Научная статья
УДК 343.2/7
DOI: 10.37973/KUI.2023.93.91.010

# ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АСПЕКТ

Адель Миннурович Каримов,
Казанский юридический институт МВД России, Казань, Россия,
karimov485@mail.ru

***Аннотация***

**Введение:** в статье проведен анализ правовых норм, устанавливающих ответственность за совершение преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (далее – ИТТ), а также положений подзаконных актов, регулирующих порядок опубликования сведений о состоянии преступности в Российской Федерации. Исследованию подвергнуты понятийный аппарат, особенности некоторых признаков объекта преступлений в сфере компьютерной информации, их объективной стороны, правоприменительная практика привлечения виновных в совершении преступлений с использованием ИТТ, к уголовной ответственности.

**Материалы и методы:** методологическую основу исследования составила совокупность общенаучных и частнонаучных методов познания: диалектический, догматический, семантический, формально-логический, статистический методы, методы анализа и синтеза. Материалами исследования послужили нормы уголовного законодательства России, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», международных договоров и соглашений Российской Федерации, подзаконных нормативных актов, статистические данные публичных образований, правоприменительная практика судов общей юрисдикции за 11 месяцев 2022 года, научная литература.

**Результаты исследования:** констатируется, что границы между двумя правовыми категориями зачастую необоснованно размываются. Автором разработаны элективные уголовно-правовые, криминологические и криминалистические признаки, по которым следует разграничивать преступления в сфере компьютерной информации и преступления, совершаемые с использованием ИТТ. Внесены предложения по закреплению в редакции Уголовного кодекса Российской Федерации (УК РФ) дефиниции юридической категории «информационно-телекоммуникационная сеть» (далее – ИТС) в виде примечания к ст. 110 УК РФ; изложен авторский научный подход к дифференциации преступлений с названными квалифицирующими признаками и преступлений в сфере компьютерной информации; сформулированы и научно обоснованы рекомендации по внесению изменений в перечень размещаемой в ИТС «Интернет» официальной статистической информации, утвержденный приказом Генпрокуратуры России от 12.10.2022 № 589.

**Обсуждение и заключение:** выявлено необоснованное смешивание двух правовых категорий: преступления в сфере компьютерной информации и преступления, совершаемые с использованием ИТТ. По факту эти категории разительно отличаются друг от друга на основании их уголовно-правовых, криминологических, криминалистических признаков. Существенно дифференцирована и их доля в структуре преступности.

*Ключевые слова: киберпреступление; компьютерная информация; информационно-телекомуникационная сеть; хакер*



**Для цитирования:** Каримов А.М. Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 1 (51). С. 75 – 82. DOI: 10.37973/KUI.2023.93.91.010

Scientific article
UDC 343.2/7
DOI: 10.37973/KUI.2023.93.91.010

# COMPUTER CRIMES AND CRIMES COMMITTED THROUGH THE USE OF MODERN TECHNOLOGY: A COMPARATIVE LEGAL ASPECT

Adel Minnurovich Karimov,
the Kazan Law Institute of MIA of Russia, Kazan', Russia,
karimov485@mail.ru

***Abstract***

**Introduction:** the article analyzes the legal norms that establish responsibility for committing crimes in the area of computer information and crimes committed with the use of information and telecommunication technologies (hereinafter – ITT), as well as the provisions of secondary legislation governing the publication of information about the state of crime in the Russian Federation. The study is subject to conceptual apparatus, peculiarities of certain features of the object of crimes in the area of computer information, their objective side, law enforcement practice of bringing the perpetrators of crimes using ITT, to criminal responsibility.

**Materials and Methods:** the methodological basis for the study is a combination of general scientific and particular scientific methods of cognition: dialectical, dogmatic, semantic, logical, methods of analysis and synthesis. The materials of the study were the criminal legislation of the Russian Federation, the Federal Law of July 27, 2006 N 149-FZ "On information, information technologies and information protection", international treaties and agreements of the Russian Federation, by-laws, statistical data of public entities, law enforcement practice, scientific literature.

**Results:** it is stated that the boundaries between the two legal categories are often unreasonably blurred. The author developed elective criminal-law, criminological and criminological characteristics that should be used to distinguish between crimes in the area of computer information and crimes committed with the use of ITT. Proposals to enshrine in the wording of the Criminal Code of the Russian Federation (CC RF) the definition of the legal category of "information and telecommunication network" (hereinafter – ITS) as a note to Art. 110 of the Criminal Code, outlined the author's scientific approach to the differentiation of crimes with the above qualifying signs of crime and computer crimes; formulated and scientifically justified recommendations for amendments to the list of official statistical information placed in the ITS "Internet", approved by Order of the General Prosecutor.

**Discussion and Conclusions:** unreasonable mixing of two legal categories was revealed: crimes in the area of computer information and crimes committed with the use of ICT. In fact, these categories are strikingly different from each other based on their criminal law, criminological, forensic features. Significantly differentiated and their share in the structure of crime.

*Keywords: cybercrime; cyberspace; information technologies; computer crimes; computer information*



**For citation:** Karimov A.M. Computer Crimes and Crimes Committed Through the Use of Modern Technology: a Comparative Legal Aspect. Bulletin of the Kazan Law Institute of MIA of Russia. 2023;14(1): 75 – 82. (In Russ.). DOI: 10.37973/KUI.2023.93.91.010

## Введение

По данным МВД России, за 2021 год на территории России зарегистрировано более 2 млн преступлений, при этом «каждое четвертое совершается с использованием IT технологий»[1]. В 2021 году было зарегистрировано 517,7 тыс. преступлений, совершенных с использованием ИТТ, или преступлений в сфере компьютерной информации. К началу 2022 года продолжилась тенденция снижения общего количества совершенных преступлений по всем условным категориям преступности, за исключением одного показателя – уровня киберпреступности, который продолжил демонстрировать хотя и небольшой, но стабильный прирост (1,4%)[2].

[1] Информация МВД России о состоянии преступности. URL: https://mvdmedia.ru/news/official/mvd-rossii-publikuet-informatsiyu-o-sostoyanii-prestupnosti-za-vosem-mesyatsev-2022-goda/(дата обращения: 24.11.2022).

[2] Краткая характеристика состояния преступности в Российской Федерации за 2020, 2021 гг., январь-август 2022 года. URL: https://мвд.рф/reports/item/32515852/ (дата обращения: 24.11.2022).

По мнению исследователей, основными векторами распространения ИТ-угроз, в том числе и для государственного сектора, выступают использование шифровальщиков, деятельность по продаже доступа в скомпрометированные сети, мошенничество, фишинг и спам [1, с. 63], а сама киберпреступность стала «одной из главных проблем XXI в.» [2, с. 52].

**Обзор литературы**

Правовую базу исследования составили УК РФ, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Конвенция о преступности в сфере компьютерной информации ETS № 185, Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности, Концепции создания Евразийской инновационной системы, указ Президента Российской Федерации от 02.12.2016 № 646, приказ Генпрокуратуры России от 12.10.2022 № 589.

Выявить особенности уголовно-правовых норм, регламентирующих ответственность за совершение киберпреступлений, определить их специфику, дифференцировать и классифицировать виды киберпреступлений позволили работы В.М. Елина [1], А.А. Лебедевой [2], Батурина, С.В. Полубинской [3], Г.Р. Григоряна [4], А.Н. Мондохонова [5].

**Материалы и методы**

Методологическую основу статьи составили диалектический подход к познанию юридической природы норм об ответственности за совершение киберпреступлений, содержанию видов компьютерной преступности, общенаучные и частные методы исследования (анализ, синтез, дедукция, индукция, статистический метод), которые применялись при изучении структуры киберпреступности, сравнении противоправных деяний, совершаемых в сфере компьютерной информации, и преступлений, совершаемых с использованием ИТТ, и формулировании предложений по совершенствованию российского уголовного законодательства и подзаконных актов.

Материалами исследования послужили положения действующего российского уголовного законодательства, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», подзаконных актов, правоприменительная практика, сведения о количестве преступлений и структуре преступности в России, научная юридическая литература.

**Результаты исследования**

Как справедливо отмечают исследователи, «высокотехнологический уклад жизни порождает и высокотехнологические преступления» [3, с. 78]. Статистические данные демонстрируют несомненную и безапелляционную актуальность темы противодействия киберпреступности, но приходится констатировать, что статистика не достаточно объективно отражают реальную картину происходящих в стране социальных процессов, которые в науке иногда называют трансформацией или цифровизацией преступности. Это обусловлено следующими факторами: во-первых, в настоящее время отмечается высокая латентность противоправных действий, совершаемых с использованием информационных технологий. Иными словами, большая часть преступлений, посягающих на общественные отношения в сфере информационных технологий, не фиксируется официальной статистикой. Это во многом обусловлено возможностью преступников оставаться анонимными (использование VPN и TOR), избегать непосредственного контакта с потерпевшими, широкой аудиторией пользователей информационных ресурсов, упрощением доступа к этим ресурсам, а также организованным и трансграничным характером подобного рода преступности.

Иная причина латентности – низкий уровень доверия граждан к правоохранительной системе. Следует согласиться с мнением исследователей, констатирующих следующее: «причины высокотехнологических преступлений – не в высоких технологиях, а в слабостях государства, которое не в состоянии обеспечить адекватное правовое регулирование и подготовку специалистов, которые могли бы эффективно противостоять высокотехнологической преступности» [3, с. 78].

Во-вторых, статистические данные МВД России формируются в соответствии с положениями приказа Генеральной прокуратуры Российской Федерации № 589, утверждающего перечень размещаемой в ИТС «Интернет» официальной статистической информации[1]. Пункт 12 данного документа регламентирует необходимость опубликования обобщенных сведений о «зарегистрированных преступлениях, совершенных с использованием ИТТ или в сфере компьютерной информации». Таким образом, количество зарегистрированных преступлений по двум отдельным

[1] Об утверждении перечня размещаемой в информационно-телекоммуникационной сети «Интернет» официальной статистической информации: приказ Генпрокуратуры России от 12.10.2022 № 589 // Законность. 2022. № 11.

показателям суммируется. Обобщение в одном пункте двух различных уголовно-правовых категорий: преступления, совершаемые с использованием ИТТ, и преступления в сфере компьютерной информации – представляется совершенно необоснованным и ошибочным.

Ответственность за преступления в сфере компьютерной информации достаточно четко регламентирована как в отечественном уголовном, так и в международном праве. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [1] в качестве таковых называет:

1. Правонарушения, связанные с использованием компьютерных средств: подлог с использованием компьютерных технологий (статья 7); мошенничество с использованием компьютерных технологий (статья 8).

2. Правонарушения, связанные с содержанием данных: правонарушения, связанные с порнографией (статья 9).

3. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем: противозаконный доступ (статья 2); воздействие на функционирование системы (статья 5); противозаконное использование устройств (статья 6); неправомерный перехват (статья 3); воздействие на данные (статья 4).

Составы преступлений из третьей группы Конвенции нашли свое отражение и в отечественном уголовном законодательстве[2], хотя Конвенция не была ратифицирована Российской Федерацией. В главе 28 УК РФ нормотворец выделил в отдельную группу ряд преступлений, которые, как и в упомянутой выше Конвенции, именуются «преступлениями в сфере компьютерной информации[3]». Однако подчеркнем, что УК РФ толкует эту правовую категорию значительно уже Конвенции и этим словосочетанием объединяет лишь 4 состава. Эти 4 состава не относятся к правонарушениям, связанным с содержанием данных или с использованием компьютерных средств, которые в тексте Конвенции также именуются преступлениями в сфере компьютерной информации.

В отличие от преступлений в сфере компьютерной информации, понятие «преступления, совершаемые с использованием ИТТ» в УК РФ, да и в ином отраслевом законодательстве, за исключением упомянутого выше пункта 12 приказа Генеральной прокуратуры РФ № 589, вовсе не используется. Это не означает, что отечественный законодатель, игнорируя положения Конвенции, оставил без внимания правонарушения, связанные с содержанием данных или связанные с использованием компьютерных средств. В законе используется иная терминология, которую можно назвать синонимичной.

УК РФ в качестве признаков, квалифицирующих преступное деяние, указал совершение преступления в информационно-телекоммуникационных сетях (включая сеть Интернет)» (ст. 110 УК РФ) и совершение преступления с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) (ст. 110[2] УК РФ). Дополнительно подчеркнем, что и систематизировал их нормотворец дифференцированно, не связывая с категорией «преступления в сфере компьютерной информации».

Иными категориями или дефинициями, каким-либо образом регулирующими общественные отношениями, связанные с противодействием преступности в сфере информационных технологий, российское законодательство не оперирует.

ИТТ – информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации[4]. ИТС – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[5]. Таким образом, следует резюмировать, что понятия ИТТ, ИТС являются, по сути, синонимичными, поскольку ни одна ИТТ не может функционировать вне ИТС.

Учитывая вышесказанное, следует заключить, что в отечественном уголовном законе, по аналогии с Конвенцией о преступности в сфере компьютерной информации (ETS № 185), можно выделить три условные группы киберпреступлений: 1) преступления в сфере компьютерной

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23.11.2001). URL: https://base.garant.ru/4089723/ (дата обращения 24.11.2022).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.09.2022) // Собрание законодательства Российской Федерации. 1996. 17 июня. № 25. Ст. 2954.

[3] Компьютерная информация – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Примечание 1 к ст. 272 УК РФ.

[4] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности (заключено в г. Санкт-Петербурге 20.11.2013) // Бюллетень международных договоров. 2015. № 10. С. 7 – 13.

[5] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации. 2006. 31 июля. № 31 (1 ч.). Ст. 3448.

информации; 2) преступления, совершаемые в ИТС; 3) преступления, совершаемые с использованием ИТС. Если первую группу преступлений законодатель объединил в одной главе, то составы, относящиеся к последним двум, в российском уголовном законе размещены хаотично, исходя из родовых и видовых характеристик объекта преступления. Они не имеют никакого отношения к главе 28 УК РФ.

Преступления в сфере компьютерной информации – предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда регламентированному законом порядку осуществления информационных процессов, посягающие на компьютерную информацию, содержащуюся на одиночном устройстве или составляющей информационной системы. Видовой объект этих преступлений – общественные отношения, складывающиеся по поводу обеспечения конфиденциальности, целостности и доступности компьютерной информации, сохранности средств, используемых для ее обработки. Исходя из приведенной дефиниции, очевидно, что такие противоправные деяния характеризуются больше не способом совершения преступления, а, скорее, предметом преступного посягательства.

Как мы уже отметили, преступления в сфере компьютерной информации размещены законодателем в одноименной главе 28 УК РФ, в которую включены общественно опасные деяния, предусмотренные: ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации»; ст. 274[1] «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Отличительными признаками механизма совершения преступлений в сфере компьютерной информации, на наш взгляд, являются «высокая квалификация» лица, совершающего подобные преступления, а также инструмент или орудие совершения преступления и сокрытия его следов. На это обратила внимание Генеральная прокуратура России еще в 2014 году. В одном из рекомендательных документов было отмечено, что специфика преступлений в сфере компьютерной информации обусловлена использованием при их совершении высоких технологий и новейших достижений науки и техники, необходимостью обладания определенным уровнем специальных познаний[1].

На наш взгляд, подобные преступления может совершить далеко не каждый человек. Этот неформальный «специальный субъект» объективно должен обладать глубокими познаниями в сфере информационных технологий, программирования, способов и методов неправомерного доступа (хакер, вирусописатель, специалист по фишингу, специалист по социальной инженерии, криптолокер-шифровальщик, специалисты по совершению DDoS-атак). Для совершения преступления он использует сложное техническое и программное обеспечение (вредоносное ПО, программы и серверы-анонимайзеры, программы криптопреобразования, ботнеты, уязвимости программного обеспечения и информационных систем («бэкдоры»)).

Необходимо отметить еще и то, что весь этот усложненный механизм совершения противоправного деяния обусловливает сложности в выявлении, раскрытии, расследовании подобного рода преступлений. Проблемы возникают при установлении IP-адресов, с которых совершались неправомерный доступ к компьютерной информации, рассылка фишинговых ссылок и вредоносного ПО, установлении собственников фишинговых страниц, криптокошельков, вирусологическом анализе троянских программ, хакерских утилит и вирусов, проведении компьютерных экспертиз.

Преступления, совершаемые с использованием ИТТ, на наш взгляд, это широкий спектр разнородных противоправных действий, отличительным признаком которых является не предмет преступного посягательства, а механизм и инструмент причинения вреда различным по родовым признакам охраняемым уголовным законом общественным отношениям или среда, в которой совершается, запрещенное уголовным законом деяние. Так, чаще всего подобным инструментом выступают ИТС «Интернет» и ее различные ресурсы (электронный банкинг, транзакции, блокчейн, социальные сети, мессенджеры, онлайн-платформы по продаже товаров, «Гидра», ее аналоги и в целом «Даркнет»[2]). Интернет же становится и средой совершения преступлений, именуемой в науке «ки-

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России). Документ опубликован не был. Текст документа приведен в соответствии с публикацией на сайте http://genproc.gov.ru по состоянию на 15.04.2014.

[2] «Теневая сеть», под которой понимается скрытая сеть, соединения которой устанавливаются по типу р-2-р (peer-to-peer, децентрализованная сеть).

берпространством». Увеличение темпов перехода традиционных сфер деятельности общества (образования, государственных услуг, покупки и продажи товаров, финансовых активов и др.) из уже ставшей аутентичной аналоговой формы в киберпространство и обусловливает рост преступных посягательств в сети. При этом ИТС, информационные ресурсы и информационные системы не становятся предметом преступных посягательств. По мнению некоторых исследователей, регламентируя уголовную ответственность за совершение преступлений с использованием ИТТ, российское уголовное законодательство делает только первые шаги, пытаясь отразить в положениях Особенной части УК РФ растущую криминальную реальность, тесно связанную с виртуальным пространством общественной жизни, и защитить активно развивающиеся электронные и цифровые формы имущественных отношений [4, с. 14].

Ответственность за преступления, совершаемые с использованием ИТТ, регламентирована в тексте Особенной части УК РФ: 1) путем закрепления квалифицированного или особо квалифицированного состава (например, п. «г» ч. 3 ст. 158); 2) путем включения в его редакцию нормы с индексом (например, ст. $159^3$). В соответствии с указанием Генпрокуратуры России № 361/11, МВД России № 1 от 30.06.2022[1], помимо указанных двух составов, к перечню преступлений, совершаемых с использованием ИТТ, относятся: 1) без дополнительных условий: ст. $159^6$, 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. $222^2$, п. «д» ч. 2 ст. 230, п. «г» ч. 2 ст. $242^2$, ст. 272, 273, 274, $274^1$; 2) при наличии определенных условий: п. «д» ч. 2 ст. 110, п. «д» ч. 3 и ч. 6 ст. $110^1$, ч. 2 ст. $110^2$, ч. 2 ст. $128^1$, ч. 3 ст. 137, п. «в» ч. 2 ст. $151^2$, ст. $171^2$, $185^3$, ч. 2 ст. $205^2$, п. «б» ч. 2 и чч. 3, 4, 5 ст. $228^1$, чч. 3, 4 ст. 230, чч. 1.1, 2 и 3 ст. $238^1$, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. $242^1$, п. «г» ч. 2 ст. 245, ч. 1.1, п. «б» ч. 2, чч. 2.1, 3 и 3.1 ст. $258^1$, ч. 2 ст. 280, ч. 2 ст. $280^1$, ст. 282, п. «в» ч. 2 и ч. 4 ст. $354^1$., ст. 119, $128^1$, 133, 135, 137, 138, $138^1$, 146, 150, 151, ч. 4 ст. 158, ст. 159, 163, 174, $174^1$, 183, 186, 187, $205^1$, 207, $207^1$, $207^2$, $207^3$, 210, 228, $228^2$, $228^3$, $228^4$, 229, 234, $234^1$, 238, 240, $280^3$, 283, $283^1$, $284^2$, 292, 296, $298^1$, 311, 327, $327^1$, 354. На основании анализа статистических данных авторы пришли к следующим выводам: «информационно-телекоммуникационные технологии преимущественно используются при совершении преступлений против собственности, а также в сфере незаконного оборота наркотических средств и психотропных веществ, что в совокупности составляет 82,6% от общего числа преступлений, совершенных с использованием информационно-телекоммуникационных технологий» [5, с. 41].

В отличие от правовой категории «преступления в сфере компьютерной информации», субъектом «преступления, совершенного с использованием ИТТ» может стать любое дееспособное лицо, достигшее возраста уголовной ответственности. Ему не нужны глубокие познания в сфере IT, сложное техническое и программное обеспечение. Достаточно иметь базовые навыки использования персонального компьютера и ресурсов ИТС «Интернет» и, соответственно, иметь под рукой устройство, подключенное к сети, хотя и это не всегда требуется. Так, например, гр. «И» примерно в 18.00, находясь по адресу: <адрес>, обнаружил утерянную платежную кредитную банковскую карту «Тинькофф Банка», №**, с чипом, позволяющим осуществлять покупки на сумму до 1000 рублей без ввода пин-кода, оформленную на имя потерпевшего № 1. После этого, предположив, что на счету данной карты могут находиться денежные средства, а также присвоив ее себе, гр. «И» зашел в магазин, путем прикладывания данной карты к платежному терминалу произвел покупку товара на сумму до 1000 рублей. Таким образом, гр. «И» совершил хищение денежных средств с банковского счета №, открытого в АО «Тинькофф Банк»[2].

Анализ применения судами пункта «г» ч. 3 ст. 158 УК РФ (с использованием ресурса www.sudact.ru было изучено 30 судебных решений, вынесенных на территории РФ в период 11 месяцев 2022 года) дает основание утверждать, что 95% случаев во многом аналогичны приведенному выше примеру. Именно пункт «г» части 3 статьи 158 УК РФ формирует в статистических отчетах МВД России значительную долю преступлений, совершаемых с ИТТ.

**Обсуждение и заключение**

При объективном анализе механизма, способа совершения преступлений с использованием ИТТ, криминологического портрета самого преступника, которого в приведенном выше примере

[1] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генпрокуратуры Российской Федерации № 361/11, МВД России № 1 от 30.06.2022 // Документ опубликован не был. СПС «КонсультантПлюс» (дата обращения: 12.12.2022).

[2] Приговор Киевского районного суда города Симферополя Республики Крым от 29.06.2021 по делу № 1-272/2021. URL: https://pravoilevo.ru/prigovor-obvinyaemomu-po-p-g-ch-3-st-158-uk-rf-krazha-sovershennaya-s-bankovskogo-scheta/(дата обращения 15.11.2022).

очень сложно назвать киберпреступником, приходим к выводу, что статистические данные официальных органов не отражают реальную картину компьютерной преступности в стране и могут ввести в заблуждение лицо, изучающее данную информацию.

Согласно статистическим данным за 2021 год, на территории РФ за совершение преступлений в сфере компьютерной информации, т.е. тех преступлений, которые совершаются «профессиональными» преступниками (хакерами, вирусописателями и др.), были осуждены 225 человек, из них: по ст. 272 УК РФ – 133 (ч. 1. – 9, ч. 2 – 13, ч. 3 – 111); по ст. 273 УК РФ – 77 (ч. 1 – 14, ч. 2 – 63); ст. 274 УК РФ – 0; ст. 274[1] – 15 (ч. 1 – 2, ч. 2 – 1, ч. 3 – 2, ч. 4 – 10)[1]. Результаты анализа статистического отчета МВД России о количестве преступлений, совершенных с использованием ИТТ или в сфере компьютерной информации (517,7 тысяч преступлений), позволяют сделать вывод, что в пункте 12 приказа Генеральной прокуратуры России доля преступлений в сфере компьютерной информации, т.е. «реальных» киберпреступлений, лишь 0,04%, а доля преступлений, совершаемых с использованием ИТТ, т.е. преступлений, совершаемых «неквалифицированными» преступниками, составляет лишь 99,96%. Данный факт подтверждает тезис, что статистические данные МВД России некорректно отражают уровень киберпреступности в стране. Это может привести к искажению общественного мнения о состоянии оперативной обстановки в государстве, поскольку в представлении большинства граждан IT-преступность – это преступные деяния, совершаемые исключительно хакерами, кракерами, вирусописателями и иными «профессиональными» преступниками.

Таким образом, на статистические данные об уровне киберпреступности в стране оказывают влияние два субъективных антропогенных фактора. Первый (понижающий) – это латентность киберпреступлений, второй (завышающий) – это непрозрачный и, вероятно, некорректный подбор критериев отнесения тех или иных преступных явлений к категории киберпреступности.

В связи с изложенным необходима дифференциация сведений об уровне преступности в сфере компьютерной информации и уровня преступлений, совершаемых с использованием ИТТ. Эти показатели следует обобщать отдельно, чтобы у граждан, изучающих статистические отчеты МВД России, не сформировался ложный вывод, согласно которому каждое четвертое преступление в РФ совершается хакерами, вирусописателями, владельцами ботнетов и иными «профессиональными» киберпреступниками. Они должны понимать, что этот показатель значительно ниже заявленного и скрыт в общем массиве преступлений, не относящиеся к реальной киберпреступности. В этих целях необходимо внести изменения в пункт 12 приказа Генеральной прокуратуры России № 589 и изложить его в следующей редакции: «Зарегистрировано преступлений в сфере компьютерной информации». Отдельно рекомендуется закрепить в частных пунктах приказа необходимость размещения сведений о зарегистрированных преступлениях, совершенных с ИТС и преступлениях, совершенных в ИТС.

Дефиницию юридической категории «ИТС» предлагаем регламентировать в УК РФ применительно к нормам, где ее использование указано в качестве квалифицирующего признака преступления. В примечании к статье 272 УК РФ приведена дефиниция словосочетания «компьютерная информация», что объективно обусловлено необходимостью разъяснения сложного технического феномена, необходимого для правильной квалификации противоправного деяния. Нелогичным с точки зрения юридической техники представляется то, что, раскрыв в виде примечания значение термина «компьютерная информация», нормотворец не раскрыл юридическое значение другого технического термина, используемого в тексте УК – «ИТС». Это понятие, несомненно, может толковаться правоприменителем неоднозначно, поскольку разнообразие сетей, их топология, специфика сфер преступного применения и информации, размещаемой в киберпространстве, обусловливают возможные сложности в уяснении сути этого технологического феномена и верной квалификации преступных посягательств, совершаемых с использованием сети или совершаемых в сети. Федеральным законом от 27.07.2006 № 149-ФЗ уже раскрыто значение этого термина, однако положения данного нормативного акта раскрывают его общую спецификацию, не конкретизируя признаки ИТС как инструмента противоправного деяния.

В связи с вышеизложенным предлагаем регламентировать в виде примечания к ст. 110 УК РФ законодательную дефиницию следующего содержания: «Под ИТС понимается технологическая система передачи данных по проводным и беспроводным каналам связи, используемая для

[1] Данные о назначенном наказании по статьям УК. URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения 10.11.2022).

передачи сообщений в социальных сетях, платформах, онлайн-сервисах или веб-сайтах, предназначенных для коммуникации пользователей, интернет-мессенджерах; совершения транзакций в электронных платежных системах в процессе расчета между интернет-пользователями при покупке-продаже товаров и оплате услуг, в том числе на онлайн-площадках».

## СПИСОК ИСТОЧНИКОВ

1. Елин В.М. О подходах к криминологической характеристике лиц, совершающих преступления в сфере компьютерной информации // Российский следователь. 2022. № 7. С. 61 – 65. DOI: 10.18572/1812-3783-2022-7-61-65
2. Лебедева А.А. Особенности расследования киберпреступлений // Безопасность бизнеса. 2021. № 6. С. 48 – 56. DOI: 10.18572/2072-3644-2021-6-48-56
3. Батурин Ю.М., Полубинская С.В. Совершенствование законодательных норм уголовно-правового цикла в контексте высокотехнологического будущего // Преступность в XXI веке. Приоритетные направления противодействия: монография / под ред. А.Н. Савенкова. Москва: ЮНИТИ-ДАНА: Закон и право, 2020. С. 78.
4. Григорян Г.Р. О социально-правовой сущности корыстных имущественных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Российская юстиция. 2020. № 10. С. 13 – 15.
5. Мондохонов А.Н. Криминализация «преступной деятельности» в условиях развития информационно-телекоммуникационных технологий // Законность. 2020. № 6. С. 38 – 43.

## REFERENCES

1. Elin V.M. O podhodah k kriminologicheskoj harakteristike lic, sovershayushchih prestupleniya v sfere komp'yuternoj informacii // Rossijskij sledovatel'. 2022. № 7. S. 61 – 65. DOI: 10.18572/1812-3783-2022-7-61-65
2. Lebedeva A.A. Osobennosti rassledovaniya kiberprestuplenij // Bezopasnost' biznesa. 2021. № 6. S. 48 – 56. DOI: 10.18572/2072-3644-2021-6-48-56
3. Baturin YU.M., Polubinskaya S.V. Sovershenstvovanie zakonodatel'nyh norm ugolovno-pravovogo cikla v kontekste vysokotekhnologicheskogo budushchego // Prestupnost' v XXI veke. Prioritetnye napravleniya protivodejstviya: monografiya / pod red. A.N. Savenkova. Moskva: YUNITI-DANA: Zakon i pravo, 2020. S. 78.
4. Grigoryan G.R. O social'no-pravovoj sushchnosti korystnyh imushchestvennyh prestuplenij, sovershaemyh s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij // Rossijskaya yusticiya. 2020. № 10. S. 13 – 15.
5. Mondohonov A.N. Kriminalizaciya «prestupnoj deyatel'nosti» v usloviyah razvitiya informacionno-telekommunikacionnyh tekhnologij // Zakonnost'. 2020. № 6. S. 38 – 43.

**Информация об авторе:**
**Каримов Адель Миннурович,** кандидат юридических наук, старший преподаватель кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России, ORCID: 0000-0003-4734-7037, karimov485@mail.ru
Автор прочитал и одобрил окончательный вариант рукописи.

**Information about the author:**
**Karimov Adel M.,** Candidate in Law (Research doctorate), Senior Lecturer of the Department of Economics, Financial Law and Information Technologies in the Activity of Internal Affairs Bodies of the Kazan Law Institute of MIA of Russia, ORCID: 0000-0003-4734-7037, karimov485@mail.ru
The author has read and approved the final version of the manuscript.

Статья получена: 23.11.2022.
Статья принята к публикации: 22.03.2023.
Статья опубликована онлайн: 24.03.2023.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.