разработаны криминалистические характеристики рассматриваемых видов преступлений, предложен алгоритм действий следователя при обнаружении их признаков в различных следственных ситуациях и др. [9; 10]. Но научных исследований в этой области для повышения квалификации практических работников еще недостаточно.

По замечанию С. В. Глазатовой, «при расследовании данного вида преступлений возникает много трудностей. В качестве негативных причин следует выделить специфические особенности несовершеннолетних преступников, отсутствие методик расследования киберпреступлений и необходимых норм процессуального права, регулирующих действия участников процесса расследования, а также порой и недостаточный уровень подготовки следователей» [11, с. 7].

В связи с этим интересным представляется предложение А. А. Бессонова, который считает целесообразным «создание специализированного госоргана по кибербезопасности, в полномочия которого войдет координация деятельности всех других государственных органов по обеспечению кибербезопасности и противодействию киберпреступности, учёт информации обо всех имевших место киберинцидентах и преступлениях, а также обеспечение государственно-частного партнёрства в обозначенной сфере»[4].

Кроме того, перспективы повышения эффективности борьбы с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, по мнению Е. А. Астаховой, связаны с рядом направлений, к которым относится совершенствование законодательной базы, межведомственного и международного сотрудничества, подготовка квалифицированных кадров и повышение профессионального уровня всех практических работников, принятие профилактических мер [12, с. 56].

Для профилактики совершения киберпреступлений необходима совместная деятельность не только государственных и образовательных учреждений, но и ученых, специалистов в области IT-технологий, семьи.

В настоящее время происходит постоянное совершенствование законодательства с учетом современных реалий использования компьютерных технологий. Например, в Уголовный кодекс

[4] Криминалистика для правосудия будущего : доклад Ректора Московской академии Следственного комитета Российской Федерации имени А. Я. Сухарева А. А. Бессонова // Фонд «Росконгресс» : [сайт]. URL: https://roscongress.org/sessions/splf-2025-delovaya-programma-kriminalistika-dlya-pravosudiya-budushchego/discussion (дата обращения: 10.07.2025).

Российской Федерации[5] совсем недавно были внесены изменения, направленные на противодействие вовлечению несовершеннолетних в схему дропперства[6]. За продажу банковских карт введена уголовная ответственность, банкам будет запрещено выдавать карты несовершеннолетним без согласия их родителей. Новое ограничение призвано защитить несовершеннолетних от втягивания в мошеннические схемы.

Кроме того, в целях недопущения неоднозначного толкования банками норм гражданского законодательства в части использования банковских счетов несовершеннолетними в возрасте от 14 до 18 лет предлагается внесение изменений в Гражданский кодекс Российской Федерации (далее – ГК РФ), устанавливающих запрет на открытие на имя несовершеннолетних детей банковских счетов без согласия их законных представителей[7].

Внесение изменений в ГК РФ позволит предотвратить совершение в отношении несовершеннолетних противоправных действий с использованием их банковских счетов, а несовершеннолетним в возрасте от 14 лет после трудоустройства в полной мере реализовывать свои трудовые права, в т. ч. право на получение заработка на банковском счете[8].

Ученые, внося свой вклад в разработку профилактических мер по предотвращению киберпреступлений, совершаемых несовершеннолетними, предлагают, например, следующие меры борьбы:

1. «Закрепить минимальный возраст уголовной ответственности киберпреступников в зависимости от тяжести и социального масштаба совершенного преступления с 14 лет.

2. Закрепить процессуальный порядок обыска, изъятия и представления в качестве доказательств материалов из сети «Интернет» и ее сервисов: социальных сетей, мессенджеров, а также иных информационных ресурсов. Особо обратить внимание на проведение данных действий в отношении несовершеннолетнего подозреваемого, обвиняемого в киберпреступлении.

3. Разработать и создать методику процесса расследования киберпреступлений, в которой необходимо учесть психологические и процессуальные особенности работы с несовершеннолетними, указав акцентирующие моменты и дополнительные возможности проведения следственных действий.

4. Ввести предлагаемую в других странах Программу родительского контроля, включающую ограничение доступа ребенка в интернет на определенные сайты и контенты, а также меры психологического надзора» [11, с. 7].

В зарубежных источниках также проводятся исследования механизма профилактики и контроля вовлечения несовершеннолетних в IT-мошенничество [13, с. 1552].

Заключение

Несмотря на проделываемую работу в области профилактики киберпреступлений, есть много направлений, которые необходимо корректировать. Например, в Узбекистане родители не просто должны дать согласие на открытие несовершеннолетними банковских счетов, а имеют право на получение информации о подозрительных операциях, совершаемых несовершеннолетними, в т. ч. в банковской сфере [14, с. 811]. Полагаем, что такое нововведение в российское законодательство только усилит родительский контроль над действиями несовершеннолетних.

Наряду с принимаемыми мерами профилактики необходимо продолжать разрабатывать наиболее действенные механизмы расследования преступлений с привлечением специалистов в этой области не только для применения технико-криминалистических средств, но и для оказания помощи в допросах несовершеннолетних киберпреступников, привыкших к специфическому сленгу. Если следователь, глубоко не разбирающийся в тонкостях рассматриваемых преступлений, сразу покажет свою некомпетентность, это окажет влияние не только на установление психологического контакта, но и, безусловно, отразится на получаемых показаниях, их полноте и достоверности. О важности профессиональной подготовки сотрудников правоохранительных органов свидетельствует, например, обстановка с киберпреступностью в Индии. В настоящее время там отсутствует надлежащее правовое обеспечение систем информационно-телекоммуникационных технологий, напрочь отсутствует подготовка специалистов в области «права» и «киберправа» и как следствие – наблюдается рост киберпреступности [15, с. 129]. Чтобы предотвратить такие последствия, необходимо планомерно осуществлять комплекс мер, о которых сказано выше.

[5] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.04.2025) // СЗ РФ. 1996. № 25. Ст. 2954.

[6] О внесении изменений в статью 187 Уголовного кодекса Российской Федерации : Федеральный закон от 24 июня 2025 г. № 176-ФЗ // СЗ РФ. 2025. № 26 (ч. I). Ст. 3506.

[7] О внесении изменений в часть первую и статью 846 части второй Гражданского кодекса Российской Федерации : Федеральный закон от 24 июня 2025 г. № 178-ФЗ // СЗ РФ. 2025. № 26 (ч. I). Ст. 3508.

[8] Пояснительная записка к законопроекту № 579819-8 «О внесении изменений в часть первую и статью 846 части второй Гражданского кодекса Российской Федерации (уточнение условий заключения договора банковского счета с несовершеннолетними в возрасте от 14 до 18 лет)» // Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество») : [официальный сайт]. URL: https://sozd.duma.gov.ru/bill/579819-8 (дата обращения: 10.07.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

Список источников

1. *Furnell S. M., Warren M. J.* Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium // Computers & Security. 1999. Vol. 18, No. 1. P. 28-34. https://doi.org/10.1016/s0167-4048(99)80006-6

2. *Joshi S., Singh S., Sharma M.* Cybercrime by Minors. // Roy P. K., Tripathy A. K. (Ed.) Cybercrime in Social Media : Theory and Solutions. New York : Chapman and Hall/CRC, 2023. P. 143–166. https://doi.org/10.1201/9781003304180

3. *Карагодин В. Н.* О некоторых современных особенностях преступлений, совершенных в отношении несовершеннолетних // Вестник Московского университета МВД России. 2024. № 1. С. 80–86. https://doi.org/10.24412/2073-0454-2024-l-80-86

4. *Федосеева О. И.* Психологические особенности формирования личности несовершеннолетнего киберпреступника // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. №. 4. С. 174-178. https://doi.org/10.36511/2078-5356-2022-4-174-178

5. *Хараrбахова М. А., Мусатова О. А., Шпагина Е. М.* Интернет и одиночество подростков // Психология и право. 2021. Т. 11. № 4. С. 2–13. https://doi.org/10.17759/psylaw.2021110401

6. *Смагин П. Г.* К вопросу о преступлениях, совершаемых несовершеннолетними с использованием информационных технологий // Социальная политика и народосбережение : [сетевое издание]. 2024. Т. 3, № 2. С. 1–10. URL: https://spnjournal.ru/04spn224.html.

7. *Cai Y.* Research on the Social Media Presentation of Juvenile Cybercrime: A Case Study of Cyberbullying / Samsilah R. [et al.] (Eds.) Catherine Lee Cheng Ean Proceedings of the 2nd International Conference on Educational Development and Social Sciences (EDSS 2025). Zhengzhou : Atlantis Press China, 2025. P. 762–768. https://doi.org/10.2991/978-2-38476-400-6_89

8. *Bahl S., Punia M.* Juvenile digital delinquency: A Comprehensive Analysis of Distinctive Behavioural Traits, Motivational Factors, and Societal Implications of Cyber Offenses Committed by Young Individuals / Sharma H. [et al.] (Eds.) Innovative Multidisciplinary Approaches to Global Challenges: Sustainability, Equity, and Ethics in an Interconnected World (IMASEE-2025). Paris : Atlantis Press, 2025. P. 19–41. https://doi.org/10.2991/978-2-38476-416-7_3

9. *Харисова З. И.* Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации // Правовое государство: теория и практика. 2025. № 2. С. 96–105. https://doi.org/10.33184/pravgos-2025.2.11

10. *Харисова З. И.* Информационно-компьютерная криминалистическая модель преступления, связанного с нарушением правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования сети «Интернет» и сети связи общего пользования: теоретико-прогностический подход // Вестник Института права Башкирского государственного университета. 2025. № 2 (26). С. 205–221. https://doi.org/10.33184/vest-law-bsu-2025.26.18

11. *Глазатова С. В., Бурцева Е. В., Медведева С. В.* Киберпреступления, совершаемые несовершеннолетними: проблемы расследования // Российский следователь. 2021. № 2. С. 7–10. https://doi.org/10.18572/1812-3783-2021-2-7-10

12. *Астахова Е. А.* Перспективы противодействия использованию информационно-коммуникационных технологий в преступных целях // Правовая политика и правовая жизнь. 2025. №. 1. С. 56–64. https://doi.org/10.24412/1608-8794-2025-1-56-64

13. *Ma Y., Liu Y., Wang H.* Study on the Prevention and Control Mechanism for Minors' Involvement in Telecom and Online Fraud / Zhan Z. [et al.] (Eds.) Proceedings of the 2024 10th International Conference on Humanities and Social Science Research (ICHSSR 2024). Zhengzhou : Atlantis Press China, 2024. P. 1551–1564. https://doi.org/10.2991/978-2-38476-277-4_173

14. *Qosimov S.* State Policy and Legal Approach to Combating Crimes Committed Through Information Technologies: Analysis and Proposals // International Journal of Artificial Intelligence. 2025. Vol. 4, No. 1. P. 807–811. URL: https://inlibrary.uz/index.php/ijai/article/view/99045.

15. *Kaur M. M., Manpreet M. H., Kaur M. H.* Judiciary's Role in the Prevention and Prosecution of Cybercrimes Against Women // ShodhPatra: International Journal of Multidisciplinary Studies. 2025. Vol. 2. Is. 1. P. 116–130. https://doi.org/10.70558/SPIJSH.2025.v2.i1.25101