Конференция участников Конвенции Организации Объединенных Наций против транснациональной организованной преступности

Distr.: General
25 March 2024
Russian
Original: English

Рабочая группа правительственных экспертов по технической помощи
Вена, 3 и 4 июня 2024 года
Пункт 3 предварительной повестки дня*
Мошенничество, совершаемое организованными группами

Мошенничество, совершаемое организованными группами

Справочный документ, подготовленный Секретариатом

I. Введение

1. Настоящий справочный документ подготовлен Секретариатом в целях содействия дискуссии по пункту 3 предварительной повестки дня пятнадцатого совещания Рабочей группы правительственных экспертов по технической помощи. В нем представлен краткий неполный обзор различных категорий мошенничества, совершаемого организованными группами в отношении частных лиц или учреждений с целью получения финансовой или иной материальной выгоды; документ призван содействовать выработке более эффективных мер противодействия организованному мошенничеству в рамках Конвенции Организации Объединенных Наций против транснациональной организованной преступности.

2. За истекшие годы мошенничество претерпело значительные изменения, поскольку преступники осваивают достижения технического прогресса и приспосабливаются к переменам в обществе. Оно становится все более изощренным, в нем применяются психологические манипуляции и технологии, используются преимущества машинного обучения, искусственного интеллекта и других технологий для автоматизации совершения правонарушений. Распространенность и масштабы мошенничества представляют серьезную угрозу для людей, экономики и процветания во всем мире и подрывают доверие общества к закону. Однако получению полного представления о мошенничестве препятствует ряд факторов. Потерпевшие часто не заявляют о мошенничестве, поскольку испытывают чувство стыда, винят в произошедшем самих себя или не решаются сделать это, а в некоторых случаях не осознают, что стали жертвой преступления. Кроме того, в большом количестве случаев объектом мошенничества становятся коммерческие предприятия, многие из которых предпочитают не сообщать о таких преступлениях, чтобы не портить свою репутацию. Анонимность и удаленность, сопровождающие акты мошенничества, скрывают

* CTOC/COP/WG.2/2024/1.

личности преступников от потерпевших и властей, что препятствует оценке основных закономерностей и связанных с ними рисков. Кроме того, динамичный характер мошенничества, обусловленный постоянной адаптацией к изменениям в правовых, социальных, коммерческих и технологических системах, означает, что новые и инновационные методы совершения преступлений могут не находить отражения в статичных официальных данных.

3. Международное сообщество признает, что масштабы мошенничества вызывают тревогу и необходимо объединить усилия для предупреждения мошенничества и борьбы с ним[1]. В своей резолюции 78/229 Генеральная Ассамблея подтвердила мандат Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН), предусматривающий, что Управление по запросам государств-членов участвует в техническом сотрудничестве с ними и оказывает им техническую помощь в борьбе с организованной преступностью во всех ее формах, включая мошенничество. Это согласуется с провозглашенной в статье 1 целью Конвенции об организованной преступности, которая заключается в содействии сотрудничеству в деле более эффективного предупреждения транснациональной организованной преступности и борьбы с ней. Учитывая меняющийся характер мошенничества и все более активное применение технологий, расширяющих его возможности, Генеральная Ассамблея в своей резолюции 74/177 призвала государства-члены прорабатывать меры и формулировать возможные выводы и рекомендации, направленные на создание защищенной и устойчивой киберсреды, уделяя особое внимание правонарушениям, связанным с кражей персональных данных.

4. Широко признается, что мошенничество может быть как организованным, так и серьезным преступлением[2]. Развитие технологий и быстрое увеличение масштабов организованной преступности привели к появлению множества новых способов массового обмана частных лиц, коммерческих организаций и даже правительств в глобальных масштабах. Это дает возможность организованным преступным группам более эффективно атаковать жертв по всему миру[3].

5. Мошенничество в рамках организованной преступности имеет свои отличительные особенности. Во-первых, оно прежде всего связано с хищением денежных средств, а не с производством или распространением незаконных товаров, что отличает его от других видов преступной деятельности. Во-вторых, многие мошеннические действия осуществляются удаленно, чему способствуют технологии, позволяющие анонимно общаться и переводить похищенные средства без физического взаимодействия между преступником и жертвой. В-третьих, для мошенничества часто необходимо, чтобы жертвы добровольно предоставляли доступ к своим средствам, при этом успех зависит от тактики обмана, которая делает незаконных субъектов неотличимыми от законных. Эти факторы определяют используемые мошенниками методы и необходимые средства и влияют на структуру организованных преступных групп.

6. Некоторые из мошенников осуществляют деятельность в организациях или профессиях, которые представляются законными. Используя знания или навыки, приобретенные в сомнительных или нерегулируемых сферах, в которых не действуют традиционные деловые или коммерческие нормы, некоторые организованные преступные группы создают структуры, схожие с законными

[1] См. резолюции 2004/26, 2007/20, 2009/22, 2011/35 и 2013/39 Экономического и Социального Совета о международном сотрудничестве в деле предупреждения и расследования случаев экономического мошенничества и преступлений с использованием персональных данных, а также преследования и наказания за такие деяния.

[2] European Union Agency for Law Enforcement Cooperation (Europol), *Internet Organized Crime Threat Assessment (IOCTA) 2023* (Luxembourg, Publications Office of the European Union, 2023); International Criminal Police Organization (INTERPOL), “2022 INTERPOL global crime trend summary report” (October 2022).

[3] INTERPOL, “INTERPOL financial fraud assessment: a global threat boosted by technology”, 11 March 2024.

организациями. Это может сопровождаться формированием штата работников, получающих заработную плату, и ясным разделением обязанностей, что фактически имитирует организационную структуру того или иного легального предприятия. Типичного портрета организованной преступной группы, занимающейся мошенничеством, не существует. Мошенничество могут совершать различные группы, в том числе сети киберпреступников, анонимно торгующие технологиями, данными и другими преступными услугами; организованные преступные группы, сформировавшиеся в том или ином населенном пункте или в социальных сетях; организованные преступные группы, структурно имитирующие штат сотрудников законной организации (например, колл-центры); преступники из числа офисных работников, совершающие мошенничество, работая в законных организациях или осуществляя законную профессиональную деятельность. Вместо иерархической структуры в организованных преступных группах часто наблюдается динамичное сотрудничество между их членами.

7. Вместе с тем получению более полного представления об организованном мошенничестве способствует не столько понимание того, как организованы преступники, сколько изучение способов осуществления мошеннической деятельности. Исторически сложилось так, что борьба с мошенничеством не считалась такой приоритетной задачей, как противодействие другим видам организованной преступности, а организованное мошенничество часто воспринималось как дополнительная преступная деятельность организованных преступных групп, совершающих другие, более серьезные преступления (например, занимающихся незаконным оборотом наркотиков)[4]. В Конвенции об организованной преступности серьезное преступление определяется как преступление, за которое предусмотрено наказание в виде тюремного заключения сроком не менее четырех лет. Однако на практике во многих государствах мошенничество не классифицируется как серьезное преступление. В связи с этим оно не подпадает под действие Конвенции об организованной преступности. Более того, даже в тех случаях, когда мошенничество наказуемо как серьезное преступление, приговор не обязательно соответствует этой категории тяжести.

II. Категории организованного мошенничества

8. Мошенничество — это преступление, которое включает разнообразные деяния и схемы поведения, применяемые в самых разных условиях и в отношении самых разных жертв. В научных исследованиях используется широкое определение мошенничества: «получение чего-то ценного или уклонение от какой-либо обязанности посредством обмана»[5]. То есть в отличие от других видов серьезных корыстных преступлений мошенничество совершается не с применением силы или принуждения, а с помощью обмана. Кроме того, жертве и преступнику необязательно находиться в одном и том же месте одновременно, и во многих случаях мошенничество не ограничивается ни административными, ни национальными границами. Мошенничество фигурирует в уголовном законодательстве многих стран, однако состав этого преступления описывается по-разному и с разной степенью конкретности[6]. В некоторых законах дается обобщенное описание деяний, составляющих мошенничество, в то время как в других указываются определенные виды деятельности, продукты или услуги, которые часто фигурируют в мошеннических схемах, например выдача себя за представителя власти либо манипулирование данными или их несанкционированное

[4] Michael Levi, “Organized fraud” in *The Oxford Handbook of Organized Crime*, Letizia Paoli, ed. (Oxford, Oxford University Press, 2014).

[5] Grace M. Duffield and Peter Grabosky, *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, No. 199 (Canberra, Australian Institute of Criminology, 2001).

[6] Были изучены юридические определения, используемые в 26 странах 7 различных регионов: Европы и Северной Америки; Латинской Америки и Карибского бассейна; Северной Африки и Западной Азии; Африки к югу от Сахары; южной части Центральной Азии; Восточной и Юго-Восточной Азии; Австралии и Новой Зеландии.

использование. В некоторых государствах введены отдельные законодательные акты против различных видов мошенничества, например компьютерного мошенничества, мошенничества в сфере кредитования, мошенничества на аукционах или мошенничества против коммерческих предприятий. В то же время некоторые основные элементы мошенничества присутствуют в большинстве юридических определений: использование обмана для получения несправедливого преимущества или выгоды и причинение ущерба другому лицу или организации. Под обманом обычно понимается бесчестное поведение, сообщение заведомо ложных сведений, ухищрения, махинации, мошеннические приемы, злоупотребление доверием, сокрытие или опущение информации. Во многих случаях причинение ущерба другому лицу подразумевается как сопутствующий элемент получения преступниками выгоды, но в некоторых законах причинение ущерба оговаривается отдельно с использованием таких понятий, как нарушение или ущемление финансовых интересов других лиц, нанесение неправомерных потерь или лишение чего-либо обманом. Ущерб может быть причинен частному лицу, компании или государству.

9. Мошенничество характеризуется широким разнообразием применяемых методов, объектов воздействия и последствий как для потерпевших, так и для более широких структур. В связи с этим для изучения характера мошенничества было разработано большое количество типологий. Хотя на национальном и международном уровнях используются и другие типологии мошенничества, в настоящем справочном документе рассматривается мошенничество, совершаемое против отдельных лиц, государственных учреждений или частных организаций с целью получения финансовой или иной материальной выгоды. В этой связи были выделены следующие основные категории, которые будут подробнее рассмотрены в дальнейших разделах справочного документа: a) мошенничество в сфере потребительских товаров и услуг; b) мошенничество в сфере потребительских инвестиций; c) мошенничество в сфере трудоустройства; d) мошенничество на основе злоупотребления личными отношениями и доверием; e) мошенничество с выдачей себя за должностное лицо; f) мошенничество с использованием персональных данных; g) мошенничество против коммерческих предприятий или организаций.

10. В каждой категории были выделены основные формы обмана, различающиеся в зависимости от ожидаемой жертвой выгоды или результата мошеннической операции. Хотя эти виды мошенничества совершаются не только организованными преступными группами, последние располагают более широкими возможностями для совершения преступлений и причинения ущерба. В каждой категории представлены различные способы манипулирования жертвами, однако мошенничество любой категории может носить транснациональный характер и совершаться с участием преступников, входящих в организованную преступную группу. Некоторые преступления имеют большие масштабы и приводят к серьезным совокупным последствиям, в других случаях ощутимый ущерб причиняется небольшим группам потерпевших.

A. Мошенничество в сфере потребительских товаров и услуг

11. Мошенничество в сфере потребительских товаров и услуг — один из самых распространенных видов мошенничества: большое количество людей сообщает о том, что они подвергались обману, становились объектами мошенничества или получали мошеннические сообщения с предложениями о покупке товаров или услуг. Эта разновидность мошенничества предполагает продажу товаров или услуг, либо не существующих на самом деле, либо значительно отличающихся от рекламируемых. Как правило, мошенники продают широко востребованные товары или предлагают продукты и услуги по ценам ниже рыночных. Некоторые мошенники ориентируют свои предложения на группы, которые считаются наиболее восприимчивыми к конкретной схеме мошенничества. В мошенничестве могут фигурировать как полностью вымышленные продавцы и

товары, так и компании, предоставляющие недостоверную информацию о поставляемых ими товарах или услугах. Подтверждение факта мошенничества при получении товара или услуги, в отношении которой, как считается, были предоставлены недостоверные сведения, может оказаться непростой задачей. Иногда мошенники пользуются финансовой неграмотностью жертв, чтобы продать им финансовые услуги, например кредиты, страховку или пенсионные планы. Такие услуги обычно связаны с продуктами, которые будут иметь ценность в будущем, и жертвам либо дается слишком оптимистичный прогноз будущих показателей, либо не разъясняются надлежащим образом риски. Мошенники также могут умалчивать о сопутствующих сборах, комиссиях или законных требованиях, что может привести к дополнительным тратам и штрафам для потерпевших[7].

12. Продукты и услуги, которые обычно фигурируют в случаях мошенничества в сфере потребительских товаров и услуг, включают драгоценные камни, домашних животных, билеты на мероприятия, медицинскую продукцию, сулящие крупные вознаграждения лотереи или розыгрыши призов или финансовые продукты и услуги, например страхование. Вместе с тем разнообразие продуктов и услуг, которые могут использоваться в мошеннических схемах, практически безгранично, поскольку мошенники стремятся непрерывно адаптироваться к новым рынкам и запросам потребителей и извлекать из них выгоду.

13. Для продвижения товаров и услуг используются различные средства распространения информации, в том числе онлайновые. К ним относятся фиктивные сайты, сайты легальных магазинов и аукционов, рассылки рекламных сообщений по электронной почте, почтовые рассылки и так называемые «котельные» — колл-центры, из которых совершается большое количество звонков с целью маркетинга или продаж. Некоторые преступники пользуются процветающим рынком списков потенциальных клиентов, которые составляются как законными, так и незаконными способами (например, в результате несанкционированного доступа к данным или фишинговой кампании в интернете), или даже списками лиц, ставших жертвами в прошлом (так называемые списки «лохов»). Информационные и коммуникационные технологии значительно расширили возможности маркетинга и продажи товаров и услуг в глобальных масштабах и при сравнительно низких затратах. В некоторых случаях потребитель может потерять деньги, но в зависимости от обстоятельств и методов, используемых преступниками, финансовые потери может понести торговая площадка или компания — поставщик финансовых услуг. Применяются следующие основные методологии:

a) разработка фиктивных сайтов с целью маркетинга и/или продажи товаров и услуг. Преступники могут рекламировать сайт, используя такие цифровые каналы, как социальные сети или рассылка рекламных сообщений по электронной почте, или производить манипуляции с поисковыми системами в интернете, чтобы увеличить вероятность посещения их сайта лицами, которые ищут соответствующие товары или услуги;

b) функционирование на легальных торговых и аукционных площадках или в социальных сетях фиктивных продавцов, которые используют аккаунты, открытые с помощью фиктивных или украденных персональных данных. Такие продавцы используют возможности легальных платформ, которые обеспечивают доступ к большому количеству пользователей, ищущих товары и услуги. Например, одна организованная преступная группа разместила сотни или даже тысячи объявлений о продаже дорогих товаров, таких как автомобили, на нескольких аукционных сайтах[8].

---

[7] См. Michael Skidmore, *Protecting People's Pensions: Understanding and Preventing Scams* (London, The Police Foundation, 2020).

[8] Более подробную информацию см. в базе данных по прецедентному праву на информационно-справочном портале «Распространение электронных ресурсов и законов о борьбе с преступностью» (ШЕРЛОК) Управления Организации Объединенных Наций

14. Обман потребителей в интернете необязательно должен носить изощренный или сложный характер. Для неправомерного использования законного сайта продаж или аукциона достаточно одного человека, который откроет учетную запись на сайте аукциона и разместит объявление о продаже несуществующего товара. Однако часть преступлений, связанных с обманом потребителей, носит транснациональный характер и совершается при участии организованных преступных групп. Наличие организации редко обнаруживается при общении с жертвой, скорее — при понимании планирования и подготовки преступлений. Основные этапы включают создание и рекламирование сайта или платформы, взаимодействие с жертвой для поддержания обмана (или получения от нее дальнейших платежей) и перемещение денег. Преступники применяют различные методы получения платежей, оставляя почти незаметный финансовый след. К таким методам относятся убеждение поставщика платежных услуг в том, что компания преступников является легальной, перенаправление клиентов на фиктивные платежные сайты, предложение жертвам платить с помощью предоплаченных дебетовых карт или использование счетов третьих лиц, так называемых «денежных мулов», либо счетов, открытых с использованием украденных или поддельных персональных данных. Организованные преступные группы, действующие из других юрисдикций, обычно привлекают соучастников в стране назначения для содействия отмыванию денег[9].

B. Мошенничество в сфере инвестиций

15. Мошенничество в сфере инвестиций обычно связано с продажей акций и облигаций компаний или валюты, а в некоторых схемах предлагается вложить деньги в материальные активы — от недвижимости или коммерческих объектов до вин и крепких спиртных напитков.

16. Для совершения таких преступлений может требоваться глубокое понимание системы регулирования и соответствующих мер контроля, регулирующих функционирование рынков, а граница между законной и незаконной практикой может быть проницаемой и слабо заметной. В некоторых случаях преступники используют механизмы доверия, регистрируясь в качестве регулируемой организации или используя других легальных субъектов, имеющих статус регулируемой организации. Действуя в такой серой зоне между законной и незаконной деятельностью, они создают препятствия для правоохранительных или других регулирующих органов, которым необходимо разобраться в ситуации, представить достаточные и убедительные доказательства обмана и подтвердить факт совершения преступления. В действительности некоторые преступники могут использовать аморальные схемы, которые наносят большой ущерб инвесторам, но при этом, как оказывается, не являются преступными. Распространенными схемами деятельности преступников являются финансовая пирамида и схема Понци, при которых инвестиционная модель основана на постоянном привлечении новых инвесторов для поддержания собственного существования вместо получения прибыли от настоящих продуктов или инвестиций, которых в этом случае может и не быть.

17. Представляется, что масштабы мошенничества в сфере инвестиций растут — отчасти из-за увеличения числа случаев мошенничества с инвестициями в криптовалюты. В этой новой среде инвестиционного мошенничества преступники используют преимущества скорости и гибкости, которые предоставляет цифровое пространство, что позволяет им осуществлять массовый маркетинг

по наркотикам и преступности, *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*. Доступно по адресу https://sherloc.unodc.org/.

[9] Christine Conradt, “Online auction fraud and criminological theories: the Adrian Ghighina case”, vol. 6, No. 1, *International Journal of Cyber Criminology*, (January/June 2012); Jack M. Whittaker and Mark Button, “Understanding pet scams: a case study of advance fee and non-delivery fraud using victims’ accounts”, *Journal of Criminology*, vol. 53, No. 4 (September 2020).

быстро и с относительно низкими затратами[10]. Сложности регулирования новых финансовых рынков, например рынка криптовалюты, обусловливают наличие более широких лазеек, которыми могут пользоваться преступники. Методы, используемые при мошенничестве с инвестициями в криптовалюту, различаются по технической сложности и новизне, причем некоторые приемы заимствованы из других методов, например, манипулирования рынком и финансового груминга; к таким приемам относятся разработка и маркетинг фиктивных платформ для криптовалютных инвестиций и мошенническое сворачивание деятельности или так называемое «выдергивание ковра», предполагающие искусственное завышение стоимости предметов мошенничества, которые становятся бесполезными, как только преступники выводят все вложенные в них средства.

18. Успех мошенничества в сфере инвестиций зависит от таких факторов, как эффективная коммуникация; использование различных методов убеждения потенциальных инвесторов, например кампаний целевого или массового маркетинга; агрессивные методы продаж; производство ресурсов для создания и поддержания авторитета и доверия, включая развитие бренда, разработку сайтов и создание других маркетинговых материалов. Преступники могут использовать отдельные каналы связи или комбинацию таких каналов, которые задействуются на разных этапах совершения преступления. Например, первоначальный контакт с жертвой может производиться через фишинговый сайт, после чего совершается звонок с предложением покупки, а продолжается взаимодействие через мошеннический сайт. Для взаимодействия с жертвами мошенники могут использовать следующие методы:

a) телемаркетинг, то есть использование колл-центров или «котельных» для агрессивного маркетинга и продаж, часто в форме инициативных звонков конкретным лицам, выбираемым с использованием списков потенциальных клиентов, либо составленных собственными силами, либо купленных у других законных или незаконных субъектов, которые собирают и продают такие персональные данные о потребителях. В некоторых случаях в таких списках фигурируют лица, о которых известно, что они ранее становились жертвами обмана и поэтому восприимчивы к похожим способам инвестирования; особенно подвержены такой опасности доверчивые пожилые люди. Колл-центры могут управляться непосредственно преступниками, применяющими данную мошенническую схему, или передаваться на подряд специалистам, способным оказывать услуги «котельной». Такие центры могут располагаться за пределами стран, в которых находятся жертвы, в некоторых случаях — в юрисдикциях, известных менее строгими мерами контроля за подобной деятельностью[11];

b) онлайновые методы. В некоторых странах наблюдается существенный рост числа случаев онлайнового мошенничества в сфере инвестиций, при которых первоначальный контакт происходит через такие средства интернет-коммуникации, как социальные сети, мошеннические сайты и приложения, которые играют главную роль в обмане. Возможности масштабного и целевого маркетинга значительно расширяет доступность цифровых технологий и больших массивов данных о потребителях. Например, чтобы завлечь и выявить лиц, заинтересованных в предлагаемом продукте или услуге, и заложить основу для последующей адресной коммуникации, могут использоваться фишинговые кампании. Для рекламы своей продукции преступники обычно используют социальные сети и приложения для цифровой коммуникации, в некоторых случаях используя образы знаменитостей или представителей популярной культуры, чтобы убедить жертв вложить свои средства. Проникнув на основные

[10] Arianna Trozze, Toby Davies and Bennett Kleinberg, “Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering”, vol. 46, *Journal of Forensic Science International: Digital Investigation* (2023).

[11] Neal Shover, Glenn. S. Coffe and Clintin R. Sanders, “Dialing for dollars: opportunities, justifications, and telemarketing fraud”, *Qualitative Sociology*, vol. 27, No. 1 (March 2004).

финансовые рынки, такие схемы мошенничества с криптовалютой могут привести к серьезным финансовым потерям;

c) личное общение. Часто вопрос инвестиций крайне важен для жертв, поскольку речь идет о крупных суммах денег, и в некоторых случаях для установления необходимого доверия с целью получения инвестиций требуется личный контакт. Некоторые мошенники выбирают жертв среди лиц, с которыми они уже имеют социальные или деловые связи, чтобы использовать существующее доверие.

19. Преступники, занимающиеся мошенничеством в сфере инвестиций, прилагают все усилия, чтобы создать видимость законности, и обычно используют структуру, процессы и деловой лексикон формально законной организации, включая четкое разделение труда, иерархию и распределение обязанностей между сотрудниками. Сложность организации варьируется в зависимости от стремления мошенников избежать подозрений или обнаружения и продолжать совершать преступления[12]. Организации, действующие по принципу «урвать побыстрее», могут осуществлять деятельность в течение короткого времени, а потом исчезнуть вместе с деньгами инвесторов, в то время как другие схемы могут функционировать, оставаясь незамеченными в течение многих лет.

20. Потерпевшие от мошенничества в сфере инвестиций несут самые большие потери по сравнению с другими видами мошенничества против отдельных лиц[13]. Жертвам внушают совершенно ложные или сильно преувеличенные ожидания прибыли. Многие инвесторы теряют все свои средства или большую их часть. Независимо от того, какой именно метод используется, жертвам обычно сообщается ожидаемый размер прибыли, которую они получат от своих инвестиций в будущем, а это значит, что могут пройти годы после первоначального вложения средств, прежде чем потерпевшие поймут, что стали жертвой мошенничества. Детали различных схем и лежащий в их основе обман могут быть весьма разнообразными, но в итоге инвесторы, как правило, теряют все свои деньги или большую их часть. Вот лишь некоторые примеры:

a) полный обман, при котором инвестиционная услуга или продукт никогда не существовали;

b) недобросовестная продажа не имеющих ценности или завышенных по цене акций в качестве крайне рискованных инвестиций, которые вряд ли принесут обещанный доход или обернутся полным провалом;

c) методы манипулирования рынком, искусственно завышающие стоимость инвестиций для ничего не подозревающих инвесторов.

21. Значимость финансовых потерь для потерпевших зависит от их финансовых или личных обстоятельств. Имеют значение также методы, используемые преступниками, которые, например, могут избрать своей целью пенсионные накопления, от чего могут серьезно пострадать отдельные люди[14]; в то же время целью некоторых инвестиций в криптовалюты может быть получение меньших сумм, но от большего числа потерпевших. Что касается жертв финансовых пирамид и схем Понци, то те, кто вкладывает и выводит средства на ранних стадиях, могут ничего не потерять. После хищения денег жертва может подвергнуться повторному нападению со стороны тех же или других преступников, в некоторых случаях выдающих себя за сотрудников законной организации. Они утверждают, что способны отследить и вернуть потерянные средства, но требуют от жертвы предварительную плату; эта схема известна как мошенничество с возвратом средств.

---

[12] Michael Levi, “Organized fraud and organizing frauds: unpacking research on networks and organization”, *Criminology and Criminal Justice*, vol. 8, No. 4 (December 2008).

[13] См. также United States Department of Justice, “Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes”, press release, 3 April 2023.

[14] См. Skidmore, *Protecting People’s Pensions*.

C. Мошенничество в сфере трудоустройства

22. Мошенничество в сфере трудоустройства подразумевает массовый маркетинг фиктивных или вводящих в заблуждение объявлений о вакансиях на сайтах поиска работы. Масштабы использования онлайн-объявлений о вакансиях значительно выросли в легальном секторе, особенно после глобальной пандемии, когда кадровые агентства предлагали более гибкий график работы и возможность работать на дому. Мошенники используют в своих целях спрос на привлекательные должности, особенно среди тех слоев населения, для которых законные возможности такого рода ограничены из-за недостаточной квалификации и уровня подготовки или из-за отсутствия свободных рабочих мест в местной экономике[15]. По данным исследований, чаще всего мошенники избирают своими жертвами ищущих работу лиц, наименее обеспеченных в материальном отношении или находящихся в тяжелой жизненной ситуации.

23. Такое мошенничество обычно предполагает размещение в интернете объявления о вакансии, которая либо полностью вымышлена, либо гораздо менее выгодна, чем утверждается. Примерами могут послужить объявления о возможностях предпринимательской деятельности, работе на дому или работе в модельном бизнесе. В некоторых случаях мошенники просят жертву перед занятием должности оплатить предварительные расходы разного рода: на покупку набора для начинающих, командировку, обучение или проверку кредитной истории. В результате жертвы во многих случаях теряют свои деньги, так и не получив обещанной работы. В других схемах мошенники отправляют жертвам поддельные чеки для оплаты начальных расходов жертв, а затем заявляют, что сумма ошибочно завышена, и просят жертву перевести деньги обратно преступнику. Жертва теряет переведенные деньги и, когда выясняется, что чек поддельный, вынуждена оплатить указанную в нем сумму.

24. Мошенники в сфере трудоустройства также могут стремиться завладеть персональными данными жертв, которые те предоставляют в процессе подачи заявления, что делает их уязвимыми для дальнейших атак. А в некоторых случаях оказывается, что сама работа носит криминальный характер. Так, жертву могут вовлечь в процесс отмывания денег (например, в качестве «денежного мула») или заставить выполнять функции курьера для доставки товаров, приобретенных мошенническим путем (т. е. при мошенничестве с использованием персональных данных). В наиболее серьезных случаях жертва становится предметом торговли людьми для принудительного труда и принудительной преступной деятельности[16].

D. Мошенничество на основе злоупотребления личными отношениями и доверием

25. Важнейшую роль при любом виде мошенничества играет процесс установления доверия. В случае мошенничества, связанного со злоупотреблением личными отношениями и доверием, преступники используют силу личных отношений для установления доверия, необходимого для манипулирования жертвами и

---

[15] Alexandrea J. Ravenelle, Erica Janko and Ken Cai Kowalski, “Good jobs, scam jobs: detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic”, *New Media and Society*, vol. 24, No. 7 (July 2022), pp. 1591–1610; Delali Kwasi Dake, “Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites”, *International Journal of Computer Applications*, vol. 184, No. 51 (March 2023).

[16] С более подробной информацией об этих двух формах эксплуатации можно ознакомиться также в публикации Организации Объединенных Наций «Global Report on Trafficking in Persons 2022» («Всемирный доклад о торговле людьми за 2022 год») и публикации УНП ООН «Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia: policy report» (Bangkok, 2023) («Казино, кибермошенничество и торговля людьми в целях принуждения к преступной деятельности в Юго-Восточной Азии. Программный доклад», Бангкок, 2023 год).

их обмана, иногда неоднократного. При таком мошенничестве жертва не ожидает получения товара или услуги, а рассчитывает на установление искренних отношений с преступником. Сложность этой разновидности мошенничества заключается не столько в эксплуатации технических или технологических систем, сколько в динамике отношений между жертвой и преступником.

26. Многие мошенники устанавливают контакты в интернете и на протяжении нескольких месяцев или даже лет применяют методы социальной инженерии, чтобы завоевать доверие жертвы. Жертвы обычно ожидают романтических отношений, но такая связь может принимать и другие формы, например доверительной дружбы, или даже стремления, чтобы отношения были установлены с членом семьи жертвы. Ряд исследований выявили уязвимые места в демографической группе стареющих и пожилых людей, связанные с такими факторами, как одиночество, социальная изоляция и желание завести новые отношения. Преступники находят и используют такие слабости в своих целях, завязывая дружеские или романтические отношения. Кроме того, преступники могут выдавать себя за члена семьи или друга, попавшего в крайне затруднительное положение и нуждающегося в деньгах для выхода из сложившейся ситуации. Такое мошенничество может быть целенаправленным и включать использование персональных данных, взятых из постов друга или родственника в социальных сетях, чтобы сделать общение с жертвой более правдоподобным. Как правило, о таких критических ситуациях сообщается с помощью текстовых сообщений. Существуют примеры использования искусственного интеллекта для имитации голоса члена семьи или друга в ходе телефонного разговора.

27. Одной из основных разновидностей в этой категории является мошенничество с использованием романтических отношений, когда преступники строят романтические отношения в интернете с целью обмана жертв и вымогательства у них денег. Финансовые потери жертвы здесь могут достигать крупных сумм. Такое мошенничество находит жертв в самых разных регионах мира и процветает в связи с увеличением масштабов использования социальных сетей и, в частности, вследствие более широкой общественной тенденции к поиску романтических отношений в сети. Первоначальный контакт с жертвами обычно происходит в социальных сетях или на сайтах знакомств и в приложениях для знакомств, когда преступник создает фиктивную личность и соответствующую анкету. Один преступник может использовать несколько личностей, чтобы выбрать и завлечь потенциальную жертву. После установления отношений преступник может извлечь из них финансовую выгоду, сначала попросив у жертвы небольшую сумму денег, затем переходя к более крупным суммам и во многих случаях придумывая кризисные ситуации (например, резкое ухудшение здоровья или необходимость срочной поездки), чтобы оказать давление на жертву и заставить ее действовать быстро. Если имел место обмен изображениями сексуального характера, жертва может подвергнуться вымогательству денег.

28. В последнее время наблюдается соединение мошенничества со злоупотреблением романтическими отношениями с мошенничеством в сфере криптовалютных инвестиций. Мошенничество в форме романтического завлечения или так называемое «откармливание свиней» (этот термин не рекомендуется использовать из уважения к жертвам таких преступлений) предполагает установление преступником личных отношений с онлайн-жертвой. Вместо выдумывания кризисной ситуации мошенники используют близкие отношения и доверие, чтобы заманить жертву в мошенническую инвестиционную схему. Для преступников это может включать дополнительные этапы планирования и подготовки, в том числе разработку мошеннического сайта или приложения, доступ к которому может быть предоставлен жертве, и даже клиентское обслуживание для инвесторов[17]. Включение в схемы обмана криптовалютных инвестиций имеет ряд

[17] Cassandra Cross, “Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud”, *Current Issues in Criminal Justice* (2023); Fangzhou Wang and Xiaoli Zhou, “Persuasive schemes for financial exploitation in online romance scam: an anatomy on Sha Zhu Pan (杀猪盘) in China”, *Victims and Offenders*, vol. 18, No. 5 (2023).

последствий: расширение круга потенциальных жертв за счет более молодых возрастных групп; знакомство жертв с незнакомым и волатильным рынком высокого риска, в связи с чем снижается вероятность осознания ими того, что они стали жертвами мошенничества; усложнение для следователей по уголовным делам задачи отслеживания преступников по движению денежных средств.

29. Большинство исследований мошенничества, основанного на злоупотреблении романтическими отношениями, посвящено потерпевшим и произошедшему с ними, а не преступникам, которые менее заметны. Считается, что такого рода мошенничество, как правило, носит транснациональный характер и совершается организованными преступными группами, численность которых больше в определенных регионах. В контексте такой разновидности мошенничества, как «откармливание свиней», некоторые организованные преступные группы создают более сложные, похожие на коммерческие организации структуры, в которых существует четкое разделение труда (например, контакты с жертвами, информационные технологии и отмывание денег) и осуществляется вербовка лиц, нуждающихся в деньгах и уязвимых к эксплуатации, включая торговлю людьми[18].

30. Независимо от особенностей жертв, мошенничество на основе злоупотребления личными отношениями и доверием может причинять значительный ущерб. Потерпевшие не только лишаются денег, но и испытывают страдания от предательства и разрыва значимых для них личных отношений. Кроме того, такое мошенничество наносит жертвам значительный психологический и эмоциональный вред. В некоторых случаях потерпевшие даже отказываются признавать, что стали жертвой мошенничества.

E. Мошенничество с выдачей себя за должностное лицо

31. Мошенничество с выдачей себя за должностных лиц, или мошенничество с выдачей себя за другое лицо, заключается в манипуляциях с сообщениями, чтобы они выглядели как сообщения от государственных служащих или иных должностных лиц, например от сотрудников полиции, налоговых органов, банков или правительственного учреждения. При таком мошенничестве используются различные предлоги и сценарии, включая выдачу себя за сотрудника налогового органа или другого государственного учреждения, требующего погасить имеющуюся задолженность; банковского служащего, утверждающего, что средства на банковском счету находятся под угрозой похищения преступниками; сотрудника полиции, утверждающего, что жертва совершила уголовное правонарушение.

32. Главной отличительной особенностью мошенничества с выдачей себя за другое лицо является применение методов убеждения, которые не столько апеллируют к желаниям и потребностям жертв (как, например, в мошенничестве в сфере потребления), сколько вызывают у них страх, ужас, тревогу и беспокойство. Состояние повышенного эмоционального возбуждения мешает принимать решения и делает жертв более подверженными манипуляциям. Эти сообщения содержат угрозы о неблагоприятных последствиях, в том числе тех или иных правовых санкциях, если жертва не отправит платеж или не переведет средства.

33. Это мошенничество обычно включает такие способы массового распространения информации, как рассылка рекламных сообщений по электронной почте, общение в социальных сетях, текстовые сообщения, автоматические телефонные звонки или так называемый «роботизированный набор номера», когда телефонные звонки совершаются автоматически с воспроизведением записанного сообщения. Эти технологии обеспечивают почти одновременный контакт с тысячами жертв сразу, что позволяет охватить огромную аудиторию.

[18] UNODC, “Casinos, cyber fraud, and trafficking in persons”.

F. Мошенничество с использованием персональных данных

34. Мошенничество с использованием персональных данных[19] подразумевает использование украденной или ложной информации о личности для получения прямого доступа к товарам, услугам или денежным средствам жертв, например использование украденной информации для совершения покупок или доступа к финансовым счетам. Мошенничество с использованием персональных данных может совершаться без непосредственного общения или непосредственных действий со стороны лица, чьи персональные данные незаконно используются, поскольку объектом мошенничества часто является поставщик товаров, услуг или денежных средств. Таким образом, ущерб причиняется различным потерпевшим субъектам, включая жертву, чьи персональные данные были неправомерно использованы, поставщика финансовых услуг или другую компанию, у которых снимаются денежные средства, и в некоторых случаях — поставщика товаров или услуг, приобретенных на украденные средства.

35. Различная персональная информация может быть использована в разных целях. Это могут быть персональные данные, составляющие цифровые идентификаторы людей в различных онлайн-средах, например имя и фамилия или дата рождения; данные финансовых счетов, например номера кредитных карт; информация об учетных записях в интернете, включая имена пользователей и пароли; биометрические данные, например цифровой отпечаток пальца, украденный с электронного устройства.

36. Преступники могут получить доступ к этой информации посредством проникновения в систему, использования схем социальной инженерии, например фишинговых или смишинговых операций, или приобретения данных на криминальных онлайн-рынках. Эти данные могут использоваться для покупки товаров и услуг, подачи заявок на получение кредитов и другого финансирования или доступа к счетам жертв и вывода с них денег. В отношении упомянутых средств можно дополнительно отметить следующее:

a) проникновение в систему: некоторые мошенники активно добывают персональную информацию с помощью незаконных хакерских методов, установки вредоносных программ или фишинга;

b) криминальные онлайн-рынки: существует динамичная подпольная экономика, связанная с покупкой и продажей информации о личностях, которой могут воспользоваться мошенники. Возможность получить информацию таким образом устраняет некоторые технические барьеры для мошенников, которые в противном случае не имели бы таких возможностей для кражи личных данных;

c) социальная инженерия: во многих случаях применяется рекламное объявление или другое незапрашиваемое сообщение, отправленное по электронной почте или другим способом онлайн-связи, смс-сообщение или незапрашиваемый телефонный звонок, с помощью которых жертву обманом заставляют предоставить персональные данные. Степень изощренности может варьироваться, но более сложными методами, например имитацией легальных сайтов, преступники могут добиться более эффективного и прямого несанкционированного доступа к онлайновым учетным записям.

37. Для совершения мошенничества с использованием персональных данных преступники применяют различные методы. К основным методам относятся захват учетной записи, мошенничество с использованием карты без ее предъявления и мошенничество с подачей заявок, которые заключаются в следующем:

a) захват учетной записи: это мошенничество предусматривает получение преступниками достоверных идентификационных данных для входа в учетные записи пользователей. Это могут быть учетные записи для банковских счетов и других видов финансовых счетов (например, у поставщиков виртуальной

[19] См. также UNODC *Handbook on Identity-related Crime* (Vienna, 2011).

валюты), сайтов розничной торговли или учетные записи у поставщиков товаров и услуг. Учетная запись может быть использована в различных целях, включая прямой перевод средств на счета, контролируемые преступниками, или мошенническое приобретение товаров или услуг с помощью данной учетной записи. В некоторых случаях получение информации для доступа к учетной записи жертвы является первым из шагов, необходимых для получения денег, товаров или услуг с помощью последующих проникновений в систему. В процессе может потребоваться преодоление таких мер безопасности, как двухфакторная аутентификация. Поэтому преступники прибегают к дополнительным методам, например подмене SIM-карт или использованию альтернативных способов оплаты;

b) использование карты без ее предъявления: этот метод предусматривает совершение удаленных несанкционированных покупок онлайн или по телефону. Получения финансовых идентификационных данных жертвы достаточно для того, чтобы обмануть как поставщика финансовых услуг, так и коммерческого продавца, при этом отсутствует необходимость прямого взаимодействия с жертвой или физического доступа к платежной карте. Для использования финансовых идентификационных данных жертвы мошенникам обычно необходимо произвести следующие ключевые действия:

i) приобретение знаний, ресурсов и финансовых идентификационных данных на криминальных онлайн-рынках;

ii) маскировка заказов с целью избежать срабатывания алгоритмов обнаружения мошенничества на том или ином коммерческом сайте;

iii) получение заказов по адресу, по которому нельзя отследить преступников;

iv) перепродажа товаров в качестве индивидуального продавца или продажа оптом, выдавая себя за законного торговца на широко используемых онлайн-площадках;

c) мошенничество с подачей заявок: мошенники пользуются широкой доступностью персональных данных и используют их для подачи заявки на кредит на имя жертвы. Обычно это делается для получения кредита у организации, предоставляющей финансовые услуги. Чтобы убедительно выдавать себя за то или иное лицо, преступникам необходимо получить совокупность персональных данных (например, имя и фамилия, адрес или дата рождения). Одна из новых тенденций — использование технологий для создания синтетических личностей путем комбинирования реальных и вымышленных идентификационных данных. После создания таких личностей их можно развивать, чтобы со временем они становились более кредитоспособными и в конечном счете можно было подавать заявки на получение финансовых продуктов высокой стоимости.

38. Важно отметить, что связь с организованной преступностью и участие организованных преступных групп не являются необходимыми условиями совершения мошенничества с использованием персональных данных. Однако навыки и ресурсы, которыми располагает организованная преступность, значительно расширяют возможности для совершения мошенничества с использованием персональных данных в крупных масштабах и получения высокой прибыли. Особенно серьезной эту угрозу делает распространение в интернете доступных целей в условиях роста цифровой экономики. Манипулирование идентификационными данными и их неправомерное использование могут служить различным целям при совершении преступлений организованными группами, включая противодействие попыткам отследить исполнителей преступной деятельности[20].

[20] Simon Baechler, “Document fraud: will your identity be secure in the twenty-first century? ”, *European Journal on Criminal Policy and Research*, vol. 26, No. 3 (June 2020).

G. Мошенничество против коммерческих предприятий или организаций

39. Мошенничество против коммерческих предприятий или организаций, как правило, предполагает неправомерное использование внутренних систем или деловых отношений для обмана жертвы. Такое мошенничество могут совершать как сотрудники организации, так и лица, не имеющие к ней отношения. Некоторые виды обмана не относятся к схемам, изначально разработанным для совершения мошенничества, а применяются вполне законными предприятиями и субъектами или с использованием законных продуктов, в некоторых случаях из-за жестких внутренних требований, сомнительных методов работы или культуры труда.

40. Ниже представлен ряд примеров мошенничества против коммерческих предприятий или организаций.

a) Одним из наиболее распространенных видов мошенничества, совершаемого посредством кибертехнологий, является компрометация корпоративной электронной почты. Объектами этого вида мошенничества, обычно совершаемого преступниками извне, становятся предприятия и организации любого размера и в самых разных отраслях. Преступники проникают в системы и, используя методы социальной инженерии, убеждают сотрудников совершить несанкционированный перевод средств на счета, находящиеся под контролем преступников. Потери жертв могут быть очень велики. Первый шаг — проникновение в коммуникационную систему организации, чтобы убедить получателей сообщений в своей легитимности. Основные методы включают взлом учетных записей электронной почты сотрудников, рассылку фишинговых сообщений с целью получения данных об учетных записях сотрудников или эксплуатация операторов связи для имитации доменных имен, знакомых организации-объекту[21]. Злоумышленники используют различные сценарии, которые включают эксплуатацию существующих отношений между двумя компаниями и выставление поддельного счета-фактуры; отправление якобы от старшего сотрудника сообщения электронной почты с просьбой о срочном предоставлении средств; выдачу себя за юриста, который просит перевести деньги для решения деликатного вопроса[22]. Коммуникация может занять некоторое время, и преступники могут потратить его на изучение организации и ее систем, чтобы неоднократно совершать мошенничество в отношении нее.

b) Мошенничество с финансовой отчетностью включает в себя множество методов, с помощью которых законные специалисты по финансовым рынкам дезинформируют других субъектов, например инвесторов, органы регулирования и других участников рынка, и искажают их представление о финансовом состоянии и перспективах какой-либо компании или фонда. Похожие разновидности бухгалтерского мошенничества позволяют также скрывать неправомерное присвоение, нецелевое использование или хищение денежных средств. Причиной подобного мошенничества могут быть слишком жесткие требования в отношении ожидаемых показателей работы. Совершать такого рода мошенничество могут, например, руководители компаний, недобросовестные финансовые трейдеры или руководители хедж-фондов, отчитывающиеся о финансовых показателях. В некоторых случаях последствиями такого мошенничества могут

[21] Norah Saud Al-Musib and others, “Business email compromise (BEC) attacks”, *Materials Today: Proceedings*, (vol. 81, Part 2 (2023)); Geoffrey Simpson, Tyler Moore and Richard Clayton, “Ten years of attacks on companies using visual impersonation of domain names” — научная статья, представленная на Симпозиуме по исследованиям электронных преступлений (eCrime), который был организован Рабочей группой по борьбе с фишингом и проведен 16–19 ноября 2020 года в Бостоне (Соединенные Штаты Америки).

[22] Alessandro E. Agazzi, “Business Email Compromise (BEC) and cyberpsychology”, доступно по адресу https://arxiv.org/; Al-Musib and others, “Business email compromise (BEC) attacks”.

быть затронуты, помимо самой компании, другие коммерческие организации, отрасли или даже экономика в целом[23].

c) Мошенничество с использованием фирм, функционирующих в течение длительного периода времени, или недавно учрежденных фирм может совершаться как существующими торговыми компаниями, так и компаниями, которые могли быть приобретены или учреждены с мошеннической целью. Компании создают кредитную историю, зарабатывают доверие или приобретают репутацию, которые используются для обмана покупателя, продавца или кредитора с целью побудить их поставить товары или предоставить финансирование. Учредители таких компаний при этом осознают, что не имеют возможности или не собираются платить.

III. Темы для рассмотрения

41. Рабочая группа, возможно, пожелает обсудить следующие темы:

a) характер организованного мошенничества в различных юрисдикциях;

b) использование Конвенции об организованной преступности для предупреждения организованного мошенничества и борьбы с ним, а также криминализация мошенничества как серьезного преступления, определение которого дано в статье 2 Конвенции;

c) возможности для эффективного международного сотрудничества, в том числе с частным сектором;

d) предоставление информации о предупреждении организованного мошенничества, о защите потерпевших и свидетелей мошенничества, а также лиц, сообщающих информацию, о преследовании организованных преступных групп, занимающихся организованным мошенничеством, и о содействии налаживанию партнерских отношений для этих целей;

e) определение соответствующих потребностей в технической помощи, связанной с осуществлением Конвенции об организованной преступности, в целях предупреждения организованного мошенничества и борьбы с ним.

IV. Последующие меры и возможные рекомендации

42. Рабочая группа, возможно, пожелает вынести следующие рекомендации:

a) рекомендовать государствам-участникам, которые еще не сделали этого, рассмотреть возможность криминализации мошенничества как серьезного преступления в соответствии с определением, данным в пункте (b) статьи 2 Конвенции об организованной преступности, с тем чтобы в случаях, когда это преступление носит транснациональный характер и совершается с участием организованной преступной группы, можно было эффективно задействовать предусмотренный Конвенцией механизм международного сотрудничества;

b) настоятельно призвать государства-участники использовать инструментарий, предлагаемый Конвенцией об организованной преступности, для разработки или изменения национального законодательства, когда это необходимо и целесообразно, с целью предупреждения мошенничества, в том числе мошенничества, совершаемого организованными преступными группами, и борьбы с ним;

c) рекомендовать государствам-участникам проводить, при необходимости во взаимодействии с другими соответствующими субъектами, анализ тенденций, характеризующих деятельность организованных преступных групп,

[23] United Kingdom of Great Britain and Northern Ireland, Serios Fraud Office, “Senior bankers sentenced to 9 years for rigging EURIBOR rate”, 1 April 2019.

относящуюся к организованному мошенничеству, и предоставлять информацию и данные об этих тенденциях Управлению Организации Объединенных Наций по наркотикам и преступности;

d) просить Управление Организации Объединенных Наций по наркотикам и преступности при наличии внебюджетных ресурсов осуществлять сбор, анализ и распространение информации об организованном мошенничестве;

e) настоятельно призвать государства-участники оказывать друг другу самое широкое международное содействие, включая взаимную правовую помощь, в расследовании, уголовном преследовании и судебном разбирательстве в связи с организованным мошенничеством и смежными преступлениями, охватываемыми Конвенцией об организованной преступности и протоколами к ней;

f) рекомендовать государствам-участникам развивать сотрудничество с соответствующими заинтересованными сторонами, включая частный сектор, организации гражданского общества, средства массовой информации, образовательные учреждения и научное сообщество, в вопросах предупреждения организованного мошенничества и борьбы с ним, в том числе посредством проведения образовательных и информационных кампаний;

g) просить Управление Организации Объединенных Наций по наркотикам и преступности при наличии внебюджетных ресурсов продолжать разработку инструментария оказания технической помощи и предоставление государствам-участникам по их просьбам технической помощи, в том числе в области развития потенциала, с целью помочь им эффективно применять положения Конвенции об организованной преступности для предупреждения организованного мошенничества и борьбы с ним;

h) просить государства-участники, которые еще не сделали этого, обновить информацию о своем законодательстве, касающемся криминализации организованного мошенничества, на информационно-справочном портале «Распространение электронных ресурсов и законов о борьбе с преступностью» (ШЕРЛОК).