Научная статья
https://doi.org/:10.29039/2312-7937-2025-4-140-144
EDN: https://elibrary.ru/rvoply

ТУТОВА ОЛЬГА ВАСИЛЬЕВНА
кандидат педагогических наук, доцент
Крымский филиал Краснодарского университета МВД России
(Симферополь, Россия)
tutova-ov@yandex.ru
SPIN-код: 7896-5001
https://orcid.org/0009-0001-5023-8119

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. *В статье отмечено, что развитие информационно-коммуникационных технологий способствует возникновению новых видов преступлений. Быстрое преобразование форм преступной деятельности, а также появление новых видов и методов совершения преступлений в этой области приводит к тому, что система противодействия преступлениям в сфере информационно-коммуникационных технологий сталкивается с системными проблемами, требующими комплексного решения.*

Анализ современного состояния противодействия киберпреступности, в том числе статистический анализ, позволил автору выделить основные проблемы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Автором приведены их авторские классификации: по отношению к деятельности уполномоченных субъектов и по сферам возникновения и характеру влияния на систему противодействия рассматриваемой категории преступлений.

В статье проанализированы причины возникновения проблем противодействия IT-преступности, рассматриваются вопросы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, описываются некоторые современные проблемы противодействия IT-преступности.

Ключевые слова: *IT-преступление, информационно-коммуникационные технологии, проблемы противодействия преступности, пути противодействия преступности*

Для цитирования: *Тутова О.В. Современные проблемы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Вестник ВИПК МВД России. 2025. № 4 (76). С. 140–144; https://doi.org/:10.29039/2312-7937-2025-4-140-144.*

TUTOVA OLGA V.
PhD in Pedagogics, Associate Professor
Crimean Branch of the Krasnodar University of the Ministry of Internal Affairs of Russia
(Simferopol, Russia)

ACTUAL PROBLEMS OF COUNTERACTION TO CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract. *The article notes that the development of information and communication technologies contribute to the emergence of new types of crimes. The rapid transformation of forms of criminal activity, as well as the emergence of new types and methods of committing crimes in this area, leads to the fact that the system of countering crimes in the field of information and communication technologies is facing systemic problems that require a comprehensive solution.*

The analysis of the current state of countering cybercrime, including statistical analysis, allowed the author to identify the main problems of countering crimes committed using information and communication technologies. The author presents their author's classifications: in relation to the activities of authorized entities and by the scope and nature of their impact on the system of countering the category of crimes under consideration.

The article analyzes the causes of the problems of countering IT crime, examines the issues of countering crimes committed using information and communication technologies, and describes some modern problems of countering IT crime.

Keywords: *IT crime, information and communication technologies, problems of crime prevention, ways of crime prevention*

For citation: *Tutova O.V. Actual problems of counteraction to crimes committed using information and communication technologies // Vestnik Advanced Training Institute of the MIA of Russia. 2025. № 4 (76). P. 140–144; https://doi.org/:10.29039/2312-7937-2025-4-140-144.*

Развитие информационно-коммуникационных технологий, улучшение инструментов и методов общения между людьми, а также широкое применение электронных платежных систем не только способствуют улучшению социальной коммуникации и облегчают гражданам доступ к их финансовым средствам, но и создают условия для появления новых видов преступлений, которые не ограничиваются территориальными рамками.

Широкое внедрение информационно-коммуникационных технологий вызывает быстрое преобразование форм преступной деятельности, а также появление новых видов и методов совершения преступлений в этой области. Современное состояние киберпреступности характеризуется не только количественным ростом, но и качественными изменениями – появлением новых форм противоправной деятельности, усложнением методов совершения преступлений (в том числе методов социальной инженерии) и расширением географии киберугроз. При этом система противодействия данным видам преступлений сталкивается с системными проблемами, требующими комплексного решения.

Анализ статистических показателей преступности в Российской Федерации в период с 2018 по 2024 год указывает на цифровую трансформацию преступности в целом.

Доля преступлений, совершённых с использованием информационно-коммуникационных технологий, в общей структуре преступности в 2018 году составляла всего 8,8%, к концу 2024 года – увеличилась до 40%.

Структура IT-преступности в 2024 году на 49,7% представлена мошенничествами, 15,4% составляют преступления в сфере незаконного оборота наркотических средств, по 13,8% занимают кражи и преступления в сфере компьютерной информации, на иные составы приходится всего 7,3%. Таким образом, кражи и мошенничества рассматриваемой категории составляют 63,5% от структуры IT-преступности[1].

Анализ современного состояния противодействия киберпреступности, в том числе статистический анализ, позволяет выделить несколько ключевых тенденций.

Во-первых, наблюдается устойчивый рост количества преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее – IT-преступления). При этом латентность такого вида преступлений достаточно высока, а эффективность раскрытия преступлений остается сравнительно низкой [5, с. 165–170].

Во-вторых, появление новых видов и способов совершения IT-преступлений напрямую связано с протекающими в современном обществе процессами цифровизации и технологизации.

В-третьих, противодействие IT-преступности определяет необходимость подготовки и постоянного совершенствования профессиональных компетенций сотрудников, специализирующихся на выявлении, предупреждении, раскрытии и расследовании рассматриваемых преступлений.

В-четвертых, совершенствование программных и аппаратных средств информационных технологий расширяет для злоумышленников возможности анонимизации в глобальном информационном пространстве, обеспечивая высокий уровень анонимности при доступе к информации и использовании различных коммуникационных каналов связи.

Все это обуславливает актуальность противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, и важность рассматриваемых проблем.

Кроме того, наряду с традиционными (мошенничества, кражи с банковских счетов) появляются новые формы IT-преступлений, связанные с использованием криптовалюты при осуществлении легализации преступных доходов, а также искусственно-

[1] URL: https://мвд.рф/reports/item/60248328.

го интеллекта при совершении преступлений [1, с. 75–78].

В рамках проведенного нами опроса, касающегося противодействия преступлениям, совершаемым с спользованием информационно-коммуникационных технологий, проанкетированы 112 сотрудников оперативных подразделений (подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий, подразделений уголовного розыска и подразделений по контролю за оборотом наркотиков) органов внутренних дел из 8 субъектов Российской Федерации (Брянская область, Оренбургская область, Кемеровская область – Кузбасс, Республика Бурятия, Республика Хакасия, Республика Крым, Республика Тыва, г. Москва), имеющих опыт работы в оперативных подразделениях по линии противодействия IT-преступлениям.

Из опрошенных респондентов 43,8% сотрудников оценили эффективность противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, в своем подразделении (регионе) как низкую или крайне низкую, 46,4% – как среднюю и всего 10,7% – как высокую.

Таким образом, поверхностный анализ результатов экспертных оценок эффективности противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, позволяет сделать вывод о том, что проблемы в рассматриваемой области имеют место быть и требуют тщательного исследования для выработки наиболее оптимальных методов их решения.

Подходы к классификации проблем противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, достаточно многообразны, что обусловлено как высокой динамикой изменения преступности в направлении цифровизации, так и рядом субъективных факторов, возникающих в процессе осуществления оперативно-служебной деятельности соответствующими субъектами противодействия IT-преступлениям.

По отношению к деятельности уполномоченных субъектов проблемы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, можно разделить: *на объективные и субъективные*.

Как справедливо отмечает С.В. Дырма, к числу объективных проблем можно отнести высокий уровень анонимизации пользователей в сети Интернет, экстерриториальный характер преступности, использование средств электронной коммерции при реализации объективной стороны преступления и т.п. [2, с. 73–81].

К субъективным проблемам следует отнести низкий уровень профессиональной квалификации сотрудников, специализирующихся в области противодействия IT-преступлениям, низкий уровень мотивации данных сотрудников, сопутствующие проблемы кадрового обеспечения и др.

В рамках данного исследования предлагаем рассмотреть один из наиболее обоснованных и практически значимых, на наш взгляд, подходов к классификации рассматриваемых проблем. По сферам возникновения и характеру влияния на систему противодействия предлагаем классифицировать проблемы на три основные категории:

1. Правовые проблемы – связаны с несовершенством законодательства, пробелами в нормативном регулировании, сложностями правоприменения.

2. Организационные проблемы – обусловлены недостатками в структуре, управлении, ресурсном обеспечении субъектов противодействия.

3. Тактические проблемы – касаются методов, технологий и практических механизмов выявления, пресечения, раскрытия и расследования IT-преступлений.

Представленный подход базируется на системном анализе деятельности правоохранительных органов и иных субъектов противодействия IT-преступности. Он позволяет не только дифференцировать проблемы по уровням их решения (законодательный, управленческий, оперативно-практический), но и определить приоритетные направления совершенствования системы противодействия IT-преступлениям, а также обеспечить комплексный подход к разработке разноплановых мер противодействия.

Правовые проблемы возникают из-за несоответствия нормативной базы динамично развивающимся киберугрозам. Они требуют изменений на уровне законов, подзаконных актов и судебной практики.

Современная система противодействия киберпреступности в России включает широкий круг субъектов – от специализированных подразделений правоохранительных органов до частных компаний в сфере информационной безопасности. Однако ее эффективность ограничивается рядом системных проблем. Прежде всего, это необходимость совершенствования нормативно-правового регулирования. Несмотря на наличие в Уголовном кодексе РФ[1] статей, предусматривающих ответственность

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс»: [сайт] (дата обращения: 02.07.2025).

за преступления в сфере информационных технологий (ст. 272–274.5 УК РФ), законодательство не успевает за стремительным развитием киберпреступности. Особенно остро стоит проблема квалификации новых видов цифровых преступлений и сбора цифровых доказательств.

Организационные проблемы напрямую связаны с недостатками в структуре, координации, кадровом и техническом обеспечении субъектов противодействия. Эти проблемы связаны с управленческими решениями и требуют оптимизации работы субъектов противодействия IT-преступлениям, например проблемы информационно-аналитического и материально-технического обеспечения, вопросы реализации внутреннего (внутриведомственного) и внешнего (межведомственного и международного) взаимодействия [3, с. 315–316].

Согласно результатам проведенного нами опроса к числу организационных проблем в области противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, 37,5% опрошенных отнесли низкий уровень взаимодействия оперативных подразделений и органов предварительного расследования, 50% – отметили низкий уровень взаимодействия с кредитными организациями, 57,1% – высказались о низком уровне взаимодействия с операторами связи и интернет-провайдерами, 33,9% – указали на спорные вопросы, связанные с разграничением компетенции отдельных подразделений, 42,9% – отметили проблемы правового регулирования деятельности органов внутренних дел в вопросах противодействия IT-преступности, 55,4% – в качестве проблемы указали на необходимость проведения оперативно-розыскных мероприятий на территории других субъектов Российской Федерации и 37,5% – высказались о низком уровне методического обеспечения, отсутствии универсальных алгоритмов выявления, раскрытия и расследования преступлений.

Техническое оснащение правоохранительных органов также отстает от уровня развития современных информационно-коммуникационных технологий. Актуальными остаются вопросы доступа к современным средствам цифровой криминалистики, системам анализа больших данных и другим необходимым инструментам.

Серьезной проблемой является дефицит квалифицированных кадров в правоохранительных органах. Раскрытие и расследование киберпреступлений требует специальных познаний в области информационных технологий и информационной безопасности, которые не всегда имеются у сотрудников оперативных подразделений и сотрудников органов предварительного расследования. При этом уровень подготовки специалистов в образовательных организациях МВД России не всегда соответствует современным требованиям [4, с. 34–47; 6, с. 302–304].

Существенной проблемой является низкий уровень взаимодействия между правоохранительными органами и негосударственными организациями (интернет-провайдерами, операторами связи, кредитными и иными организациями). Компании, оказывающие услуги в сфере информационно-коммуникационных технологий, зачастую обладают более полной информацией о киберугрозах, чем правоохранительные органы. Однако механизмы обмена этой информацией либо отсутствуют, либо работают недостаточно эффективно. Безусловным приоритетом в рассматриваемом направлении является внедрение и совершенствование систем электронного документооборота.

Международное сотрудничество в сфере противодействия киберпреступности также сталкивается с существенными трудностями. Различия в национальных законодательствах, отсутствие унифицированных процедур экстрадиции, политические разногласия – все это ограничивает возможности совместного противодействия транснациональной IT-преступности. Особенно остро эта проблема проявилась в последние годы на фоне геополитической напряженности.

Тактические проблемы связаны с необходимостью разработки и внедрения конкретных методов и технологий противодействия IT-преступности. Эти проблемы носят прикладной характер и требуют внедрения как новых тактических приемов, так и программно-технических средств.

Пути решения данных проблем лежат в плоскости разработки типовых алгоритмов раскрытия и расследования различных видов IT-преступлений, внедрения программных и аппаратно-программных комплексов противодействия современным киберугрозам.

Таким образом, предложенная классификация позволяет четко структурировать проблемы по уровням их решения, определить ответственных субъектов (законодатели – для правовых проблем, руководство ведомств – для организационных, сотрудники-исполнители – для тактических), а также разработать адресные меры по совершенствованию системы противодействия.

Подобный подход соответствует принципам комплексности и практической применимости, что делает его оптимальным для использования в научных исследованиях и практической деятельности правоохранительных органов.

Для повышения эффективности противодействия киберпреступности необходимо комплексное решение указанных проблем. В первую очередь требуется совершенствование законодательной базы с учетом новых видов цифровых преступлений. Особое внимание следует уделить вопросам сбора и фиксации цифровых доказательств, их допустимости в судебном процессе. Необходима модернизация системы подготовки кадров для правоохранительных органов, включая совершенствование специализированных учебных программ по цифровой криминалистике.

Важным направлением является развитие технической базы правоохранительных органов, внедрение современных систем анализа киберугроз, создание единых платформ для обмена информацией между всеми субъектами противодействия киберпреступности.

Международное сотрудничество, несмотря на существующие политические сложности, остается важным инструментом противодействия транснациональной киберпреступности. Необходимо развивать двусторонние и многосторонние форматы взаимодействия, уделяя особое внимание вопросам правовой помощи и выработки общих стандартов в сфере кибербезопасности.

Повышение цифровой грамотности населения, безусловно, остается важным элементом государственной политики в сфере противодействия киберпреступности. Это предусматривает включение не только образовательных программ в школы и вузы, но и масштабные информационные кампании для широких слоев населения.

Таким образом, современное состояние противодействия преступлениям в сфере информационно-коммуникационных технологий характеризуется наличием значительных проблем, требующих системного решения. Только комплексный подход, включающий правовые, организационные, технические и международные аспекты, может обеспечить эффективную защиту от постоянно эволюционирующих киберугроз. Реализация предложенных мер позволит существенно повысить уровень кибербезопасности и создать надежные механизмы защиты интересов граждан, бизнеса и государства в цифровом пространстве.

Список источников

1. Григорусь Л.Н., Тутова О.В. NFT как средство легализации (отмывания) доходов, полученных преступным путем // Информационные технологии в деятельности органов внутренних дел: сб. науч. тр. Междунар. науч.-практ. конф. (Москва, 18 апреля 2024 г.). – М.: Московский ун-т МВД России им. В.Я. Кикотя, 2024.
2. Дырма С.В. К вопросу противодействия организованной преступности в сфере информационно-коммуникационных технологий // Актуальные вопросы теории и практики привлечения к уголовной ответственности лиц, занимающих высшее положение в преступной иерархии, 2023.
3. Дырма С.В. Проблемы противодействия кражам и мошенничествам, совершаемым с использованием информационно-коммуникационных технологий // Евразийский юридический журнал. 2023. № 12 (187).
4. Кобозев А.А., Оточина И.А. Основы законодательного регулирования организации подготовки кадров в МВД России: сущность, состояние и тенденции развития // Вестник ВИПК МВД России. 2023. № 3 (67).
5. Мудаев К.В. Механизмы противодействия экономической преступности в цифровой среде: российский и китайский опыт // Новая наука: проблемы и перспективы. 2025. № 7.
6. Тутова О.В. Обучение как один из методов противодействия социальной инженерии // Евразийский юридический журнал. 2023. № 10 (185).

Информация об авторе:

Тутова Ольга Васильевна,
старший преподаватель кафедры гуманитарных и социально-экономических дисциплин

About the author:

Tutova Olga V.,
senior lecturer of the Department of humanitarian and socio-economic disciplines

Статья поступила в редакцию 11.10.2025