

Дата поступления рукописи в редакцию: 30.05.2026 г.
Дата принятия рукописи в печать: 25.06.2026 г.

DOI: 10.24412/2782-3849-2026-6-246-249

НАБИЕВ Ф.Ф.,

доцент кафедры уголовного права и криминологии Уфимского юридического института МВД России,
кандидат юридических наук, доцент, полковник полиции,

e-mail: mail@law-books.ru

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: СОВРЕМЕННОЕ СОСТОЯНИЕ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

◇ **Аннотация.** В статье анализируются современные тенденции преступности в сфере информационно-телекоммуникационных технологий и компьютерной информации. Обосновывается комплексный подход к предупреждению киберпреступлений, включающий правовые, технические, организационные и виктимологические меры.

◇ **Ключевые слова:** киберпреступность, информационно-телекоммуникационные технологии, компьютерная информация, предупреждение преступлений, виктимологическая профилактика, социальная инженерия, дропперы, уголовная статистика, цифровая безопасность.

NABIEV F.F.,

Associate Professor of the Department of Criminal Law and Criminology at the Ufa Law Institute of the Ministry of Internal Affairs of Russia, Candidate of Law, Associate Professor, Police Colonel

PREVENTION OF CRIMES IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES: CURRENT STATUS, PROBLEMS AND PROSPECTS

◇ **Annotation.** The article analyzes modern crime trends in the field of information and telecommunication technologies and computer information. An integrated approach to the prevention of cybercrimes is being substantiated, including legal, technical, organizational and victimological measures.

◇ **Key words:** cybercrime, information and telecommunication technologies, computer information, crime prevention, victimological prevention, social engineering, droppers, criminal statistics, digital security.

Противодействие киберпреступности в современных условиях представляет собой одну из наиболее сложных и динамично развивающихся задач для всей системы правоохранительных органов. За последнее десятилетие произошел кардинальный рост числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ). Согласно официальным данным, за 12 лет, с 2013 по 2024 год, общее число киберпреступлений в стране увеличилось почти в 70 раз — с 11 тысяч до 765 тысяч, причем только в 2024 году рост составил 13%, а доля IT-преступлений среди всех видов преступлений достигла 40% [1]. Эта тревожная динамика, сопровождающаяся материальным ущербом, исчисляемым сотнями миллиардов рублей, обуславливает необходимость не только совершенствования уголовно-правовых и оперативно-розыскных мер, но и разработки эффективной, многоуровневой

системы предупреждения данных деяний.

Анализ статистических показателей последних лет демонстрирует, что проблема не теряет своей остроты, хотя и появляются первые признаки перелома негативной тенденции. За 2025 год в России зафиксировали 675 372 киберпреступлений — это на 11,8% меньше, чем за тот же период годом ранее. Основную долю киберпреступлений — 63,5 % — по-прежнему составляют хищения и мошенничества: зафиксировано 428 991 таких случаев. Замглавы МВД России Андрей Храпов, подводя итоги 2025 года, сообщил о 663 тыс. киберпреступлений, что на 12% меньше, чем годом ранее. Он также привел следующие данные: число случаев неправомерного доступа к компьютерным данным сократилось на 44%, до 58 тыс.; количество краж сократилось на 23,8%, до 80 тыс. случаев; число случаев мошенничества снизилось на 9%, до 344 тыс. При этом сумма

зарегистрированного материального ущерба незначительно сократилась — с 205 млрд руб. до 189,5 млрд руб. [2]. Таким образом, несмотря на позитивные сдвиги, проблема остается масштабной, ущерб — колоссальным, а сумма похищенных у граждан средств за 8 месяцев 2025 года уже достигла 134 млрд рублей.

Одной из ключевых особенностей киберпреступности, определяющих специфику ее предупреждения, является ее латентный, высокоадаптивный и транснациональный характер. Как справедливо отметил замминистра внутренних дел А. Храпов: «С каждой мерой, которая вступала в действие, мы фиксировали резкий спад регистрируемых преступлений с последующим частичным ростом, что говорит о том, что к этим мерам преступники приспосабливаются и понимают, как им надо дальше действовать». Эта характеристика отражает фундаментальную проблему: субъекты преступной деятельности в цифровой среде обладают высокой мобильностью и способностью быстро видоизменять способы совершения преступлений в ответ на принимаемые правоохранительные и профилактические меры. Увеличение количества преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий [9, с. 145], обуславливает появление новых криминальных проявлений, наиболее широкое распространение среди которых получили совершенные с помощью сети Интернет».

В этой связи система предупреждения противоправных деяний в сфере ИТТ не может быть ограничена исключительно уголовно-правовыми запретами. Система мер предупреждения противоправных деяний, совершаемых с использованием компьютерных и телекоммуникационных технологий, включает в себя действия целенаправленного [5, с. 82] и специализированного характера [6, с. 64], непосредственно направленных на выявление, пресечение, раскрытие и расследование киберпреступлений, устранение причин и условий их совершения, минимизацию и, впоследствии, ликвидацию их последствий. В своей основе она должна носить комплексный характер, охватывая правовые, технические, организационные и, что особенно важно, виктимологические меры. Не случайно в качестве одного из наиболее эффективных способов предупреждения преступлений в данной сфере называется соблюдение элементарных требований информационной защиты [7, с. 59], что является наиболее эффективным способом по предупреждению указанных видов преступлений. К числу таких правил относятся: отказ от перехода по сомнительным

ссылкам, игнорирование звонков и сообщений от незнакомцев по финансовым вопросам, неразглашение паролей и кодов доступа.

При этом преступный инструментарий постоянно совершенствуется. Злоумышленники активно используют методы социальной инженерии, когда человек под психологическим воздействием добровольно передает конфиденциальные данные или переводит свои сбережения. Многие потерпевшие впоследствии сообщают, что действовали «под гипнозом», в результате профессиональной манипуляции со стороны преступников. Главным инструментом злоумышленников остаются мессенджеры — через них в 2025 году совершено 244,6 тыс. преступлений, что на 17,5% превышает показатели за аналогичный период 2024 года.

Значительное место в системе предупреждения занимают общесоциальные меры, направленные на формирование у населения культуры кибербезопасности. В этих целях органами внутренних дел на регулярной основе проводятся встречи с гражданами, в ходе которых основной задачей по предупреждению данного вида преступлений является повышение правовой грамотности [8, с. 126] и информирование граждан о противодействии таким преступным проявлениям».

Однако очевидно, что одних лишь разъяснительных мер недостаточно. Требуется системная государственная политика, включающая создание правовых и технических механизмов противодействия. Важным шагом в этом направлении стало утверждение Правительством РФ Концепции государственной системы противодействия преступлениям, совершаемым с использованием цифровых технологий. Данный документ предусматривает разработку правовых и технических мер, создание специализированных подразделений для расследования таких преступлений, а также пересмотр уголовного законодательства, включая введение новых категорий преступлений, связанных с цифровыми технологиями». Ключевым элементом новой системы должна стать цифровая платформа, обеспечивающая быструю передачу информации между правоохранительными органами, Центральным банком и операторами связи, что позволит оперативно выявлять обстоятельства преступлений и приостанавливать подозрительные операции [3].

Реализация указанных концептуальных положений уже началась. В 2025 году вступил в силу закон об уголовной ответственности для дропперов — подставных банковских клиентов, через карты которых проводятся мошеннические операции. Правительством утвержден план

реализации концепции противодействия киберпреступности, который включает комплекс мер по совершенствованию законодательства, техническому противодействию злоумышленникам, повышению цифровой грамотности населения и синхронизирует работу всех ведомств. Принят и реализуется комплекс из 30 первоочередных мер. В частности, операторы связи и интернет-провайдеры будут обязаны уведомлять правоохранительные органы о преступлениях, совершенных с помощью цифровых технологий, а также прорабатывается вопрос об усилении ответственности за нарушения в сфере персональных данных.

Кроме того, предупреждение преступлений в сфере ИТТ немыслимо без развития научно-технического и криминалистического обеспечения данной деятельности. Как отмечается в современной научной литературе, особое значение имеет формирование на основе криминалистической характеристики указанного вида преступлений частных криминалистических методик расследования, создания криминалистических учетов цифровых доказательств, разработки специализированного программного обеспечения в виде систем поддержки принятия решений [4].

Таким образом, предупреждение преступлений в сфере информационно-телекоммуникационных технологий и компьютерной информации представляет собой многогранную и динамичную систему, эффективность которой зависит от слаженного взаимодействия уголовно-правовых, технических, организационных и виктимологических мер. Несмотря на обнадеживающую статистику 2025 года, демонстрирующую первые успехи в борьбе с этим видом преступности, полное решение проблемы невозможно без постоянного совершенствования законодательства, внедрения передовых технологий, повышения цифровой грамотности населения и тесного международного сотрудничества. Только комплексный подход, сочетающий превентивные меры с неотвратимостью уголовной ответственности, позволит создать надежную защиту личности, общества и государства от современных киберугроз.

Список литературы:

[1] Данные ГИАЦ МВД России за период с 2013 по 2025 гг. file:///C:/Users/fnabiev147/Desktop/Sbornik_dlya_UOS_07.pdf (дата обращения: 17.04.2026).

[2] Выступление заместителя министра МВД России Храпова А. https://www.kommersant.ru/doc/8442339?from=horisontal_lenta (дата обращения: 17.04.2026).

[3] Концепция противодействия киберпреступлениям https://www.senatinform.ru/news/kabmin_utverdil_kontseptsiyu_protivodeystviya_kiberprestupleniyam/ (дата обращения: 18.04.2026).

[4] Харисова З.И. Криминалистическая характеристика преступлений, связанных с неправомерным доступом к компьютерной информации <https://pravgos.ru/index.php/journal/article/view/1130> (дата обращения: 18.04.2026).

[5] Мирхайдарова, М. Ю. Некоторые вопросы рабочего этапа предъявления лица для опознания по голосовым и речевым свойствам опознаваемого лица / М. Ю. Мирхайдарова // Право и государственность. – 2026. – № 1(10). – С. 82-88. – DOI 10.70569/2949-5725.2026.10.1.012. – EDN MIGCFP.

[6] Шевелева, С. С. Сбалансированная цифровизация уголовного судопроизводства: критерии допустимости и минимизация латентных рисков / С. С. Шевелева // Право и государственность. – 2025. – № 4(9). – С. 61-64. – DOI 10.70569/2949-5725.2025.9.4.011. – EDN HWOGAY.

[7] Карагодина, В. И. Отмывание денег через электронные платежные системы / В. И. Карагодина // Право и государственность. – 2025. – № 4(9). – С. 58-60. – DOI 10.70569/2949-5725.2025.9.4.010. – EDN ZKPFDR.

[8] Адвокатская деятельность и адвокатура в России в 2 Ч. Часть 1 : Учебник / И. Л. Трунов, Н. Б. Сонькин, В. А. Вайпан [и др.]. – 3-е изд., пер. и доп. – Москва : Издательство Юрайт, 2020. – 220 с. – (Высшее образование). – ISBN 978-5-534-04003-6. – EDN CXXGJC.

[9] Хасанова, З. И. О некоторых вопросах установления уголовной ответственности за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан / З. И. Хасанова, М. С. Шайхуллин // Право и управление. 2025. № 12. С. 144-149. – DOI 10.24412/2224-9133-2025-12-144-149. – EDN TIOFGV.

References:

[1] Data from the GIAC of the Ministry of Internal Affairs of Russia for the period from 2013 to 2025 file:///C:/Users/fnabiev147/Desktop/Sbornik_dlya_UOS_07.pdf (accessed on: 17.04.2026).

[2] Speech by Deputy Minister of the Ministry of Internal Affairs of Russia A. https://www.kommersant.ru/doc/8442339?from=horisontal_lenta (date of appeal: 17.04.2026).

[3] The concept of countering cybercrime https://www.senatinform.ru/news/kabmin_utverdil_kontseptsiyu_protivodeystviya_kiberprestupleniyam/ (accessed on: 18.04.2026).

[4] Harisova Z.I. Forensic characterization of crimes related to illegal access to computer information <https://pravgos.ru/index.php/journal/article/view/1130> (date of appeal: 18.04.2026).

[5] Mirkhaidarova, M. Yu. Some issues of the working stage of presenting a person for identification by the voice and speech properties of the identified person/M. Yu. Mirkhaidarov // Law and statehood. – 2026. – № 1(10). – S. 82-88. – DOI 10.70569/2949-5725.2026.10.1.012. – EDN MIGCFP.

[6] Sheveleva, S. S. Balanced CMF of criminal proceedings: criteria for admissibility and minimization of latent risks/S. S. Sheveleva // Law and statehood. – 2025. – № 4(9). – S. 61-64. – DOI 10.70569/2949-5725.2025.9.4.011. – EDN HWOYAY.

[7] Karagodina, V.I. Money laundering through electronic payment systems/V.I. Karagodina // Law

and statehood. – 2025. – № 4(9). – S. 58-60. – DOI 10.70569/2949-5725.2025.9.4.010. – EDN ZKPFDR.

[8] Advocacy and advocacy in Russia in 2 Part 1: Textbook/I. L. Trunov, N. B. Sonkin, V. A. Vaipan [and others]. – 3rd ed., Per. And add. – Moscow: Yurayt Publishing House, 2020. – 220 p. – (Higher education). – ISBN 978-5-534-04003-6. – EDN CXXGJC.

[9] Khasanova, Z. I. On some issues of establishing criminal liability for the public dissemination of knowingly false information about circumstances posing a threat to the life and safety of citizens/Z. I. Khasanova, M. S. Shaikhullin // Law and Management. 2025. № 12. S. 144-149. – DOI 10.24412/2224-9133-2025-12-144-149. – EDN TIOFGV.



**ЮРИДИЧЕСКОЕ ИЗДАТЕЛЬСТВО
«ЮРКОМПАНИ»**

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.

ЮРКОМПАНИ

www.law-books.ru