Секция «Юриспруденция: актуальные вопросы правотворчества и правоприменения (СИУ РАНХиГС)»

Влияние технологий на рост киберпреступности: проблемы и вызовы интернет-мошенничества

Оолак Ксения Уран-ооловна
Студент (специалист)
Новосибирский государственный университет экономики и управления «НИНХ», Новосибирск, Россия
E-mail: oolak06@list.ru

Технологии открывают для общества огромные возможности, но не стоит забывать и о проблемах, с которыми может столкнуться каждый из нас благодаря этим «возможностям», в частности, с такой проблемой, как интернет-мошенничество. Фото, видео, геолокация, личные переписки, приложения с важными данными и огромное количество иных информаций хранятся на электронных носителях, что подтверждает тот факт, что каждый владелец подвергает свои данные опасности.

Наиболее полное определение киберпреступности, соответствующее рекомендациям экспертов ООН звучит следующим образом: киберпреступностью признается совокупность преступлений, совершенных в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

Так, можно выделить основной отличительный признак данного вида преступления, а именно совершение преступления в электронной среде.

Четкого определения интернет-мошенничества Уголовный кодекс РФ не предусматривает, но опираясь на Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий и диспозицию статьи 159 можно дать определение, где под интернет-мошенничеством понимается хищение, совершаемое путём обмана или злоупотребления доверием с использованием информационных технологий.

Под информационной технологией понимается обеспечивающее сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу, распространение и защиту информации технологический комплекс[3].

На сегодняшний день в сети Интернет существует огромное количество видов мошенничества. Основными видами мошенничества признаются: интернет-попрошайничество; скимминг; фишинг; вишинг; компьютерные вирусы; DDoS; хакерские атаки, стоит отметить, что это не все виды мошенничества [2].

По данным МВД за январь-декабрь 2024 года уровень преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее-ИТТ) по сравнению с предыдущими месяцами выросло на 13,1%. На рост данного вида преступления существенно повлияло развитие технологий, что упростило совершение данных преступлений, о чем свидетельствует количество преступлений совершенных с помощью ИТТ за 2024 год с использованием и применением: компьютерной техники — 42347 преступление (+16,4); программных средств—13461 (+10,6%); сети «Интернет» —649064 (+23,2%); средств мобильной связи—346035 (+14,3). Из которых мошенничества (ст. 159, 159.3, 159.6 УК РФ) —380344, что на +6,8% выше [4, с.28].

Стремительное развитие технологий приводит к такой проблеме, как отставание нормативной базы. Уголовный кодекс РФ не предусматривает конкретной нормы за использование ИТТ при совершении преступления в форме мошенничества.

Таким образом, считаю, что путем решения данной проблемы является усовершенствование законодательства в виде дополнения Уголовного Кодекса. Предлагаю ввести статью 159.7 «Цифровое мошенничество». В-первую очередь, стоит разграничить предлагаемую норму с уже существующими ст.159.6 и 28 главой УК.

В статье 159.6 объективная сторона выражается в «хищении путем вводы, удаления…либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей», то есть объектом воздействия в данном случае компьютерная информация. Предлагаемая статья предусматривает хищение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием с использованием ИТТ, где использование ИТТ будет средством совершения преступления, а обман и злоупотребление доверием-способом совершения преступления (в данном же случае потерпевший вводится в заблуждение и добровольно передает имущество и права на него) [1].

Глава 28 УК РФ предусматривают преступления в сфере компьютерной информации. Видовым объектом в указанной главе выступают общественные отношения в сфере обеспечения нормального оборота компьютерной информации, а в предлагаемой норме объект-общественные отношения в сфере собственности. В составах указанных в главе 28 нет непосредственной цели хищения путем обмана или злоупотребления доверием потерпевшего. Предлагаемая статья предусматривает преступный умысел в безвозмездном завладении чужим имуществом мошенническим путем, а преступления главы 28 направлены на сбой целостности компьютерной информации.

Субъект преступления 159.6-общий. Обязательный признак-способ совершения данного преступления.

Состав материальный, то есть преступление окончено с момента фактического незаконного перехода имущества во владение виновного и получения им возможности распоряжаться по своему усмотрению, а также с момента незаконного перехода виновному права на имущество потерпевшего.

Субъективная сторона выражена в прямом умысле. Лицо должно осознавать, что вводит потерпевшего в заблуждение, также должно понимать, что это действие он выполняет с использованием ИТТ.

Обязательным признаком субъективной стороны-корыстный мотив и цель в виде незаконного безвозмездного изъятия имущества.

Квалифицирующие признаки: совершение группой лиц по предварительному сговору, лицом с использованием своего служебного положения, а равно в крупном размере, организованной группой либо в особо крупном размере, а также такие квалифицирующие признаки, как использование ИИ, массовый характер.

Источники и литература

1) 1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 15.10.2025 г.) // Собрание законодательства Российской Федерации — 1996. — № 25. — Ст. 2954.

2) 2. Рожкова Диана Сергеевна, Муромская Дарья Алексеевна МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ // Вестник ПензГУ. — 2022. — №3 (39). URL: https://cyberleninka.ru/article/n/moshennichestvo-v-internete-1 с.2

3) 3. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий URL: https://www.mid.ru/ru/foreign_policy/international_contracts/international_contracts/multilateral_contract/53417/

4) 4. Состояние преступности в России за январь - декабрь 2024 года // Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр» URL: https://portal.tpu.ru/SHARED/n/NIKOLAENKOVS/student/risk_management/Sbornik_UOS_2024.pdf?ysclid=mnpwcb30ke949494595 с.28