ДЫРМА СЕРГЕЙ ВАЛЕРЬЕВИЧ
Крымский филиал Краснодарского университета МВД России
(Симферополь, Россия)

S.dyrma@mail.ru

Понятие и признаки преступления, совершённого с использованием информационно-коммуникационных технологий

Аннотация. В статье освещаются вопросы, касающиеся понятия особенностей преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Автор рассматривает отдельные особенности данных преступлений через призму их уголовно-правовой и криминалистической характеристики.

Предложено авторское определение понятия преступления, совершённого с использованием информационно-коммуникационных технологий, а также классификация рассматриваемой категории преступлений.

Ключевые слова и словосочетания: преступление, информационно-коммуникационные технологии, правовое регулирование, технологии передачи информации

Для цитирования: *Дырма С. В. Понятие и признаки преступления, совершённого с использованием информационно-коммуникационных технологий // Вестник ВИПК МВД России. – 2024. – № 4 (72). – С. 72-77; doi: 10.29039/2312-7937-2024-4-72-77*

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

THE CONCEPT AND SIGNS OF A CRIME COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Annotation. The article discusses issues related to the concept of the features of crimes committed using information and communication technologies. The author examines the individual features of crimes committed using information and communication technologies through the prism of their criminal law and criminalistic characteristics. The article proposes the author's definition of the concept of a crime committed using information and communication technologies, as well as the classification of the category of crimes under consideration.

Key words and word combinations: crime, information and communication technologies, legal regulation, information transfer technologies

For citation: *Dyrma S. V. The concept and signs of a crime committed Using information and communication technologies // Vestnik Advanced Training Institute of the MIA of Russia. - 2024. - No. 4 (72). - P. 72-77; doi: 10.29039/2312-7937-2024-4-72-77*

Интенсификация процессов интеграции информационных технологий в современном мире, активное их развитие и совершенствование указывают на исключительную роль данных технологий в жизни общества. Информационные технологии и создаваемая ими глобальная технологическая инфраструктура, по своей сути, становятся неким базисом

функционирования различных сфер жизни общества, в частности основой для функционирования и развития социальных коммуникаций.

Информационно-коммуникационные технологии, будучи в значительной степени приложенными к понятию «коммуникация» как к одному из способов человеческого бытия, оказывают существенное влияние на социальную коммуникацию в обществе, обеспечивают усиление технологизации социальных коммуникаций, создавая целый виртуальный мир со своими нормами и правилами.

Развитие информационно-коммуникационных технологий, появление новых средств и методов межличностной коммуникации, активное использование электронных платежных средств, несомненно, обеспечивают благоприятные условия для совершенствования социальной коммуникации, а также упрощают доступ граждан к своим финансовым ресурсам. Вместе с тем развитие современных технологий предопределяет возникновение новых форм совершения преступлений дистанционного характера.

Активное и непрерывное распространение информационно-коммуникационных технологий приводит не только к возникновению новых видов социальной коммуникации, но и к стремительному изменению форм преступной активности, формированию новых видов и способов совершения преступлений в данной сфере. В значительной степени последний тезис применим к кражам и мошенничествам, совершаемым с использованием информационно-коммуникационных технологий. Многообразие способов совершения преступлений данной категории в настоящее время достаточно велико, при этом практически ежегодно появляются все новые способы их совершенствования.

Для того, чтобы отграничить преступления, совершённые или совершаемые с использованием информационно-коммуникационных технологий, от иных видов преступлений, необходимо исследовать особенности данной категории преступлений.

Преступление, совершённое или совершаемое с использованием информационно-коммуникационных технологий, как понятие, не имеет конкретной нормативной регламентации.

Определение понятия информационно-коммуникационных технологий в научных кругах не вызывает существенных споров. Так, в некоторых научных трудах термин «информационно-коммуникационные технологии» определен как процессы, методы поиска, сбора, формирования, хранения, обработки, представления, предоставления, передачи, распространения информации и способы осуществления таких процессов и методов с применением средств вычислительной техники и средств телекоммуникации [4, с. 23].

Схожие по смыслу определения понятия информационно-коммуникационных технологий мы встречаем и в иных источниках. Так, согласно национальному стандарту РФ ГОСТ Р 52653-2006 «Информационно-коммуникационные технологии в образовании. Термины и определения», утвержденному приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 419-ст, информационно-коммуникационная технология представляет собой информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации.

Рассматривая данный вопрос в разрезе нормативного регулирования, следует отметить, что в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определены понятия, лежащие в основе термина «информационно-коммуникационные технологии»:

информация – сведения (сообщения, данные) независимо от формы их представления;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [2].

Понятие преступления, совершённого с использованием информационно-коммуникационных технологий, по нашему мнению, не столь однозначно и требует исследования, в том числе с учетом анализа статистических сведений по преступлениям указанной категории, нормативных актов, регулирующих особенности формирования статистической отчетности, а также мнений ученых по данному вопросу.

Необходимость в определении понятия преступления, совершённого или совершаемого с использованием информационно-коммуникационных технологий, обусловлено не только повсеместным распространением подобных деяний, изменением на протяжении последних

лет структуры преступности в целом, но и необходимостью внесения соответствующих квалифицирующих признаков в диспозиции некоторых норм Уголовного кодекса Российской Федерации.

В статье 14 Уголовного кодекса Российской Федерации понятие преступления определено как виновно совершённое общественно опасное деяние, запрещенное настоящим Кодексом под угрозой наказания [1].

В наиболее общем понимании понятие преступления, совершённого с использованием информационно-коммуникационных технологий, можно сформулировать с учетом положений Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также Уголовного кодекса Российской Федерации.

Вопрос о понятии преступления, совершённого с использованием информационно-коммуникационных технологий, в научных кругах является достаточно актуальным. Так, например, профессор Е.А. Русскевич в своих научных трудах преступления, совершаемые с использованием информационно-коммуникационных технологий, определяет как общественно опасные уголовно-противоправные деяния, совершаемые в отношении и (или) посредством методов, процессов или программно-технических средств, интегрированных с целью хранения, обработки или передачи компьютерной информации [3, с. 25].

Согласно анализу статистических сведений в период с 2018 по 2023 год при общем снижении количества зарегистрированных в Российской Федерации всех видов преступлений на 0,2% (с 1 991 532 до 1 947 161) [6], количество зарегистрированных преступлений, совершенных с использованием информационно-коммуникационных технологий, увеличилось на 387,5% (с 174 674 до 676 951) [7] (рис. 1).

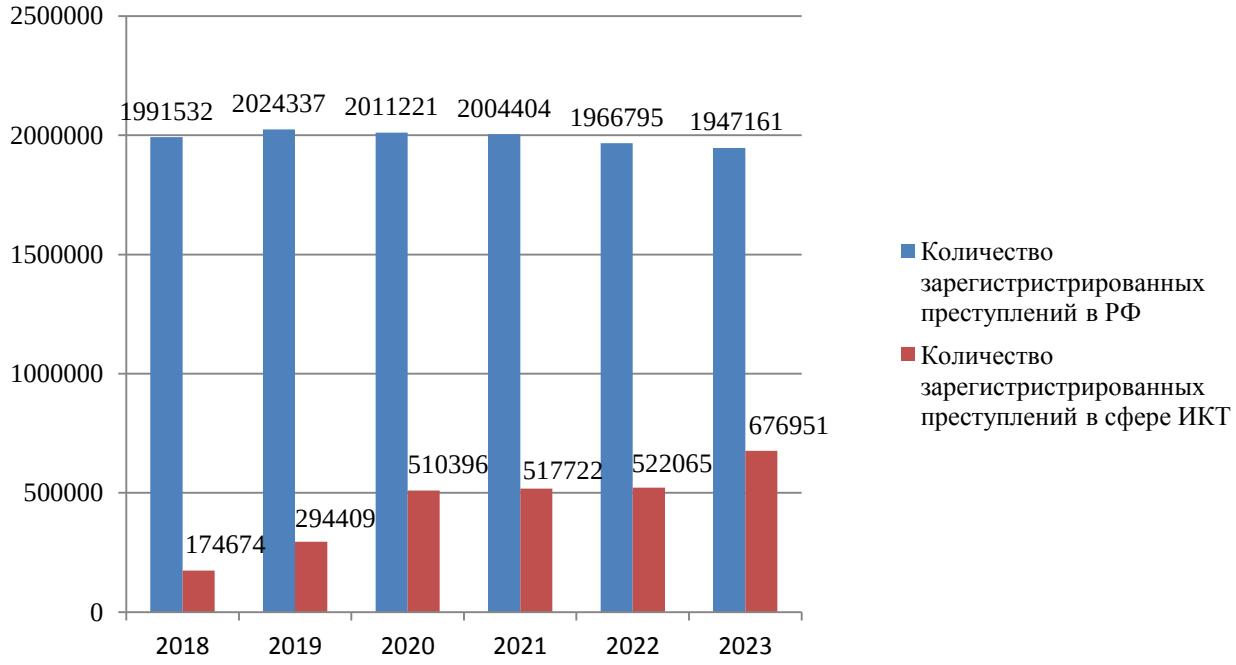

Рис. 1. *Статистические сведения о преступлениях, зарегистрированных на территории РФ в период с 2018 по 2023 год*

Проведенный анализ статистических сведений о состоянии преступности позволяет сделать вывод о том, что мы живем в эпоху цифровой трансформации преступности. В 2018 года доля IT-преступлений в общей структуре преступности в Российской Федерации составляла 8,8%, а по итогам 2023 года указанная доля увеличилась до 34,8%. Таким образом, в настоящее время каждое третье преступление, совершаемое в стране, является IT-преступлением.

Определяя главные отличительные особенности IT-преступлений от иных общественно опасных деяний, следует отметить, что программные и аппаратные средства информационных технологий (мобильные телефоны, Интернет и иные средства коммуникации) используются для реализации объективной стороны преступления. Например, при совершении IT-преступлений против собственности современные информационно-коммуникационные технологии используются для осуществления коммуникации злоумышленника с потенциальным потерпевшим либо используются для хищения денежных средств с банковских счетов различными способами.

В структуре IT-преступности наибольшую долю составляют именно преступления против собственности, к числу которых относятся кражи и мошенничества. Доля подобных преступлений в структуре IT-преступности по итогам 2023 года составила 69,8%.

В зависимости от родового объекта преступного посягательства предлагаем классифицировать преступления, совершённые с использованием информационно-коммуникационных технологий, на:

преступления против личности (п. «д» ч. 2 ст. 110, п. «д» ч. 3 и ч. 6 ст. 110.1, ч. 2 ст. 110.2, ст. 119, 128.1, 133, 135, 137, 138, 138.1, 146, 150, 151, п. «в» ч. 2 ст. 151.2 УК РФ);

преступления в сфере экономики (п. «г» ч. 3 ст. 158, ч. 4 ст. 158, ст. 159, 159.3, 159.6, 163, 171.2, 174, 174.1, 183, 185.3, 186, 187 УК РФ);

преступления против общественной безопасности и общественного порядка (ст. 205.1, ч. 2 ст. 205.2, 207, 207.1, 207.2, 207.3, 210, п. «в» ч. 3 и п. «в» ч. 5 ст. 222, п. «в» ч. 3 и п. «в» ч. 5 ст. 222.1, п. «в» ч. 3 и п. «в» ч. 5 ст. 222.2, 228, п. «б» ч. 2 и ч. 3, 4, 5 ст. 228.1, 228.2, 228,3, 228.4, 229, п. «д» ч. 2, ч. 3, 4 ст. 230, 234, 234.1, 238, ч. 1.1, 2 и 3 ст. 238.1, 240, п. «г» ч. 2 ст. 242.1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.2, п. «г» ч. 2 ст. 245, ч. 1.1, п. «б» ч. 2, ч. 2.1, 3 и 3.1 ст. 258.1, ст. 272, 273, 274, 274.1 УК РФ);

преступления против государственной власти (ст. 283, 283.1, 284.2, 288, 292, 296, 298.1, 311, 327, 327.1 УК РФ);

преступления против мира и безопасности человечества (ст. 354, п. «в» ч. 2 и ч. 4 ст. 354.1 УК РФ).

По наличию квалифицирующих признаков все IT-преступления можно классифицировать на:

– квалифицированные;

– неквалифицированные.

По способам совершения рассматриваемые преступления возможно разделять на совершённые с использованием:

– средств мобильной связи;

– сети Интернет;

– электронных платежных систем и расчетных (пластиковых) карт;

– специальных средств и техники;

– компьютерных программ.

Рассматривая особенности преступлений, совершаемых с использованием информационно-коммуникационных технологий, следует отметить:

– преступления в основном совершаются лицами, находящимися в различных регионах Российской Федерации либо на территории стран ближнего зарубежья, в том числе лицами, отбывающими наказание в местах лишения свободы;

– отсутствует визуальный контакт между потерпевшим и подозреваемым либо между приобретателем или сбытчиком наркотических средств;

– злоумышленники часто меняют используемые абонентские номера и аппараты мобильной связи, используемые для совершения преступлений;

– предметом хищения при совершении преступлений против собственности в большинстве случаев являются электронные денежные средства, которые зачисляются потерпевшим на счёт подозреваемого (реже денежные средства передаются потерпевшим по указанию подозреваемого соучастникам преступления);

– при совершении преступлений используются современные средства коммуникации, электронные платёжные системы, позволяющие обеспечить злоумышленникам высокий уровень конспирации (например, ресурсы IP-телефонии в сочетании с программами по подмене абонентского номера);

– при совершении преступлений злоумышленниками используются программы, позволяющих менять адрес пользователя в сети Интернет, создавая динамические либо нераспознаваемые IP-адреса, что значительно усложняет их идентификацию.

По нашему мнению, первой существенной отличительной особенностью рассматриваемых преступлений от иных видов уголовно-противоправных деяний является то, что преступления указанной категории предполагают активное использование информационных технологий в ходе реализации объективной стороны того или иного преступления.

Например, злоумышленник с использованием сети «Интернет» создает сайт или иной информационный ресурс с предложением инвестиционных вложений в области криптовалюты. Доверчивые граждане зачисляют свои денежные средства на якобы инвестиционный счет неизвестного лица в расчете на потенциальную прибыль. Однако в последующем выясняется, что вывод денежных средств с псевдоинвестиционного счета невозможен, а денежные средства поступают в распоряжение злоумышленника.

В рассматриваемой ситуации объективная сторона мошенничества, выразившаяся во введении в заблуждение потерпевшего, осуществлялась при непосредственном использовании глобальной сети «Интернет». Получение денежных средств, добытых преступным путем, было реализовано злоумышленником также с использованием информационных технологий, а именно с использованием банковского счета. Таким образом, данное преступление было совершено с использованием информационно-коммуникационных технологий.

Рассмотрим следующий пример из правоприменительной деятельности: злоумышленник с использованием сайтов популярных объявлений о продаже товаров находит объявление о продаже мобильного телефона за 10 000 рублей, далее с использованием мобильной связи договаривается с ним о встрече и сделке купли-продажи. После этого злоумышленник с использованием банковского мобильного приложения проверяет абонентский номер продавца и определяет, что его абонентский номер подключен к системе мобильного банка «С». Далее злоумышленник с использованием прикладного программного обеспечения – графического редактора – создает поддельный шаблон перевода денежных средств по абонентскому телефону продавца с указанием суммы перевода на 10 000 рублей. При встрече с продавцом мобильного телефона злоумышленник получает от продавца реализуемый товар и на своем телефоне демонстрирует заранее подготовленное изображение с подложным изображением перевода денежных средств по его абонентскому номеру. Далее злоумышленник, сославшись на потенциальную возможность длительности межбанковского перевода и воспользовавшись доверчивостью продавца, получает имущество и в дальнейшем продает его третьим лицам в целях получения денежных

средств, а потенциальный потерпевший лишь спустя некоторое время понимает, что никакого перевода денежных средств на его банковский счет не было.

В данной ситуации получение злоумышленником чужого имущества осуществлялось при непосредственном контакте с потенциальным потерпевшим, а информационные технологии, в частности средства мобильной связи, глобальная сеть «Интернет» и прикладное программное обеспечение, использовались лишь при подготовке к совершению рассматриваемого преступления, но не при реализации его объективной стороны, ввиду чего отнести его к категории IT-преступлений было бы ошибочно.

Второй отличительной особенностью IT-преступлений, по нашему мнению, является использование злоумышленниками технологий дистанционной передачи информации в ходе реализации объективной стороны преступления, что подчеркивает экстерриториальный характер подобных преступлений.

Сомнительным было бы отнесение к категории IT-преступлений мошенничества, при котором злоумышленник с использованием средств усиления звуковых сигналов, например мегафона, убеждал граждан приобрести акции несуществующей компании, с последующим получением от потерпевших наличных денежных средств.

Если рассматривать уголовно-правовую характеристику кражи и мошенничеств, совершаемых с использованием информационно-коммуникационных технологий, следует подчеркнуть, что их видовым объектом, как и любой другой формы хищения, является собственность, непосредственным объектом – частная собственность, а именно денежные средства, хранящиеся на банковских счетах граждан. Вместе с тем некоторые способы совершения мошенничеств, совершаемых и с использованием информационно-коммуникационных технологий, предполагают получение наличных денежных средств от потерпевших, например при использовании классической схемы звонка псевдородственника, якобы совершившего дорожно-транспортное происшествие, которому нужны денежные средства для решения вопроса об избежании уголовной ответственности. В данном случае злоумышленники, как правило, используют услуги так называемых «курьеров» для получения наличных денежных средств от потерпевших [5, с. 316].

Объективная сторона рассматриваемых преступлений, как и иных видов киберпреступлений, выражена в форме действия, субъективная сторона характеризуется умыслом.

Таким образом, изложенное позволяет сделать вывод о том, что преступления, совершаемые с использованием информационно-коммуникационных технологий, представляют собой запрещенные Уголовным кодексом Российской Федерации общественно опасные действия, умышленно совершенные с использованием технологий дистанционной передачи информации.

В условиях повсеместной информатизации современного общества очевидным фактом является то, что преступления, совершаемые с использованием информационно-коммуникационных технологий, представляют серьезную угрозу складывающимся отношениям в экономической, политической, социальной и других сферах жизни общества и государства.

На современном этапе одним из важнейших приоритетов правоохранительной деятельности в Российской Федерации является выработка и совершенствование механизмов наиболее эффективного противодействия деятельности криминальных структур, активно использующих достижения в области информационных технологий для совершения преступлений против личности, собственности, общественного порядка и общественной безопасности.

Список источников.

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс» (дата обращения: 20.04.2024).

2. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «КонсультантПлюс» (дата обращения: 02.04.2024).
3. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: автореф. дис. … д-ра юрид. наук. – М., 2020.
4. Куняев Н.Н. О развитии правового регулирования в области использования информационно-коммуникационных технологий // Юридический мир. 2010. № 7.
5. Дырма С.В. Проблемы противодействия кражам и мошенничествам, совершаемым с использованием информационно-коммуникационных технологий // Евразийский юридический журнал. 2023. № 12.
6. [Электронный ресурс] // URL: http://crimestat.ru/offenses_chart (дата обращения: 10.04.2024).
7. Статистическая отчетность формы федерального статистического наблюдения
№ 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» // ЦСИ ФКУ «ГИАЦ МВД России» (10.5.0.16/csi).