Старцева Дарья Вадимовна
магистрант
ФГАОУ ВО «Казанский (Приволжский)
федеральный университет»
г. Казань, Республика Татарстан

КИБЕРПРЕСТУПНОСТЬ В ПЕРИОД ПАНДЕМИИ

Аннотация*: в статье анализируются общие международные и отечественные проблемы в сфере киберпреступлений, а также актуальные тенденции их развития в период пандемии. Анализ зарубежных и российских данных позволяет сделать вывод о том, что информационное пространство в период пандемии стало одной из самых распространенных сфер для совершения различных преступлений. Пандемия COVID-19 способствовала росту преступности в сфере информационно-телекоммуникационных технологий, а также развитию разнообразия способов их совершения.*

Ключевые слова*: информационно-телекоммуникационные технологии, киберпреступность, мошенничество, мошенничество в сфере компьютерной информации, мошенничество с использованием электронных средств платежа.*

В XXI веке сеть Интернет охватила практически все сферы деятельности человека, каждый день общество взаимодействует и коммуницирует посредством Интернета, допускает его в каждую часть своей жизни. Безусловно, появление и развитие сети Интернет колоссально облегчает жизнь человека, общества и государства, так как можно, не выходя из дома, разрешить огромное количество вопросов и проблем. С появлением такого опасного вируса, как COVID-19, общество оказалось заперто в своих домах и было вынуждено полностью перейти на дистанционное выполнение таких задач, как покупки, доставка, развлечения и т. д. Тем самым человек «остался наедине с Интернетом».

Преступная активность в онлайн-режиме, входящая, согласно рейтингу Всемирного экономического форума (ВЭФ), в пятерку глобальных рисков, угрожает существованию и успешному функционированию целому ряду отраслей. По

данным ВЭФ, только в 2019 году потери мировой экономики от кибератак оцениваются в 2,5 трлн долларов, а к 2022 г. этот показатель может достичь 8 трлн долларов [2]. Наибольшие показатели ее проявления – это мошеннические посягательства. Преступления в сфере информационно-телекоммуникационных технологий становятся главным и определяющим вектором развития современной преступности во всем мире [5, с. 155–158].

По данным Национального бюро расследования мошенничества Англии, за 2019 год ущерб только от мошенничества, совершенного с использованием информационно-телекоммуникационных технологий, составил 2,3 миллиарда фунтов стерлингов [8].

По данным сети Consumer Sentinel Network, поддерживаемой Федеральной торговой комиссией США, в 2019 году потребители сообщили, что потеряли более 1,9 миллиарда долларов в связи с жалобами на мошенничество [9].

К сожалению, на сегодняшний день по всему миру складывается подобная ситуация и Российская Федерация не исключение.

Согласно статье 1 Указа Президента РФ «О стратегии развития информационного общества в Российской Федерации на 2017–2020г.» от 09.05.2017 г., стратегия определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленных на развитие информационного общества, обеспечение национальных интересов и реализацию стратегических национальных приоритетов [1]. Положения данной статьи позволяют получить возможность свободного доступа к национальным и мировым информационным телекоммуникационным сетям. Данный доступ во многом обусловливает и криминальный характер деятельности. На мой взгляд, вполне возможно сделать предположение о том, что, чем больше «площадок» для совершения преступлений и непосредственно просвещенность общества, тем выше рост преступности. А пандемия лишь «добавляет» разновидность и тематику способов мошенничества посредством Интернета: преступники используют саму тему коронавируса во вредоносных рассылках, поддельных удостоверениях личности и т. п.

Согласно статистике приведенной МВД России на 2018 год зарегистрированных случаев мошенничества (159–159.6 УК РФ) – 215036, на 2019 г. – 257187, на 2020 г. – 335536. Раскрыты из них: 2018 год – 57418, 2019 год – 64378, 2020 год – 67476. Исходя из вышеперечисленных статистических данных, рост зарегистрированных случаев явно и неуклонно растет. Снижение процента раскрываемости, может быть связано с высокой анонимностью пользователей информационного пространства.

В общем количестве зарегистрированных мошеннических действий, совершенных с использованием информационно-телекоммуникационных технологий, классические виды составляют большую часть. Мошенничество в сфере компьютерной информации становится альтернативой традиционному финансовому преступлению с низким уровнем риска [4, с. 92].

Такие преступления на сегодняшний день имеют относительно небольшой риск разоблачения, соответственно такая динамика делает этот вид преступной деятельности очень привлекательным для организованной преступности [3, с. 60]. Из-за технической сложности и необходимости специальных навыков, такие преступления сложно будет выявить и расследовать. В связи с тем, что технологии не стоят на месте, с каждым годом правоохранительным органам все сложнее выявлять такие преступления и расследовать их.

Одна из причин, почему сложно распознать схемы преступников, это отсутствие единства международного законодательства. Организованные преступные группы действуют на международном уровне и используют разное законодательство государств. Специфика данной категории преступлений также является то, что члены одной организованной преступной группы могут находиться на разных континентах или использовать различные способы маскировки своего места нахождения, а также свободно перемещаться, так как они «не привязаны» к месту преступления, поэтому физически обнаружить всю группу крайне сложно.

Безусловно, такая проблема требует решения на международном законодательном уровне. Стоит отметить, что Россия инициировала в рамках ООН разработку всеобъемлющей международной конвенции о противодействии

использования ИКТ в преступных целях. В этом контексте на рассмотрение 74-й сессии Генассамблеи внесён проект резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях» [10], соавторами которого выступили 47 государств. Резолюция, принятая при поддержке большинства стран Азии, Африки, Латинской Америки, постановила учредить специальный межправительственный комитет экспертов открытого состава для разработки упомянутой конвенции с учётом существующих международных документов и предпринимаемых на национальном и региональном уровнях усилий по борьбе с киберпреступлениями. Восприимчивость международного сообщества к российскому начинанию свидетельствует, что заключение подобного договора – веление времени, осознание новой реальности, связанной со стремительно возрастающей направленностью преступлений в сфере информационно-телекоммуникационных технологий и возникающими в этой связи проблемами.

Список литературы

1. Указ Президента РФ от 09.05.2017 «О стратегии развития информационного общества в Российской Федерации на 2017–2020 г.».

2. Статья министра иностранных дел Российской Федерации С.В. Лаврова «Глобальные проблемы кибербезопасности и международные инициативы России по борьбе с киберпреступностью» для журнала «Внешнеэкономические связи». Москва. 28 сентября 2020 г. [Электронный ресурс] // Официальный сайт Министерства иностранных дел Российской Федерации.

3. Веснина С.Н. Способы неправомерного завладения компьютерной информацией, передаваемой посредством электронной почты / С.Н. Веснина, А.В. Неустроева, Е.В. Жидкова // Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения): сборник статей Международной научно-практической конференции [Электронный ресурс]. – М.: Академия управления МВД России, 2018. – С. 60–64.

4. Иванцов С.В. Информационно-телекоммуникационные технологии – современная реальность преступности / С.В. Иванцов, Т.В. Молчанова // Вестник Санкт-Петербургского университета МВД России. – 2020. – №4 (88). – С. 89–96.

5. Иванцов С.В. Использование информационно-телекоммуникационных сетей для совершения преступлений: вопросы уголовно-правового воздействия и предупреждения // С.В. Иванцов // Уголовно-правовое воздействие и его роль в предупреждении преступности: сборник по материалам IV Всероссийской научно-практической конференции «Саратовские уголовно-правовые чтения» / под общ. ред. Н.А. Лопашенко. – Саратов, 2019. – С. 155–158.

6. Серёгин Ю.Н. Проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / Ю.Н. Серёгин // На пути к гражданскому обществу. – 2018. – №1 (29). – С. 26–33.

7. Урбан В.В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию / В.В. Урбан // Вестник Восточно-Сибирского института МВД России. – 2019. – №1 (88). – С. 55–63.

8. Панель мониторинга мошенничества и киберпреступности NFIB [Электронный ресурс]. – Режим доступа: https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html (дата обращения: 02.09.2021).

9. Отчёты о краже личных данных и киберпреступности, 2015–2019 гг. [Электронный ресурс]. – Режим доступа: https://www.iii.org/fact-statistic/facts-statistics-identity-theftand-cybercrime (дата обращения: 01.09.2021).

10. Противодействие использованию информационно-коммуникационных технологий в преступных целях: проект резолюции Генеральной Ассамблеи ООН, 25 November 2019 [Электронный ресурс]. – Режим доступа: https://undocs.org/pdf?symbol=ru/A/74/401 (дата обращения: 02.09.2021).