УДК. 343.3/.7
5.1.4. «Уголовно-правовые науки»

К ВОПРОСУ ОПРЕДЕЛЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Подчерняев Александр Николаевич
кандидат юридических наук, доцент,
начальник кафедры уголовного права,
криминологии и психологии;
Федеральное государственное казенное
образовательное учреждение высшего
образования «Орловский юридический институт
Министерства внутренних дел Российской
Федерации имени В.В. Лукьянова»

Аннотация. В статье представлена классификация преступлений на основе уголовного законодательства, а также с учетом предмета преступного посягательства, способа, мотивации преступника. Определена тенденция к формированию новых видов преступлений. Аргументировано объединение современных киберпреступлений, преступлений с использованием высоких технологий или IT-технологий, в ходе совершения которых субъект применяет компьютерные технологии, программное обеспечение, Интернет-ресурсы, средства современной связи и т.д. в самостоятельную группу. Обосновано понятие «Преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации». Автором классифицированы данные преступления и подвергнуты статистическому анализу. Выявлены тенденции преступности рассматриваемого вида. Сформулированы выводы о подходах к классификации преступлений, совершенных с использованием информационно-телекоммуникационных технологий, а также об их распространенности. Аргументировано значение пра-

вильного толкования понятия и классификации современных преступлений в выработке государственной политики в данной сфере.

Ключевые слова: преступность, преступления, информационно-телекоммуникационные технологии, IT-преступления, компьютерные преступления, киберпреступления, статистика, состояние преступности.

Жизнедеятельность любого общества сопровождают такие негативные явления, как, например, преступность, посягающие на все многообразие отношений, складывающихся в нем. Все преступления классифицированы на: деяние небольшой тяжести, средней тяжести, тяжкие и особо тяжкие[1]. При этом уголовным законодательством предусмотрено деление преступлений на виды, такие как, например, против жизни и здоровья; против свободы, чести и достоинства личности; половой неприкосновенности и половой свободы личности; против конституционных прав и свобод человека и гражданина; против семьи и несовершеннолетних; против собственности; в сфере экономической деятельности и т.д.[2] Существуют также преступления со специальным субъектом, например, должностные, охватывающие уголовно наказуемые деяния, совершаемые должностными лицами.

В актуальное уголовное законодательство постоянно вносятся изменения и дополнения. Подобные процессы в области уголовного законодательства характеризуются сочетанием криминализации и декриминализации деяний [1]. Складывается предпосылки формирования новых видов преступлений.

Такими новыми преступлениями можно считать посягательства, в ходе которых преступники применяют компьютерные технологии, программное обеспечение, Интернет-ресурсы, средства современной связи и т.д. Данные посягательства могут называть киберпреступлениями, преступлениями с использованием высоких технологий или IT-технологий. Все эти деяния объединяет технический компонент.

В Российской Федерации, на фоне снижения общего уровня преступности (почти на 2 % за последние пять лет, и на 24 % с 2010 года) некоторые ее виды демонстрируют рост. Так, с 2017 года в информационных материалах о

---

[1] Уголовный кодекс Российской Федерации: Федер. Закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».URL: http://www.consultant.ru. Текст: электронный.

[2] См.: главы 16-34 УК РФ.

состоянии преступности в России публикуется, в качестве самостоятельного показателя, количество преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, которые демонстрируют рост более чем в 5 раз к 2022 году (90587 преступлений в 2017 году против 512038 в 2022 году).

Преступления с использованием информационно-телекоммуникационных технологий составляют, в основном, хищения имущества путем кражи 21,8% и мошенничества 49,3% (113565 и 257606 преступлений соответственно). Также распространение получило использование информационно-телекоммуникационных технологий при незаконном производстве, сбыте или пересылке наркотических средств 11,9% (62209 преступлений).

Незначительный удельный вес составляют факты проявления в сети «Интернет» терроризма 0,1% (490 преступлений) и экстремизма 0,1% (493 преступления), однако, при этом, нужно учитывать существенный рост за прошедший год – 55,6% фактов публичных призывов к осуществлению террористической деятельности, публичного оправдания терроризма или пропаганды терроризма с использование информационно-телекоммуникационных сетей [2].

Учитывая значительные темпы роста числа преступлений, совершаемых с использованием компьютерных технологий, принципиальным с точки зрения понятийно-категориального аппарата становится вопрос о том, являются ли указанные преступные посягательства отдельным видом преступности, либо же «цифровые» преступления методологически вернее все же рассматривать в рамках традиционной структуры преступности. В этой связи анализ актуальной юридической литературы показывает, что специалисты в области криминалистики в рамках научного осмысления проблемы выработки и реализации методики расследования рассматриваемых преступлений фактически понимают под преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей любые подобные деяния, которые так или иначе связаны с Интернет-технологиями, не проводя различий в зависимости от субъективных признаков [3].

Отмеченный подход представляется справедливым в прикладной сфере, тогда как теоретическое осмысление проблемы киберпреступлений в рамках современной уголовно-правовой доктрины предполагает комплексный под-

ход. С этой точки зрения важным является не столько установление самого факта применения преступником цифровой технологии, но также направленность умысла, преступная мотивация и иные факторы. Таким образом, едва ли возможно объединить в рамках одного структурного элемента, скажем, незаконный сбыт наркотиков с использованием для преступной коммуникации цифрового мессенджера и создание вредоносных компьютерных программ.

При этом в рамках уголовно-правового анализа понятия киберпреступлений также отмечается отсутствие единых трактовок. Отдельные авторы понимают под киберпреступлением, в принципе, любое преступное посягательство, совершенное с применением компьютерных технологий [4]. Другие авторы обращают внимание на обязательную цель киберпреступника – неправомерное использование компьютера, компьютерной сети либо сетевого устройства [5].

Применяя подобный подход, очевидно, возможно предложить классификацию киберпреступлений в традиционном стиле – по объектам преступления, по способу совершения, по направленности преступного умысла и т.д.

Вместе с тем, вырабатываемый в рамках современной правоприменительной деятельности подход предполагает более глубокую дифференциацию[3]. Так, согласно такому подходу предлагается следующая классификация:

- преступления, без дополнительных условий (любые преступные посягательства так или иначе связанные с цифровой сферой, например, кража, предметом которой выступают электронные денежные средства);

- преступления с альтернативным квалифицирующим признаком, связанным с использованием информационно-телекоммуникационных сетей (примером таких преступлений могут служить доведение до самоубийства, клевета, нарушение неприкосновенности частной жизни и другие преступления, квалифицирующим признаком которых будет являться их

[3] Указание Генпрокуратуры России № 11/11, МВД России № 1 от 17.01.2023 «О введении в действие перечней статей Уголовного Кодекса Российской Федерации, используемых при формировании статистической отчетности» Доступ из справ.-правовой системы «КонсультантПлюс».URL: http://www.consultant.ru. Текст: электронный.

совершение с использованием информационно-телекоммуникационных сетей);

- преступления, предполагающие в рамках объективной стороны состава совершение конкретных киберпреступных действий (использование сети Интернет либо Даркнет, использование т.н. «фишинговых» сайтов и т.п.).

Проведение подобной классификации представляется вполне обоснованным и методологически верным. Кроме того, очевидно и несомненное прикладное значение такой классификации киберпреступлений, поскольку она позволяет дифференцировать разнородные преступные посягательства, а также индивидуализировать процессуальные и криминалистические подходы к выявлению, раскрытию киберпреступлений, доказывания вины преступника и, наконец, осуществления превентивной деятельности.

Любопытный подход к проведению классификации киберпреступлений приводит в своем исследовании Шавалеев Б.Э. Так, ученый предлагает классифицировать рассматриваемые преступления на четыре группы:

- преступления в сфере компьютерной информации;

- преступления в сфере информационно-телекоммуникационных сетей и технологий;

- преступления в сфере электронных средств платежа;

- иные преступления, сопряженные с использованием информационных технологий [6].

Несомненным достоинством приведенной классификации представляется проведение различий между преступлениями в сфере компьютерной информации и преступлениями, совершаемыми в сфере компьютерных технологий, поскольку схожие по внешним признакам деяния могут обнаруживать принципиальные расхождения по объекту и предмету посягательства. Впрочем, оставляет некоторые вопросы последняя из предложенных групп киберпреступлений, которая может включать практически любые преступления, в которых виновный так или иначе воспользовался цифровыми технологиями.

Уяснение понятия и классификации современных преступлений позволяет более четко представить характер совершаемых сегодня преступлений, а также сопоставить теоретические и практические подходы к учету и анализу преступности как в целом, так и отдельных видов, что создает предпосылки

верного определения количественных и качественных показателей преступности, и, как следствие, выработки государственной политики в данной сфере.

СПИСОК ИСТОЧНИКОВ

1. Цепелев В.Ф. Современное состояние российского уголовного законодательства и его влияние на разработку и реализацию уголовной политики // Российский следователь. 2019. № 7. Доступ из справ.-правовой системы «КонсультантПлюс». http://www.consultant.ru. (дата обращения: 14.04.2023).
2. Официальный сайт МВД России. Состояние преступности в Российской Федерации. [Электронный ресурс]. Доступ из сети Интернет URL: http:// мвд.рф/Deljatelnost/statistics. (дата обращения: 14.04.2023).
3. Урбан В.В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестник Восточно-Сибирского института МВД России. 2019. № 1 (88). С. 55-63.
4. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола, Иркутск, 20 марта 2015 года. Иркутск: Восточно-Сибирский институт МВД России, 2015. С. 120-125.
5. Антонов А.Г., Алешина-Алексеева Е.Н., Соколова А.В. К вопросу о понятии и видах киберпреступлений // Вестник Пермского института ФСИН России. 2023. № 1 (48). С. 5-10.
6. Шавалеев Б.Э. Классификация киберпреступлений // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 3 (49). С. 93-97.

ON THE QUESTION OF DEFINITION OF CRIMES COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Alexander Podchernyaev

Candidate of juridical sciences, assistant professor,
Chief in Criminal Law, Criminology and Psychology;
Federal State Educational Institution of Higher Education
"Oryol Law Institute of the Ministry of Internal Affairs of
the Russian Federation named after V.V. Lukyanov"

Conclusions. The article presents the classification of crimes on the basis of criminal law, as well as taking into account the subject of the criminal attack, the method, the motivation of the offender. The trend towards the formation of new types of crimes is determined. The grouping of modern cybercrimes, crimes using high technologies or IT technologies, in the course of which the subject uses computer technologies, software, Internet resources, means of modern communication, etc., into an independent group is argued. The concept of "Crimes committed with the use of information and telecommunication technologies or in the field of computer information" is substantiated. The author classified these crimes and subjected them to statistical analysis. The tendencies of crime of the considered type are revealed. Conclusions are formulated on approaches to the classification of crimes committed with the use of information and telecommunication technologies, as well as on their prevalence. The importance of the correct interpretation of the concept and classification of modern crimes in the development of state policy in this area is argued.

Key words: crime, crimes, information and telecommunication technologies, IT-crimes, computer crimes, cybercrimes, statistics, state of crime.

Հոդվածը գրախոսվել է՝ 01. 08.2023թ.:
Ներկայացվել է տպագրության՝ 01.08.2023թ.: