УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
https://doi.org/:10.29039/2312-7937-2026-1-77-81
EDN: https://elibrary.ru/zoylkn

ДЫРМА СЕРГЕЙ ВАЛЕРЬЕВИЧ
Крымский филиал Краснодарского университета МВД России
(Симферополь, Россия)
s.dyrma@mail.ru

СУБЪЕКТЫ И ФОРМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. *В статье исследуются вопросы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.*

Автором рассматриваются некоторые особенности реализации функций отдельных субъектов противодействия IT-преступности через призму соответствующего правового регулирования, а также формы противодействия рассматриваемой категории преступлений.

Предложена авторская классификация форм противодействия IT-преступности, отражающая комплексный и многогранный подход деятельности государственной системы противодействия киберпреступлениям.

Ключевые слова: *IT-преступление, информационно-коммуникационные технологии, субъекты противодействия преступности, формы противодействия преступности*

Для цитирования: *Дырма С. В. Субъекты и формы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Вестник ВИПК МВД России. 2026. № 1 (77). С. 77–81; https://doi.org/:10.29039/2312-7937-2026-1-77-81.*

DYRMA SERGEY V.
Crimean Branch of the Krasnodar University of the Ministry of Internal Affairs of Russia
(Simferopol, Russia)

SUBJECTS AND FORMS OF COUNTERACTION TO CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract. *The article discusses the issues of countering crimes committed using information and communication technologies.*

The author examines some features of the implementation of the functions of individual subjects of countering IT-crime through the prism of relevant legal regulation, as well as the forms of countering this category of crimes.

The article proposes an author's classification of the forms of countering IT-crime, which reflects a comprehensive and multifaceted approach to the activities of the state system of countering cybercrimes.

Keywords: *IT crime, information and communication technologies, subjects of crime prevention, forms of crime prevention*

For citation: *Dyrma S. V. Subjects and forms of counteraction to crimes committed using information and communication technologies// Vestnik Advanced Training Institute of the MIA of Russia. 2026. № 1 (77). P. 77–81; https://doi.org/:10.29039/2312-7937-2026-1-77-81.*

Актуальность исследования вопросов противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий[1], обусловлена необходимостью совершенствования механизмов борьбы с данными видами преступлений, поскольку традиционные методы правоохранительной деятельности зачастую оказываются недостаточно эффективными в условиях глобального цифрового пространства.

Как уже было ранее отмечено, современное общество стремительно трансформируется под влиянием цифровых технологий, что, с одной стороны, открывает новые возможности для развития экономики, науки и коммуникации, а с другой – создает предпосылки для возникновения новых форм преступной деятельности. Преступления, совершаемые с использованием информационно-коммуникационных технологий[2], представляют достаточно серьезную угрозу для безопасности личности, бизнеса и государства в целом. Киберпреступность отличается высокой латентностью, транснациональным характером и постоянной эволюцией методов реализации преступного умысла, что определяет потребность в комплексном подходе к противодействию подобным преступлениям[3].

Анализ субъектного состава противодействия IT-преступности, а также форм и методов их работы являются важными компонентами для комплексного понимания масштабов реализации государственной системы противодействия противоправным деяниям, совершаемым с использованием ИКТ.

Вопросы координации между государственными органами, коммерческими организациями и международными структурами требуют тщательного исследования для разработки оптимальных стратегий профилактики и пресечения преступлений в IT-сфере.

Государственная система противодействия противоправным деяниям в сфере ИКТ представляет собой достаточно сложный механизм, включающий в себя множество субъектов, выполняющих специфические функции в рамках единой стратегии обеспечения безопасности личности, общества и государства от противоправных посягательств.

Основными категориями участников рассматриваемой системы являются органы государственной власти, правоохранительные структуры, специализированные учреждения, а также организации, обеспечивающие техническую и информационную поддержку.

Центральное место в системе противодействия IT-преступлениям занимают правоохранительные органы, которые находятся на передовой в борьбе с киберпреступностью. В Российской Федерации к правоохранительным органам, выполняющим функции противодействия IT-преступности, относятся:

• Министерство внутренних дел Российской Федерации (МВД России) – выполняет функции выявления, предупреждения, пресечения, раскрытия и расследования преступлений против личности, совершаемых с использованием ИКТ, IT-преступлений в сфере экономики, преступлений против здоровья населения и общественной нравственности, совершаемых в цифровой среде, и др.);

• органы Федеральной службы безопасности (ФСБ России) – играют важную роль в обеспечении кибербезопасности, выполняют функции противодействия угрозам, направленным на критическую информационную инфраструктуру государства, включая объекты государственного управления, оборонно-промышленного комплекса, финансовой системы и транспорта, а также осуществляют мониторинг и пресечение деятельности, связанной с кибершпионажем, терроризмом и экстремизмом в интернет-пространстве;

[1] Далее – IT-преступление.
[2] Далее – ИКТ.
[3] Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий: распоряжение Правительства Российской Федерации от 30.12.2024 № 4154-р // Информационно-правовое обеспечение «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/411152413/ (дата обращения: 02.07.2025).

• Следственный комитет Российской Федерации (СК РФ) – выполняет функции выявления и расследования IT-преступлений, в пределах своей компетенции (в соответствии с положениями Уголовно-процессуального кодекса РФ)[1];
• органы прокуратуры Российской Федерации (Прокуратура РФ) – выполняют функции надзора за соблюдением и исполнением законов, надзор за соблюдением прав и свобод человека и гражданина, уголовное преследование, координацию деятельности правоохранительных органов по борьбе с преступностью, в том числе IT-преступностью[2];
• Федеральная служба исполнения наказаний (ФСИН России) – выполняет функции по контролю и надзору в сфере исполнения уголовных наказаний в отношении осужденных, освобожденных условно-досрочно от отбывания наказания, условно осужденных и осужденных, контролю за нахождением лиц, подозреваемых либо обвиняемых в совершении преступлений, в местах исполнения наказаний и за соблюдением ими наложенных судом запретов и (или) ограничений[3].

Важным элементом государственной системы являются также судебные органы, которые обеспечивают правовую оценку киберпреступлений и выносят соответствующие решения по уголовным и административным делам. Судебная практика в данной сфере постоянно развивается, что требует от судей глубокого понимания специфики цифровых технологий и методов совершения преступлений с их использованием.

Еще одним значимым субъектом является Федеральная служба по техническому и экспортному контролю (ФСТЭК России), которая отвечает за разработку и внедрение требований по защите информации в государственных информационных системах и на объектах критической инфраструктуры. ФСТЭК России устанавливает стандарты и методики обеспечения безопасности, проводит сертификацию средств защиты информации, а также координирует деятельность по предотвращению кибератак на стратегически важные объекты.

Особое место в системе противодействия IT-преступности занимает Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Роскомнадзор осуществляет функции по надзору за соблюдением законодательства в сфере связи, информационных технологий и массовых коммуникаций. В компетенцию данного органа входит блокировка противоправного контента, включая материалы, связанные с распространением экстремистской идеологии, детской порнографии, призывами к массовым беспорядкам и другими запрещенными видами информации.

Помимо федеральных структур в систему противодействия киберпреступности входят специализированные научно-исследовательские и образовательные учреждения, такие как Академия ФСБ России, Московский государственный технический университет им. Н. Э. Баумана и другие вузы, готовящие кадры для работы в сфере информационной безопасности. Эти организации не только обеспечивают подготовку специалистов, но и занимаются разработкой новых технологий защиты информации, проведением фундаментальных и прикладных исследований в области кибербезопасности.

Отдельного внимания заслуживает взаимодействие государственных структур с частным коммерческим сектором, включая телекоммуникационные компании, интернет-провайдеров, операторов связи, разработчиков программного обеспечения и организаций, в том числе специализирующихся на кибербезопасности. Упомянутое сотрудничество позволяет оперативно выявлять и пресекать кибератаки, обмениваться информацией об угрозах, а также разрабатывать совместные стратегии защиты граждан и организаций в рамках противодействия IT-преступности.

Кроме этого, в условиях глобализации и транснационального характера IT-преступности

[1] О Следственном комитете Российской Федерации: федеральный закон от 28.12.2010 № 403-ФЗ // СПС «КонсультантПлюс»: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_108565/ (дата обращения: 02.07.2025).
[2] О прокуратуре Российской Федерации: федеральный закон от 17.01.1992 № 2202-1 (ред. от 03.02.2025) // СПС «КонсультантПлюс»: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_262/ (дата обращения: 02.07.2025).
[3] О службе в уголовно-исполнительной системе Российской Федерации и о внесении изменений в Закон Российской Федерации «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы»: федеральный закон от 19.07.2018 № 197-ФЗ // СПС «КонсультантПлюс»: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_302867/ (дата обращения: 02.07.2025).

особую значимость приобретает международное сотрудничество. Российская Федерация активно взаимодействует с зарубежными партнерами в рамках международных организаций, таких как Интерпол, Шанхайская организация сотрудничества (ШОС), Организация Договора о коллективной безопасности (ОДКБ) и другие. Это сотрудничество включает в себя обмен оперативной информацией, взаимодействие в рамках расследования отдельных преступлений, разработку единых стандартов противодействия преступлениям, совершаемым с использованием ИКТ.

Таким образом, субъекты противодействия IT-преступлениям представляют собой взаимосвязанные элементы государственной системы противодействия противоправным деяниям в сфере ИКТ, представляющей собой многоуровневую структуру, объединяющую усилия правоохранительных органов, регуляторов, научных и образовательных учреждений, а также иных организаций. Эффективность этой системы напрямую зависит от оперативности и слаженности взаимодействия всех ее участников, постоянного совершенствования правовой базы, внедрения инновационных технологий защиты информации и подготовки высококвалифицированных кадров в сфере борьбы с IT-преступностью.

Противодействие преступности — это целенаправленная, комплексная, последовательная деятельность государства и общества по предупреждению преступности, выявлению и расследованию совершенных преступных деяний, привлечению виновных в совершении преступлений к уголовной ответственности и ее реализации, а также по устранению либо минимизации вреда, причиненного отдельными преступлениями и преступностью в целом посредством реализации мер правового, информационно-пропагандистского, культурно-образовательного, социального, экономического характера [2, с. 98].

Формы противодействия IT-преступлениям во многом схожи с описанными в научных трудах отечественных ученых формами противодействия преступлениям, однако имеют свою уникальную специфику, обусловленную особенностями реализации объективной стороны преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Противодействие IT-преступности представляет собой систему мер, направленных на предупреждение, выявление, пресечение и раскрытие противоправных деяний, а также минимизацию их последствий. Традиционно формы противодействия классифицируются по нескольким критериям, включая этап применения, субъектный состав, способы реализации и сфера воздействия.

По нашему мнению, наиболее приемлемо было бы разделить все формы противодействия IT-преступности на следующие взаимосвязанные категории:

1. Технические.
2. Предупредительные (профилактические).
3. Оперативно-розыскные.
4. Процессуальные.

Технические формы противодействия занимают особое место в борьбе с преступлениями в сфере информационно-коммуникационных технологий, поскольку именно они обеспечивают непосредственную защиту информационных систем от несанкционированного доступа и других форм кибератак. К ним относятся: использование систем обнаружения и предотвращения вторжений (IDS/IPS), применение криптографических методов защиты данных, внедрение биометрической аутентификации, развитие технологий искусственного интеллекта для анализа киберугроз.

Профилактические меры занимают ключевое место в системе противодействия преступности, поскольку направлены на устранение причин и условий, способствующих совершению правонарушений[1]. В традиционной криминологии к ним относятся: правовое воспитание, социально-экономические программы, административный надзор и другие формы воздействия на потенциальных правонарушителей. В сфере ИКТ профилактика приобретает особые черты, связанные с технической природой киберпреступлений. Важнейшими направлениями здесь становятся: повышение цифровой и финансовой грамотности населения, разработка и внедрение стандартов информационной безопасности, проведение регулярного аудита защитных систем, создание механизмов раннего обнаружения уязвимостей.

Оперативно-розыскные формы противодействия предполагают активные дей-

[1] Об основах системы профилактики правонарушений в Российской Федерации: федеральный закон от 23.06.2016 № 182-ФЗ // Информационно-правовое обеспечение «Гарант». URL: https://base.garant.ru/71428030/ (дата обращения: 02.07.2025).

ствия правоохранительных органов и спецслужб, направленные на выявление и пресечение преступной деятельности. В цифровой среде оперативно-розыскная деятельность существенно трансформируется, поскольку требует применения специализированных технологий мониторинга теневого сегмента сети Интернет, цифровой криминалистики и анализа больших данных. Особую роль играет взаимодействие с интернет-провайдерами и владельцами цифровых платформ для оперативного удаления противоправного контента и блокировки вредоносных ресурсов, а также выявления, предупреждения и раскрытия подготавливаемых, совершаемых или совершённых преступлений.

Процессуальные формы противодействия связаны с применением норм материального и процессуального права для привлечения преступников к ответственности. В случае с ИКТ-преступлениями возникают существенные сложности, обусловленные проблемами юрисдикции, сбором и закреплением цифровых доказательств, а также необходимостью специальных познаний у судей и сотрудников органов предварительного расследования. Совершенствование процессуальных механизмов включает разработку специализированных методик расследования и гармонизацию международного законодательства в сфере киберпреступности.

Эффективное противодействие IT-преступлениям требует применения комплексного подхода, объединяющего усилия государства, бизнеса и гражданского общества. Постоянное обновление методов защиты и правовых механизмов позволит минимизировать риски в условиях цифровой эпохи.

Кроме этого, нельзя не согласиться с мнением исследователей о том, что в нынешних условиях борьбы с киберпреступностью к расследованию таких дел должны привлекаться узкоспециализированные следователи, специалисты и эксперты из IT-сферы и области технического функционирования компьютерных систем [1, с. 111].

Таким образом, формы противодействия преступлениям, в том числе совершаемым с использованием информационно-коммуникационных технологий, представляют собой динамично развивающуюся систему мер, требующую постоянной адаптации к новым вызовам. Дальнейшее совершенствование этой системы должно основываться на интеграции передовых технологий, международном сотрудничестве и развитии профессиональных компетенций всех субъектов, участвующих в обеспечении защиты от новых видов цифровых преступлений.

Список источников

1. Михайлова И. А., Лимать А. С., Гилаев Р. И. О деятельности правоохранительных органов по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий // Вестник экономики, права и социологии. 2024. № 2.
2. Тимко С. А. Формы противодействия преступности // Научный вестник Омской академии МВД России. 2021. № 2 (81).

Информация об авторе:

Дырма Сергей Валерьевич,
старший преподаватель
кафедры гуманитарных
и социально-экономических дисциплин

About the author:

Dyrma Sergey V.,
senior lecturer of the department
of humanitarian
and socio-economic disciplines

Статья поступила в редакцию 11.10.2025;
одобрена после рецензирования 25.01.2026; принята к публикации 23.03.2026.
The article was submitted to the editorial office 11.10.2025;
approved after reviewing 25.01.2026; accepted for publication 23.03.2026.