МОШЕННИЧЕСТВО В СЕТИ ВО ВРЕМЯ ПАНДЕМИИ

ONLINE FRAUD DURING THE PANDEMIC

УДК 004

Судаков Артём Владимирович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва, E-mail: artyom.sudakov.97@mail.ru

Грамзин Андрей Владимирович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Дудин Денис Артурович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Щербатюк Дарья Сергеевна, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Поремский Александр Романович, Студент магистратуры 2 курса, Кафедра ИУ8 «Информационная безопасность», Московский государственный технический университет им. Н. Э. Баумана, Россия, г. Москва

Sudakov Artyom Vladimirovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman Russia, Moscow

Gramzin Andrey Vladimirovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman

Russia, Moscow

Dudin Denis Arturovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman, Russia, Moscow

Shcherbatyuk Daria Sergeevna, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman
Russia, Moscow

Poremsky Alexander Romanovich, Master's student of the 2nd year, Department of IU8 "Information Security", Moscow State Technical University N. E. Bauman
Russia, Moscow

Аннотация

Статья посвящена изменениям в современной интернет-преступности во время пандемии COVID-19. Учтены причины роста числа уголовных преступлений в форме мошенничества, определены новые способы совершения «вирусных» случаев мошенничества и представлена актуальная статистика интернет-преступности.

Annotation

The article is devoted to the changes in modern Internet crime during the COVID-19 pandemic. The reasons for the increase in the number of criminal offenses in the form of fraud, considered new ways of committing "viral" fraud cases are identified, and current statistics of Internet crime are presented.

Ключевые слова: интернет, преступность, пандемия, мошенничество, коронавирус.

Keywords: Internet, crime, pandemic, fraud, coronavirus.

Время пандемии новой коронавирусной инфекции (COVID-19) обернулось самыми негативными последствиями для всего человечества. К сожалению, Российская Федерация в этом плане не исключение. Помимо ухудшения экономических показателей, возникла социальная напряженность, которая

привела к непредсказуемому и, что еще более опасно, неконтролируемому росту преступности.

После начала пандемии COVID-19 мошенники начали активно использовать тему заражения во вредоносных рассылках. Предложили купить диджитал и предупредили о штрафах за нарушение карантина.

Основные цели киберпреступников во время пандемии COVID-19 не изменились. Они все еще пытаются украсть деньги и информацию, которые затем можно продать, но преступники скорректировали свои методы «в соответствии с текущей повесткой дня». Об этом говорится в сообщении компании Group-IB, полученном РБК [1].

По данным Group-IB, после вспышки пандемии COVID-19 масштабы киберугроз резко выросли, в основном из-за увеличения атак с использованием социальной инженерии и использования темы коронавируса во вредоносных рассылках (отправка сообщений). о штрафах за нарушение карантина, поддельных цифровых удостоверениях личности, приглашениях от имени службы видеоконференцсвязи Zoom и т. д.) и активном вербовке новых участников в преступные сообщества.

Экономические и финансовые преступления — это чрезвычайно разнообразная и серьезная угроза, от которой ежегодно страдают миллионы граждан и тысячи предприятий в ЕС. Такие преступления подрывают экономику и финансовый сектор и лишают нас возможностей для процветания, экономического роста и занятости.

Финансовые и экономические преступления охватывают ряд различных видов преступной деятельности, от простого мошенничества до крупных и сложных финансовых систем, часто связанных как с законными, так и с незаконными транзакциями. Сочетание законности и незаконности часто затрудняет правоохранительным органам определение степени незаконности этих действий. С помощью легальных финансовых систем преступникам удается отмывать преступные деньги и поддерживать свою преступную деятельность.

Несмотря на усилия по борьбе с экономическими и финансовыми преступлениями, возможности для таких преступлений увеличились, поскольку рынки законных финансовых услуг стали более разнообразными, а технологии меняют способ и скорость финансовых транзакций.

Сегодня экономические и финансовые преступления имеют относительно небольшой риск разоблачения, и правоохранительные органы могут принести очень высокую прибыль.

Такая динамика делает этот вид преступной деятельности очень привлекательным для организованной преступности. Из-за сложности этих преступлений и того факта, что они требуют специальных знаний, их всегда было трудно выявить и расследовать. Новые технологии и оцифровка финансовых транзакций еще больше усложнили работу правоохранительных органов. Многие из этих преступлений теперь еще труднее обнаружить и еще труднее расследовать [2].

Мошеннические системы часто не распознаются. Успешное применение этих сложных систем требует тесного международного сотрудничества между несколькими юрисдикциями, часто включая отказ от сотрудничества оффшорных налоговых убежищ, поскольку преступники действуют за пределами международных границ. Организованные преступные группы (ОПГ) действуют на международном уровне и пользуются различными законами в отдельных странах.

Растет понимание того, что определенные виды деятельности в финансовом секторе, которые когда-то считались недобросовестными методами ведения бизнеса, вполне могут быть преступными. Крупные рискованные инвестиции, искажение финансовой отчетности и соглашения с целью повлиять на банковские процентные ставки относятся к категории серьезных преступлений и преступлений организованных преступных групп. Огромные убытки, причиненные финансовыми манипуляциями на высоком уровне, разрушают системы социального обеспечения и дестабилизируют экономику.

Растет число мошеннических программ, нацеленных на частных лиц, предприятия и государственный сектор. Во время пандемии COVID-19 в Европе было достаточно свидетельств того, как быстро преступники адаптируют свои планы к меняющимся обстоятельствам, чтобы использовать страхи и уязвимости.

Будущие последствия пандемии COVID-19 станут проверкой устойчивости экономической и социальной инфраструктуры к внешним воздействиям.

Потребители меняют свое финансовое поведение и инструменты, которые они используют для доступа к средствам и управления ими. Решения Fintech становятся стандартным способом взаимодействия потребителей с поставщиками финансовых услуг.

В целом 58% потребителей в ЕС, хранящих свои деньги в банках, в настоящее время используют цифровые интернет-решения, такие как веб-сайты или приложения, для проведения транзакций на регулярной основе. В то же время эти меры представляют собой шаг вперед с точки зрения удобства использования и доступности финансовых услуг как для клиентов, так и для поставщиков финансовых услуг. Такие изменения также сопряжены с серьезными рисками [3].

Клиенты не всегда являются опытными пользователями таких услуг, и из-за отсутствия технических знаний и опыта они уязвимы для атак киберпреступников, которые используют методы фишинга и хакерские программы для получения доступа к учетным записям в Интернете.

Со стороны поставщиков финансовых услуг более широкое использование цифровых технологий и отсутствие прямого взаимодействия с клиентами могут ослабить процедуры идентификации, установленные для предотвращения налогового мошенничества, отмывания денег и использования финансовых систем для финансирования преступности и терроризма.

Ослабление систем идентификации клиентов увеличивает уязвимость финансовых услуг, которые могут использоваться для различных видов преступной деятельности, в том числе для мошенничества в онлайн-банке.

Согласно исследованию, с конца 2019 года количество пользователей мобильного банкинга увеличилось на 50%. Вероятно, что пандемия COVID-19 и меры по борьбе с ней ускорят переход к цифровым и / или финансовым технологическим решениям.

По мере того, как финтех приобретает прочную репутацию, необходимо продвигать финтех-инновации в области кибербезопасности, чтобы защитить растущее число клиентов от угрозы киберпреступности.

Экономический спад создает благоприятные возможности для совершения преступлений.

В то время как легальная экономика сложна для легальной экономики, преступные корпорации оказываются в положении, когда они могут воспользоваться преимуществами и возможностями этого спада. Некоторые отрасли сильнее пострадали от негативных экономических условий: например, строительство и гостиничный бизнес, путешествия и туризм. Компании, работающие в этих секторах, часто уязвимы для проникновения и захвата преступниками в трудные времена.

Из-за того, что во время экономического спада трудно получить капитал за счет кредита, отдельные граждане и предприятия вынуждены пользоваться неконтролируемыми финансовыми услугами, которые все чаще появляются в сети в виде нелицензированных банков или кредитных организаций, предлагающих различные типы кредиты, а в некоторых случаях обманывают своих клиентов.

Кроме того, проблемные компании и частные лица из-за отсутствия доступного капитала могут стать объектами инвестиций, источником которых является преступная деятельность. В прошлом этот тип уязвимости особенно наблюдался в секторе недвижимости.

Преступники, которые ищут правительственные уловки, обманывая их, нацелены на экономические стимулы, подобные тем, которые предлагаются в контексте пандемии COVID-19. В некоторых случаях преступники могут попытаться прибегнуть к коррупции, чтобы получить такое финансирование.

Во времена экономических трудностей возникают различные формы инвестиционного мошенничества. Ожидается, что вторая волна COVID-19 приведет к подобным случаям мошенничества в случае затяжной рецессии. Например, мошеннические предложения инвестировать в компании, производящие предметы санитарии и гигиены, особенно маски и другие средства индивидуальной защиты (СИЗ). Говорят, что некоторые из этих компаний исчезают после получения инвестиций.

Предыдущие исследования показали, что мошеннические инвестиционные программы могут приносить сотни миллионов долларов прибыли ежегодно и обычно управляются сетями от 10 до 20 подозреваемых.

По результатам некоторых расследований преступлений организованных преступных групп с делами о коррупции можно сделать вывод о широком распространении коррупции. Практически во всех серьезных случаях серьезных преступлений или преступлений организованных преступных групп есть случаи коррупции, начиная от подкупа низших должностных лиц и заканчивая коррупцией на самом высоком политическом уровне [1].

Случаи коррупции еще не полностью расследованы. Из-за того, что преступные деньги отправляются через интернет-переводы, а наличные деньги используются для незначительного подкупа, часто бывает сложно отслеживать финансовые потоки и выявлять факты о коррупции.

Преступления против интеллектуальной собственности: контрафактная и некачественная продукция

Производство контрафактной продукции и пиратская деятельность включают различные виды незаконной деятельности, связанные с нарушением прав на зарегистрированные товарные знаки и патенты (в случае контрафактной продукции), а также авторские права и промышленные изображения (в случае

пиратства). Все эти действия вместе составляют преступления против прав интеллектуальной собственности. Важность и объем прав интеллектуальной собственности продолжают расти, давая преступникам больше причин для использования и нарушения этих прав на прибыль.

Таким образом, можно констатировать, что ограничительные меры и меры стимулирования, созданные и реализуемые нашим государством для минимизации возникновения коронавирусных инфекций среди населения, одновременно стали условиями для совершения корыстных преступлений. Во время пандемии была существенно пошатнута психология самого общества, что также усугубило правовую аномию. Очевидно, что пик заболеваемости еще не пройден, а значит, о выходе из нынешнего кризиса говорить рано. Новые методы и формы преступной деятельности, которые мы, скорее всего, рассматривали, и дальше будут пользоваться популярностью у современных преступников. В этом контексте в ближайшем будущем важна незамедлительная разработка новых общих криминологических и специальных мер по предупреждению подобных методов преступного поведения.

Литература

1. Багреева Е.Г. Криминологический анализ и тенденции преступности в период и после пандемии в Российской Федерации и Республике Болгарии / Е.Г. Багреева, А.И. Мантарова – Юриспруденция, 2020. - 258 с.
2. Быковская Ю. В. Анализ динамики и структуры преступности экономической направленности в Российской Федерации в современных условиях борьбы с пандемией / Быковская Ю. В. - Экономика и предпринимательство, 2020. – 331 с.
3. Бочкарева Е. В. Самодетерминация преступности во время пандемии COVID-19 / Бочкарева Е. В. - Пенза, 2020. – 300 с.

Literature

1. Bagreeva E.G. Criminological analysis and crime trends during and after the pandemic in the Russian Federation and the Republic of Bulgaria / E.G. Bagreeva, A.I. Mantarova - Jurisprudence, 2020 .-- 258 p.

2. Bykovskaya Yu. V. Analysis of the dynamics and structure of economic crime in the Russian Federation in modern conditions of the fight against a pandemic / Bykovskaya Yu. V. - Economy and entrepreneurship, 2020. - 331 p.
3. Bochkareva E. V. Self-determination of crime during the COVID-19 pandemic / Bochkareva E. V. - Penza, 2020. - 300 p.