УДК 343.973

КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СЕТИ ИНТЕРНЕТ

Кунделеев С.В.
Магистрант 1 курса
ЧОУ ВО ЮУ (ИУБиП)
e-mail: kundeleyevstudy@gmail.com
Коханова В.С.
Магистрант 3 курса
ЧОУ ВО ЮУ (ИУБиП)
e-mail: kohanovavs@yandex.ru

Аннотация: Статья посвящена актуальным вопросам сохранения правового порядка в сфере информационно-телекоммуникационных сетей и сети Интернет. В настоящее время значительная доля преступлений совершается по средствам электронных устройств и цифровых технологий, что создает новые трудности по их предупреждению.
Ключевые слова: информационно-коммуникационные технологии, Интернет, киберпреступность, квалификация преступлений, мошенничество.

CRIMINOLOGICAL ASPECTS OF IMPROVING THE SYSTEM OF COMBATING CRIME ON THE INTERNET

Kundeleyev S.V.
Kokhanova V.S.

Abstract: The article is devoted to topical issues of maintaining legal order in the field of information and telecommunication networks and the Internet. Currently, a significant proportion of crimes are committed through electronic devices and digital technologies, which creates new difficulties in preventing them.
Keywords: information and communication technologies, cybercrime, qualification of crimes, fraud, the Internet.

В настоящее время многие ключевые аспекты экономической действительности общества из мира реального уже перетекли в мир цифровых технологий. В области информационно-телекоммуникационных сетей и сети Интернет оказание различных услуг, осуществление

коммерческой и некоммерческой деятельности стало возможным и даже необходимым с точки зрения удобства, конкурентоспособности и тенденций развития мирового общества. Вместе с тем преступность как явление начала адаптироваться под такие условия, проявляясь в совершенно новых формах, свойственных исключительно нашему времени.

Однако, Уголовный кодекс не вводит особых категорий для определения новых видов преступлений, появившихся в связи с развитием цифровых технологий. Категория «киберпреступник» так же не имеет нормативно-правовой основы. Однако существовать эти понятия не перестают. Более того, отсутствие законодательно закрепленной дефиниции не делает неопределимым само правонарушение [1, с. 622].

Специфика преступлений в виртуальном пространстве вызывает массу трудностей в их выявлении, фиксировании и квалификации. Проблема заключается в том, что развитие компьютерных технологий позволяет мошенникам, хакерам, вымогателям и прочим киберпреступникам быстро менять способы и виртуальные инструменты для совершения преступных деяний, их подготовки или организации.

Как отмечает Закутняя К.А., на сегодняшний день информационная безопасность в России становится одним из ключевых направлений национальной безопасности государства [2].

В рамках данной работы уделено особое внимание преступлениям, классифицируемым Уголовным Кодексом Российской Федерации как кража и мошенничество [3]. То есть фиктивная продажа услуг, приобретение и распространение данных зарегистрированных банковских карт, причинение ущерба имуществу путем обмана, получение и разглашение сведений, составляющих коммерческую тайну и прочие преступные деяния с использованием средств информационно-телекоммуникационных сетей.

По данным Главного Информационного-аналитического Центра Министерства Внутренних Дел Российской Федерации о состоянии преступности в России за январь-февраль 2020 года зарегистрировано 63000

преступлений, совершенных с использованием информационно-телекоммуникационных технологий, из которых большую часть составляют мошенничество и кража [4].

Удельный вес совершенных преступлений такой категории в общей структуре преступности в крупных регионах варьируется между 25 и 34 процентами. Около половины из этих преступлений остаются не раскрытыми.

Киберпреступности присущ дистанционный характер. В таких условиях преступник не только может скрывать следы своих действий при помощи профессиональных знаний о высоких технологиях, но и действовать выгодно с территориальной точки зрения. Проблема состоит в том, что преступнику не обязательно физически находиться на территории того государства, субъектам которого наносится ущерб. В такой ситуации правоохранительные органы не всегда могут осуществлять противодействие.

Вследствие специфичности методов и инструментов преступных афер возникают парадоксы и противоречия в правовом понимании этих действий.

Как отмечает Фоменко А.И. чтение информации с экрана монитора не относится ни к уничтожению, ни к блокированию, ни к копированию, ни к модификации информации, но вместе с тем нарушает права владельца информации, особенно если информация составляет личную или коммерческую тайну [5].

Может отсутствовать связь между временем совершения преступления и наступлением последствий, а также местом. Возникают проблемы идентификации личности, осуществивших те или иные действия. Разрабатываются новые способы шифрования информации, а также обеспечения анонимности. Потому правоохранительные органы сталкиваются с проблемами выявления, фиксации, документирования и квалификации преступлений, а также организации уголовно-процессуального противодействия.

К способам улучшения системы противодействия киберпреступности можно отнести совершенствование криминологических тактик, расширение правового поля в области информационно-телекоммуникационных сетей, разработку углубленной системы квалификации преступлений, преобразование требований к сбору информации, выработку способа её проверки, повышение компетенции кадров в оценке доказательств преступлений при расследовании.

Необходима разработка специального продвинутого программного обеспечения для сотрудников правоохранительных органов, профессионально подготовленные сотрудники для работы в этом профиле. Также необходимо разработать способы транспортировки изымаемой компьютерной техники, позволяющие сохранить необходимые для следствия данные от дистанционного вмешательства.

Стихийность преступлений в виртуальном пространстве вызывает потребность в оперативном мониторинге за подобными недоброкачественными изменениями, потому контроль телефонных и иных переговоров может способствовать верному и скорому выявлению преступной деятельности.

Кроме того, вопрос территориального несоответствия требует тесного сотрудничества разных государств. Эффективность данного метода гораздо больше вышеперечисленных, однако, требует преодоления ряда препятствий. Так как преступность в виртуальном пространстве – лишь одна сторона медали. С другой же располагается большая сеть самых различных сфер жизни людей на всей территории Земли. Реализация всех полезных мер по противодействию киберпреступности в полном масштабе невозможна в силу различий правовых систем различных государств, а также их экономических и политических интересов.

Однако, именно международное сотрудничество представляет наибольший интерес, ведь наиболее крупные экономические преступления в области информационно-телекоммуникационных сетей совершаются

дистанционно на большом расстоянии. Как отмечают Гридина Ю.А. и Русскова А.А., «нужно победить киберпреступность не только в самой стране, но и в мире» [6; с. 1]. Такое сотрудничество сегодня осуществляется только в форме направления запросов о правовой помощи.

В результате проведенного исследования можно сделать несколько основополагающих выводов. Проблема обеспечения криминологической безопасности в условиях информационно-коммуникационных технологий является существенной. Для эффективного противодействия киберпреступности необходимо совершенствовать криминологические тактики, расширять правовое поле в области информационно-телекоммуникационных сетей, разработать углубленную систему квалификации преступлений, преобразовать требования к сбору информации, выработать способа её проверки, повысить компетенции кадров в оценке доказательств преступлений при расследовании. А также нужно усиливать международное сотрудничество в области уголовного процесса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кибальник А.Г., Коханова В.С. Уголовно-правовые аспекты квалификации экономических преступлений в условиях цифровой экономики // Интеллектуальные ресурсы – региональному развитию. – 2020. – №1. – С. 617-625.
2. Закутняя К.А. К вопросу о правовых мерах противодействия организованной преступности в сфере высоких технологий // Интеллектуальные ресурсы – региональному развитию. – 2019. – №1. – С. 507-511.
3. Уголовный кодекс Российской Федерации от 13.06.1996 г. N 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.
4. Статистика преступности в РФ от 20.03.20 по материалам Министерства Внутренних Дел Российской Федерации. – URL: https://xn--b1aew.xn--p1ai/reports/item/19897618 (дата обращения: 27.03.20).
5. Фоменко А.И. О некоторых мерах предупреждения преступлений в сфере компьютерной информации // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2018. – №5 (96). – С. 95-97.
6. Гридина Ю.А., Русскова А.А. Киберпреступность как новая криминальная угроза // Интеллектуальные ресурсы – региональному развитию. – 2019. – №2. – С. 299-304.