

ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Эльвира Гумеровна Юзиханова¹, Наталья Александровна Корсикова²

¹ Санкт-Петербургский университет МВД России, г. Санкт-Петербург, Россия
uzikhanovaeg@yandex.ru

 <https://orcid.org/0000-0003-4864-9020>

² Санкт-Петербургский государственный университет аэрокосмического приборостроения,
г. Санкт-Петербург, Россия
korsikova-nataly@mail.ru

 <https://orcid.org/0000-000-1565-3464>

Аннотация. В настоящее время в мире происходит активная цифровизация, которая оказывает влияние на все сферы жизни общества. Информационные потоки особенно развивают такие сферы как социальное обеспечение, финансы, экономику, делая их проще и доступнее для общества. Несмотря на это, многие новые идеи и разработки зачастую несут за собой и отрицательные последствия. Деньги, являясь универсальным средством платежа, во все времена притягивали внимание преступников, и если раньше для незаконного завладения ими необходимо было контактировать с собственником средств и преодолевать какие-либо физические барьеры, то сейчас посредством информационно-телекоммуникационных технологий похитить деньги возможно, не выходя из дома. Данная простота и эффективность незаконных действий привели к резкому росту преступлений в сфере информационно-телекоммуникационных технологий, а хищений денежных средств в особенности.

Данное исследование посвящено содержанию фактов наличия определенных проблем правового регулирования преступлений, связанных с применением компьютерных технологий и информационно-коммуникационной сети «Интернет», и определению приоритетных направлений профилактики рассматриваемых преступлений.

Ключевые слова: профилактика, информационно-телекоммуникационные технологии, киберпреступность

Для цитирования: Юзиханова Э. Г., Корсикова Н. А. Профилактика преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Правопорядок: история, теория, практика. 2025. № 4 (47). С. 143–146. DOI: 10.47475/2311-696X-2025-47-4-143-146

Research article

PREVENTION OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES


Elvira G. Yuzikhanova¹, Natalia A. Korsikova²

¹ St. Petersburg University of the Ministry of Internal Affairs of Russia,
St. Petersburg, Russia

uzikhanovaeg@yandex.ru

 <https://orcid.org/0000-0003-4864-9020>

² St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia
korsikova-nataly@mail.ru

 <https://orcid.org/0000-0002-1565-3464>

Abstract. Currently, the world is undergoing active digitalization, which affects all spheres of society. Information flows especially develop such areas as social security, finance, and economics, making them easier and more accessible to society. Despite this, many new ideas and developments often have negative consequences.

Money, being a universal means of payment, has always attracted the attention of criminals, and if earlier it was necessary to contact the owner of the funds and overcome any physical barriers in order to illegally seize them, now it is possible to steal money using information and telecommunication technologies without leaving home. This simplicity and effectiveness of illegal actions have led to a sharp increase in crimes in the field of information and telecommunication technologies, and especially embezzlement of funds. This study is devoted to the content of the facts of the existence of certain legal problems.

Keywords: prevention, information and telecommunication technologies, cybercrime

For citation: Yuzikhanova EG, Korsikova NA. Prevention of crimes committed using Information and telecommunication technologies. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2025;(4):143-146. DOI: 10.47475/2311-696X-2025-47-4-143-146 (In Russ.)

Введение

Несмотря на отсутствие единого определения, киберпространство сегодня составляет неотъемлемую часть нашей жизни, а киберпреступления становятся все более распространенными и опасными. В связи с этим, развитие методов борьбы с киберпреступлениями и повышение информационной безопасности является актуальной задачей современного общества.

Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, могут быть совершены только с использованием компьютерных устройств. «К числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переработанные промышленным либо кустарным способом»¹.

Современные технологии и информационные системы постоянно развиваются. В связи с этим возникают новые факторы, которые изменяют способы и методы совершения преступлений. Воздействие таких факторов на формирование преступных схем имеет множественное проявление и является катализатором увеличения количества преступлений в сфере информационных технологий.

Особое место в этом списке занимают электронные мошенничества, которые становятся все более распространенными. К таким видам преступлений можно отнести хакерство, незаконное использование чужой информации и другие. Быстрое развитие технологий

приводит к тому, что расследование таких преступлений становится значительно усложненным [3, с. 146].

В результате комплексность воздействия новых информационных технологий и рост количества преступлений в данной сфере требует более серьезного и тщательного подхода со стороны правоохранительных органов и специалистов в области кибербезопасности.

Материал и методы

Эмпирической составляющей настоящей статьи являются:

- статистические материалы Главного информационно-аналитического центра МВД РФ по преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий;
- научно-исследовательские работы, проведенные другими исследователями Российской Федерации.

При проведении настоящего исследования использовались такие методы, как сравнительно-правовой, метод анализа и синтеза, статистический метод.

Описание исследования

С помощью современных технологий стали возможны глобальные транзакции без контроля со стороны государства. Это привело к возникновению черных онлайн-рынков, занимающихся продажей запрещенных товаров. Криптовалюты стали предпочтительным средством платежа на таких рынках благодаря своей анонимности и отсутствию регулирующих органов. Наиболее популярная система для работы на этих рынках — прокси-сервер «Тог» [1, с. 1–3], который позволяет установить анонимное сетевое соединение. Криптовалюты стали центральным инструментом для проведения нелегальных операций на черных онлайн-рынках, таких как продажа наркотиков, психотропных средств и оружия.

В этой связи одним из важнейших направлений по профилактике преступлений, связанных с информационно-коммуникационными технологиями, является интерпретация портрета современного преступника и создание типологии личности преступника в данной области.

Среди противоправных действий в сфере компьютерной информации наибольшая доля приходится

¹ Постановление Пленума Верховного Суда РФ от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 15.07.2025).

на хищения электронных денежных средств, совершаемые посредством использования информационно-телекоммуникационных технологий. За 2024 г. на территории Российской Федерации было зафиксировано более 200000 преступлений с использованием банковских карт. Ученые относят к таким видам мошенничества скимминг, шимминг, фишинг, кардинг, ливанскую петлю, снифферинг, социальную инженерию [2, с. 106].

Важнейшей предпосылкой становления правонарушителей в области компьютерной информации является наличие специальностей в высших образовательных учреждениях, где обучающиеся получают профессиональные навыки и знания в области программирования. Также важным фактором становления правонарушителей является влияние семейного и внесемейного окружения на процесс формирования личности.

В процессе взлома преступники используют методы уязвимостей в системе безопасности, ставят под сомнение целостность системы и нарушают законность доступа к информации. Кракерами¹ могут быть как отдельные лица, так и организованные группы. Некоторые из них используют свои знания для монетизации, продавая полученную информацию, тогда как другие похищают информационные ресурсы для противостояния социальному порядку или для укрепления своей позиции в обществе.

В рамках борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, также выделяются и другие категории преступников в зависимости от их специализации и видов деятельности.

В итоге профессионалы-компьютерщики с высшим техническим, экономическим или юридическим образованием усложняют жизнь законодателям, ведь эти преступники контролируют порядка 80 % всех крупных краж с использованием информационно-телекоммуникационных технологий. Электроника столь мощна, что имеющий достаточно знаний в этой области специалист может проделать любую преступную махинацию. Опыт, знание всевозможных языков программирования, особенностей аппаратной части и мастерство обращения с несколькими компьютерными платформами и системами дают им возможность скрыть свои преступные деяния на долгое время, установив программное обеспечение для сокрытия их следов. Владение огромными объемами информации о криптографии и системах электронных транзакций позволяет им уверенно и безнаказанно оперировать

¹ Программист-любитель или пользователь специалист, нелегально проникающий в чужие базы данных, в сети и иные накопители информации (нередко с целью получения материальной выгоды) // URL: <https://dic.academic.ru/dic.nsf/efremova/275988/кракер> (дата обращения: 15.07.2025).

электронными деньгами. Хотя законодательные органы пытаются исправить ситуацию в области кибербезопасности, многие остаются под угрозой ежедневных хакерских атак.

Заключение и вывод

Таким образом, актуальными задачами являются комплексное исследование этого вопроса, разработка правовых мер, направленных на повышение уровня информационной безопасности, предупреждение подобных преступлений, а также подготовка специалистов, способных осуществлять практику раскрытия и расследования данных противоправных посягательств.

При этом важно не только обеспечить защиту от внешних угроз, но и организовать отслеживание и контроль внутренних нарушений. Данная проблема касается как государственных, так и коммерческих организаций, а также отдельных граждан, которые часто не являются осведомленными о возможных угрозах в сети.

Реализация данного подхода требует значительного расширения парка высокотехнологичного оборудования и техники. Это является основным условием для повышения уровня борьбы с киберпреступностью и создания прочной защиты информационно-коммуникационных систем от кибератак. При этом важно учесть, что оборудование и техника должны быть современными и отвечать всем современным требованиям. Только в этом случае можно обеспечить быстрое и качественное реагирование на новые виды киберугроз и эффективную защиту систем от них.

Важно также учитывать тот факт, что развитие информационных технологий ведет к появлению новых видов киберпреступлений, требующих от следователей более глубокого понимания их специфики и использования соответствующих методов раскрытия. Это подчеркивает необходимость постоянного обучения и повышения уровня компетенции сотрудников правоохранительных органов и следователей в области информационных технологий [3, с. 201].

Современная проблематика профилактики предупреждения преступлений, связанных с нарушениями информационной безопасности, находится в центре внимания органов государственной власти. Несмотря на активное противодействие киберпреступности, существуют значительные проблемы и недочеты, требующие дополнительных мер по защите общества от возможных атак.

В связи с этим правоохранительным органам необходимо приложить большие усилия на разработку оптимальных механизмов и методик предотвращения киберпреступности, а также более углубленного изучения киберсреды.

Список источников

1. Dingleline R., Mathewson N., Syverson P. Tor: Луковый маршрутизатор второго поколения / пер. А. Абакумкина и Р. Инфлянскаса. URL: <https://www.opennet.ru/soft/tordesign.pdf> (дата обращения: 15.07.2025).
2. Урсаева Ю. А., Сорокашиш И. Ю., Зиниша О. С. Мошенничество с банковскими картами в современном мире // Научные исследования XXI века. 2020. № 2 (4). С. 105–108.
3. Криминология. Общая и особенная части: учебник / Под общ. ред. Н. А. Корсиковой. СПб., 2022. 527 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Юзиханова Эльвира Гумеровна

Доктор юридических наук, профессор, начальник кафедры криминологии Санкт-Петербургского университета МВД России
Россия, 198206, г. Санкт-Петербург, ул. Летчика Пилютова, д. 1
E-mail: uzikhanovaeg@yandex.ru
ORCID: 0000-0002-1565-3464

Корсикова Наталья Александровна

кандидат юридических наук, доцент, доцент кафедры гражданского права Санкт-Петербургского государственного университета аэрокосмического приборостроения
Россия, 190121, г. Санкт-Петербург, ул. Большая Морская, д. 67
E-mail: korsikova-nataly@mail.ru
ORCID: 0000-0002-1565-3464

INFORMATION ABOUT THE AUTHORS

Elvira G. Yuzikhanova

Doctor of Legal Science, Professor, Head of the Department of Criminology of the St. Petersburg University of the Ministry of Internal Affairs of Russia
1 Pilyutova str., St. Petersburg 198206, Russia
E-mail: uzikhanovaeg@yandex.ru
ORCID: 0000-0002-1565-3464

Natalia A. Korsikova

Candidate of Legal Science, Associate Professor, Associate Professor of the Department of Civil Law, St. Petersburg State University of Aerospace Instrumentation
67 Bolshaya Morskaya str., St. Petersburg 190121, Russia
E-mail: korsikova-nataly@mail.ru
ORCID: 0000-0002-1565-3464

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 20.07.2025.

Дата рецензирования статьи / Revised: 08.09.2025.

Дата принятия статьи к опубликованию / Accepted: 15.09.2025.