2023. Т. 9, № 4. С. 102–107
2023, vol. 9, no. 4, pp. 102–107

ТРИБУНА МОЛОДОГО УЧЕНОГО
TRIBUNE OF YOUNG SCIENTIST

DOI: 10.18287/2542-047X-2023-9-4-102-107

НАУЧНАЯ СТАТЬЯ

УДК 343.3/.7

Дата поступления: 06.08.2023
рецензирования: 09.09.2023
принятия: 15.11.2023

Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана

А. Г. Корпеев
Самарский национальный исследовательский университет
имени академика С. П. Королева, г. Самара, Российская Федерация
E-mail: atakor@mail.ru

Аннотация: В уголовно-правовых доктринах Российской Федерации и Туркменистана, а также в нормативных правовых актах и иных официальных документах, принятых в этих государствах, существуют разные подходы к классификации преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Данные различия приводят к снижению результативности уголовно-правового противодействия соответствующей разновидности противоправных деяний. В связи с этим автором анализируются альтернативные подходы к классификации преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Делается вывод, что, исходя из структурных особенностей Уголовных кодексов Российской Федерации и Туркменистана, данные разновидности общественно опасных деяний следует классифицировать в зависимости от особенностей объекта и субъекта этих противоправных посягательств, характера и степени общественной опасности деяния, формы вины, а также способов и средств совершения названных преступлений. Сделанные в настоящей статье выводы и рекомендации имеют определенную теоретическую значимость и могут использоваться для дальнейшего исследования классификации и типологии преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий) по уголовному законодательству Российской Федерации и Туркменистана.
Ключевые слова: классификация преступлений; основания классификации преступлений; виды преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий); объект преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий); способы и средства преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий).
Цитирование. Корпеев А. Г. Классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по уголовному законодательству Российской Федерации и Туркменистана // Юридический вестник Самарского университета Juridical Journal of Samara University. 2023. Т. 9, № 4. С. 102–107. DOI: https://doi.org/10.18287/2542-047X-2023-9-4-102-107.
Информация о конфликте интересов: автор заявляет об отсутствии конфликта интересов.

Ата Гельдыевич Корпеев – помощник ректора, Самарский национальный исследовательский университет имени академика С. П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

SCIENTIFIC ARTICLE

Submitted: 06.08.2023
Revised: 09.09.2023
Accepted: 15.11.2023

Classification of crimes committed using information and telecommunication networks (technologies) under the criminal legislation of the Russian Federation and Turkmenistan

A. G. Korpeev
Samara National Research University, Samara, Russian Federation
E-mail: atakor@mail.ru

Abstract: In the criminal law doctrines of the Russian Federation and Turkmenistan, as well as in the legal acts and official documents adopted in these states, there are different approaches to the classification of crimes committed using information and telecommunication networks (technologies). These differences lead to a decrease in the effectiveness of criminal law counteraction of the corresponding type of illegal acts. In this regard, the author analyzes alternative approaches to the classification of crimes committed using information and telecommunication networks (technologies). It is concluded that based on the structural features of the Criminal Codes of the Russian Federation and Turkmenistan these types of socially dangerous acts should be classified depending on the characteristics of the object and subject of these unlawful attacks, the nature and degree of public danger of the act, the form of guilt, as well as the methods and means of committing these crimes. The conclusions and recommendations made in this article have a certain theoretical significance and can be used to further study of the classification of crimes committed using information and telecommunication networks (technologies) under the criminal legislation of the Russian Federation and Turkmenistan.
Key words: classification of crimes; grounds for classifying crimes; types of crimes committed with the use of information and telecommunication networks (technologies); object of crimes committed with the use of information and telecommunication networks (technologies); methods and means of crimes committed using information and telecommunication networks (technologies).
Citation. Korpeev A. G. *Klassifikatsiya prestupleniy, sovershaemykh s ispol'zovaniem informatsionno-telekommunikatsionnykh setey (tekhnologiy), po ugolovnomu zakonodatel'stvu Rossiyskoy Federatsii i Turkmenistana* [Classification of crimes committed using information and telecommunication networks (technologies) under the criminal legislation of the Russian Federation and Turkmenistan]. *Iuridicheskii vestnik Samarskogo universiteta* Juridical Journal of Samara University, 2023, vol. 9, no. 4, pp. 102–107. DOI: https://doi.org/10.18287/2542-047X-2023-9-4-102-107 [in Russian].
Information on the conflict of interest: author declares no conflict of interest.

Ata G. Korpeev – assistant rector, Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russian Federation.

По данным Международного Союза Электросвязи, являющегося учреждением в структуре деятельности ООН, в настоящее время в мире пользуются глобальными сетями телекоммуникации 3,2 миллиарда человек, из них 2 миллиарда человек - жители развивающихся стран [1]. Аудиторией информационно-телекоммуникационных сетей в основном являются молодые люди в возрасте от 15 до 28 лет. Столь быстрое развитие информационно-телекоммуникационных сетей (технологий) имеет как положительные, так и отрицательные аспекты. Последние связаны с негативными последствиями от использования высоких технологий в преступных и иных противоправных целях.

В настоящее время во всем мире наблюдается рост преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Согласно статистическим данным МВД РФ, в 2021 году только в Российской Федерации совершено около 520 тысяч преступлений с использованием информационно-телекоммуникационных сетей (технологий) [2]. В 2022 году в Российской Федерации было зарегистрировано уже 1.5 млрд кибератак [3]. Связано это, конечно, с высоким технологическим развитием общества и проводимой политикой цифровизации, направленной на внедрение различных информационно-телекоммуникационных технологий во все сферы жизни современного человека.

Использование информационно-телекоммуникационных сетей в противоправных целях может привести к необратимым последствиям ввиду следующих обстоятельств. Во-первых, функциональная составляющая таких сетей расширяет возможности для злоумышленников использовать их при совершении самых разных преступлений, начиная от умышленного причинения вреда личности и до различных деяний против общества, государства, мира и безопасности человечества. Во-вторых, различные информационно-телекоммуникационные сети имеют функциональную возможность для их конспиративного использования злоумышленниками при осуществлении деяния, что приводит к значительному повышению уровня латентности преступности. В-третьих, использование информационно-телекоммуникационных сетей в противоправных целях может носить транснациональный характер, что приводит к затруднению в расследовании и привлечении к ответственности виновных лиц.

В научной сфере такие преступления определяются как общественно опасные деяния, посягающие, помимо безопасности компьютерных систем, на иные правоохраняемые объекты, к первостепенным из которых относятся: личная безопасность, собственность, имущественные права, национальная и мировая безопасность (кибертерроризм) [4, с. 18–21].

В связи с большой значимостью обеспечения информационной безопасности в Российской Федерации принята Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы. Одним из ее принципов является обеспечение государственной защиты интересов российских граждан в информационной среде [5]. В свою очередь, в Туркменистане разработана и утверждена Государственная программа по обеспечению кибербезопасности на 2022–2025 годы.

В уголовном законодательстве России и Туркменистана установлена ответственность за ряд преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий) и посягающих на общественные отношения, возникающие в различных сферах человеческой жизни.

2023. Т. 9, № 4. С. 102–107
2023, vol. 9, no. 4, pp. 102–107

В современной уголовно-правовой науке остро стоит вопрос о классификации этих преступлений с целью приведения более глубокой систематизации действующего уголовного законодательства Российской Федерации и Туркменистана в части данных разновидностей преступлений, а также решения вопросов дифференциации ответственности и индивидуализации наказания. В свою очередь, вопрос о классификации киберпреступлений упирается в проблематику социально-правовой сущности данных разновидностей преступлений, определения содержания объективных и субъективных признаков «цифровых» посягательств, уточнения категорий этих общественно опасных деяний, а также установления за их совершение меры уголовной ответственности.

Процесс появления таких составов преступлений в Уголовном кодексе Российской Федерации (далее – УК РФ) и Уголовном кодексе Туркменистана (далее – УК Туркменистана) напрямую связан со многими международными нормативными правовыми актами. Одним из таких является Европейская конвенция о киберпреступлениях, принятая в Будапеште 23 ноября 2001 года [6]. В данном документе определяется понятие информационно-телекоммуникационных сетей и содержится классификация указанных преступлений на две группы. Первая группа включает в себя преступления, предметом которых является компьютерная информация, например, незаконный перехват компьютерных данных. Вторая группа включает в себя преступления, где информационно-телекоммуникационные сети выступают в качестве средства совершения преступления, например, совершение умышленного причинения материального ущерба другому человеку путем удаления информации.

Таким образом, в рамках Совета Европы преступления с применением информационно-телекоммуникационных технологий можно условно классифицировать на две группы деяний, в которых данные технологии являются: 1) предметом деяния; 2) средством совершения деяния.

Российская Федерация оставила за собой право ратификации данной Конвенции, но по настоящее время так ее и не ратифицировала. Между тем часть правил Конвенции имплементированы в отечественное уголовное законодательство в виде составов преступлений, расположенных в главе 28 «Преступления в сфере компьютерной информации» УК РФ. Такому примеру последовал и Туркменистан, закрепив в своем уголовном законодательстве главу 33 «Преступления в сфере компьютерной информации».

Весомый вклад в противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (технологий), внесло Содружество Независимых Государств (далее – СНГ), участниками которого являются Российская Федерации и Туркменистан. На площадке СНГ было принято соглашение в области обеспечения информационной безопасности от 20 ноября 2013 года (далее – Соглашение), которое заложило методологические принципы борьбы с киберпреступлениями в рамках СНГ [7].

В данном Соглашении закреплено понятие вышеуказанных преступлений. Согласно ст. 2 Соглашения под преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей (технологий), понимаются использование информационных ресурсов и/или воздействие на них в информационном пространстве в противоправных целях [7].

В Соглашении приведена следующая классификация таких преступлений: в первую группу входят противоправные деяния, направленные на компьютерную информацию (несанкционированный доступ к информации, воздействие на информацию), во вторую группу входят деяния, совершаемые с использованием информационно-телекоммуникационных сетей (технологий) (незаконная трансграничная передача информации, информационный терроризм) [7].

Исходя из содержания постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет», данные деяния классифицируются на совершаемые: 1) в сфере компьютерной информации; 2) с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет [8].

Этому есть обоснование. Как уже отмечалось, законодатели Российской Федерации и Туркменистана при закреплении составов преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), руководствовались международным опытом классификации таких деяний. В связи с этим уголовное законодательство России и Туркменистана схоже на сегодняшний день в части системы расположения таких составов преступлений, а именно это так называемая «специальная» группа составов, закрепленных в главе 28 «Преступления в сфере компьютерной информации» УК РФ, главе 33 «Преступления в сфере компьютерной информации» УК Туркменистана, а также квалифицированные составы общеуголовных преступлений с признаком «использование информационно-телекоммуникационных сетей (в том числе сети Интернет)», которые рассредоточены по разным разделам и главам Особенной части УК РФ и УК Туркменистана.

Такого рода классификация деяний является логичной и обоснованной с точки зрения структурных особенностей уголовного законодательства Российской Федерации и Туркменистана. В первом случае закреплены специальные составы, объектом которых является компьютерная информация и различные компьютерные средства

(ст. 272–274[2] УК РФ, ст. 333–335 УК Туркменистана). Тем самым законодатель реализует охранительную функцию важной для личности, общества и государства компьютерной информации. Во втором случае законодатели двух стран, понимая всю опасность противоправного использования информационно-телекоммуникационных сетей (технологий), дифференцируют уголовную ответственность в имеющихся составах преступлений, объектами которых могут являться жизнь и здоровье личности (пп. «д» ч. 2 ст. 110, пп. «д» ч. 3 ст. 110[1] УК РФ, пп. «б» ч. 3 ст. 133, ч. 2 ст. 110[2], ч. 1 ст. 106 УК Туркменистана), общественная безопасность (ч. 2 ст. 205[2] УК РФ, пп. «в» ч. 3 ст. 222 УК РФ, пп. «б» ч. 2 ст. 228[1] УК РФ, пп. «г» ч. 2 ст. 245 УК РФ, пп. «б» ч. 2 ст. 258[1] УК РФ, ч. 2 ст. 175 УК Туркменистана), порядок в сфере экономической деятельности (ч. 1 ст. 171[2] УК РФ, ч. 1 ст. 185[3], ст. 254 УК Туркменистана), собственность (ч. 1 ст. 159[6] УК РФ).

Опираясь на сложившуюся структурную особенность уголовного законодательства России и Туркменистана, представляется возможным условно классифицировать данные деяния на две группы. Первая группа деяний характеризуется тем, что совершается в отношении компьютерного устройства либо информации, содержащейся на этом устройстве. Вторая группа деяний – преступления, в которых соответствующие технические средства, включая сеть Интернет, являются средством совершения преступления. Как видно, основанием деления киберпреступлений выступают прежде всего объективные признаки их составов. Это объект, предмет, способ и средство совершения киберпреступлений.

Необходимо также отметить, что в уголовно-правовой доктрине посвящено много научных работ проблеме классификации преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Так, А. А. Ходусов предлагает следующим образом классифицировать данные деяния, основываясь на объекте: 1) преступления против конституционных прав и свобод гражданина, 2) преступления против жизни и здоровья населения, 3) преступления против чести и достоинства, 4) преступления против собственности, 5) преступления в сфере компьютерной информации, 6) преступления против общественной нравственности, 7) преступления против безопасности государства. При этом, как отмечает сам А. А. Ходусов, эта классификация не является идеальной, так как не характеризует данные общественно опасные деяния, а лишь дает им уголовно-правовую оценку [9, с. 90–91].

Классификация преступлений по родовому объекту посягательства является устоявшейся разновидностью дифференциации преступлений не только в рамках российского уголовного законодательства, но и в рамках уголовного законодательства Туркменистана. Объекты данных посягательств делятся по категориям общественной ценности на небольшой ценности (компьютерная информация, общественная нравственность, личные права и свободы человека и гражданина), средней ценности (интересы семьи и несовершеннолетних, собственность, экономическая деятельность, интересы государственной власти), ценные (общественная безопасность) и особо ценные (жизнь человека, мир и безопасность человека, основы конституционного строя и безопасности государства), что позволяет с практической точки зрения верно квалифицировать совершенное противоправное деяние.

С. С. Витвицкая предлагает квалифицировать вышеуказанные деяния в зависимости от субъекта преступления. Это преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), общим или специальным субъектом [10, с. 19–21].

Вместе с тем в уголовном законодательстве России и Туркменистана выделяются следующие категории субъектов рассматриваемых преступлений: лица, осуществляющие неправомерный доступ к охраняемой законом компьютерной информации (ч. 1 ст. 272 УК РФ, 333 УК Туркменистана); лица, осуществляющие неправомерный доступ к охраняемой законом компьютерной информации в группе по предварительному сговору или организованной группой (ч. 2 ст. 272 УК РФ, 335 УК Туркменистана); лица, осуществляющие неправомерный доступ к охраняемой законом компьютерной информации с использованием своего служебного положения (ч. 2 ст. 272 УК РФ); лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети и осуществляющие неправомерный доступ к охраняемой законом компьютерной информации (ч. 2 ст. 272 УК РФ) или нарушающие правила эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ); лица, создающие, внесшие изменения в существующие вредоносные программы, использующие, распространяющие такие программы или машинные носители с такими программами (ч. 1 ст. 273 УК РФ). В рамках этих категорий выделяются как общие, так и специальные субъекты.

Однако в ч. 2 ст. 272 УК РФ, ч. 2 ст. 334 УК Туркменистана законодатели определяют дополнительный признак субъекта преступления, указывая на лицо, которое имеет доступ к электронно-вычислительной машине, к ее системе или их сети, что говорит о наличии специального субъекта в составах рассматриваемых преступлений.

Исходя из вышесказанного, следует констатировать, что исследуемые преступления могут совершать лица, имеющие доступ к электронно-вычислительной машине, а также лица, не имеющие доступа к электронно-вычислительной машине, но при этом осуществляющие неправомерный доступ к охраняемому законом объекту.

Преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), также можно классифицировать исходя из преследуемых виновными целей:

1) преступления, в которых различные средства компьютерных технологий являются конеч-

ной целью преступника, например, противоправное действие направлено на уничтожение такой технологии (ст.ст. 272–273 УК РФ, ст. 334 УК Туркменистана);

2) преступления, при совершении которых компьютерные технологии являются промежуточной целью преступника, т. е. воздействуя на данные технологии, преступник достигает главную цель (например, корыстную - пп. «д» ч. 2 ст. 110, пп. «д» ч. 3 ст. 110^1, пп. «б» ч. 3 ст. 133, ч. 2 ст. 110^2 , ч. 2 ст. 205^2, пп. «в» ч. 3 ст. 222, пп. «б» ч. 2 ст. 228^1, пп. «г» ч. 2 ст. 245, пп. «б» ч. 2 ст. 258^1 УК РФ, а равно ч. 1 ст. 106 и ч. 2 ст. 175 УК Туркменистана);

3) преступления, где высокие технологии являются автоматизированным средством соответствующих общественно опасных деяний (например, ст.ст. 274^1–274^2 УК РФ, ст. 333 и 335 УК Туркменистана).

Согласно ст. 15 УК РФ и ст. 11 УК Туркменистана основанием деления преступлений является общественная опасность преступных деяний. Исходя из этого преступления, совершаемые с использованием информационно-телекоммуникационных сетей (технологий), можно классифицировать по характеру и степени общественной опасности (категориям) на тяжкие (например, ч. 1 ст. 205^1 УК РФ, пп. «д» ч. 2 ст. 230 УК РФ, п. 1.1 ст. 238^1 УК РФ, ст. 107 УК Туркменистана) и особо тяжкие преступления (например, ч. 2 ст. 205^2 УК РФ, ч. 3 ст. 271 УК Туркменистана).

Данная классификация имеет важное значение для решения ряда вопросов уголовно-правового характера: определения опасного и особо опасного рецидива, назначения соответствующего вида наказания, освобождения от уголовной ответственности, определения наличия смягчающих и отягчающих обстоятельств и иных вопросов в рамках уголовно-правовой науки.

Исходя из вышеизложенного, следует констатировать, что классификация преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), по различным основаниям имеет весьма разнообразное прикладное значение. Классификация таких преступлений на основании объекта преступного деяния способствует правильной систематизации таких деяний в рамках Особенной части действующего уголовного законодательства Российской Федерации и Туркменистана. Классификация, основанная на способе и средстве совершения киберпреступлений, имеет не только уголовно-правовое (к примеру, повышение уровня общественной опасности), но и криминалистическое значение. В свою очередь, классификация в зависимости от субъекта криминального деяния способствует определению как основания, так и дифференциации уголовной ответственности в рамках действующего законодательства Российской Федерации и Туркменистана.

В заключение следует отметить, что на сегодняшний день в уголовно-правовой науке сложился комплекс теоретико-прикладного знания о классификации преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий). Действующее уголовное законодательство Российской Федерации и Туркменистана схожи в системе описания и расположения конструкций преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), что позволяет обеспечить их классификацию в зависимости от характера и степени общественной опасности, объекта, субъекта противоправного посягательства, а также способа и средства совершения киберпреступлений. Проблематику классификации преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), трудно считать исчерпанной. В связи с высоким ростом преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (технологий), и их постоянным видообразованием уголовное право России и Туркменистана должно симметрично отражать соответствующие криминогенные тенденции в сфере высоких технологий путем усовершенствования правовых средств противодействия данной разновидности деяний и практики их применения, а также дальнейшей научной проработки путей оптимизации уголовно-правовой материи в киберпространстве.

Библиографический список

1. Официальный сайт Международного союза электросвязи. URL: https://www.un.org/ru/ecosoc/itu/ (дата обращения: 03.08.2023).

2. Официальный сайт МВД России: состояние преступности. URL: https://мвд.рф/reports (дата обращения: 03.08.2023).

3. Игнатова О., Куликов В. Кто кого обманывает // Российская газета. 2022. 14 июля.

4. Мирончик А. С., Суслопаров А. В. Хищение в электронной среде как разновидность информационных преступлений: проблемы разграничения и квалификации // Юридические исследования. 2019. № 9. С. 17–30. DOI: https://doi.org/10.25136/2409-7136.2019.9.30745. EDN: https://www.elibrary.ru/oniejg.

5. Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 03.08.2023).

6. Конвенция о преступности в сфере компьютерной информации от 23 ноября 2001 года ETS № 185 // ЭПС «Система ГАРАНТ». URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (дата обращения: 03.08.2023).

7. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20.11.2013 // СПС «КонсультантПлюс». URL: https://docs.cntd.ru/document/420278452 (дата обращения: 03.08.2023).

8. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 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://vsrf.ru/documents/own/31913/ (дата обращения: 03.08.2023).

9. Безручко Е. В., Ходусов А. А. Преступления, совершаемые с использованием информационно-телекоммуникационных средств: философско-правовое конструирование эффективных классификаций // Философия права. 2020. № 3. С. 89–95. URL: https://cyberleninka.ru/article/n/prestupleniya-sovershaemye-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-sredstv-filosofsko-pravovoe-konstruirovanie/viewer.

10. Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. Т. 1, № 1. С. 126–136. DOI: https://doi.org/10.23947/2949-1843-2023-1-1-126-136.

References

1. *Ofitsial'nyy sayt Mezhdunarodnogo soyuza elektrosvyazi* [Official website of the International Telecommunication Union]. Available at: https://www.un.org/ru/ecosoc/itu/ (accessed: 03.08.2023) [in Russian].

2. *Ofitsial'nyy sayt MVD Rossii: sostoyanie prestupnosti* [Official website of the Ministry of Internal Affairs of Russia: the state of crime]. Available at: https://mvd.rf/reports (accessed: 03.08.2023) [in Russian].

3. Ignatova O., Kulikov V. *Kto kogo obmanyvaet* [Who is deceiving whom]. *Rossiyskaya gazeta*, 2022, July 14 [in Russian].

4. Mironchik A. S., Susloparov A. V. *Khishchenie v elektronnoy srede kak raznovidnost' informatsionnykh prestupleniy: problemy razgranicheniya i kvalifikatsii* [Electronic theft as a kind of computer crime: problems that arise during differentiation and qualification of this kind of crime]. *Yuridicheskie issledovaniya* [Legal Studies], 2019, no. 9, pp. 17–30. DOI: https://doi.org/10.25136/2409-7136.2019.9.30745. EDN: https://www.elibrary.ru/oniejg [in Russian].

5. *Ukaz Prezidenta RF ot 09.05.2017 № 203 «O strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017-2030 gody»* [Decree of the President of the Russian Federation dated 09.05.2017 № 203 «On the strategy for the development of the information society in the Russian Federation for the period 2017–2030»]. *Retrieved from legal reference system «ConsultantPlus»*. Available at: http://www.kremlin.ru/acts/bank/41919 (accessed: 03.08.2023) [in Russian].

6. *Konventsiya o prestupnosti v sfere komp'yuternoy informatsii ot 23 noyabrya 2001 goda ETS № 185* [Convention on Cybercrime as of November 23, 2001 ETS № 185]. *Retrieved from legal reference system «Sistema GARANT»*. Available at: https://base.garant.ru/4089723/ (accessed: 03.08.2023) [in Russian].

7. *Soglashenie o sotrudnichestve gosudarstv-uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v oblasti obespecheniya informatsionnoy bezopasnosti ot 20.11.2013* [Agreement on cooperation between the member states of the Commonwealth of Independent States in the field of information security as of 20.11.2013]. *Retrieved from legal reference system «ConsultantPlus»*. Available at: https://docs.cntd.ru/document/420278452 (accessed: 03.08.2023) [in Russian].

8. *Postanovlenie Plenuma Verkhovnogo Suda RF ot 15.12.2022 № 37 «O nekotorykh voprosakh sudebnoy praktiki po ugolovnym delam o prestupleniyakh v sfere komp'yuternoy informatsii, a takzhe inykh prestupleniyakh, sovershennykh s ispol'zovaniem elektronnykh ili informatsionno-telekommunikatsionnykh setey, vklyuchaya set' «Internet»* [Plenum of the Supreme Court of the Russian Federation as of 15.12.2022 № 37 «On some issues of judicial practice in criminal cases on crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet»]. *Retrieved from legal reference system «ConsultantPlus»*. Available at: https://vsrf.ru/documents/own/31913/ (accessed: 03.08.2023) [in Russian].

9. Bezruchko E. V., Khodusov A. A. *Prestupleniya, sovershaemye s ispol'zovaniem informatsionno-telekommunikatsionnykh sredstv: filosofsko-pravovye konstruirovanie effektivnykh klassifikatsiy* [Crimes committed using information and telecommunication means: philosophical and legal formation of effective classifications]. *Filosofiya prava* [Philosophy of Law], 2020, no. 3, pp. 89–95. Available at: https://cyberleninka.ru/article/n/prestupleniya-sovershaemye-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-sredstv-filosofsko-pravovoe-konstruirovanie/viewer [in Russian].

10. Vitvitskaya S. S., Vitvitsky A. A., Isakova Yu. I. *Kiberprestupleniya: ponyatie, klassifikatsiya, mezhdunarodnoe protivodeystvie* [Cybercrimes: Concept, Classification, International Countering]. *Pravovoy poryadok i pravovye tsennosti* [Legal Order and Legal Values], 2023, vol. 1, no. 1, pp. 126–136. DOI: https://doi.org/10.23947/2949-1843-2023-1-1-126-136 [in Russian].