Секция «Уголовное право»

Уголовно-правовые меры противодействия экономическим киберпреступлениям

Шведкин Данила Андреевич
Студент (бакалавр)
Ульяновский государственный университет, Ульяновск, Россия
E-mail: dshvedkin03@mail.ru

Шведкин Данила Андреевич

Уголовно-правовые меры противодействия экономическим киберпреступлениям

Ключевые слова: экономические киберпреступления, особенности, противодействие

В настоящий момент в быту все чаще звучат такие понятия как «киберпространство», «цифровое пространство», «информационное пространство», «виртуальное пространство». Связано это с тем, что сфера цифровизации и информатизации представляет собой одну из самых динамично развивающихся сфер, в связи с чем вопросы ее регулирования обсуждаются на различных уровнях, в том числе на законодательном и научном. Злоумышленники не отстают от темпов развития технологий и также активно внедряются в экономическую сферу, поэтому проблема стремительного развития экономических киберпреступлений на данный момент считается одной из приоритетных. Статистические данные, предоставленные «Лабораторией Касперского», говорят о том, что на долю Российской Федерации приходится около 20% всех мировых атак[1]. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»[2] особое внимание уделяет укреплению устойчивого информационного пространства и повышению безопасности российского общества в цифровом поле от дестабилизирующего информационно-психологического. В данном документе также отмечается, что столь стремительное развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

исходя из нематериального характера пространства, в которых совершаются данные деяния, возникает сразу несколько особенностей. Среди них:

1. дистанционный способ их совершения, заключающийся в отсутствии физического взаимодействия между злоумышленником и потерпевшим, что также обусловливает еще одну особенность - анонимность злоумышленников[3]. Показательно Постановление № 1-413/2020 от 29 июля 2020 г. по делу № 1-413/2020 Вахитовского районного суда г. Казани[4]. Виновный совершил мошенничество в сфере компьютерной информации, вступив в преступную группу, занимающуюся хищением денежных средств через мнимую продажу авиабилетов: неустановленные лица создали сайты для обмана граждан. В результате, потерпевший, пытаясь купить авиабилет, попал на мошеннический сайт и оплатил билет, в результате чего с его карты были списаны денежные средства в размере, признанном судом значительным.

2. отсутствие физических следов – после совершения то затрудняет процесс доказывания и выявления преступника. Цифровой след, оставляемый злоумышленником, при наличии специальных знаний и оборудования легко поддается изменению, удалению, сокрытию, ввиду чего процесс доказывания совершенного деяния существенно усложняется.

3. трансграничный характер - отсутствие географических пределов киберпространства обусловливает возможность совершения преступного в одной стране или ее территориальном субъекте, в том числе и против другой страны[5].

Во-вторых, подобного рода преступления является многообъектными, а конкретно - двуобъектными[6]. В доктрине уголовного права многообъектными являются составы,

объект которых по своей структуре сложен и содержит одновременно несколько охраняемых уголовным законом общественных благ[7]. Применительно к экономическим киберпреступлениям это общественные отношения в сфере безопасности обращения компьютерной информации и общественные отношения, связанные с нею, а также это отношения собственности.

В-третьих, экономические киберпреступления можно отнести к разряду высоколатентных преступлений[8]. Эта особенность находится в прямой зависимости от многих факторов, среди которых в том числе трансграничный характер, вариативность и частота обновления способов совершения, особая подготовленность преступников и множество других детерминантов. Связано это также и с тем, что потерпевшие от таковых преступных посягательств зачастую могут и не понимать, что их данные были утеряны, или что их финансовые средства находятся под угрозой. Экономические киберпреступления также очень сложны в обнаружении, ввиду чего могут быть восприняты как технические неполадки и сбои, что затрудняет их учет и анализ.

виртуальное пространство должно в полной мере быть подконтрольно закону. На сегодняшний день не осталось сфер, где цифровые и информационные технологии не решали бы важнейшие задачи, напротив – они уже давно стали неотъемлемой частью функционирования множества важнейших процессов. Игнорирование проблем экономических киберпреступлений несомненно приведет к разрушению нашего общества. По нашему мнению, в первую очередь необходимо устранение плюрализма толкований путем внедрения в уголовное законодательство официальных терминов для обозначения реалий цифровой экономики. Целесообразно пересмотреть некоторые составы преступлений в главах 21, 22 и 28 УК РФ с учетом нынешних реалий цифровой экономики, а также разработать рекомендации для разъяснения вопросов квалификации экономических киберпреступлений. Такая необходимость возникает ввиду того обстоятельства, что традиционные правила квалификации не всегда применимы в условиях конкуренции уголовно-правовых норм. Кроме того, речь идет не только об устранении сложностей квалификации, но и о повышении цифровой грамотности населения в целях снижения виктимности граждан и укрепления цифрового суверенитета России в целом. Механизмы экономического и инфраструктурного характера не должны быть просто частью государственной стратегии, но являться гибкими и учитывать запросы властных структур и потребности представителей бизнеса и IT-сектора.

[1] Ляпин А.Е.. "КИБЕРПРЕСТУПНОСТЬ КАК НОВЫЙ ОБЪЕКТ СТАТИСТИЧЕСКОГО АНАЛИЗА" Статистика и экономика, no. 6, 2021, pp. 4-16.

[2] Указ Президента РФ от 02.07.2021 № 400 О Стратегии национальной безопасности Российской Федерации // Официальный интернет-портал правовой информации http://pravo.gov.ru/ - 03.07.2021.

[3] Анастасия Эдуардовна Пяткина. "ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В УСЛОВИЯХ СОВРЕМЕННОЙ РОССИИ" Государственная служба и кадры, no. 2, 2021, pp. 181-183. doi:10.24412/2312-0444-2021-2-181-183

[4] //sudact.ru/regular/doc/ftR7s3xLHjHQ/

[5] Гайдин Александр Иванович, and Головчанский Алексей Владимирович. "СРЕДСТВА АНОНИМИЗАЦИИ В МЕХАНИЗМЕ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМОЙ В СЕТИ ИНТЕРНЕТ" Вестник Воронежского института МВД России, no. 2, 2022, pp. 205-213.

[6] Иванова Лилия Викторовна. "Виды киберпреступлений по российскому уголовному законодательству" Юридические исследования, no. 1, 2019, pp. 25-33.

[7] Автореферат диссертации на соискание ученой степени доктора юридических наук Карабанова Елена Николаевна М НОГООБЪЕКТН Ы Е ПРЕСТУПЛЕНИЯ: ТЕОРИЯ,

ЗАКОНОДАТЕЛЬСТВО, ПРАКТИКА Специальность: 12.00.08 - «Уголовное право и криминология; уголовно-исполнительное право»

[8] Могунова М. М. "ПОНЯТИЕ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ И СПОСОБЫ СОВЕРШЕНИЯ ФИНАНСОВО-ОРИЕНТИРОВАННЫХ КИБЕРПРЕСТУПЛЕНИЙ" Вестник Омского университета. Серия «Право», vol. 19, no. 1, 2022, pp. 80-86.