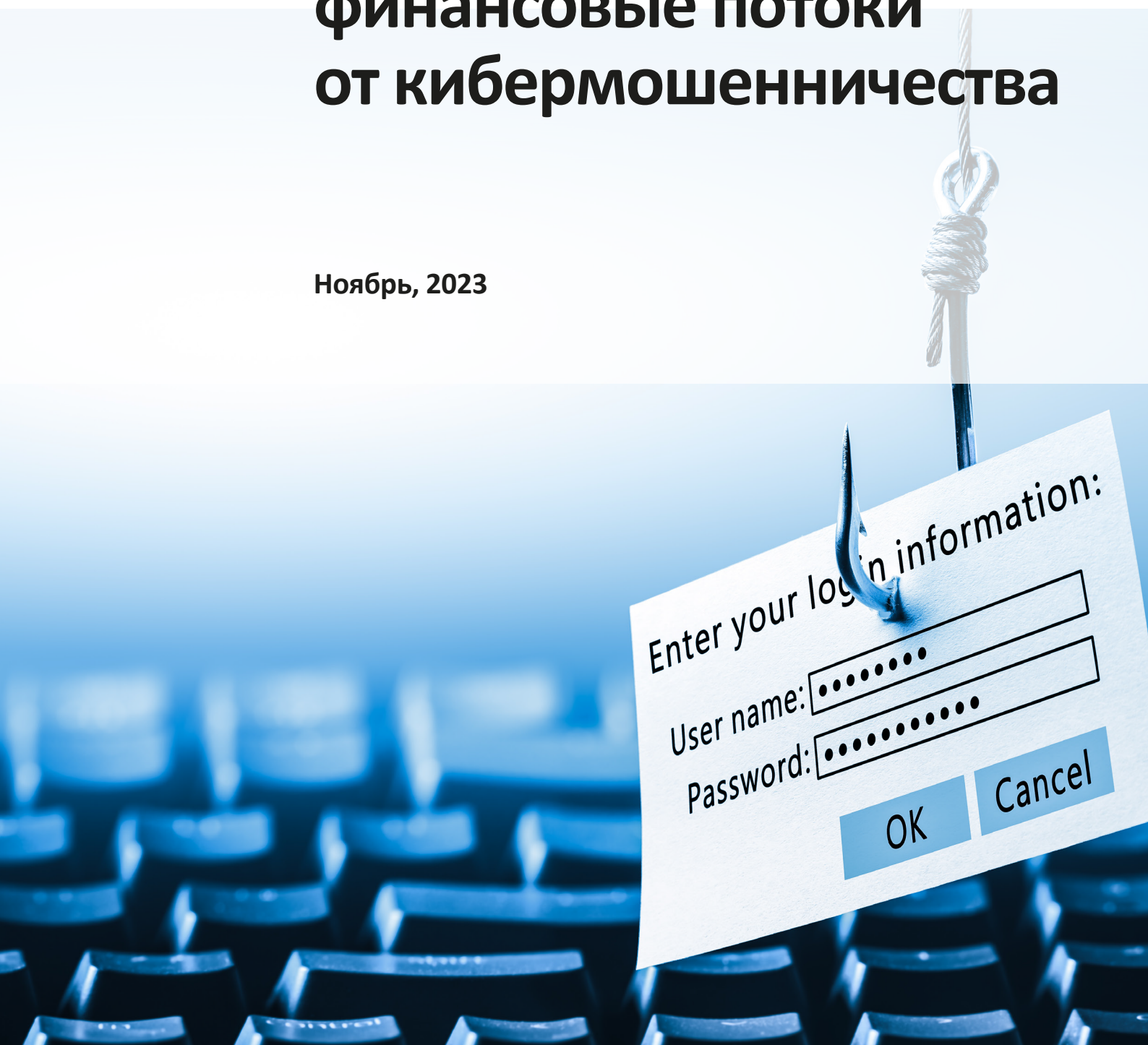
Незаконные финансовые потоки от кибермошенничества

Ноябрь, 2023



Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимой межправительственной организацией, разрабатывающей и популяризующей свои принципы и политику для защиты всемирной финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ). Подробная информация о ФАТФ размещена на сайте **www.fatf-gafi.org**. Данный документ и/или любая включенная в него карта подготовлены без предубеждения и ущемления статуса или суверенитета над любой территорией, международных границ и разграничительных линий, а также названий любых территорий, городов или областей.

Целью Группы подразделений финансовой разведки «Эгмонт» является создание форума для подразделений финансовой разведки (ПФР) по всему миру для улучшения сотрудничества в борьбе с отмыванием денег и финансированием терроризма и содействия реализации внутренних программ в этой области. Более подробная информация о Группе «Эгмонт» размещена на сайте: www.egmontgroup.org.

Задачами Интерпола являются предоставление возможности 195 странам-членам для совместной борьбы с трансграничной преступностью и содействие глобальной безопасности. Интерпол ведет глобальные базы данных, содержащие информацию о преступниках и преступлениях, предоставляет оперативную и криминалистическую поддержку, аналитические услуги и обучение. Эти полицейские возможности предоставляются по всему миру и поддерживают четыре глобальные программы: финансовые преступления и коррупция; борьба с терроризмом; киберпреступность; организованная и современная преступность.

Ссылка для цитирования:

FATF – Interpol - Egmont Group (2023), Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, France
www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/iIllicit-financial-flows-cyber-enabled-fraud.htm

Фото на обложке ©Getty Images

Содержание

Перечень сокращений

ПОД/ФТ	Противодействие отмыванию денег и финансированию терроризма
BEC	Компрометация деловой электронной почты
НПК	Надлежащая проверка клиента
КМ	Кибермошенничество
УНФПП	Установленные нефинансовые предприятия и профессии
ФУ	Финансовое учреждение
ПФР	Подразделение финансовой разведки
IBAN	Международный номер банковского счета
IP	Межсетевой протокол
ОД	Отмывание доходов (полученных преступным путем)
ВПП	Взаимная правовая помощь
PSP	Провайдеры платежных услуг
ГЧП	Государственно-частное партнерство
СПО	Сообщение о подозрительной операции
ФТ	Финансирование терроризма
TBML	Отмывание денег через торговые операции
ВА	Виртуальные активы
ПУВА	Провайдеры услуг виртуальных активов
vIBAN	Виртуальный международный номер банковского счета
VPN	Виртуальная частная сеть
VoIP	IP-телефония

Основные положения

На сегодняшний день кибермошенничество (КМ) становится все более распространенным видом транснациональной организованной преступности. Преступные синдикаты КБ зачастую имеют четкую структуру, состоящую из отдельных подгрупп, специализирующихся в различных областях преступной деятельности, включая отмывание денег. Данные подгруппы также могут быть слабо организованы и децентрализованы в различных юрисдикциях, что еще больше затрудняет расследование деятельности КМ. Синдикаты КМ также связаны с другими видами преступлений, в частности с торговлей людьми и принудительным трудом в колл-центрах КМ, а также с ФРОМУ, связанным с незаконной киберактивностью из Корейской Народно-Демократической Республики (КНДР).

В процесс отмывания денег через КМ вовлечены группы ОД и профессиональные посредники. Сеть счетов ОД, как правило, состоит из денежных мулов, но может также включать фиктивные или легальные компании. В сети ОД также участвуют различные типы финансовых учреждений (ФУ), включая банки, провайдеров платежей и денежных переводов, а также провайдеров услуг виртуальных активов (ПУВА). Для дальнейшего сокрытия финансовых следов своих незаконных доходов преступники используют комбинацию различных методов ОД, таких как использование наличных денег, отмывание денег через торговые операции и нелицензированные услуги.

Благодаря цифровизации технологии позволяют преступникам, занимающимся КМ, развивать и увеличивать масштабы, размах и скорость своей противоправной деятельности. Они используют различные инструменты и приемы, чтобы обмануть жертв, воспользовавшись их чувствами и эмоциями, и выманить как можно больше средств. Синдикаты КМ также используют технологические достижения для упрощения и ускорения процесса отмывания преступных доходов. Виртуальные сервисы, такие как удаленное открытие счетов в Интернете, позволяют преступникам легко открывать зарубежные счета и отмывать доходы за рубежом, причем финансовые операции осуществляются практически мгновенно. Преступники используют социальные сети и платформы обмена сообщениями для масштабной вербовки денежных мулов за рубежом. Кроме того, преступники умело используют уязвимости, возникающие в новых цифровых финансовых институтах и продуктах, а также в нетрадиционных секторах, таких как электронная коммерция, социальные сети и платформы потокового вещания.

Для более эффективного реагирования на КМ юрисдикциям следует:

- реализовывать инициативы по увеличению числа сообщений о жертвах и подозрительных операциях;
- эффективно анализировать значительные объемы поступающей информации;
- учитывая всеобъемлющий характер КМ, для комплексного противодействия и предотвращения КМ и связанных с ним видов ОД необходимы сильные внутренние координационные механизмы.

Как правило, предикатные преступления в области КМ совершаются не там, где происходит процесс ОД. Доходы могут быстро отмываться через сеть счетов, которая часто охватывает несколько юрисдикций и финансовых учреждений. Юрисдикции должны сотрудничать на многосторонней основе для эффективного

и оперативного перехвата доходов от КМ, которые отмываются трансгранично. С этой целью юрисдикции должны использовать и поддерживать существующие (и любые будущие) многосторонние механизмы (такие как I-GRIP Интерпола и проект BEC[1] Группы «Эгмонт») для быстрого международного сотрудничества и информационного обмена для эффективного противодействия КМ.

В заключительной части отчета приводится перечень риск-индикаторов, а также полезных требований и мер контроля в области противодействия мошенничеству, которые могут быть использованы организациями государственного и частного секторов для выявления и предотвращения КМ и связанного с ним ОД.

[1] Business Email Compromise – компрометация деловой электронной почты *(прим. пер.)*.

1. Вступительная часть

1. Онлайн-мошенничество и махинации уже заняли центральное место в киберпреступности. Без контроля они будут только усложняться и представлять все большую угрозу и риск по мере того, как все больше организованных преступных групп будут заниматься данной противоправной деятельностью и использовать возможности, предоставляемые новыми технологиями, такими как генеративный искусственный интеллект[2].

2. Под председательством Сингапура ФАТФ приступила к реализации новой инициативы, направленной на противодействие незаконным финансовым потокам от кибермошенничества. Настоящий отчет является результатом первого совместного проекта Группы «Эгмонт», ФАТФ и Интерпола и отражает твердое коллективное намерение пресечь деятельность транснациональных организованных преступников и их сетей.

1.1. Направление и область применения

3. Настоящий отчет посвящен незаконному финансированию, возникающему в результате мошенничества, которое осуществляется в киберсреде или с ее помощью, (i) связано с транснациональной преступностью, такой как транснациональные субъекты и финансовые потоки, и (ii) включает обманные методы социальной инженерии (т.е. манипулирование жертвами с целью получения доступа к конфиденциальной или личной информации). Признавая наличие множества разновидностей такого мошенничества, в настоящем отчете основное внимание уделяется следующим видам преступной деятельности (в совокупности именуемым кибермошенничеством (КМ)):

   - **Компрометация деловой электронной почты (Business Email Compromise, BEC):** жертвы получают по электронной почте инструкции, выдаваемые за инструкции от их клиентов или поставщиков, с просьбой перевести средства на новые платежные счета.
   - **Фишинг (от англ. Phishing):** жертвы обманным путем вынуждены сообщить конфиденциальную информацию, например, личные данные, банковские реквизиты или учетные данные для входа в систему. Затем преступник использует полученную информацию для снятия денег с платежных счетов жертв, открытия новых платежных счетов или совершения мошеннических операций.
   - **Мошенничество с использованием социальных сетей и телекоммуникаций:** сценарий, при котором преступники, выдавая себя за государственных служащих, родственников или друзей, связываются с жертвами через мобильные или социальные сети и, воспользовавшись их эмоциями, склоняют к оплате или передаче контроля над платежными счетами, а также к совершению финансовых операций, таких как оформление кредита или открытие счета для получения преступных доходов.
   - **Мошенничество в сфере интернет-трейдинга/торговых платформ:** жертвы вводятся в заблуждение фальшивой рекламой или консультантами в Интернете на несуществующих или поддельных (мошеннических)

[2] См. также Международный валютный фонд (август 2023 г.) Заметка о финтехе: Генеративный искусственный интеллект в финансах: анализ рисков.

платформах для торговли или инвестиций, связанных как с фиатными, так и с виртуальными активами.

- **Любовное мошенничество:** жертв обманом заставляют переводить деньги преступникам, убеждая их в том, что они состоят в романтических отношениях.
- **Мошенничество с трудоустройством:** фальшивые предложения о работе в социальных сетях заставляют жертв платить мошенникам под различными предлогами, включая предоплату за покупку товаров для повышения продаж торговой платформы или гарантийный взнос для обеспечения занятости.

4. Незаконное финансирование, связанное с программами-вымогателями и другими преступлениями с использованием вредоносных программ, не входит в сферу компетенции данного отчета. Более подробную информацию о программах-вымогателях, а также информацию об отмывании денег через виртуальные активы (ВА) и провайдеров услуг виртуальных активов (ПУВА), а также о трудностях и успешных практиках снижения таких рисков можно получить в отчете ФАТФ «Противодействие финансированию программ-вымогателей» (март 2023 г.). Данная информация представляется важной, поскольку виртуальные активы и ПУВА иногда используются для отмывания доходов от КМ.

1.2. Цели и структура

5. Целью данного отчета является повышение уровня информированности компетентных органов об угрозе, которую представляет собой КМ. Отчет основывается на результатах работы, уже проделанной ФАТФ и другими международными организациями (в том числе Группой «Эгмонт», Европолом и Интерполом), и направлен на выявление значимых и возникающих тенденций, необходимых для более глубокого понимания рисков.

- **В главах 2 и 3** отчета рассматриваются текущие операционные риски в отношении КМ и дается представление о рисках, методах и трендах в области КМ и связанного с ним отмывания денег (ОД), включая влияние и уязвимость цифровизации и новых технологий.
- **В главах 4 и 5** отчета представлены примеры успешной практики и операционных решений, используемых юрисдикциями для решения задач по противодействию и пресечению КМ и сопутствующего ОД, включая механизмы международного сотрудничества и возврата активов.

1.3. Методология

6. Эксперты из Сингапура (от имени ФАТФ), ПФР Гонконга (от имени Группы «Эгмонт») и Интерпола выступили соруководителями данного проекта. Кроме того, в составе проектной группы свой вклад в работу внесли представители следующих юрисдикций и организаций: Азербайджан, Бразилия, Бельгия, Канада, Китай, Совет Европы, Европейская комиссия, Европол, Германия, Межправительственная группа по борьбе с отмыванием денег в Западной Африке (ГИАБА), Индия, Италия, Израиль, Япония, Малайзия, Мексика, Комитет экспертов по оценке мер борьбы с отмыванием денег и финансированием терроризма (МАНИВЭЛ), Пакистан, Португалия, Саудовская Аравия, Того, Великобритания и США.

7. Выводы отчета основаны на:

   - Обзоре существующей литературы и материалов из открытых источников по данной теме. В их числе данные и исследования, проведенные Группой «Эгмонт» и Интерполом.
   - Запросе в Глобальную сеть ФАТФ и Группу «Эгмонт», объединяющую более 200 юрисдикций и 170 ПФР соответственно, на получение информации о рисках, правоприменительных механизмах и стратегиях, а также о внутренних и международных механизмах сотрудничества и координации. В общей сложности проектная группа получила информацию от более чем 80 делегаций.
   - Обсуждении и обмену мнениями в ходе Совместной встречи экспертов ФАТФ (апрель 2023 г.) и Консультативного форума для частного сектора (май 2023 г.), включая целенаправленное взаимодействие с частным сектором.

2. Риск-среда: кибермошенничество

2.1. Возрастание угрозы отмывания доходов (ОД)

8. Количество КМ значительно увеличилось в мировом масштабе. Несмотря на отсутствие полной оценки глобальных масштабов КМ, многие юрисдикции сообщают об их постоянном росте в последние годы. Незаконные доходы от КМ часто переводятся в иностранные юрисдикции. В дальнейшем такие доходы могут отмываться через финансовые системы других юрисдикций, являющихся третьими сторонами.

9. Согласно отчету Интерпола о тенденциях развития мировой преступности в 2022 году[3], мошенничество в Интернете является одним из направлений киберпреступности, которое чаще всего воспринимается как представляющее «высокую» или «очень высокую» угрозу в глобальном масштабе. Большинство юрисдикций, предоставивших информацию для данного проекта, признают риски ОД, возникающие в результате КМ, в рамках своих национальных оценок рисков. Регионы с высокой степенью использования безналичных и цифровых технологий (например, где основная часть финансового посредничества осуществляется через онлайн-сервисы), как ожидается, более уязвимы к рискам ОД, связанным с этим преступлением, хотя транснациональный характер КМ означает, что преступники могут выбирать жертв вне зависимости от международных границ. В приведенной ниже вставке собрана информация из различных источников[4] для получения регионального обзора угроз, связанных с КМ.

Вставка 1. Усиление угроз ОД: региональные тенденции в области КМ

Африка: в Африке стремительная цифровизация финансового сектора открыла перед преступниками множество возможностей для совершения ОД, что привело к резкому росту мошенничества в сфере интернет-банкинга, включая фишинг, кражу личных данных и мошенничество с виртуальными активами. Рост финансовых потерь в результате таких преступлений представляет собой повышенную угрозу ОД. Например, в Западной Африке КМ, по имеющимся данным, рассматривается как один из основных источников преступных доходов.

Северная и Южная Америка: КМ было определено как растущий или возникающий риск. Одна из юрисдикций отметила, что количество сообщений о КМ растет из года в год, и отметила, что связанный с этим риск ОД будет соответственно расти. Другая юрисдикция сообщила, что в период с 2021 по 2022 гг. объем мошенничества с инвестициями в виртуальные активы увеличился более чем на 180%, так как преступники воспользовались шумихой и общественным резонансом в отношении виртуальных активов.

Азиатско-Тихоокеанский регион: юрисдикции отнесли КМ к высокому или значительному риску ОД. Например, в одной из юрисдикций отмечается, что большинство сообщений о мошенничестве в той или иной форме содержат КМ, и наблюда-

[3] См. Интерпол (2022 г.): Отчет о тенденциях развития мировой преступности.
[4] Включает информацию и данные, предоставленные юрисдикциями, а также отчеты Интерпола и Европола.

ется рост числа случаев ОД, связанных с КМ. Другая юрисдикция подчеркнула роль транснациональных субъектов, обманывающих жертв с помощью множества незаконных инвестиционных приложений. Пандемия COVID-19 способствовала ускоренной цифровизации услуг и поведения частных лиц, правительств и бизнеса в регионе. В результате число случаев КМ и связанного с ними ОД увеличилось и, как ожидается, будет продолжать расти.

Карибский регион: регион в значительной степени подвержен риску отмывания денежных средств и связанных с ним преступлений, причем за последние пять лет увеличился общий объем мошенничества, связанного с КМ. Растущий сектор виртуальной коммерции в Карибском бассейне также представляет собой фактор уязвимости, в том числе из-за наличия ПУВА, включая микшеры (виртуальных валют), которые могут использоваться для отмывания незаконных средств в пользу организованных преступных групп, включая КМ.

Европа: в целом КМ оценивается как фактор, представляющий риск ОД. Многие юрисдикции отмечают значительный рост этой деятельности, причем КМ воспринимаются как представляющее высокую степень угрозы. Для отмывания доходов от КЭФ нередко используются ВА (в частности, это касается мошенничества в сфере онлайн-торговли, связанного с ВА, например, мошеннических первичных предложений монет).

Ближний Восток и Северная Африка (БВСА): как и в других регионах мира, в период пандемии в странах БВСА наблюдалось ускорение темпов цифровизации, поскольку правительства, предприятия и граждане массово переходили на работу в режиме онлайн. Финансовое мошенничество в Интернете, в том числе фишинг, мошенничество с использованием чужих личных данных, а также онлайн-мошенничество, относятся к категории высоких угроз. Регион БВСА также уязвим для ОД, поскольку страны-члены ССАГПЗ, в частности, служат важными транспортными узлами для мировой торговли и финансовой деятельности.

10. Цифровизация и развитие новых технологий являются ключевыми факторами, определяющими рост КМ. Цифровые услуги стали неотъемлемой частью повседневной жизни и государственных функций. В результате все больше граждан (включая уязвимые группы) участвуют в онлайн-деятельности. В то же время цифровизация означает, что юрисдикции становятся все более взаимосвязанными, а информация и средства быстро распространяются через границы. Эти два фактора принципиально изменили криминальный расклад и создали условия для роста угроз КМ.

11. Пандемия COVID-19 ускорила переход от очных финансовых операций к открытию счетов, платежам и кредитованию через Интернет. Значительно возросло число мошеннических действий, таких как телефонное мошенничество и мошенничество по электронной почте; банковское мошенничество, мошенничество с пожилыми людьми и мошенничество в сфере здравоохранения (например, связанное со средствами индивидуальной защиты и другими медицинскими товарами), а также мошенничество с инвестициями через Интернет благодаря использованию смартфонов, электронной почты и социальных сетей.

Такие изменения в финансовом поведении отразились и на схемах ОД, включая более широкое использование цифровых банковских и платежных платформ и дистанционных операций (см. также раздел «Влияние цифровизации и новых технологий на ОД» на стр. 27)[5].

12. Все более широкое использование смартфонов, технологий (с постоянно развивающимися новыми инструментами и приложениями), а также дистанционные финансовые операции значительно повышают уязвимость пользователей. В сочетании с технологиями, обеспечивающими анонимность, такими как виртуальные частные сети (VPN) и «луковые маршрутизаторы»[6] , это позволяет преступникам скрывать свою противоправную деятельность от посторонних глаз. С помощью технологий преступники могут увеличить масштаб, размах и скорость своей преступной деятельности. Кроме того, наблюдается переход преступников на модель «преступление как услуга»[7], что также значительно уменьшает препятствия для синдикатов КМ, а также способствует расширению специализации по различным направлениям КМ, распределенным между различными подгруппами (см. раздел 2.2 ниже)[8].

13. Во многих случаях организованные преступные группы расширяют или адаптируют свою деятельность для включения в нее КМ, используя существующие методы отмывания других незаконно полученных средств.

Вставка 2. Распространенная преступная сеть ОД, используемая для совершения КМ и других преступлений

Сеть ОД осуществляет операции по организации азартных игр в Интернете и КМ в здании принадлежащей ей компании в особой экономической зоне (ОЭЗ) страны А. В этом комплексе расположено около десяти компаний, которые сами занимаются игорным бизнесом и КМ или сдают помещения в аренду другим лицам. Сеть включает в себя якобы легальные предприятия в приграничных районах соседней страны Б. Во главе сети стоят граждане страны Б, которые используют банковские счета в валюте страны Б для перемещения денег из ОЭЗ в страну С, где находятся основные инвесторы компании. Доллары США из ОЭЗ отмываются через обменные пункты в стране В, где деньги конвертируются в валюту страны В и затем переправляются в страну С. На границе страны С деньги переводятся инвесторам компании.

Источник: Транснациональная организованная преступность, казино и отмывание денег в Юго-Восточной Азии: Анализ угроз (УНП ООН, 2022 г.)

---

[5] См. отчеты ФАТФ (май 2020 г.) «Риски отмывания доходов и финансирования терроризма, связанные с COVID-19, и меры политического реагирования« и (декабрь 2020 г.) «Обновление: риски отмывания доходов и финансирования терроризма, связанные с COVID-19».

[6] Также известное как TOR, программное обеспечение с открытым исходным кодом, позволяющее пользователям анонимно выходить в Интернет.

[7] Именно здесь происходит разделение труда, когда преступные группы развивают и предлагают другим нишевые криминальные возможности, навыки и опыт.

[8] См. Европол (июль 2023 г.) «Оценка угрозы организованной преступности в Интернете (IOCTA) 2023»; и Интерпол (2022 г.) «Финансовые и киберпреступления вызывают наибольшую обеспокоенность мировой полиции, говорится в новом докладе Интерпола».

2.2.Криминологическая характеристика КМ

Элементы кибермошенничества

14. Исходя из опыта юрисдикций, преступники, занимающиеся КМ, могут использовать один или несколько из перечисленных ниже элементов, чтобы успешно обмануть жертву и заставить ее совершить мошеннический перевод. Различные варианты КМ могут по-разному сочетать перечисленные выше элементы.
    - Добыча информации (например, с помощью фишинга);
    - Социальный обман или инжиниринг, а также использование эмоциональной уязвимости (например, выдача себя за другое лицо или организацию и использование этого в качестве предпосылки для создания срочности, страха или доверия; или выдвижение ложных требований для легкого заработка денег);
    - Онлайн-средства или платформы (которые могут использоваться либо для общения, либо для совершения жертвами сделок в случаях мошенничества в сфере онлайн-торговли).
15. Жертва может не поддаться на один вид КМ; в конечном итоге цель состоит в том, чтобы побудить ее к переводу средств, и для достижения этой цели преступники используют различные методы. Преступники подходят к делу творчески и могут использовать или переходить к другим типам КМ, если первоначальный обман начинает давать сбой. Например, жертва фишинга или мошенничества с использованием социальных сетей может быть убеждена и направлена тем же преступником в схему инвестиционного мошенничества, используя «доверие», уже созданное в ходе первоначальной мошеннической схемы.

Вставка 3. Одни и те же жертвы, несколько преступлений

«Свинобойня» – это комбинация любовной аферы и инвестиционного мошенничества. При таком способе преступники устанавливают доверительные отношения с жертвой и убеждают ее вложить сбережения в мошеннические криптовалютные торговые платформы. Мошенничество совершается в течение длительного времени, что приводит к потере крупных сумм денег.

После раскрытия мошенничества преступники часто связываются со своими жертвами, представляясь юристами или представителями правоохранительных органов, и предлагают помощь в возврате средств за вознаграждение.

Источник: Европол (2023), Оценка угрозы организованной преступности в Интернете (IOCTA) 2023 г.

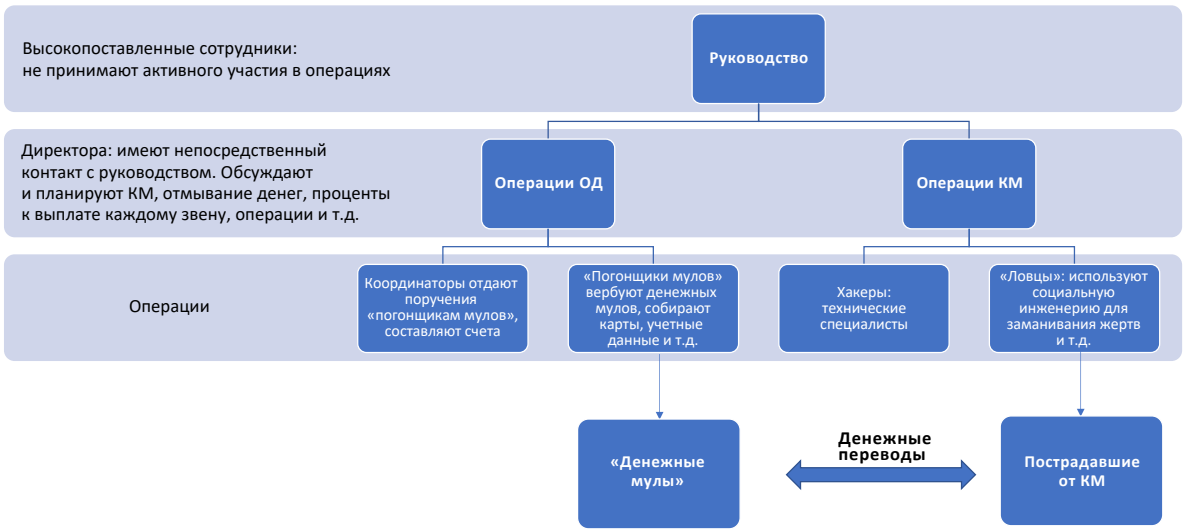
Структура организованной преступности

16. КМ и сопутствующее ОД зачастую осуществляются транснациональными организованными преступными группами или синдикатами. Хотя их структура может быть различной, синдикаты КМ нередко действуют как иерархические организации (см. пример на рис. 1). Они также могут быть слабо организованными, что позволяет им сохранять гибкость, а их члены могут вступать и выходить по мере необходимости. Такие синдикаты также могут быть организованы

вокруг отдельных подгрупп, специализирующихся на криминальной экспертизе (например, в соответствии с приведенными выше элементами КМ (поиск информации, социальный обман; или другая техническая экспертиза, например создание онлайн-платформы или ОД). Во многих случаях такие синдикаты КМ децентрализованы и никогда не общаются лично (например, по зашифрованным каналам в Интернете), что затрудняет расследование их деятельности.

17. Кроме того, в состав синдикатов КМ зачастую входят хорошо образованные и технически грамотные профессионалы. Это привело к тому, что подход к КМ и отмыванию незаконных доходов становится все более изощренным. Юрисдикции отметили, что синдикаты КМ могут намеренно вербовать лиц, работающих в профессиональных секторах (включая финансовые учреждения), которые могут быть использованы в качестве источников данных и информации для успешного осуществления КМ и упрощения ОД. Более подробная информация о структурировании и функционировании синдикатов КМ для целей ОД приведена далее в разделе 2.3.

Рисунок 1. Пример криминальной структуры КМ



Связи с иными видами преступной деятельности

18. Помимо ОД, синдикаты КМ могут быть связаны с другими видами преступной деятельности. К числу общеуголовных преступлений относится деятельность, связанная или необходимая для осуществления КМ, в том числе киберпреступная деятельность, такая как взлом с целью получения персональной информации, разработка и продажа криминального программного обеспечения; подделка документов и т.д. Часть преступных доходов синдикаты КМ могут пускать на приобретение нового оборудования и разработку еще более совершенных технологических средств.

Вставка 4. Операция «Сокол»

В 2020 г. в г. Лагосе (Нигерия) в результате совместного расследования киберпреступлений, проведенного Интерполом (INTERPOL-Group-IB) и полицией Нигерии, были арестованы трое подозреваемых. Предполагается, что граждане Нигерии являлись членами организованной преступной группы, ответственной за распространение вредоносных программ, проведение фишинговых кампаний и масштабных афер с компрометацией деловой электронной почты. Предположительно, подозреваемые разрабатывали фишинговые ссылки, домены и кампании массовой рассылки, в которых они выдавали себя за представителей организаций. Затем они использовали эти кампании для распространения 26 вредоносных программ, шпионского ПО и средств удаленного доступа.

Данные программы использовались для проникновения в системы организаций и частных лиц-жертв и их мониторинга, а затем запускали мошеннические схемы и выкачивали средства. По данным Group-IB, с 2017 г. эта преступная группа, предположительно, взломала системы государственных и частных компаний в более чем 150 странах. Group-IB также удалось установить, что банда разделена на подгруппы, а несколько человек до сих пор находятся на свободе.

Параллельные расследования по делу ОД показали, что подозреваемые также использовали счета иностранных банков и виртуальных активов в Великобритании, США и Таиланде для получения платежей от жертв. Трем подозреваемым были предъявлены обвинения в их противоправной деятельности, в том числе в мошенничестве и отмывании денег. Автомобиль класса люкс был конфискован, а счета подозреваемых заморожены и находятся на стадии судебного взыскания.

Источник: Нигерия

19. Растет также связь между КМ и торговлей людьми, когда жертв через поддельные объявления о работе заманивают в онлайновые колл-центры и заставляют совершать КМ в крупных масштабах. Это позволяет синдикатам КМ увеличить географическое разнообразие онлайн-жертв, на которых они могут нацелиться (поскольку жертвы торговли людьми могут эксплуатироваться в связи с их знанием языков и культурной осведомленностью). Кроме того, это позволяет усилить изощренность центров КМ за счет торговли квалифицированными специалистами, такими как работники информационных технологий или «руководители цифровых продаж»[9]. Иногда такие колл-центры намеренно действуют в пределах часовых поясов предполагаемых жертв, а для временных преступных операций используют арендованную недвижимость, что позволяет им быстро передислоцироваться и менять IP-адреса, чтобы избежать обнаружения правоохранительными органами[10].

[9] См. Интерпол (июнь 2023 г.) «Интерпол выпускает международное предупреждение о мошенничестве, вызванном торговлей людьми».

[10] См. Интерпол (июль 2023 г.) «Оперативный анализ онлайн-мошенничества и торговли людьми в Юго-Восточной Азии / Обновление 2 - От региональной к глобальной угрозе»; доступен только для национальных правоохранительных органов.

Вставка 5. Операция «Штормовики»

В рамках операции «Штормовики» были проведены правоохранительные мероприятия в отношении организованных преступных групп, которые, как предполагается, способствовали перемещению мужчин, женщин и детей из Азии через границу с целью эксплуатации и/или получения прибыли. В результате операции был произведен 121 арест в 25 странах, что привело к 193 новым расследованиям.

В ходе операции «Штормовики» полиция Малайзии и Камбоджи тесно сотрудничала по делу о 15 мужчинах и одной женщине, которых заманили в Камбоджу, пообещав выгодную зарплату за работу в колл-центре. Однако по прибытии их заперли и заставили работать по 14 часов в сутки в качестве мошенников.

Примечание: более подробно см. Интерпол (май 2022 г.) 121 арест в рамках операции по борьбе с незаконным ввозом мигрантов и торговлей людьми.

Источник: Интерпол

20. В большинстве юрисдикций не было обнаружено существенных доказательств того, что деятельность по финансированию терроризма связана с КМ. Однако в ряде случаев наблюдались случаи, когда элементы террористической деятельности и финансирования были связаны с преступными субъектами КМ. Например, сообщения о подозрительных сделках (СПО), полученные из одной юрисдикции, свидетельствуют о том, что доходы от КМ в некоторых случаях переводились в конкретные конфликтные зоны/юрисдикции, известные своей деятельностью, связанной с терроризмом.

21. Кроме того, существует связь с ФРОМУ, причем киберпреступность, как сообщается, является одним из основных источников незаконных доходов Корейской Народно-Демократической Республики (КНДР). Незаконная кибердеятельность включает в себя продажу собранной личной информации или предоставление инструментов и услуг для взлома и фишинга, которые могут быть использованы другими преступниками для совершения КМ[11].

Вставка 6. Использование КНДР фишинговых инструментов для КМ с целью финансирования программ вооружений

Согласно информации, предоставленной Группе экспертов ООН, работники информационных технологий (ИТ) Корейской Народно-Демократической Республики, связанные с Департаментом промышленности боеприпасов, зарабатывали иностранную валюту, продавая хакерские приложения для голосового фишинга и эксплуатируя многочисленные зарубежные серверы и адреса Интернет-протокола.

[11] См. также Совет Безопасности ООН (март 2023 г.) S/2023/171 Письмо Группы экспертов, учрежденной резолюцией 1874 (2009), от 3 марта 2023 г. на имя Председателя Совета Безопасности.

В июле 2020 г. четыре гражданина Республики Корея (РК) были арестованы властями Китая и экстрадированы в РК. Один из них дал показания о том, что преступные группы приобрели у ИТ-работника из КНДР персональные данные граждан РК, а также хакерские приложения для голосового фишинга.

Преступные группы обманом заставляли жертв загружать эти разработанные инструменты, чтобы похитить у них дополнительную информацию. В дальнейшем они выдавали себя за сотрудников финансовых учреждений, чтобы обманом заставить жертв перевести деньги.

Примечание: более подробную информацию см. в документе Совета Безопасности ООН (сентябрь 2022 г.) S/2022/668 Письмо Группы экспертов, учрежденной резолюцией 1874 (2009), от 2 сентября 2022 г. на имя Председателя Совета Безопасности.

Источник: Группа экспертов Организации Объединенных Наций и Южная Корея

2.3. Техники и типологии ОД

Структура сетей ОД

22. При отмывании доходов, полученных от различных видов КМ, преступники должны действовать быстро и эффективно. Юрисдикции отмечают участие профессиональных групп ОД, а также сторонних профессиональных посредников, включая юристов, бухгалтеров, налоговых консультантов, секретарей компаний и банкиров. Профессиональные группы ОД могут быть частью преступного синдиката КМ или отдельной децентрализованной организацией, предоставляющей услуги ОД по модели «преступление как услуга» (профессиональные сети ОД).

Вставка 7. Сеть QQAAZZ

Сеть QQAAZZ рекламировала свои услуги как «глобальный сервис по переводу банков в соучастники» на русскоязычных киберпреступных форумах, на которых собираются киберпреступники с целью предложить или получить специализированные навыки или услуги, необходимые для участия в различных видах киберпреступной деятельности. Сеть QQAAZZ открыла и поддерживала сотни подставных компаний и личных банковских счетов в финансовых учреждениях по всему миру, на которые поступали средства от киберпреступников, связанных с КМ. Далее эти средства переводились на другие банковские счета, контролируемые QQAAZZ, а иногда конвертировались в криптовалюту с помощью сервисов «перелива» (tumbling), призванных скрыть первоначальный источник средств. Получив комиссию в размере до 50%, QQAAZZ возвращала остаток похищенных средств своим криминальным клиентам.

В ноябре 2020 г. в результате международной операции правоохранительных органов 16 стран были арестованы 20 человек, подозреваемых в принадлежности к преступной сети QQAAZZ, пытавшейся отмыть десятки миллионов евро от имени крупнейших киберпреступников мира. В Латвии, Болгарии, Великобритании, Испании и Италии было проведено около 40 обысков в домах арестованных, а в США, Португалии, Великобритании и Испании были возбуждены уголовные дела.

Источник: Португалия и Европол

23. Как правило, доходы от КМ быстро отмываются через сеть счетов. Примеры из практики показывают, что эти сети могут быть сложными, охватывая множество стран и финансовых учреждений, хотя это может зависеть от уровня сложности преступной группы[12].

24. Сети счетов ОД, связанные с КМ, обычно включают как физических, так и юридических лиц.

    - **Индивидуальные денежные мулы** часто вербуются преступниками различными способами, в том числе через предложения о работе и рекламу, а также через социальные сети. Вербовщиков денежных мулов также называют «погонщиками мулов». Денежные мулы могут сознательно участвовать в отмывании средств или работать неосознанно (путем обмана) или по неосторожности, а также получать поощрения или вознаграждения за работу с незаконными средствами. Сложно выявить контролера мула (т.е. погонщика мула), который нанимает как добровольных, так и невольных участников, или определить происхождение мошеннических средств. В некоторых юрисдикциях были отмечены случаи вербовки иностранных граждан, не имеющих очевидной связи с юрисдикцией, которым поручалось открыть счета мулов либо с помощью физической поездки, либо через открытие виртуального счета.

Вставка 8. Поиск мулов: предложение работы

Г-жа PC - владелица магазина сари-сари, которая была завербована неким г-ном O на, как ей казалось, законное предложение работы. Г-н O – гражданин Нигерии, который был арестован в 2019 г. за якобы имевшую место многомиллионную аферу с любовными онлайн-романами, в результате которой было потеряно более 8 млн. филиппинских песо (около 129 000 евро).

Г-н O обещал г-же PC часть денег за каждую проведенную ею банковскую операцию. Всего за полгода г-жа PC провела 83 операции на сумму 3,6 млн. филиппинских песо (около 58 000 евро). Все операции были наличными (т.е. внесение наличных и снятие денег через банкомат и через кассу). В итоге г-н O был арестован при содействии г-жи PC в ходе проведения оперативно-розыскного мероприятия.

Источник: Филиппины

    - **Фиктивные компании** находятся под контролем преступников, связанных с КМ, как правило, через посредников или номинальных директоров. Нанятым индивидуальным денежным мулам также может быть поручено выступить в роли таких «подставных лиц» и открыть корпоративные счета для дальнейшего сокрытия преступной собственности. В некоторых юрисдикциях отмечалось, что подставные компании использовали виртуальные бизнес-адреса[13] для дальнейшей маскировки своей преступной деятельности. В случаях мошенничества в сфере интернет-торговли преступники также могут использовать такие фиктивные компании для открытия виртуальных счетов в торговых компаниях для обработки платежей и переводов от жертв.

[12] Более подробную информацию об использовании мулов в профессиональных организациях и сетях, занимающихся отмыванием денег, см. в отчете ФАТФ (июль 2018 г.) «Профессиональное отмывание денежных средств».

[13] Виртуальные бизнес-адреса – это реальные физические адреса, предлагаемые некоторыми провайдерами услуг, которые позволяют предприятиям получать почтовую корреспонденцию и посылки.

Вставка 9. Подставные компании в мошенничестве с использованием торговых онлайн-платформ

В ПФР Турции поступил ряд СПО, касающихся схемы мошенничества с использованием торговых онлайн-платформ, когда жертвам предлагалось сделать валютные инвестиции по телефону или через социальные сети. В основе этой схемы лежала сеть из 209 компаний, которые отмывали доходы между собой. Компании имели общих бухгалтеров, создавались в основном в одну и ту же дату и ликвидировались через короткий промежуток времени.

Анализ, проведенный ПФР Турции, показал, что подставные компании также действовали в трех различных подгруппах, в зависимости от перевода средств и связанных с ними сторонних соучастников. Было установлено, что мошенническим путем было получено и отмыто в общей сложности около 10 млрд. турецких лир (около 336,7 млн. евро).

- 135 компаний получили через платежные компании 9,6 млрд. турецких лир (около 323,2 млн. евро) выручки от мошенничества. Чтобы упростить получение транзакций от жертв, эти компании открыли виртуальные счета в точках продаж. 100 млн. турецких лир (около 3,4 млн. евро) были сняты наличными, а около 6 млрд. турецких лир (около 202 млн. евро) были переведены в золотодобывающую компанию.
- 59 компаний получили 700 млн. турецких лир (около 23,6 млн. евро) выручки от мошенничества. 200 млн. турецких лир (около 6,7 млн. евро) было выведено наличными, а остальные средства были переведены ПУВА после отмывания через счета, принадлежащие сторонним индивидуальным соучастникам.
- 23 компании получили 875 млн. турецких лир (около 29,5 млн. евро) выручки от мошенничества. 220 млн. турецких лир (около 7,4 млн. евро) было выведено наличными, а остальные средства были переведены ПУВА после отмывания через счета, принадлежащие сторонним индивидуальным соучастникам.

Источник: Турция

- **Легальные компании,** подобно индивидуальным «денежным мулам», также могут обманным путем привлекаться к получению доходов от КМ (например, в качестве инвестиций или деловой перспективы), после чего их просят либо перенаправить средства, либо вернуть их на отдельный счет, контролируемый преступниками. В некоторых случаях легальные компании охотно соглашались на такие «деловые возможности», особенно в период экономического кризиса. Привлечение легальных компаний служит дополнительным прикрытием, позволяющим скрыть незаконную деятельность.

25. Существует сходство в подходах к поиску денежных мулов в сетях ОД, связанных с КМ и другими видами преступлений. Однако юрисдикции отмечают некоторые различия, которые в большей степени могут относиться к мулам, связанным с КМ.

- **Способ вербовки:** денежные мулы КМ чаще всего вербуются через Интернет, в том числе через объявления о работе от подставных компаний или через спам-рассылку. Преступники также могут использовать экономические условия и маскировать это под законную возможность получить «легкие деньги». Жертв КМ (например, в результате любовного мошенничества) часто обманом заставляют выступать в роли денежных мулов. В некоторых случаях для открытия таких счетов используются и жертвы торговли людьми (например, нелегальные мигранты или рабочие).
- **Использование счетов:** денежные мулы, связанные с КМ, имеют счета в финансовых учреждениях, поскольку мошеннические средства можно быстро получить и отправить с помощью электронных методов платежей, в отличие от физических переводов или вкладов наличных денег. Вероятно, это связано со способом обмана жертв (т.е. с переводом средств). Учитывая преимущества цифровых банковских услуг при перемещении средств, лица, ставшие целью создания «мулов» КМ, скорее всего, обладают определенными базовыми знаниями или навыками работы с ПК и другими технологиями.

Вставка 10. Жертва любовного мошенничества превратилась в мула

В период с апреля по май 2022 г. пожилая женщина, первоначально открывшая свой банковский счет для зачисления пенсии, получила два платежа на большую сумму. Один из переводов был сделан со счета в национальном банке, а второй - от жертвы из-за рубежа.

Последующее расследование, проведенное властями Словакии, показало, что женщина общалась с неким человеком через социальные сети и стала жертвой любовного мошенничества. Пожилая женщина предоставила мошеннику свои учетные данные для интернет-банкинга, после чего ее банковский счет был использован для отмывания других преступных доходов. Часть полученных денег была обменена на криптовалюту через зарубежную платформу ПУВА.

Источник: Словакия

Техники и типологии ОД

26. Место, где происходит КМ (т.е. где находится жертва), зачастую отличается от места, где происходит отмывание доходов от КМ, а сети денежных мулов могут охватывать несколько юрисдикций. Синдикаты КМ понимают, что финансовые учреждения или компетентные органы могут установить счета для мошеннической деятельности еще до начала отмывания, что может привести к перехвату их преступных доходов до того, как они попадут на счета преступников. Чтобы повысить эффективность своей деятельности, преступники могут проводить «тесты», осуществляя операции на небольшие суммы, что позволяет им в случае неудачи изменить маршрут следования средств.
27. Тип счета первого уровня, на который поступают средства от КМ, как правило, зависит от вида КМ в целях сохранения видимости легитимности. Изменения с течением времени наблюдаются и в типе счета первого уровня.

Например, в случаях мошенничества с компрометацией деловой электронной почты (BEC) синдикаты КМ перешли от использования счетов физических лиц к использованию счетов корпораций, чтобы снизить риск обнаружения.

Таблица 1. Взаимосвязь между видом КМ и счетом первого уровня

Вид КМ	Тип счета первого уровня
Компрометация деловой электронной почты	Корпоративный (например, подставные или вновь зарегистрированные компании)
Фишинг	Индивидуальные денежные мулы
Мошенничество с использованием телекоммуникаций в социальных сетях	Индивидуальные денежные мулы
Мошенничество с использованием онлайн-трейдинга/ торговых платформ	Корпоративный (например, подставные или вновь зарегистрированные компании)
Любовное мошенничество	Индивидуальные денежные мулы
Мошенничество с трудоустройством	Индивидуальные денежные мулы

Примечание: в данной таблице предпринята попытка выделить некоторые общие тенденции, основанные на опыте юрисдикций по типам счетов первого уровня, встречающихся для того или иного типа КМ. Тем не менее, это может относиться не ко всем случаям.

28. После того как синдикат КМ открыл счет, приобретенные мошенническим путем средства быстро поступают в сеть ОД. После этого средства быстро распределяются по ряду «сквозных» операций через внутренние или зарубежные счета, которые контролируются самими мулами или синдикатом КМ. В последнем случае «мулы» сдают банковские реквизиты, карты и жетоны или предоставляют синдикату КМ доверенность, позволяющую напрямую контролировать счета. Вовлечение в процесс профессиональных посредников, например, при оформлении доверенности, придает операциям видимость законности и способствует сокрытию преступления.

29. В целях дальнейшего избежания обнаружения и сохранения анонимности синдикаты КМ используют различные методы и механизмы: например, смурфинг (структурирование или дробление крупной финансовой операции – *прим. пер.*); использование счетов различных провайдеров финансовых, денежных или платежных услуг; конвертация в другие виды финансовых активов (например, электронные деньги (ЭД)[14], предоплаченные карты, ВА). Это может увеличить время, необходимое ПФР и правоохранительным органам для получения доступа к требуемым финансовым данным через границы, сектора и учреждения, чтобы отследить, обеспечить безопасность и, наконец, вернуть незаконные доходы. Некоторые денежные мулы могут также разрешать использовать свои счета только в течение определенного и ограниченного периода времени. Ограниченный период времени, а также законные процедуры открытия счета затрудняют выявление аномальной деятельности.

[14] Электронные деньги – это цифровое представление фиатной валюты, используемое для электронного перевода стоимости, выраженной в фиатной валюте. Электронные деньги – это механизм цифрового перевода фиатной валюты, т.е. электронный перевод стоимости, имеющей статус законного платежного средства; ФАТФ (июнь 2014 г.) Виртуальные валюты: основные определения и потенциальные риски в сфере ПОД/ФТ.

Вставка 11. Подставные компании, банковские счета и виртуальные активы

В полицию Индии поступили многочисленные жалобы на то, что мобильное приложение использовалось для обмана людей под видом инвестиционной платформы для получения криптовалюты. Приложение обещало долю в прибыли, полученной от таких инвестиций. Компания заманивала жертв инвестировать в схему больше, после чего вывод средств/платежи прекращались. Веб-сайт и приложение стали недоступны, а операторы приложения перестали отвечать инвесторам. Несколько местных органов власти, проводящих расследования по жалобам клиентов в разных частях страны, запросили у ПФР Индии информацию по этому делу. Анализ, проведенный индийским ПФР, выявил две организации, управляющие приложением в Google Play Store, которые впоследствии были удалены из магазина приложений. Было установлено, что еще 34 организации связаны с этими двумя организациями. В 28 из 36 организаций директорами были иностранные граждане. Индийский Директорат по исполнению наказаний (ED) также инициировал параллельное расследование, которое выявило масштабный преступный сговор и вовлеченность нескольких подставных организаций в эксплуатацию аналогичных мошеннических приложений/сайтов для обмана доверчивых людей и извлечения доходов от преступлений. При физической проверке эти организации не удалось обнаружить по зарегистрированному адресу. Проследив финансовый след, выяснилось, что некоторые из этих организаций также участвовали в работе нелегальных приложений для ставок и займов, а также обманывали население под видом этих приложений. Незаконные деньги, собранные с жертв, переводились на счета различных подставных лиц, а часть преступных доходов в итоге конвертировалась в виртуальные активы. Доходы от преступлений в виде остатков на банковских счетах различных подставных лиц на сумму 865 млн индийских рупий (9,9 млн евро) были обнаружены и заморожены.

Источник: Индия

30. Кроме того, юрисдикции сообщали об использовании других видов технологий ОД, призванных запутать связь между различными криминальными группами КМ и ОД.

- **Наличные деньги:** во многих примерах, приведенных в данном отчете, говорится о выводе наличных денег мулами и синдикатами КМ. Движение наличных денег за пределами финансовых учреждений бывает трудно отследить. Наличные деньги могут сниматься через банкоматы после отмывания через сеть ОД, что позволяет преступникам избежать личного контакта с финансовыми учреждениями. Такие средства могут быть доставлены через границу курьерами наличных и помещены на депозит для дальнейшего отмывания. Преступные доходы могут также использоваться для приобретения ценностей и инструментов, которые впоследствии могут быть перепроданы за наличные, например, предоплаченных карт или драгоценных металлов.

Вставка 12. Снятие наличных и покупка золота и топливных карт

В марте 2023 г. бухгалтер одной из китайских компаний стал жертвой мошенничества через выдачу себя за представителей банка. Его добавили в группу в приложении для обмена сообщениями под предлогом необходимости проведения ежегодной проверки счета компании.

В дальнейшем преступники, входящие в группу обмена сообщениями, выдавали себя за законных представителей и акционеров компании и просили потерпевшего перевести 7,8 млн. юаней (около 996 000 евро) на два специально выделенных корпоративных счета, находящихся под контролем преступной группы. Полицейское расследование показало, что средства были переведены на 26 вторичных банковских счетов, а затем сняты наличными через банковские кассы или через банкомат, переведены на сторонние платежные платформы, а также использованы для покупки золота и топливных карт.

Источник: Китай

- **ОД через торговлю/услуги:** существуют различные методы ОД через торговлю/услуги, которые преступники могут использовать для трансграничного перемещения преступных доходов[15]. Применительно к доходам от КМ некоторые юрисдикции отмечают, что преступники используют такие методы отмывания денег через торговые операции (TBML), как фиктивное или поддельное выставление счетов, а также покупают за счет незаконных доходов дорогостоящие или легко реализуемые товары (например, запчасти для автомобилей, билеты, предметы домашнего обихода и т.д.). Например, в некоторых юрисдикциях сообщалось о мошеннических электронных переводах на счета законных компаний, начиная от известных брендов предметов роскоши или электроники и заканчивая небольшими местными предприятиями, для приобретения товаров. Эти товары могут быть перемещены через границу и конвертированы обратно в наличные деньги для дальнейшего распыления и интеграции. Коммерческие предприятия, не подпадающие под требования режима ПОД/ФТ, могут не обладать достаточной осведомленностью или знаниями для проведения проверки личности или мониторинга транзакций, чем и пользуются злоумышленники. Предоставление завышенных цен или фиктивных счетов на оплату ИТ-услуг или консультационных услуг также может быть частью применяемых методов ОД.

[15] См. также ФАТФ/Группа «Эгмонт» (декабрь 2020 г.) Отмывание денег в рамках торговых операции: тенденции и изменения; и ФАТФ (июль 2018 г.) Профессиональное отмывание денежных средств.

Вставка 13. КМ, мулы и TBML

Ирландские власти арестовали ключевое лицо, г-на МС, в схеме отмывания доходов от любовного мошенничества и BEC из Ирландии в Нигерию через TBML. Расследование продолжается. На данный момент власти полагают, что в схеме отмывания задействовано не менее 60 имен и 64 банковских счета.

В этой схеме доходы от мошенничества сначала переводятся на банковские счета ирландских мулов. Затем средства обналичиваются и переводятся на ирландские счета, непосредственно связанные с г-ном МС или принадлежащие ему. Многие из счетов, связанных с г-ном МС, были открыты на подставных лиц.

Нигерийская компания (контролируемая нигерийцем, предположительно находящимся в США) заказывает товары у легальных европейских или китайских компаний. Эти легальные компании занимались товарами, которые можно купить и отправить для перепродажи, включая алкоголь, одежду, электронику и фармацевтические препараты. Ирландские счета г-на МС производили оплату по соответствующим счетам-фактурам, а товары в конечном итоге отгружались компании-соучастнику в Нигерии.

В одном из случаев немецкая фармацевтическая компания получила средства в размере более 1,7 млн. евро для оплаты товаров, приобретенных нигерийской компанией. Эти средства были напрямую отслежены как доходы от любовного мошенничества и BEC по всей Европе и США и поступили с различных счетов, либо связанных с г-ном МС, либо принадлежащих ему, либо непосредственно от жертв. В итоге эти товары были отправлены в Нигерию.

Источник: Ирландия

- **Нелицензированные или незарегистрированные операторы денежных переводов и ПУВА:** преступные доходы могут переводиться за пределы юрисдикции с использованием подпольных денежных переводов или услуг «хавала», не имеющих достаточного контроля в области ПОД/ФТ. Если в преступлении участвуют ВА, синдикаты могут использовать ПУВА, расположенные в юрисдикциях с отсутствующим или слабым контролем ПОД/ФТ.
- **Методы повышения анонимности ВА[16]:** использование нехостинговых кошельков, одноранговых транзакций, пиринговых цепочек и высокорисковых бирж является предпочтительным способом быстрого отмывания ВА, связанных с КМ, за пределами юрисдикции, и часто используется в комбинации. Кроме того, преступники все чаще используют биткойн-банкоматы для перевода ценностей и сокрытия личности тех, кто контролирует средства, включая предоставление поддельных или измененных идентификационных документов, например различных идентификаторов, номеров телефонов или дат рождения при вводе или выводе средств. Они также применяют методы обфускации, включая использование микшеров или тумблеров, а также ВА с усиленной анонимностью (так называемые приватные коины, например, Monero) и сервисы децентрализованного финансирования (DeFi).

[16] Данные методы подробно рассматриваются в отчете ФАТФ (март 2023 г.) «Противодействие использованию программ-вымогателей».

Вставка 14. Комплексное ОД в нескольких секторах

Синдикат иностранных мошенников, занимавшихся любовными аферами, выбрал около 70 японских жертв. Средства в размере 3 млн. долл. США были переведены на различные банковские счета денежных мулов в Японии. Японец, выступавший в роли местного погонщика мулов, отмывал эти средства в Гане, где базировался мошеннический синдикат. Японец был арестован при содействии Ганы через Интерпол.

Средства со счетов мулов впоследствии переводились на счет японского погонщика мулов. Анализ СПО показал, что средства отмывались им по трем каналам:

- Банковские переводы осуществлялись на банковский счет, принадлежащий японскому погонщику мулов в Гане. Затем эти средства физически снимались наличными в Гане и передавались лидеру синдиката, который до сих пор находится на свободе. При осуществлении электронных переводов японец предоставлял в свой японский банк фиктивные счета-фактуры, выставляя их за законную предпринимательскую деятельность (закупку какао-бобов).
- Часть средств была обменена на ВА через ПУВА в Японии.
- Средства также были переведены в Гану через подпольный банк, связанный с ганской общиной в Японии.

Источник: Япония

Влияние цифровизации и новых технологий на ОД

31. Новые технологии предоставили потребителям новые преимущества и возможности. Происходит глубокий переход к цифровизации финансовых услуг, который ускорился в период пандемии COVID-19. Сокращение использования наличных денег и рост онлайн-активности привели к появлению новых инновационных инструментов и процессов. Цепочка финансовых платежей также становится все более динамичной и фрагментированной, увеличивается разнообразие провайдеров, предлагающих платежные и транзакционные услуги (см. также раздел 3.1 ниже).

32. Вместе с тем развитие технологий может стать преимуществом для преступных группировок, которые используют эти возможности для существенного усовершенствования своих методов ОД. Финансовые транзакции все чаще осуществляются практически мгновенно, что отчасти обусловлено ожиданиями потребителей в отношении возможности беспрепятственного проведения операций. Как уже отмечалось ранее, в сочетании с цифровыми методами анонимизации, такими как VPN, это затрудняет для властей идентификацию конечных преступников, осуществляющих эти ОД-транзакции в быстрой последовательности.

33. Цифровизация повысила простоту и скорость создания счетов для ОД и расширила трансграничный охват синдикатов КМ. Некоторые юрисдикции отметили увеличение количества удаленных виртуальных процессов в двух областях: открытие счетов и создание компаний. Такие удаленные виртуальные процессы исключают необходимость физического перемещения. Преступники могут использовать эти возможности для ОД.

Вставка 15. Масштабирование за счет цифровизации

Анализ ПФР выявил разветвленную сеть, состоящую из 147 физических лиц и 276 банковских счетов в восьми банках. Данные лица передали свои национальные цифровые идентификаторы, предназначенные для идентификации пользователей на государственных и иных интернет-площадках, преступным синдикатам. Затем синдикаты использовали цифровые идентификаторы для удаленного открытия банковских счетов и осуществляли прямой контроль над этими счетами-мулами для отмывания доходов от КМ. ПФР обнаружило эту сеть, выявив общие черты, такие как общие банковские операции, точки данных (контактная информация иностранца и идентификатор устройства), а также контактные данные (почтовый адрес, электронная почта, телефон).

Полученная разведывательная информация была передана в Команду по борьбе с мошенничеством (Anti-Scam Command, ASCom) – специальное подразделение полиции Сингапура, занимающееся борьбой с КМ и связанными с ним видами ОД. В результате проведенного ASCom расследования были арестованы 6 человек, 3 человека привлечены к ответственности за участие в преступной схеме.

Источник: Сингапур

34. Преступники могут быстро расширить (часто транснациональную) сеть денежных мулов, используя цифровые инструменты для трансграничной вербовки мулов. Социальные сети и приложения для IP-телефонии (VoIP) также были признаны предпочтительными средствами вербовки мулов. Традиционно при отмывании через сети мулов возникали определенные трудности, поскольку им требовалось время на получение и выполнение инструкций, поступавших от других преступных синдикатов. Благодаря использованию синдикатами КМ платформ мгновенного обмена сообщениями такие временные задержки значительно сократились.

35. Преступники все чаще похищают личные данные с помощью различных методов и технологических средств, включая фишинг, покупку или обман, заставляющий человека добровольно передать свои данные. Иногда для создания учетных записей преступники используют фальсифицированные и синтетические идентификационные данные, в которых сочетаются настоящая и поддельная информация. Далее преступники непосредственно создают и контролируют учетные записи, используя эти украденные или фальсифицированные идентификационные данные. Это усложняет отслеживание деятельности ОД, поскольку владельцы счетов могут даже не подозревать о своей причастности к ней.

36. Одна из делегаций отметила риск потенциального использования дипфейков (от англ. deepfake) для мошенничества с захватом аккаунтов. С помощью алгоритмов машинного обучения мошенник может создать дипфейк чьего-либо голоса или видео, который затем может быть использован для выдачи себя за этого человека по телефону или в системах биометрической аутентификации. Кроме того, дипфейки могут использоваться в сочетании с методами социальной инженерии для обмана жертв, заставляя их сообщать свои учетные данные. Технология дипфейк является сравнительно новой, поэтому в настоящее время риск мошенничества с использованием дипфейков может быть несколько ограничен. Тем не менее в будущем, если технология продолжит развиваться и станет более доступной, она может представлять значительную опасность.

Вставка 16. Удаленная кража личных данных для осуществления прямого контроля

В ряде случаев мошенничества, связанного с фишингом, злоумышленники обманом заставляли жертв устанавливать на свои компьютеры средства удаленного доступа. Во многих случаях учетные записи в ПУВА создавались на имя жертвы без ее ведома. Для этого преступники использовали данные, похищенные с помощью средств удаленного доступа. Предполагается, что преступники проводили жертв через процесс открытия счета также с помощью средств удаленного доступа, скрывая реальные интерфейсы.

В итоге жертвы обманом переводили средства на эти ПУВА-счета. В дальнейшем преступники могли напрямую использовать их для отмывания денег. В общей сложности потери жертв в результате данной мошеннической схемы составили более 600 000 евро.

Источник: Австрия

3. Другие возникающие уязвимости ОД

37. Превентивные меры, требуемые от ФУ, УНФПП и ПУВА в соответствии со стандартами ФАТФ (рекомендации 9-23), являются основой для предотвращения попадания доходов от КМ в финансовый и другие секторы. Данный раздел посвящен новым уязвимостям, связанным с ОД, которые могут быть использованы синдикатами КМ.

3.1. Риски, связанные с цифровыми финансовыми учреждениями[17]

38. Эволюция финансовых платежей привела к появлению новых цифровых финансовых институтов, таких как провайдеры платежных услуг (PSP), эмиссия электронных денег и т.д. Традиционные финансовые учреждения могут иметь в своем распоряжении больше ресурсов, что позволяет им осуществлять относительно более надежный контроль по сравнению с новыми цифровыми финансовыми учреждениями. В результате может произойти смещение, когда преступники будут пытаться использовать уязвимости этих альтернативных финансовых провайдеров с целью отмывания средств.

39. Сеть платежей также может быть фрагментирована. Между этими учреждениями могут существовать различные внутренние финансовые отношения, например, когда различные платежные учреждения осуществляют операции друг с другом или предоставляют счета более мелким провайдерам, которые, в свою очередь, предоставляют другие виды финансовых услуг (см. также вставку 17 ниже). Такая фрагментация может также повысить сложность отслеживания операций между различными типами учреждений в «платежной цепочке». Это также может создать проблемы с обеспечением оперативного получения базовой информации об отправителе и получателе переводов по всей платежной цепочке[18].

40. В соответствии со стандартами ФАТФ необходимо обеспечить надежный надзор за новыми финансовыми учреждениями, включая надлежащее лицензирование или регистрацию, и не допустить контроля преступников или их сообщников над этими организациями. Регулирующие органы должны обеспечить достаточный надзор за всеми учреждениями, осуществляющими транзакции, по своему периметру – все учреждения обязаны проводить или обеспечивать надлежащую проверку клиентов (НПК) и мониторинг транзакций на узлах отправителя и получателя.

[17] В данном отчете также признаются риски ОД, возникающие при использовании ВА и ПУВА. Более подробную информацию о регуляторных рисках и проблемах, связанных с ПУВА, можно найти в отчетах ФАТФ (март 2023 г.) «Противодействие использованию программ-вымогателей», а также (июнь 2023 г.) «Виртуальные активы: целевое обновление по внедрению стандартов ФАТФ в отношении виртуальных активов и провайдеров услуг виртуальных активов».

[18] ФАТФ также планирует обновить Рекомендацию 16 (по электронным переводам), чтобы учесть последние и предстоящие изменения в архитектуре платежных систем.

Вставка 17. Злоупотребления в секторе PSP

В ходе анализа, проведенного французскими надзорными органами в первой половине 2021 г., были выявлены основные PSP, используемые для получения мошеннических электронных переводов. Как правило, эти основные PSP предлагали «банковские сервисы как услуги», а некоторые из них имели филиал во Франции исключительно для предоставления французских IBAN, при этом их физическое присутствие было минимальным.

Анализ показал, что риск, связанный с этими основными PSP, примерно в 200 раз выше, чем у других организаций. В большинстве подобных PSP была плохо налажена проверка личности и мониторинг транзакций. Преступники открывали счета под чужим именем и могли быстро проверить, что некоторые из открытых счетов идентифицированы PSP как мошеннические, попытавшись сначала провести операции на небольшие суммы и при необходимости изменить назначение средств. Затем они быстро переводят полученные обманным путем средства на один или несколько счетов. Дробление сумм между несколькими счетами позволяет преступникам обойти ограничения, накладываемые PSP на свои услуги, такие как лимиты на снятие наличных или на пребывание в рамках порога мониторинга операций, установленного внутри PSP.

Источник: Франция

3.2. Неправомерное использование виртуальных IBAN[19]

41. Другим примером использования финансовых инноваций в целях КМ является использование виртуальных номеров международных банковских счетов (vIBAN). Выдачей vIBAN клиентам занимаются различные организации, включая банки и PSP. Хотя vIBAN используются в различных законных целях, в частности, для проведения и классификации платежей от нескольких сторон, в ряде юрисдикций отмечается злоупотребление vIBAN как инструментом, используемым для ОД, связанного с КМ.

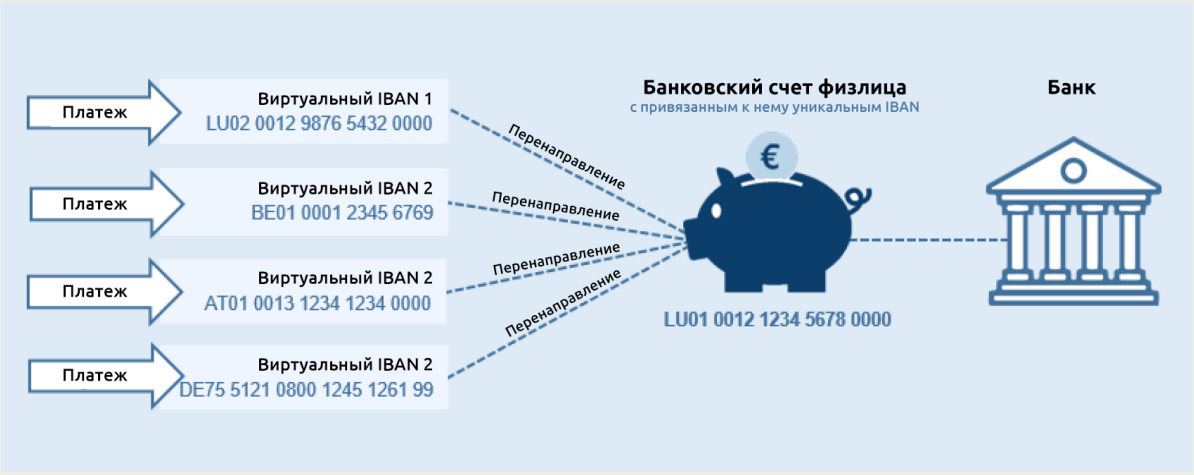
[19] Более подробную информацию о рисках и проблемах, связанных с виртуальными IBAN, см: (июнь 2023 г.) Европол, государственно-частное партнерство в области финансовой разведки (EFIPPP) Информация об угрозах, связанных с виртуальными IBAN (доступна только членам EFIPPP).

Вставка 18. Что такое vIBAN?

vIBAN функционально идентичны обычным IBAN, поскольку могут использоваться для отправки и получения платежей в глобальном масштабе. Они даже выглядят так же, как и их традиционный аналог, и тоже состоят из 34 буквенно-цифровых символов. Таким образом, функционально и визуально они неотличимы от обычных IBAN.

Основное различие между обычными и виртуальными IBAN заключается в сопоставлении счетов. Обычный IBAN сопоставляется с банковским счетом 1:1, т.е. к каждому отдельному номеру IBAN привязан только один физический банковский счет. Поэтому, если человек использует IBAN для осуществления платежа, средства автоматически попадают на тот банковский счет, к которому привязан IBAN.

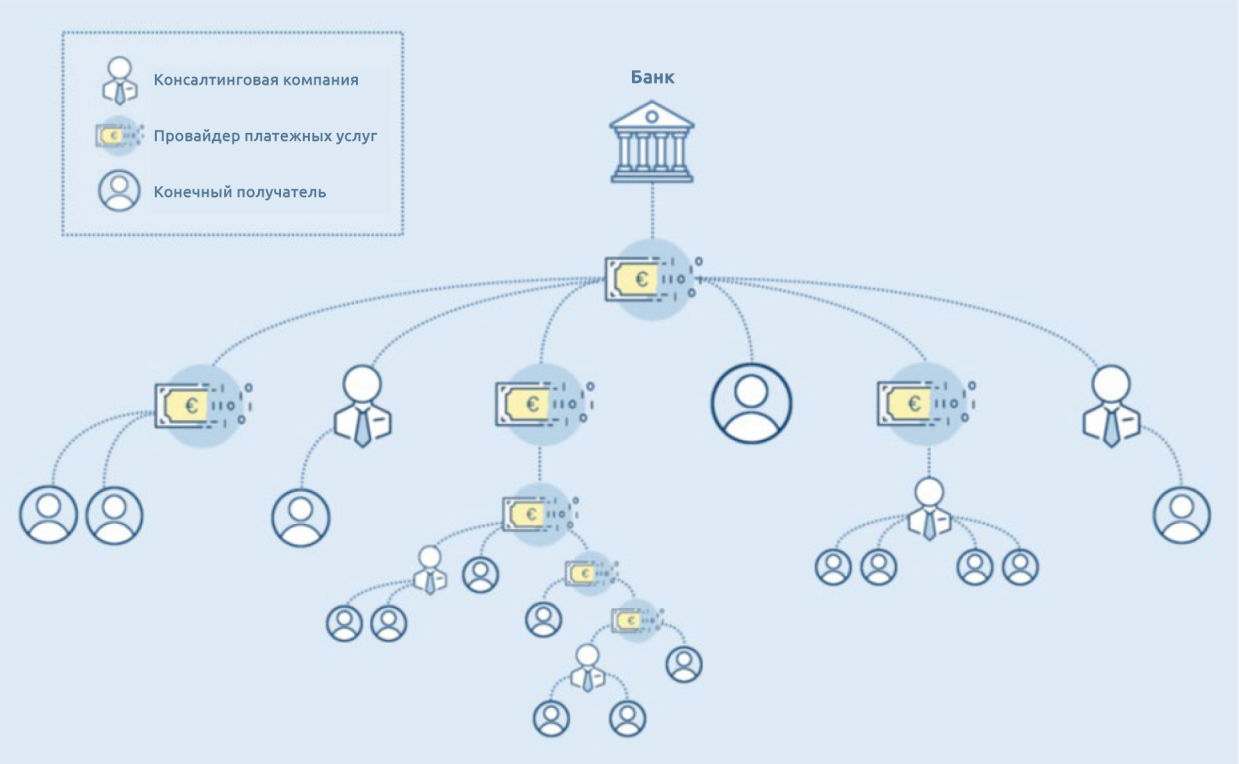
Виртуальный IBAN, напротив, представляет собой виртуальный номер, не связанный со счетом в физическом банке. Они являются идентификационными номерами, выдаваемыми банками, которые позволяют перенаправлять входящие платежи на физический IBAN, который сам связан с физическим банковским счетом. Они не могут хранить никаких средств, и их баланс постоянно равен нулю. Владельцы vIBAN могут также иметь несколько уникальных виртуальных IBAN, которые перенаправляют и централизуют все платежи на один физический банковский счет, как показано на рис. 3.



Источник: Государственно-частное партнерство Европола в области финансовой разведки

42. Поскольку IBAN и vIBAN визуально идентичны, преступники используют их для того, чтобы обмануть жертву и заставить ее думать, что она переводит средства на банковский счет, в то время как, например, vIBAN может быть использован для зачисления средств на электронный кошелек. Еще больше усложняет ситуацию то, что vIBAN могут быть перевыпущены клиентом финансового учреждения, особенно если клиентом является другое финансовое учреждение. Это затрудняет определение страны происхождения vIBAN и местонахождения основного счета.

Рисунок 2. Каскадная сеть провайдеров vIBAN, выпускающих и перевыпускающих vIBAN



Источник: Государственно-частное партнерство Европола в области финансовой разведки

43. Таким образом, преступники могут использовать vIBAN для маскировки информации о конечном бенефициарном владельце и скрывать движение незаконных денежных средств. Это может затруднить определение истинного основного счета и финансового учреждения-эмитента, а также надлежащий мониторинг операций. В конечном итоге это приводит к тому, что компетентные органы сталкиваются с трудностями при обнаружении физических счетов и замораживании средств (поскольку vIBAN – это всего лишь выданные банками идентификационные номера, а не реальные счета, на которых хранятся остатки денежных средств). В качестве положительного опыта некоторые юрисдикции сотрудничают с банками, выпускающими vIBAN, с целью быстрой идентификации платежного учреждения, связанного с такими основными счетами, в случае выявления КМ.

Вставка 19. Нецелевое использование vIBAN в целях КМ

В период с февраля по март 2023 г. в ПФР Люксембурга поступило несколько сообщений о так называемых аферах «Привет, мама», когда жертвы получали сообщения в WhatsApp с неизвестного, но местного номера телефона от мошенников, выдававших себя за их ребенка. Потерпевшие получали текстовые сообщения на люксембургском языке с люксембургских номеров мобильных телефонов с указанием люксембургского IBAN.

В ходе расследования данного дела ПФР Люксембурга обнаружило, что IBAN, предоставляемые мошенниками, являются vIBAN. Эти vIBAN были выданы люксембургским банковским учреждением люксембургскому провайдеру платежных услуг, который предлагает предоплаченные кредитные карты европейским клиентам. Эти предоплаченные кредитные карты могут быть пополнены путем перевода денег на виртуальные IBAN, которые преступники намеревались использовать для дальнейшего отмывания.

Из шести выявленных виртуальных IBAN, использовавшихся в мошенничестве, ПФР Люксембурга удалось заблокировать или отозвать 40 000 евро из 55 000 евро, полученных обманным путем. Работе ПФР Люксембурга способствовало сотрудничество между ПФР и банком-эмитентом vIBAN, что позволило быстро определить платежную организацию, владеющую базовым счетом конечного клиента.

Источник: Люксембург

3.3. Нетрадиционные секторы

44. Многие юрисдикции отметили важность работы с нетрадиционными секторами, включая платформы социальных сетей, электронную торговлю, телекоммуникационные и интернет-провайдеры, в борьбе с ОД, связанным с КМ. Хотя деятельность таких нетрадиционных секторов не регулируется в рамках ПОД/ФТ, они обладают полезной информацией, которая может помочь в расследовании случаев ОД, особенно если они используются для совершения ОД и вербовки мулов. Платформы социальных сетей, а также поставщики телекоммуникационных и интернет-услуг могут предоставлять важную цифровую криминалистическую информацию, включая IP-адреса, номера телефонов, адреса электронной почты и т.д., которая может помочь установить конечных исполнителей преступлений. Если для КМ используются мошеннические веб-сайты или рекламные объявления, то в этих секторах также будет храниться информация о финансовых операциях и платежах, связанных с преступниками (например, платежные реквизиты за размещение веб-сайтов, рекламных объявлений).

45. Опыт и примеры из практики юрисдикций также показывают, что электронная коммерция или социальные сети, потоковые или игровые платформы могут использоваться в качестве канала для отмывания доходов от КМ. Широко распространенное использование социальных сетей, стриминговых или игровых платформ позволяет пользователям получать пожертвования, подарки, токены или кредиты от зрителей и общественности. Преступники могут воспользоваться отсутствием требований ПОД/ФТ и использовать такие платформы для отмывания преступных доходов.

Вставка 20. Доходы от фишинга, отмываемые через социальные сети и стриминговые платформы

Обнаружено, что 19 банковских счетов понесли убытки в результате фишинговой атаки, направленной на клиентов некоторых банков. Анализ, проведенный ПФР Германии, показал, что операции с этих банковских счетов проводились через платежные счета, принадлежащие двум пользователям. Впоследствии эти средства были отправлены на платформу социальных сетей и стриминга. Средства использовались для пополнения счетов пользователей стриминговой платформы «коинами» (являющимися разновидностью национальной валюты пользователей платформы), которые могли быть использованы для приобретения виртуальных подарков. Такие подарки могут быть переданы создателям контента, которые могут конвертировать их в обычную валюту и вывести эквивалентную денежную стоимость.

Расследование продолжается. Данные об IP-адресах показали, что мошеннические операции осуществлялись с одних и тех же IP-адресов. Анализ, проведенный ПФР, позволяет предположить, что один из преступников отмывает значительную часть доходов от фишинга через платформу социальных сетей и стриминга, чтобы впоследствии обналичить средства.

Источник: Германия

4. Национальные оперативные меры и стратегии

46. В данной главе рассматриваются основные источники информации, на которые опираются юрисдикции при выявлении и расследовании КМ. Кроме того, анализируются национальные структуры координации и сотрудничества, а также то, как юрисдикции их используют для расследования и предотвращения КМ и связанного с ним ОД.

4.1. Основные источники выявления

47. Исходя из опыта юрисдикций и тематических исследований, существует два основных источника информации для выявления и расследования случаев ОД, связанных с КМ: информация от потерпевших и сообщения о подозрительных операциях (СПО).

48. Кроме того, в юрисдикциях реализуются различные инициативы по расширению отчетности, чтобы максимально увеличить объем информации, к которой они могут получить доступ для эффективного правоприменения. Используя эту информацию и данные, компетентные органы применяют цифровые стратегии и инструменты для анализа и выявления преступных группировок с целью повышения эффективности и целенаправленности правоохранительных действий[20].

Информация от потерпевших

49. Сообщения потерпевших являются важным источником информации для выявления и расследования случаев незаконных доходов, связанных с КМ. При некоторых видах мошенничества, таких как BEC-мошенничество и фишинг, жертвы обычно относительно быстро обнаруживают, что их обманули (например, когда их законный контрагент начинает требовать пропущенных платежей). В других видах КМ, таких как мошенничество с инвестициями, любовное мошенничество или фишинг, жертвы могут понять, что их обманули, только спустя некоторое время.

50. Своевременное обращение потерпевших важно для оперативного принятия компетентными органами мер по отслеживанию незаконных доходов и может повысить вероятность успешных результатов правоприменительной деятельности. Потерпевшие могут сообщать о предполагаемых преступлениях в правоохранительные органы, в том числе в специальные подразделения, занимающиеся сообщениями о мошенничестве. Кроме того, пострадавшие могут уведомить свои финансовые учреждения, провайдеров платежей и ПУВА о предполагаемых мошеннических операциях по их счетам. В других юрисдикциях отмечается, что потерпевшие могут обращаться не в правоохранительные органы, а в органы по защите прав потребителей финансовых услуг.

51. Вместе с тем жертвы нередко не сообщают о КМ, особенно в случаях незначительного ущерба. В сочетании с эмоциональными факторами, включая смущение или страх, жертвы могут принять решение не заявлять о случившемся.

[20] Более подробную информацию о том, как ПФР и правоохранительные могут использовать цифровую трансформацию для эффективного анализа и расследования в сфере ПОД/ФТ, см. в закрытых отчетах по цифровой трансформации ПОД/ФТ для оперативных органов: Группа «Эгмонт» – ФАТФ (октябрь 2021 г.) «Выявление подозрительной деятельности и анализ финансовой разведывательной информации (Фаза 1)» и ФАТФ (май 2022 г.) «Правоохранительные органы и обмен информацией (Фаза 2)».

52. В качестве передовой практики, направленной на увеличение количества сообщений от потерпевших, в некоторых юрисдикциях созданы специальные платформы, позволяющие потерпевшим сообщать о КМ, включая онлайн-порталы. Такие платформы могут обеспечить структурированный формат отчетности для стандартизации сбора данных, что облегчает кластерный анализ сообщений жертв и помогает выявить криминальные тенденции и закономерности. Платформы также могут содержать полезные ресурсы по профилактике КМ и оказанию помощи пострадавшим.

Вставка 21. Action Fraud в Великобритании

Action Fraud – это национальный центр Соединенного Королевства по борьбе с мошенничеством и киберпреступлениями. Он является основным координационным пунктом по вопросам мошенничества и интернет-преступлений на финансовой основе и управляется полицией лондонского Сити совместно с Национальным бюро по борьбе с мошенничеством (National Fraud Intelligence Bureau, NFIB). На сайте Action Fraud представлены различные информационные ресурсы по предотвращению преступлений, а также по защите и поддержке потерпевших.

Action Fraud также управляет круглосуточным онлайн-порталом сообщений для жертв. Сообщения о мошенничестве Action Fraud передаются в NFIB, который проводит оценку и анализ в различных регионах страны с целью выявления конечных преступников. Далее эти сообщения направляются в соответствующие местные полицейские органы Великобритании для проведения расследования. NFIB также использует подобные сообщения для выявления банковских счетов, веб-сайтов и телефонных номеров, используемых мошенниками.

Источник: Великобритания

Сообщения о подозрительных операциях

53. С учетом вероятности сокрытия информации жертвами СПО являются важным независимым источником выявления финансовых потоков, связанных с КМ.

54. Согласно данным, полученным от ПФР, большинство СПО, связанных с КМ, было подано банковским сектором. Тем не менее банкам следует продолжать укреплять свои возможности по выявлению КМ и связанного с ним ОД, поскольку синдикаты КМ постоянно совершенствуют свои методы работы. Данные также показали, что услуги перевода денег или ценностей (УПДЦ) и ПУВА подают меньше СПО. Последнее может быть связано с тем, что в некоторых юрисдикциях сектор ПУВА не полностью регулируется в соответствии со стандартами ФАТФ[21].

55. Важно обеспечить своевременный анализ СПО, связанных с КМ, учитывая возможное распыление доходов от КМ. Некоторые ПФР применяют систему приоритетов для отсеивания большого количества СПО и сосредоточения внимания на СПО с повышенным риском, к которым относятся и СПО, связанные с КМ. Другие проводят обучение сотрудников своих ПФР по рискам ОД, относящимся к КМ, что позволяет им отбирать и классифицировать поступающие СПО, связанные с КМ. Все эти меры способствуют своевременному анализу ПФР, позволяя правоохранительным органам оперативно реагировать на инциденты, относящиеся к КМ.

[21] См. также ФАТФ (июнь 2023 г.) «Виртуальные активы: целевое обновление по внедрению стандартов ФАТФ в отношении виртуальных активов и провайдеров услуг виртуальных активов».

Вставка 22. Расстановка приоритетов и кластеризация СПО, связанных с КМ

В период с 2021 по 2022 гг. в ПФР Чили поступило более 1500 СПО, связанных со схемой мошенничества на торговых онлайн-площадках. Для обработки такого объема ПФР Чили применило методы кластеризации для анализа, и в этих СПО были обнаружены определенные закономерности.

ПФР применило инструмент интеллектуального анализа текста, используя обнаруженные ключевые слова и известные фразы. Впоследствии были выявлены географические кластеры, что позволило целенаправленно и в совокупности передать дела в прокуратуру. Благодаря кластеризации следствию удалось установить, что денежные средства впоследствии были сняты через банкоматы и переданы лицу, занимающему более высокий иерархический уровень в организованной преступной группе.

Источник: Чили

56. Помимо выявления, юрисдикции также стремятся повысить осведомленность и улучшить дальнейшую отчетность. Многие юрисдикции выпустили те или иные руководства по КМ или провели обучающие семинары для сотрудников банков и других секторов, чтобы повысить информированность всей отрасли о последних тенденциях, связанных с КМ, и типологиях ОД. В Приложении А представлен перечень риск-индикаторов, которые могут быть использованы для выявления КМ. ПФР других юрисдикций разработали стратегические аналитические документы по КМ. Целью данных инициатив является повышение эффективности выявления и предотвращения преступлений, связанных с КМ и ОД, сотрудниками банков, находящимися «на передовой линии», и т.д.

Вставка 23. Стратегический анализ мулов, связанных с КМ

Стратегический анализ, проведенный ПФР Испании, был направлен на изучение выявленного профиля денежных мулов: банковские счета, открытые одним физическим лицом в трех и более финансовых учреждениях в течение 20 дней. На основе информации, полученной в период с декабря 2020 по февраль 2022 гг. из Реестра банковских счетов (BAR), было обнаружено около 40 тыс. других банковских счетов, связанных с примерно 10 тыс. физических лиц. 15% выявленных банковских счетов имели совпадения в базах данных ПФР Испании. Данные счета были отнесены к высокорисковым, и совместно с четырьмя финансовыми учреждениями было начато пилотное исследование, направленное на углубление понимания профиля риска на основе этих счетов.

Целью пилотного проекта было пресечение КМ и других возможных случаев мошенничества, а также укрепление взаимодействия с частным сектором. Кроме того, пилотный проект был направлен на повышение способности финансовых учреждений обнаруживать пробелы в своих системах и получать дополнительную информацию о КМ для выявления и предотвращения дальнейших преступлений. В конечном итоге результатом пилотного проекта стало внедрение системы перекрестного контроля с использованием BAR для проактивного выявления сетей ОД, связанных с КМ.

Источник: Испания

4.2. Координация и взаимодействие на национальном уровне

Координация между компетентными органами

57. С учетом комплексного характера КМ существует настоятельная необходимость в сильной координации действий различных ведомств. В некоторых юрисдикциях координация осуществляется на основе общегосударственного стратегического подхода, определяющего политику юрисдикции в области КМ. В этом случае создается всеобъемлющий межфункциональный орган, в состав которого входят ключевые министерства судебной, правоохранительной, регулятивной и инфокоммуникационной сфер. Координационный подход позволяет юрисдикциям выявлять ключевые уязвимости и разрабатывать последовательные ответные меры в ключевых направлениях.

58. В рамках координации внутренней оперативной деятельности для повышения эффективности раскрытия и расследования могут привлекаться и технические агентства, в частности:

    - Развитие каналов связи между ПФР, полицией и прокуратурой для обеспечения централизованной отчетности, упорядоченного обмена информацией и доказательной базой, а также инструкциями по замораживанию и аресту активов. Это может также включать использование автоматизированной сортировки данных, помогающей выявлять возможные факты, представляющие интерес, и быстро определять соответствующий правоохранительный орган для проведения расследования. Такая координация также позволяет избежать дублирования усилий правоохранительных органов, поскольку преступники, занимающиеся КМ, могут нацеливаться на жертв в разных регионах юрисдикции (см. раздел 4.3.1 ниже).
    - Привлечение технических экспертов по киберпреступлениям, в частности, по сетевым вторжениям и другим преступлениям в сфере технической инфраструктуры, а также органов по защите частной жизни. Такая практика отражает многогранность КМ и значимость цифровых криминалистических данных (таких как IP-адреса, идентификаторы, привязанные к интернет-доменам, и т.д.) для выявления синдикатов КМ и дальнейшего расследования случаев ОД.

Вставка 24. Объединенный координационный центр по борьбе с киберпреступностью

Федеральная полиция Австралии (ФПА) возглавляет Объединенный координационный центр по борьбе с киберпреступностью (Joint Policing Cybercrime Co-ordination Centre, JPC3). В состав JPC3 входят правоохранительные органы федерации и штатов, государственные аналитики, включая АУСТРАК (ПФР Австралии – прим. пер.), и отраслевые партнеры, например, аналитики австралийских банков. JPC3:

- Координирует действия полиции Австралии по борьбе с киберпреступностью, наносящей большой ущерб, с целью оказания наибольшего воздействия на преступную среду;

- Повышает эффективность обмена разведданными и выработки целей между полицией Австралийского Союза, штатов и территорий и отраслевыми структурами;
- Координирует работу совместных целевых групп с полицией и отраслевыми партнерами по противодействию первоочередным угрозам киберпреступности;
- Обеспечивает национальную координацию наращивания потенциала через повышение квалификации, совместное обучение и разработку инструментов для совместной работы;
- Обеспечивает последовательную реализацию национальных мер по профилактике, повышению осведомленности и информированию отраслей и общественности.

В состав JPC3 входит служба по предупреждению преступлений, которая работает с отраслевыми и общественными организациями в области борьбы с киберпреступностью. С целью оказания эффективной поддержки JPC3 в АУСТРАК также имеется группа по борьбе с финансовыми киберпреступлениями, которая занимается предоставлением финансовой разведывательной информации о киберпреступлениях и киберзависимых преступлениях, связанных с финансами, в том числе об ОД от кибермошенничества.

В январе 2020 г. ФПА разработала операцию «ДОЛОС», которая представляет собой возглавляемую ФПА межведомственную целевую группу[22], противодействующую транснациональным киберпреступникам, осуществляющим или способствующим осуществлению BEC. Операция «ДОЛОС» проводится среди отдельных австралийцев и представителей малого и среднего бизнеса, ставших жертвами BEC, и пресекает потоки доходов, поступающих в синдикаты BEC и из них. С момента начала операции «ДОЛОС» оперативной группой были разработаны новые методы, позволяющие снизить ущерб, наносимый австралийцам и предприятиям. В период с 1 июля 2022 г. по 30 июня 2023 г. операция «ДОЛОС» позволила предотвратить потерю более 30,6 млн. австралийских долларов жертвами из Австралии и других стран благодаря разрушению финансовой операционной модели, используемой преступниками.

Источник: Австралия

Оперативное партнерство с частным сектором

59. Юрисдикции также стремятся сотрудничать с частным сектором в рамках государственно-частного партнерства (ГЧП). Такое ГЧП может способствовать повышению эффективности усилий по обнаружению, выявлению скрытых сетей ОД путем обмена тактической информацией и повышению эффективности оперативных мер по возврату активов.

[22] В состав целевой группы входят представители полиции различных штатов и территорий, разведывательных служб и служб кибербезопасности, ПФР, а также представители финансового сектора.

Вставка 25. Проект: оперативные действия по предотвращению мошенничества

ПФР Шри-Ланки запустило проект под названием «Оперативные действия по предотвращению мошенничества» (Rapid Actions to Prevent Scams, RAPS), направленный на немедленное принятие мер после того, как жертва сообщает о возможном КМ. Целью проекта является пресечение мошеннических действий в финансовой системе Шри-Ланки, в том числе КМ, благодаря объединению усилий ПФР и сотрудников комплаенс департаментов финансовых учреждений, с тем чтобы оперативно выявлять незаконные операции со счетами, используемые преступниками и их пособниками.

Механизм предполагает выявление анкет мошенников на основе поступающих жалоб от населения, и анкетные данные таких мошенников передаются специалистам по комплаенсу финансовых учреждений. На основании этой информации финансовые учреждения отслеживают действия по счетам потенциальных мошенников и предпринимают соответствующие действия по пресечению использования финансовой системы в преступных целях. Кроме того, информация о мошенниках передается в полицию Шри-Ланки для проведения расследований в отношении данных лиц.

Источник: Шри-Ланка

60. В связи с заметным ростом объемов КМ и связанного с ним риска ОД многие юрисдикции создали специализированные центры реагирования при правоохранительных или регуляторных органах для активизации борьбы с КМ и повышения информированности общественности (см. также раздел 4.3.2. ниже о специализированных подразделениях по борьбе с КМ). В качестве положительного примера можно привести совместное размещение представителей финансовых учреждений и ПУВА в подобных центрах реагирования, что обеспечивает доступ к финансовым данным в режиме реального времени и отслеживание различных финансовых организаций и секторов, а также расширяет возможности компетентных органов по перехвату и замораживанию средств.

Вставка 26. Совместное размещение банковских служащих

В Саудовской Аравии создан Объединенный оперативный центр (ОРЦ) для банков. В задачи ОРЦ входит отслеживание и мониторинг случаев финансового мошенничества, которым могут подвергнуться клиенты банка. Объединенный оперативный центр объединяет все банки и связанные с ними финансовые учреждения для борьбы с подтвержденными случаями финансового мошенничества.

ОРЦ размещается в банках Саудовской Аравии, что позволяет объединить усилия для обеспечения стабильности банковского сектора. ОРЦ работает в круглосуточном режиме и призван обеспечить быстрое и эффективное сотрудничество и интеграцию между всеми банками Саудовской Аравии, чтобы сдержать распространение случаев мошенничества, а также оперативно реагировать на поступающие жалоб и, по возможности, принимать незамедлительные меры по предотвращению противоправных действий.

Источник: Саудовская Аравия

61. Кроме того, такие партнерства являются полезной платформой для обмена передовым опытом, общими типологиями и совместной разработки рекомендуемых мер по пресечению незаконной деятельности.

Вставка 27. Государственно-частное партнерство Европола в области финансовой разведки

Государственно-частное партнерство Европола в области финансовой разведки (EFIPPP) является первым транснациональным государственно-частным механизмом обмена информацией в области ПОД/ФТ. EFIPPP объединяет правоохранительные органы, ПФР и частные структуры в различных странах ЕС и за его пределами.

Рабочая группа по угрозам и типологиям в рамках EFIPPP имеет специальные направления работы по различным вопросам, связанным с КМ и их механизмами деятельности, включая BEC, инвестиционное мошенничество, счета мулов, виртуальные IBAN и криптоактивы. Хотя целью EFIPPP является создание стратегических типологических отчетов, оно также служит платформой для обсуждения вопросов содействия оперативному сотрудничеству между его членами.

Источник: Европол

62. Состав участников ГЧП может быть различным. Многие юрисдикции по-прежнему ориентированы на традиционные заинтересованные стороны (в частности, банки и другие финансовые учреждения), однако все чаще в них участвуют УНФПП, ПУВА и другие нетрадиционные сектора (например, операторы телекоммуникационного бизнеса и интернет-провайдеры). Конкретный состав зависит от целей и задач ГЧП.

Вставка 28. Сотрудничество с телекоммуникационным сектором

В последние годы в Китае продолжается наращивание усилий по борьбе с мошенничеством в телекоммуникационных сетях и его регулированию, и 1 декабря 2022 г. был официально введен в действие «Закон КНР о борьбе с мошенничеством в телекоммуникационных сетях», который обеспечил надежные гарантии верховенства закона для противодействия и предотвращения преступной деятельности мошенников в телекоммуникационных сетях, и соответствующие преступные действия были эффективно пресечены.

Закон объединяет усилия государственных органов (включая правоохранительные, финансовые, телекоммуникационные и интернет-информационные органы), а также финансовых учреждений (банков и небанковских провайдеров платежных услуг), операторов телекоммуникационного бизнеса и интернет-провайдеров для создания системы раннего предупреждения и противодействия. Данная система позволяет выявлять потенциальных жертв за счет своевременного предупреждения, что дает возможность принять соответствующие и оперативные меры по их предотвращению.

Финансовые учреждения также могут использовать эту систему при открытии банковских и платежных счетов, а также при оказании платежно-расчетных услуг. Система используется для повышения эффективности процессов надлежащей проверки клиентов и позволяет ФУ принимать меры по снижению рисков, чтобы предотвратить использование банковских, платежных и т.п. счетов для мошеннических действий.

Источник: Китай

4.3. Полезные внутренние стратегии правоприменения

63. В данном разделе рассматриваются некоторые примеры успешной практики и полезные стратегии правоприменения, используемые юрисдикциями. В целом эти стратегии позволяют использовать источники информации, рассмотренные ранее в разделе 4.1, с целью более эффективного выявления, расследования и предотвращения КМ и связанного с ним ОД.

64. Данные полезные стратегии правоприменения, как правило, предполагают участие множества ведомств и организаций частного сектора. Таким образом, для реализации этих стратегий, как правило, требуется четкая координация и сотрудничество на национальном уровне (см. раздел 4.2 выше).

Надлежащее разграничение ответственности

65. За последние несколько лет многие юрисдикции сообщали об увеличении суммы ущерба и объема дел, связанных с КМ. Хотя некоторые отдельные дела могут быть связаны с небольшими потерями, объем таких афер означает, что общая сумма преступных доходов, накопленных каждым синдикатом, потенциально велика.

66. Несколько юрисдикций указали, что большой объем сообщений о КМ указывает на необходимость разграничения ответственности за расследование. Как показывает положительная практика, в юрисдикциях, где различные ведомства по борьбе с мошенничеством или киберпреступностью осуществляют надзор за делами, связанными с КМ, стремятся определить компетентный орган или органы, которые будут заниматься данными делами. В других юрисдикциях было принято законодательство, направленное на объединение сложных расследований, в которых участвуют несколько жертв одного и того же синдиката, таким образом, чтобы надзор за всем расследованием осуществлял один компетентный орган. Эти инициативы позволяют избежать дублирования усилий различных компетентных органов и предотвратить «"выпадение" дел из поля зрения», а также учитывать транснациональный характер данного преступления.

Вставка 29. Использование технологий для разграничения ответственности за расследование

В сентябре 2022 г. полиция Гонконга создала Центр обработки и анализа электронных преступлений (e-Hub) с целью повышения эффективности работы с сообщениями о технологических преступлениях и обмане. Центр e-Hub использует усовершенствованную компьютерную систему для проведения корреляционного анализа распространенных видов кибермошенничества и выявления кластеров дел.

В 2022 г. количество случаев обмана увеличилось на 45,1% и составило 27 923, что равняется почти 40% от общего числа преступлений. Почти 80% случаев обмана были связаны с КМ. Все больше людей сообщают о КМ через Интернет, и многие электронные сообщения оказываются связанными между собой, например, через одну и ту же преступную группу. Коррелирующие дела передаются в одну следственную группу для совместного расследования, что позволяет лучше координировать ресурсы.

Используя алгоритмы кластеризации, e-HUB может выявлять закономерности и сходства в данных, которые могут быть не очевидны сразу, что позволяет глубже понять масштаб и характер дел. К ним относятся общие типы используемых криминальных цифровых инструментов и счетов денежных мулов, а также способы планирования, осуществления и сокрытия КМ.

Источник: Гонконг, Китай

Специальные подразделения по борьбе с КМ и соответствующим ОД

67. С целью укрепления возможностей ПОД/ФТ в условиях меняющегося криминального ландшафта во многих юрисдикциях были созданы специальные подразделения или целевые группы по расследованию КМ и связанного с ними ОД. В данных юрисдикциях выделяются дополнительные ресурсы на расширение возможностей по проведению финансовых расследований, сбору оперативной информации, обучению сотрудников правоохранительных органов и наращиванию потенциала частного сектора. Такие централизованные подразделения консолидируют опыт правоохранительных органов в борьбе с КМ и позволяют им эффективнее пресекать операции от КМ, отслеживать отмытые средства и возвращать соответствующие доходы.

68. Юрисдикции отмечают, что у такой структуры есть множество преимуществ. Консолидация всех дел, связанных с КМ, в одном правоохранительном подразделении позволяет проводить более качественный анализ, использовать аналитику данных и анализ сетевых связей для выявления синдикатов. Кроме того, это подразделение может служить единым контактным центром для заинтересованных сторон из частного сектора и иностранных партнеров, а в долгосрочной перспективе способствует развитию стратегических отношений. В результате повышается эффективность мер, принимаемых правоохранительными органами, таких как отключение телефонных линий, удаление подозрительных сетевых имен и рекламы, а также обеспечивается более высокий показатель возврата активов.

Вставка 30. Национальный центр реагирования на мошенничество

Национальный центр реагирования на мошенничество (НЦРМ) в Малайзии — это многоплановый механизм реагирования, объединяющий различные ресурсы и опыт Национального центра по борьбе с финансовыми преступлениями, Королевской полиции Малайзии (КПМ), Центрального банка и других государственных и частных структур.

НЦРМ служит центром сбора информации о мошенничестве, поступающей из различных источников, и использует сетевой анализ для выявления сетей мулов и отмывания денег. Частные структуры, включая финансовые учреждения, отслеживают перемещение средств с одного уровня на другой и впоследствии удерживают счета «мулов». КПМ проводит дальнейшее расследование и принимает меры, например, выдает ордер на замораживание счетов.

Источник: Малайзия

Расширение доступа к финансовой информации

69. В связи с большим объемом и оперативностью дел, связанных с КМ, своевременный доступ к финансовой и банковской информации имеет решающее значение для ускорения расследования и отслеживания доходов от КМ. Некоторые юрисдикции прибегают к технологиям, позволяющим оперативно реагировать на быстрые потоки доходов от КМ, зачастую во взаимодействии с частным сектором. Другие полагаются на центральные реестры или разрабатывают базы данных для оптимизации процесса поиска информации. Как правило, эти передовые методы основаны на создании централизованной платформы, объединяющей различные заинтересованные стороны для ускорения информационного обмена.

    - **Поиск информации с помощью технологий:** чтобы обеспечить оперативное предоставление финансовыми учреждениями необходимой информации правоохранительным службам, компетентным органам в той или иной юрисдикции целесообразно согласовать области данных, которые могут быть использованы при проведении расследований. Направление различных запросов, каждый из которых требует индивидуального ответа от соответствующего финансового учреждения, может отнимать у частного сектора много времени. В качестве положительного опыта правоохранительные органы некоторых стран разработали стандартный шаблон, включающий заранее согласованные поля данных, запрашиваемые ими у финансовых учреждений. В дальнейшем запросы могут агрегироваться, рассылаться финансовым учреждениям партиями и иметь машиночитаемую форму. Кроме того, финансовые учреждения могут предоставлять правоохранительным органам ответы на соответствующие запросы в цифровом виде, что позволяет более эффективно анализировать данные.

Вставка 31. Использование роботизированной автоматизации процессов для ускорения доступа к финансовой документации, хранящейся в финансовых учреждениях

Своевременный доступ к банковской и финансовой информации имеет решающее значение для эффективного перехвата и возврата активов. Сингапур использует роботизированную автоматизацию процессов (RPA) для получения банковской информации за меньшее время, чем это требовалось ранее. Теперь запросы направляются в банки в электронном виде по стандартному шаблону. Банки автоматизируют процесс получения финансовой информации и затем отправляют ее обратно правоохранительному органу в электронном виде. Электронные данные также могут быть немедленно использованы для анализа соответствующим компетентным органом.

Благодаря этому процессу время обработки запросов сократилось на 97%, что позволило повысить эффективность расследований. Информация теперь предоставляется в цифровом формате, готовая к анализу. Для банков эта инициатива привела к значительному снижению затрат за счет отказа от ручного исполнения запросов. Кроме того, благодаря автоматизированным процессам в банках появилась возможность поиска данных, которые могут быть использованы для дальнейшего выявления скрытых сетей ОД.

Источник: Сингапур

- **Упрощение отслеживания активов в разных ФУ:** проведение сквозных транзакций и перемещение счетов между несколькими финансовыми учреждениями увеличивает объем работы правоохранительных органов по отслеживанию активов, поскольку требуется время на сбор информации от соответствующих финансовых учреждений, прояснение всех уровней транзакций и определение происхождения и конечного назначения средств. Это может быть непросто, учитывая скорость проведения операций. Эффективная практика включает разработку платформ, способствующих быстрому отслеживанию и обмену информацией между различными ФУ для перехвата незаконных доходов.

Вставка 32. Система учета и управления сообщениями граждан о финансовом кибермошенничестве (CFCFRMS)

CFCFRMS — это онлайн-система, разработанная Координационным центром по борьбе с киберпреступностью Индии для оперативного информирования о финансовых кибермошенничествах и предотвращения потока доходов от мошенничества в финансовом секторе. Система объединила правоохранительные органы и финансовые учреждения по всей стране (банки, кошельки, платежные агрегаторы, платежные шлюзы, платформы электронной коммерции и т.д.) для совместной работы и принятия немедленных мер по жалобам, поступившим на CFCFRMS. В настоящее время к работе с модулем подключены все государственные органы власти штатов и союзных территорий, а также 243 финансовых учреждения.

Как только жертва сообщает в компетентных орган о факте мошенничества, информация о бенефициаре мошеннической операции записывается и передается в систему CFCFRMS в виде тикета. Данный тикет передается в соответствующее финансовое учреждение (банк, платежный кошелек и т.д.), которое видит тикет на панели своей системы. Организация проверяет, находятся ли мошеннические деньги на счете, и переводит его в режим ожидания. Если деньги были выведены на счет другой организации, то тикет передается на следующий уровень организации. Процесс повторяется до тех пор, пока деньги не будут перехвачены. В случае изъятия денег реквизиты изъятия заполняются ФУ для проведения дальнейших мероприятий правоохранительными органами.

Система оказалась весьма эффективной с точки зрения предотвращения попадания преступных средств в руки мошенников. С момента своего создания в апреле 2021 г. система смогла перехватить более 6,02 млрд. индийских рупий (около 66,1 млн евро).

Источник: Индия

- **Использование центральных реестров:** центральные банковские реестры позволяют правоохранительным органам получить быстрый доступ к основной банковской информации и ускорить расследование КМ. Эта информация позволяет правоохранительным органам проверить банки, в которых подозреваемый имеет счета, или личность владельца счета. Таким образом, упрощается процесс поиска информации, что позволяет правоохранительным органам уже на ранних этапах расследования сосредоточиться только на тех финансовых учреждениях, в которых у подозреваемого имеются счета.

Вставка 33. Выявление скрытых счетов денежных мулов

На Мальте после серии подозрительных операций в адрес различных бенефициаров было направлено СПО в отношении подозреваемого денежного мула. Средства переводились в различные местные и международные банки, связанные с предполагаемым любовным мошенничеством.

Поиск в национальном реестре счетов Центрального банка позволил ПФР сразу же выявить еще один активный счет, принадлежащий подозреваемому мулу в другом банке. ПФР смогло оперативно составить целостную картину и определить объем необходимого дополнительного финансового анализа. В итоге это помогло ПФР быстро выявить общие черты дальнейшего отмывания денежных средств в отношении других иностранных лиц.

Источник: Мальта

- **Создание баз данных для обмена информацией в рамках частного сектора:** в случае профессиональных сетей ОД многие учетные записи «мулов» могут быть известны или подозреваться в связи с предыдущими мошенничествами (например, любовными, лотерейными, трудовыми) или действиями по присвоению идентификационных данных. Кроме того, данные и процессы, используемые для выявления мошенничества и для выявления сетей «мулов», аналогично дублируют друг друга. В качестве положительного опыта некоторые юрисдикции используют централизованную обработку данных, охватывающих базы данных по борьбе с мошенничеством и ПОД, для выявления более глубоких сетей ОД в различных ФУ с целью предотвращения мошенничества и обеспечения возврата активов.

Вставка 34. Централизованная база данных между частным сектором

В Бразилии недавно было принято постановление об обязательном создании базы данных, в которой централизовано хранится информация о мошенничестве (включая попытки) всех финансовых и платежных организаций. Функционирование этой базы данных обеспечивается Центральным банком Бразилии (Banco Central do Brasil, BCB) и, как ожидается, начнется в ноябре 2023 г.

Постановление устанавливает обязательность обмена информацией о случаях мошенничества (включая попытки) для учреждений и определяет минимальный объем информации, подлежащей обмену. Это включает в себя идентификацию лиц, причастных к совершению мошенничества (в том числе денежных мулов), финансового учреждения (учреждений) и используемого счета (счетов). Система призвана упростить обмен информацией между представителями частного сектора с целью предотвращения и борьбы с мошенничеством, а также возврата доходов от незаконного мошенничества.

Источник: Бразилия

Пресечение деятельности денежных мулов

70. Как было отмечено ранее, денежные мулы играют важную роль в сетях ОД, связанных с КМ. Мулы вербуются с помощью множества методов. В зависимости от способа вербовки, а также от того, были ли они невольно обмануты или использованы, они могут иметь различный уровень знаний и вовлеченности в основную схему КМ (см. раздел 2.3 выше).

71. В этой связи у компетентных органов могут возникнуть трудности при предъявлении обвинений в ОД. Бывает сложно собрать достаточные доказательства, подтверждающие наличие у мула преступных намерений в отношении ОД (т.е. степень осознания им своего участия в процессе отмывания). Для решения этой проблемы в некоторых юрисдикциях были приняты законодательные акты, снижающие критерий mens rea (преступного умысла), необходимый для совершения преступления ОД, например, с «знания» на «подозрение».

Вставка 35. Статья 9(3) Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (заключена в г. Варшаве 16.05.2005)

Одним из основных вопросов эффективного уголовного преследования за преступления в сфере ОД является необходимость доказательства mens rea, т.е. того, что лицо, отмывающее деньги, знало, что доходы, с которыми оно работает, являются доходами от преступления. В сложных делах об отмывании денег, в которых фигурируют профессиональные отмыватели, обвиняемый, как правило, отрицает, что ему было достоверно известно, что средства, с которыми он работал, являются доходами от преступлений. Следовательно, демонстрация того, что «субъективная сторона» обвиняемого достигла соответствующего порога, является одной из наиболее сложных задач в доказывании преступления ОД.

Помня о трудностях доказывания mens rea, авторы Варшавской конвенции ввели новые элементы в ее статью 9, где излагается состав преступления ОД. Помимо элементов, уже содержащихся в Венской и Палермской конвенциях, статья 9 Варшавской конвенции в пункте 3 делает еще один шаг вперед, устанавливая, что преступление ОД имеет место даже в том случае, если преступник только подозревал или должен был предполагать, что доходы были получены преступным путем.

Источник: МАНИВЭЛ

72. Другие юрисдикции решают проблему денежных мулов, как правило, через просвещение населения и работу с потенциальными мулами. Глобальные кампании в социальных сетях, такие как #IDontbeaMule, поддерживаемая Европолом, и #YourAccountYourCrime Интерпола, могут служить полезными платформами для координации международной осведомленности о борьбе с деятельностью денежных мулов, особенно в условиях трансграничного отмывания средств мулами. Сотрудничество с частным сектором может обеспечить максимальный эффект и результаты таких информационно-разъяснительных мероприятий. Органы власти могут также использовать существующие механизмы обнаружения (СПО и сообщения потерпевших) для выявления потенциальных денежных мулов, которые могли работать с доходами от КМ. Целевая информационная и предупредительная работа может побудить таких потенциальных «мулов» воздержаться от повторения подобного поведения в будущем. Записи о проведенной работе или предупреждениях могут быть использованы в качестве полезного доказательства при определении преступного умысла ОД в случае рецидива.

4.4. Предотвращение и пресечение

73. С учетом быстроты распыления средств во многих юрисдикциях разрабатываются инициативы по предотвращению КМ и связанных с ним видов ОД. Такой подход снижает общую рентабельность синдикатов КМ и значительно уменьшает затраты ресурсов на последующие этапы – от расследования до работы с пострадавшими.

Обучение и работа с населением

74. Превентивный подход может быть реализован за счет просвещения населения и повышения бдительности в отношении случаев эксплуатации, включая проведение национальных информационных кампаний по повышению киберграмотности. Для решения этой задачи в некоторых юрисдикциях используются технологии, позволяющие проводить информационные кампании для граждан с целью помочь им обнаружить мошеннические операции, повысить осведомленность о характерных признаках и побудить их сообщать о фактах мошенничества.

Вставка 36. Использование технологий для просвещения населения по вопросам КМ

В сентябре 2022 г. полиция Гонконга запустила универсальную систему поиска мошенников и «подводных камней» – «Scameter». Это приложение призвано помочь населению выявить мошенников и «подводные камни» в Интернете.

При столкновении с подозрительными звонками и онлайн-продавцами, нежелательными запросами друзей, сообщениями о произвольном наборе персонала, подозрительными мошенническими инвестиционными сайтами и т.п. пользователи могут ввести в Scameter имя или номер счета, номер платежного счета, номер телефона, адрес электронной почты, URL и т.п. подозреваемых мошенников, чтобы оценить риск мошенничества и кибербезопасность.

Данные и рейтинг Scameter поступают из различных надежных источников, включая открытые сообщения в полицию, информацию, предоставляемую организациями, базу данных подозрительных телефонных номеров, а также базу данных и анализ в режиме реального времени от компаний, занимающихся информационной безопасностью.

Источник: Гонконг, Китай

Обеспечение безопасности и контроля противодействия мошенничеству для достижения результатов по ПОД/ФТ

75. Опыт государственного и частного секторов начинает показывать, что процессы борьбы с мошенничеством и ПОД являются взаимодополняющими. Это включает в себя использование технологий, помогающих пользователям автоматически отклонять получение мошеннических сообщений, сотрудничество с частным сектором в области сканирования ситуации с целью упреждающего смягчения возникающих трендов мошенничества, создание функций, средств контроля и правил защиты учетных записей, а также предупреждающих сообщений в антивирусном ПО о потенциальных фишинговых сайтах (см. Приложение В, где собраны удачные примеры внедрения финансовыми регуляторами требований по борьбе с мошенничеством наряду с контролем ПОД/ФТ).

76. Другим положительным опытом является поощрение ФУ к внедрению мониторинга транзакций в режиме реального времени для выявления и предотвращения мошеннических или незаконных действий в режиме онлайн. Отслеживая

аномальную информацию о владельцах счетов (например, физические, IP- и электронные адреса, номера мобильных телефонов и т.д.) и транзакции в режиме реального времени, ФУ могут быстро выявлять, расследовать и сообщать о любой необычной или подозрительной деятельности.

77. Мониторинг транзакций в режиме реального времени, предполагающий использование сложного программного обеспечения и алгоритмов для отслеживания финансовых операций, считается эффективным средством обнаружения и предотвращения КМ. В условиях информационного потока, вызванного цифровизацией, выявление КМ может быть затруднено ручными методами. Мониторинг операций в режиме реального времени может помочь финансовым учреждениям выявить и расследовать подозрительную активность по нескольким счетам или операциям, даже если эти счета или операции не связаны напрямую, что позволит предотвратить будущие преступления[23].

Устранение преступных инструментов

78. Поскольку КМ может осуществляться и в нетрадиционных секторах (см. раздел 3.3. выше), некоторые юрисдикции усилили меры по предотвращению мошенничества и контролю в таких нетрадиционных секторах. В частности, они направлены на устранение инструментов КЭФ, например, через отключение мобильных линий и мошеннических веб-страниц, используемых преступниками, фильтрацию фишинговых сообщений и вредоносных веб-ссылок и т.д.

Вставка 37. Устранение подозрительных веб-сайтов и фишинговых кампаний

В Саудовской Аравии правоохранительные и регулирующие органы сотрудничают с операторами связи, что значительно расширяет их возможности по прогнозированию, предотвращению, обнаружению и эффективному реагированию на мошеннические действия. Для борьбы с криминальными структурами Национальное управление кибербезопасности Саудовской Аравии ввело жесткие требования к защите брендов, направленные на противодействие сайтам-клонам и фишинговым сообщениям на социальных платформах. Кроме того, Центральный банк Саудовской Аравии (SAMA) создал надежные системы кибербезопасности и противодействия мошенничеству, определяющие обязательные базовые контрольные требования для регулируемых организаций. Данные механизмы направлены на проактивную защиту от возникающих угроз мошенничества, тем самым обеспечивая стабильность и безопасность финансового сектора королевства.

Ключевым аспектом указанных национальных и нормативных требований является проактивный мониторинг преступных инструментов со стороны организаций. Это предполагает постоянное наблюдение за потенциальными мошенническими действиями, такими как подозрительные веб-сайты и фишинговые кампании, с помощью современных технологий и мер по защите бренда, применяемых организациями.

[23] Более подробную информацию о том, как технологии могут быть использованы в целях ПОД/ФТ, можно найти в отчете ФАТФ (июль 2021 г.) «Возможности и проблемы новых технологий в целях ПОД/ФТ».

При обнаружении таких действий оперативно информируются соответствующие органы. Своевременное уведомление обеспечивает оперативное принятие мер по расследованию и пресечению преступных операций, предотвращая дальнейший ущерб и снижая последствия мошеннических действий.

Источник: Саудовская Аравия

Предотвращение распыления активов

79. Во многих юрисдикциях одним из наиболее сложных аспектов расследований, связанных с КМ, является высокая скорость отмывания доходов от КМ. По общему мнению, для компетентных органов крайне важно иметь возможность оперативно вмешаться и установить контроль над доходами от КМ до того, как они исчезнут с различных банковских счетов. Юрисдикции применяют различные меры для более эффективного возврата активов, связанных с КМ (см. раздел 5.1 ниже).

80. Кроме того, целесообразно привлекать ключевых представителей частного финансового сектора для содействия и поощрения их активного перехвата незаконных средств после получения уведомления о мошенничестве от пострадавшего клиента до обращения компетентных органов. Это включает обмен информацией между национальными и зарубежными ФУ или ПУВА (см. также вставку 41 ниже).

Вставка 38. Бюллетень Группы «Эгмонт» о BEC-мошенничестве

В июле 2019 г. Группа «Эгмонт» выпустила бюллетень, в котором предупредила входящие в нее ПФР и их юрисдикции о растущей угрозе BEC-мошенничества, представив основные сценарии и риск-индикаторы, связанные с BEC. Кроме того, в бюллетене было указано, каким образом финансовые учреждения (ФУ) могут способствовать выявлению, предотвращению и информированию о случаях BEC-мошенничества за счет расширения взаимодействия и сотрудничества между своими внутренними подразделениями по ПОД, коммерческой деятельности, предотвращению мошенничества и кибербезопасности.

Для содействия расследованию инцидентов, связанных с BEC, и возврату средств потерпевших финансовым учреждениям-получателям, получившим информацию о том, что на счет одного из их клиентов был осуществлен мошеннический перевод (например, сообщение SWIFT recall), рекомендовано не проводить никаких операций, которые могут привести к потере средств, и обратиться в правоохранительные органы или ПФР для оценки правомерности полученной транзакции.

Источник: Группа «Эгмонт»

5. Международное сотрудничество и возврат активов

81. Как уже говорилось ранее, юрисдикция, в которой происходит КМ (т.е. где обычно находится жертва), как правило, отличается от юрисдикции, в которой отмываются доходы. Это может привести к трудностям в проведении трансграничных расследований и эффективном международном сотрудничестве для успешного получения информации и доказательств, ликвидации синдикатов КМ и возврата незаконных доходов. Например, в юрисдикции, где отмывались доходы, связанные с КМ, могут возникнуть трудности с идентификацией каждой жертвы, связанной со счетом ОД, поскольку они могут быть распределены по нескольким юрисдикциям.

82. Децентрализованный характер КМ создает дополнительные сложности. Могут возникнуть несоответствия в приоритетах юрисдикций в области международного сотрудничества, например, в случаях, когда жертвы юрисдикции А переводят деньги в юрисдикцию Б, а жертвы юрисдикции Б находятся в юрисдикции С (т.е. для юрисдикции А приоритетным может быть сотрудничество с юрисдикцией Б, а для юрисдикции Б – сотрудничество с юрисдикцией С). Необходимость задействования множества заинтересованных сторон и партнеров, как государственных, так и частных, за рубежом также затрудняет выявление и отслеживание незаконных средств.

    - Синдикаты КМ используют различные финансовые услуги и классы активов. Транзакции могут осуществляться практически мгновенно через границы между различными провайдерами и секторами. Это затрудняет отслеживание и атрибуцию переводов средств.

    - Кроме того, соответствующие цифровые криминалистические доказательства могут находиться в разных юрисдикциях, что затрудняет составление полной картины деятельности преступных синдикатов и отмывания доходов. Ситуация осложняется еще и тем, что цифровые криминалистические доказательства нестабильны и могут быть легко потеряны, если их не сохранить в кратчайшие сроки.

83. Официальное сотрудничество, включая взаимную правовую помощь, как правило, занимает много времени. Учитывая стремительный характер цифровых преступлений и связанной с ними деятельности по ОД (когда доказательства могут быстро исчезнуть, если их не сохранить), расчет на официальное сотрудничество может привести к значительному снижению эффективности. Для того чтобы не терять оперативности в оказании трансграничной помощи для успешного пресечения преступной деятельности, связанной с КМ, компетентные органы все чаще полагаются на неформальные механизмы сотрудничества, обмениваясь информацией напрямую со своими зарубежными коллегами. Это может происходить на уровне правоохранительных органов или ПФР по различным каналам, включая Защищенную сеть «Эгмонт», Интерпол I-24/7, а также другие неформальные сети, такие как Камденская межведомственная сеть по возврату активов (CARIN) и региональные межведомственные сети по возврату активов (ARINs).

Вставка 39. Перехват доходов от КМ через неформальные многосторонние сети

Для борьбы с ростом случаев КМ французские следственные органы активно используют неформальные сети для эффективного международного сотрудничества и соответствующего возврата активов, среди которых подсеть Европейских офисов по возврату активов (AROs) Камденской межведомственной сети по возврату активов (CARIN). Французский ARO тесно сотрудничает с членами этих двух сетей, которые позволяют быстро обмениваться информацией между правоохранительными органами и ПФР, специализирующимися на розыске, аресте и конфискации преступных активов, особенно в экстренных случаях, когда ответы на запросы поступают в течение 8 часов. Такое сотрудничество позволяет быстро сохранить средства на первоначально выявленном счете назначения и на всех последующих многоуровневых счетах.

Так, в 2022 г. французский ARO связался со словацким ARO в связи с мошенническим банковским переводом на сумму 1 875 000 евро в ущерб французской компании-жертве и попросил заморозить эти средства на банковском счете получателя в Словакии. Обмен информацией между двумя офисами ARO позволил заморозить средства, а словацким властям - получить всю информацию, необходимую для составления и исполнения судебного запроса о замораживании. В итоге сумма в размере 1 874 907 фунтов стерлингов была заморожена и впоследствии возвращена пострадавшей компании.

Источник: Франция

84. Для достижения максимальной эффективности при расследовании ОД, связанного с КМ, и возврате доходов сотрудничество должно носить не двусторонний, а многосторонний характер. В данном разделе рассматриваются проблемы и примеры передовой практики в области международного взаимодействия по двум оперативным направлениям: (i) возврат активов и (ii) правоприменение и судебное преследование.

5.1. Возврат активов

85. Одной из основных проблем при возврате активов от КМ является быстрый темп отмывания. Для снижения этой проблемы существуют многосторонние программы «быстрого реагирования», созданные различными организациями для отслеживания и возврата доходов от КМ, включая Глобальную программу быстрого вмешательства в платежи Интерпола (I-GRIP), Проект BEC Группы «Эгмонт» и Цепь уничтожения финансовых мошенников (Financial Fraud Kill Chain) США. Опыт этих организаций показывает, что вмешательство наиболее эффективно в течение 24-72 часов после совершения мошеннической операции. Подобная практика позволяет снизить риск распыления средств по нескольким последующим слоям, что значительно сужает рамки расследования ОД и облегчает возврат незаконных доходов.

Вставка 40. Цепь уничтожения финансовых мошенников и Группа по возврату активов

Цепь уничтожения финансовых мошенников (FFKC) была создана ФБР и Сетью по борьбе с финансовыми преступлениями (ПФР США) в 2016 г. в ответ на рост числа схем компрометации деловой электронной почты. В рамках FFKC оказывается содействие в возврате международных электронных переводов, отправленных в результате мошеннических схем, за счет использования связей ФинСЕН с Группой подразделений финансовой разведки «Эгмонт». Этот процесс может быть реализован только в том случае, если мошеннический электронный перевод отвечает следующим критериям: (1) сумма перевода составляет 50 000 долларов США и выше; (2) перевод является международным; (3) инициировано уведомление об отзыве SWIFT; (4) перевод был осуществлен в течение последних 72 часов.

В 2018 г. Центр жалоб на интернет-преступления (IC3) ФБР создал Группу по возврату активов (Recovery Asset Team, RAT) для устранения уязвимостей в электронных переводах внутри страны. RAT упрощает взаимодействие с финансовыми учреждениями и оказывает помощь местным отделениям ФБР в замораживании средств при внутренних переводах, осуществленных под обманным предлогом. RAT добился значительных успехов, заморозив на сегодняшний день 73% средств, о которых IC3 сообщила как о мошеннических (433,3 млн. долл. из 590,62 млн. долл.). Как показывает пример из практики США, в некоторых случаях эта программа позволяет быстро выявить подставные счета и заморозить средства, что делает возможным их полное возвращение.

Источник: США

86. В основном такие многосторонние программы нацелены на выполнение двух задач: сбор минимального объема информации, необходимого для действий правоохранительных органов, и передача этой информации в «правильные руки». Для обеспечения эффективного трансграничного реагирования все узлы многосторонних сетей также устанавливают правила и процедуры управления. Хотя такие многосторонние сети обычно носят глобальный характер, региональные инициативы также могут быть полезны для решения задач, опираясь на уже налаженное региональное сотрудничество.

Вставка 41. Международный проект по борьбе с мошенничеством

Учитывая трансграничный характер мошенничества, в рамках Консультативной группы финансовой разведки (FICG)[1] была разработана региональная инициатива под названием «Международный проект по борьбе с мошенничеством» (Multi-jurisdictional Anti-Fraud Project). Эта инициатива, возглавляемая совместно ПФР Малайзии, Индонезии и Сингапура, направлена на выявление, отслеживание и возврат средств пострадавшим.

Создан механизм реагирования на трансграничные операции между странами-членами FICG. Данный проект позволит членам FICG быстро и легко обмениваться финансовой разведывательной информацией, что обеспечит оперативность действий властей по борьбе с мошенничеством и возврату похищенных средств.

Источник: Малайзия

[1] FICG — это региональная организация, объединяющая ПФР стран Юго-Восточной Азии, Новой Зеландии и Австралии.

Трансграничный сбор и обмен информацией: «сбор минимального объема информации»

87. КМ является одной из форм мошенничества и в соответствии с Рекомендацией 3 ФАТФ должно квалифицироваться как предикат к ОД. Кроме того, в отличие от традиционных форм мошенничества, совершаемых между знакомыми, когда трудно отличить мошенничество от потенциальных гражданских споров между должником и кредитором, в случаях с КМ, в которых мошенничество, как правило, совершается между незнакомыми людьми, относительно легче установить преступность prima facie. Это уменьшает необходимость в длительном запросе о помощи для формулирования и определения криминальной связи, как это обычно требуется для других видов преступлений (которые не признаются предикатным преступлением во всем мире).

88. В качестве положительного примера можно привести использование шаблонов в различных программах быстрого реагирования для ускорения сбора и обмена информацией. Шаблоны позволяют быстро собрать минимальный объем информации, необходимый для установления факта преступления. Это помогает сконцентрировать усилия подразделений быстрого реагирования на важнейших видах доказательств или информации, которую необходимо получить на начальных этапах рассмотрения уголовного дела. Кроме того, подобные шаблоны позволяют снизить риски, связанные с качеством обмениваемой информации, и улучшить трансграничное реагирование правоохранительных органов.

89. В дополнение к краткому описанию фабулы преступления КМ шаблоны обычно направлены на получение основных данных, необходимых для продвижения усилий по отслеживанию средств. Стандартизация запросов позволяет запрашиваемым юрисдикциям быстро обрабатывать любые поступающие запросы, ускоряя возможности правоохранительных органов по перехвату незаконных средств, попавших в их юрисдикцию.

90. Поля данных в шаблонах могут включать информацию о счетах инициатора и бенефициара, а также информацию о транзакции (дата, время, суммы перевода).

Для повышения эффективности шаблоны могут также включать информацию о следующем пункте назначения средств, если средства уже были переведены со счета бенефициара. Кроме того, целесообразно свести к минимуму любые ограничения для юрисдикций по распространению любой информации, которой они обмениваются с соответствующими компетентными органами внутри страны после ее получения.

Вставка 42. I-GRIP Интерпола

Интерпол разработал Глобальный протокол быстрого вмешательства в платежи (I-GRIP), являющийся международным механизмом прекращения платежей, который позволяет странам-членам подавать и обрабатывать запросы на отслеживание, перехват или временное замораживание незаконных доходов от КМ. Данный механизм, получивший название I-GRIP, первоначально был опробован в пилотном режиме как Протокол быстрого реагирования по борьбе с отмыванием денег (ARRP) в 2022 г. и официально запущен в ноябре 2022 г. благодаря многочисленным успешным случаям остановки платежей в ходе пилотной фазы.

I-GRIP способствует оперативной связи между национальными центральными бюро (НЦБ) Интерпола с целью недопущения перевода подозрительных незаконных активов между странами-участницами. Запросы, направляемые через I-GRIP, должны содержать достаточно подробную информацию, на основании которой принимающее НЦБ может принять соответствующие меры, а именно: дату операции, валюту и сумму, номера счетов и названия финансовых учреждений на счетах получателя и отправителя.

Источник: Интерпол

91. Кроме того, стандартизированные поля данных в шаблонах позволяют международным организациям с централизованными возможностями легко анализировать данные и максимально эффективно проводить расследования и возвращать активы. Например, Интерпол использует информацию, передаваемую по его каналам, для создания внутренней базы данных – Аналитического файла по финансовым преступлениям (FINCAF) – с целью облегчения анализа оперативной информации транснационального масштаба о различных видах финансовых преступлений и выявления связей между трансграничными делами и расследованиями, угрозами, криминальными тенденциями и преступными сетями (см. также вставку 45 ниже).

92. Для дальнейшего ускорения действий по возврату активов некоторые юрисдикции предоставили иностранным потерпевшим возможность подавать жалобу на КМ ннапрямую в свои правоохранительные органы, в том числе через свою онлайн-платформу отчетности, чтобы напрямую фиксировать необходимые поля данных для принятия мер по принудительному взысканию (см. раздел «Информация от потерпевших» выше). Это устраняет дополнительный уровень коммуникации и позволяет компетентным органам оперативно принимать любые доступные меры в отношении подозрительных операций, совершенных по счетам бенефициаров в их юрисдикции.

Необходимые полномочия для действий: «правильные руки»

93. Поскольку скорость имеет первостепенное значение, любая собранная информация в идеале должна напрямую передаваться органам, уже обладающим соответствующими полномочиями и опытом для поиска и возврата активов. Таким образом, по получении запроса можно сразу же принять обеспечительные меры, чтобы предотвратить дальнейшее отмывание или распыление активов. Тем самым правоохранительные органы получают жизненно важное время, необходимое для продолжения расследования, разработки и сбора доказательств и последующего направления официальных запросов о ВПП.

Вставка 43. Запрос об отсрочке платежа от подотчетного лица

В ПФР Италии поступил запрос об отсрочке от обязанной организации в связи с четырьмя подозрительными электронными переводами на сумму 490 000 евро. Транзакции осуществлялись по поручению итальянской компании, занимающейся оптовой торговлей одеждой, для различных фирм в одной из стран Дальневосточной Азии.

Подотчетная организация посчитала эти четыре транзакции подозрительными, поскольку средства были получены из входящих переводов, которые были отозваны банком-заказчиком на основании того, что средства были отправлены в результате «мошенничества генерального директора» одной из западноевропейских компаний-жертв. ПФР Италии также получило спонтанное информирование от ПФР указанной западноевропейской страны. Кроме того, в ПФР поступило сообщение о возможной связи итальянской компании со схемами мошенничества с НДС, в которых участвовала указанная азиатская страна через отдельную восточноевропейскую страну, что еще раз указывает на связи между КМ и другими видами организованной преступности.

Операции были успешно отложены. Это позволило иностранным властям выдать постановление о наложении ареста для возврата средств в Италию.

Источник: Италия

94. Однако такое прямое взаимодействие может быть сопряжено с трудностями, обусловленными различиями в законодательной и правоприменительной базе разных юрисдикций. Некоторые успешные практики по решению данных проблем включают создание внутренних координационных механизмов для облегчения передачи запросов в соответствующие органы, а также использование каналов сотрудничества между государственным и частным секторами и возможность ФУ добровольно принимать временные меры после получения от компетентных органов информации о подозрительных операциях.

Руководство и правила: «коллективное соглашение»

95. Управление и правила для многосторонних структур обеспечивают гарантии и обязательства по взаимному распознаванию преступной деятельности и оперативным действиям при получении информации. Благодаря этому удается преодолеть проблему несовпадения приоритетов международных агентств, по-

скольку условия присоединения и оказания помощи были согласованы заранее. Как показывает практика, эти правила и критерии должны быть четкими и понятными.

96. Указанные принципы применимы не только к неформальным, но и к формальным механизмам международного сотрудничества. В качестве примера можно привести Регламент (ЕС) 2018/1805 Европейского парламента и Совета, который позволяет взаимно признавать иностранные постановления о замораживании и конфискации. Подобный механизм прямого исполнения позволяет оперативно осуществлять трансграничное вмешательство.

97. Ускорение информационного обмена не должно происходить в ущерб защите и конфиденциальности данных. Чтобы обеспечить безопасность передаваемой информации, многосторонние структуры обычно используют существующие защищенные каналы связи, такие как Интерпол, Европол и Группа «Эгмонт». Наличие таких защищенных каналов связи позволяет многосторонним структурам свободно расширяться, поскольку отпадает необходимость в создании двусторонних каналов связи.

Вставка 44. Проектная группа Группы «Эгмонт» по BEC-мошенничеству

С целью противодействия растущей и серьезной угрозе, исходящей от BEC для финансовых институтов и их клиентов, 11 ПФР создали «Проектную группу Группы "Эгмонт" по BEC-мошенничеству», которая занимается анализом тенденций, индикаторов и методологий BEC, а также обменом ключевыми выводами с ПФР. Общая финансовая типология и примеры из практики показывают, что наиболее эффективным способом борьбы с этим видом преступлений является оперативное реагирование, направленное на пресечение и отслеживание электронных переводов.

В этой связи Проектной группой были разработаны протоколы между правоохранительными органами и ПФР, а также между иностранными ПФР для отслеживания и замораживания доходов от BEC-мошенничества.

- При получении СПО, относящегося к подозрительным трансграничным потокам BEC, направляющее ПФР разрабатывает запрос «быстрого реагирования» в принимающее ПФР.
- Запрос должен содержать согласованные основные данные и информацию, необходимые для обмена в целях правоприменения.
- От принимающего ПФР требуется принять (по возможности) незамедлительные меры по приостановке и возврату незаконных доходов, в идеале – в течение 72 часов после совершения преступления.

Для обмена запросами «быстрого реагирования» в рамках проекта BEC используется защищенная платформа связи Группы «Эгмонт».

Источник: Группа «Эгмонт»

5.2. Правоприменение и судебное преследование

98. Помимо возврата активов, транснациональный характер КФ также привел к возникновению трудностей на всех этапах правоприменительного процесса – от сбора оперативной информации и проведения расследования до сбора доказательной базы для судебного преследования. Развитие технологий увеличило скорость проведения транзакций и способствовало проведению разрозненных трансграничных операций. Кроме того, это увеличило время и усилия, необходимые правоохранительным органам для их отслеживания и идентификации.

Сбор цифровых доказательств

99. Несмотря на отсутствие прямой связи с ОД, цифровые криминалистические доказательства могут дать критически важные подсказки, которые помогут правоохранительным органам продолжить расследование ОД. Широкое распространение и простота использования услуг по сокрытию личных данных, таких как VPN, еще больше осложняют работу по поиску конечных исполнителей КМ.

100. К сожалению, в настоящее время не существует единого глобального режима, регулирующего продолжительность хранения цифровых данных, в том числе в отношении провайдеров технических услуг. Несколько юрисдикций отметили значительный риск утечки цифровых доказательств. Задержки в создании официальных механизмов сотрудничества также создают проблемы для оперативного получения цифровых доказательств.

101. Существует несколько эффективных методов, позволяющих смягчить эти проблемы.

- **Использование неформальных каналов** для сбора и обеспечения безопасности оперативной информации. После этого используются официальные каналы сотрудничества для получения необходимых доказательств и заявлений для подготовки судебного разбирательства.
- Такие **конвенции и инструменты расследования,** как Конвенция по киберпреступности, известная также как Будапештская конвенция, позволяют оперативно сохранять электронные данные и передавать спонтанную информацию, что способствует более быстрому выявлению конечных исполнителей КМ. Кроме того, в соответствии с Будапештской конвенцией создается круглосуточная сеть, обеспечивающая немедленную помощь следствию в предоставлении технических консультаций, сборе доказательств, сохранении данных и т.д.
- **Прямое сотрудничество** с иностранными провайдерами услуг для получения необходимых криминалистических доказательств, таких как информация об абонентах, без прохождения процедуры ВПП. По мнению одной из юрисдикций, прямое добровольное сотрудничество с иностранным провайдером услуг является наиболее эффективным механизмом сбора соответствующих цифровых доказательств[24].

[24] Дополнительную информацию о добровольном сотрудничестве с иностранными провайдерами услуг см. также в публикации Совета Европы (июль 2020 г.) «Будапештская конвенция о киберпреступности: преимущества и влияние на практике».

Вставка 45. Будапештская конвенция

Будапештская конвенция устанавливает процессуальные полномочия для: ускоренного сохранения хранимых данных, ускоренного сохранения и частичного раскрытия данных о трафике, выдачи ордера на производство, обыска и ареста компьютерных данных, сбора данных о трафике в режиме реального времени и перехвата данных о контенте. Конвенция также обеспечивает быстрый и эффективный режим международного сотрудничества.

Второй дополнительный протокол к Конвенции о киберпреступности, касающийся расширения сотрудничества и раскрытия электронных доказательств, также обеспечивает правовую основу для раскрытия информации о регистрации доменных имен и прямого сотрудничества с поставщиками услуг для получения информации об абонентах, эффективные средства получения информации об абонентах и данных трафика, немедленное сотрудничество в чрезвычайных ситуациях, инструменты взаимной помощи, а также гарантии защиты персональных данных.

Источник: Совет Европы

Совместные правоприменительные действия

102. Трансграничные совместные следственные группы (ССГ) представляют собой юридическое соглашение между компетентными органами двух или более юрисдикций с целью проведения уголовных расследований. Они могут содействовать обмену информацией и трансграничному отслеживанию финансовых потоков. Как правило, информационный обмен осуществляется на основе различных рамочных программ и соглашений (например, Евроюст, Объединенная целевая группа по борьбе с киберпреступностью при поддержке Европола).

103. Кроме того, ССГ являются важным координационным центром для многосторонних правоприменительных действий против КМ, учитывая их транснациональный и децентрализованный характер. Благодаря снижению препятствий для преступной деятельности синдикаты КМ могут легко перемещаться и создавать новые цифровые центры операций в удаленных местах. В этой связи необходимо координировать действия для одновременного пресечения деятельности различных подгрупп (которые могут действовать на территории нескольких юрисдикций).

Вставка 46. Совместные действия против крупномасштабного инвестиционного мошенничества[1]

Сербия совместно с Австрией, Болгарией и Германией при поддержке Евроюста приняла участие в успешных операциях против двух организованных преступных групп, подозреваемых в крупномасштабном инвестиционном мошенничестве в сфере киберторговли. Власти Сербии арестовали пятерых подозреваемых и провели обыски в девяти местах, изъяв пять квартир, три автомобиля, значительную сумму наличных денег и ИТ-оборудование. Под наблюдением оказались также более 30 счетов в сербских банках. Кроме того, четверо подозреваемых были арестованы в Болгарии, а 2,5 млн евро были заморожены на банковском счете компании, участвовавшей в мошеннической схеме в Германии.

На основе информации, полученной в ходе этой операции, через два дня власти быстро провели еще одну операцию против одной из компаний в Белграде, арестовав одного подозреваемого и изъяв серверы, другое ИТ-оборудование и документы.

В данном случае сербские власти, в частности, воспользовались статьей 26 Будапештской конвенции (Спонтанная информация) для обмена информацией с другими партнерами. Евроюст оказал дальнейшее содействие расследованию, профинансировав работу совместной следственной группы (ССГ), а также организовав координационное совещание в своих помещениях в Гааге и видеоконференцию.

Источник: Сербия; Совет Европы (июль 2020 г.) Будапештская конвенция о киберпреступности: преимущества и влияние на практике

[1] Более подробную информацию см. также в пресс-релизе Евроюста (апрель 2020 г.): https://www.eurojust.europa.eu/news/action-against-large-scale-investment-fraud-several-countries.

104. При этом совместные действия по обеспечению соблюдения законодательства сопряжены с определенными трудностями.

- **Правовые барьеры** могут ограничивать неформальный обмен информацией даже в рамках совместных следственных групп. В одной из юрисдикций было отмечено, что для обмена информацией все еще приходится полагаться на запросы о взаимной правовой помощи, что может снижать эффективность и вовлеченность. Кроме того, могут существовать ограничения на обмен информацией, особенно в отношении детализации информации о финансовых операциях.
- **Неодинаковые возможности и приоритеты** также могут препятствовать участию юрисдикций в совместных действиях. Как отмечалось ранее, внутренние приоритеты могут не совпадать с совместными действиями, и юрисдикции могут столкнуться с проблемой балансирования этих интересов в условиях ограниченности ресурсов, несмотря на рост КМ.

105. В дополнение к ССГ совместные операции, организуемые многосторонними организациями, такими как Интерпол, также являются важным координационным центром для многосторонних действий по борьбе с КМ. Хотя такие операции могут быть более неформальными, чем ССГ, в отсутствие официальных юридических соглашений, они все же могут служить важной платформой для совместных действий соответствующих юрисдикций по противодействию КМ.

Вставка 47. Операция Интерпола HAECHI

С 2020 г. Интерпол проводит ежегодную операцию HAECHI, направленную на борьбу с финансовыми преступлениями в киберпространстве и связанным с ними ОД, и поддерживает обмен информацией между участвующими юрисдикциями. В рамках последней операции HAECHI III (2022 г.), в которой приняли участие 30 юрисдикций, было арестовано почти 1 000 подозреваемых и заблокировано 2 800 банковских счетов и счетов виртуальных активов, связанных с незаконными доходами в размере 130 млн. долл. В рамках HAECHI III Интепрол координировал многочисленные дела между странами-участницами для совместной борьбы с КМ.

Операция HAECHI также послужила платформой для FINCAF, который собирает информацию из различных источников и выявляет связи между расследованиями, ведущимися в разных странах-участницах. Структура FINCAF позволяет включать данные и другие элементы информации, относящиеся к любым видам финансовых преступлений и преступлений, имеющих транснациональный характер. Интерпол использует FINCAF для взаимодействия со странами-членами с целью усиления общих тактических мер борьбы с международной организованной преступностью, такой как КМ. FINCAF является важным инструментом, позволяющим получить более полное представление о трансграничной преступной деятельности, преступных организациях, их групповых структурах, индивидуальных ролях и ключевых лицах, методах деятельности и мошеннических финансовых операциях.

Источник: Интерпол

Государственно-частное сотрудничество

106. Сотрудничество между государственным и частным секторами может выходить за пределы национальных границ, что позволяет добиться больших результатов, учитывая транснациональный охват КМ. Подобно национальным ГЧП, такое сотрудничество может охватывать типологии или стратегический обмен, а также оперативную координацию. Состав таких партнерств также зависит от целей и может включать как традиционные для ПОД/ФТ, так и нетрадиционные сектора.

Вставка 48. Европейская программа по борьбе с денежными мулами

Европейская программа по борьбе с денежными мулами – это международная операция, в основе которой лежит обмен информацией между государственным и частным секторами для противодействия сложным современным преступлениям.

В 2022 г. при постоянной координации Европейской банковской федерации около 1800 банков и финансовых учреждений оказали содействие правоохранительным органам в проведении данной операции, наряду с онлайн-сервисами денежных переводов, криптовалютными биржами, финтех- и ЗСК-компаниями, а также транснациональными корпорациями компьютерных технологий.

В операции участвовали правоохранительные органы из 25 юрисдикций[1], а также Европол, Евроюст и Интерпол. Было выявлено 8 755 денежных мулов, а также 222 вербовщика. В общей сложности было перехвачено 17,5 млн евро и арестовано 2 469 денежных мулов.

Источник: Европол

[1] Австралия, Австрия, Болгария, Великобритания, Венгрия, Гонконг (Китай), Греция, Ирландия, Испания, Италия, Кипр, Колумбия, Молдова, Нидерланды, Польша, Португалия, Румыния, Сингапур, Словацкая Республика, Словения, США, Чешская Республика, Швейцария, Швеция, Эстония

6. Заключение и приоритетные направления

107. КМ совершается транснациональными организованными преступными синдикатами. Как ожидается, масштабы и объем КМ будут расти по мере усиления тенденции цифровизации и распространения виртуальных услуг по всему миру. Юрисдикции также должны помнить о дополнительных уязвимостях в различных секторах, включая цифровые финансовые институты и нетрадиционные сектора, которые преступники могут использовать для совершенствования методов КМ и ОД благодаря растущей цифровизации.

108. Юрисдикции должны сосредоточиться на преодолении разрозненности для ускорения и расширения сотрудничества между различными секторами и организациями как на национальном, так и на международном уровнях. Вследствие децентрализованного характера КМ и связанного с ним ОД жизненно важная финансовая информация и доказательства часто разрознены в разных местах. В результате затрудняются усилия по расследованию и ликвидации синдикатов КМ, а также по отслеживанию и возврату доходов от КМ.

109. КМ может иметь значительные и катастрофические финансовые последствия для жертв. Но последствия не ограничиваются денежными потерями; они могут иметь разрушительные социальные и экономические последствия. Выводы, сделанные в настоящем отчете, указывают на три приоритетные области, в которых юрисдикции должны действовать для более эффективной борьбы с КМ и связанным с ним ОД: усиление координации на национальном уровне; поддержка многостороннего сотрудничества; усиление мер по выявлению и пресечению.

Приоритетные направления эффективного противодействия КМ и связанному с ним ОД

Усиление внутренней координации между государственным и частным секторами

- Юрисдикции должны разработать координационные механизмы, объединяющие усилия соответствующих компетентных органов для комплексного противодействия КМ и отмыванию доходов от данной деятельности. Это касается как технических специалистов по киберпреступности, так и представителей нетрадиционных секторов, таких как платформы социальных сетей, электронная торговля, телекоммуникации и интернет-провайдеры. Юрисдикции также должны использовать партнерские отношения между государственным и частным секторами для повышения эффективности выявления и расследований, а также ускорения оперативных мер по возврату активов.
- Эффективная практика предполагает создание специального централизованного подразделения, которое может собирать необходимую информацию и координировать действия различных государственных и частных структур, включая проведение расследований, возврат активов и предотвращение мошенничества.

Поддержка многостороннего международного сотрудничества

- Чтобы повысить эффективность возврата активов и избежать утечки доходов от КМ, юрисдикции должны совместно работать над оперативным перехватом доходов от КМ. Оперативный опыт показывает, что вмешательство, как правило, наиболее эффективно в течение 24-72 часов после возникновения факта КМ. Для эффективного отслеживания и возврата доходов от КМ, которые отмываются и распределяются в разных юрисдикциях, необходим глобальный единый подход.
- Для этого юрисдикции должны использовать и поддерживать существующие (и любые будущие) многосторонние механизмы (такие как I-GRIP Интерпола и проект BEC Группы «Эгмонт») для быстрого международного сотрудничества и обмена информацией в целях борьбы с КМ. Такие многосторонние механизмы также позволяют юрисдикциям сотрудничать и коллективно ликвидировать транснациональные синдикаты КМ.

Усиление мер по выявлению и пресечению

- Для повышения эффективности выявления подозрительных операций юрисдикции должны обеспечить простоту представления информации пострадавшим, например, с помощью специальных платформ, позволяющих упорядочить представление информации. Юрисдикции также должны сотрудничать с частным сектором для улучшения отчетности о подозрительных операциях.
- Юрисдикции должны способствовать повышению осведомленности и бдительности в отношении КМ путем просвещения населения, в том числе для распространения информации о признаках КМ и повышения киберграмотности. Профилактика играет ключевую роль в снижении общей доходности синдикатов КМ. Юрисдикции также могут сотрудничать с частным сектором для поддержки стратегий предотвращения КМ, таких как защита потребителей и устранение преступных инструментов.

Приложение 1: риск-индикаторы КМ

Приведенные ниже потенциальные риск-индикаторы основаны на опыте и данных, полученных от юрисдикций, входящих в Глобальную сеть ФАТФ, Группу «Эгмонт» и частный сектор. Данные индикаторы направлены на повышение эффективности выявления подозрительных операций, связанных с КМ. Перечень классифицирован по различным направлениям – от открытия счета до мониторинга операций. Индикаторы могут быть актуальны для регулируемых организаций, включая ФУ, ПУВА, УНФПП и другие финансовые и платежные учреждения.

Наличие одного индикатора в отношении клиента или операции само по себе не может служить основанием для подозрений в совершении преступления, связанного с КМ, равно как и не обязательно является четким указанием на такую деятельность. Однако он может послужить поводом для дальнейшего мониторинга и проверки в случае необходимости.

Характер операций

- Быстрые или незамедлительные операции с большими или малыми суммами после открытия счета, не соответствующие его назначению.
- Быстрое или немедленное снятие наличных или перевод крупных сумм после получения перевода средств с целью опустошения счета.
- Частые и крупные операции, не соответствующие экономическому профилю владельца счета (например, внезапные международные переводы, снятие наличных денег с использованием платежных карт в иностранных банкоматах, приобретение в больших объемах ВА или товаров для вывоза за рубеж, платежи в пользу нелицензированных иностранных УПДЦ).
- Переводы средств в юрисдикции с высоким риском отмывания денег и из них.
- Крупные частые операции с недавно созданными компаниями и/или чья основная деятельность не совпадает с деятельностью, осуществляемой бенефициаром, или имеет общую цель.
- Небольшие платежи в пользу бенефициара, за которыми после успешного завершения быстро следуют платежи в пользу того же бенефициара на более крупную сумму.
- Частые и/или крупные покупки на круглую сумму, что может свидетельствовать о покупке подарочных карт.

Инструкции и комментарии к клиентской операции

- Клиентская транзакция запрашивает дополнительные платежи сразу после успешного платежа на счет, который ранее не использовался клиентом для оплаты услуг своих поставщиков/продавцов. Такое поведение может быть характерно для преступника, пытающегося провести дополнительные несанкционированные платежи, узнав об успешном проведении мошеннического платежа.
- Кажущиеся законными инструкции по транзакциям клиента отличаются по языку, срокам и суммам от ранее проверенных инструкций по транзакциям.

- Инструкции по проведению операций содержат пометки, утверждения или формулировки, обозначающие запрос на проведение операции как «Срочный», «Секретный» или «Конфиденциальный».
- В качестве обоснования операции клиент представляет плохо оформленные сообщения/электронные письма (орфографические и/или грамматические ошибки).
- Инструкции по проведению операции направляют платеж известному бенефициару, однако информация о счете бенефициара отличается от той, которая использовалась ранее.
- Предполагаемый бенефициар в описании операции и имя владельца счета, известное банку-получателю, не совпадают.
- Переводы, заказанные физическими лицами (предполагаемыми инвесторами), не обладающими финансовым опытом и знаниями, в пользу компаний (во многих случаях, созданных в юрисдикциях с высоким уровнем риска), у которых основания для платежей связаны с инвестициями и финансовыми продуктами.
- Несоответствие контрагентов наименованию предприятия/компании, указанной на счете, что может служить прикрытием для перемещения крупных сумм средств в международном масштабе (например, компания, указанная как мебельная, осуществила многократный крупный перевод в адрес компании, указанной как нефтетрейдинговая).
- Операции, проводимые при несовпадении часовых поясов устройств.

Подозрения в отношении владельца счета

- Владелец счета не желает или не может пройти проверку НПК.
- Владелец счета не знает об источнике средств, проходящих по его счету, или утверждает, что совершает операции от чужого имени.
- Частая смена названий юридических лиц/индивидуальных предпринимателей с использованием иностранных выражений и терминологии.
- Клиент демонстрирует недостаточную осведомленность о характере, предмете, сумме или цели операции/операций или отношений либо дает нереальные, запутанные или непоследовательные объяснения, что вызывает подозрение, что клиент выступает в роли мула.

Подозрение в личности пользователя счета

- Пользователь пытается скрыть свою личность, используя общие, фальсифицированные, украденные или измененные идентификационные данные (адрес, номер телефона, электронная почта).
- Частая смена контактных данных, номеров телефонов, адресов электронной почты после открытия счета.
- Адреса электронной почты, не соответствующие имени владельца счета, или схожие адреса электронной почты на нескольких счетах.
- Нерегулярные данные в профиле клиента, например, общие учетные данные (например, общие для двух или более пользователей) с другими счетами.

- Аномалии, выявленные по поведению в Интернете, например, замедленный ввод данных, задержка нажатия клавиш, признаки автоматизации, многократные неудачные попытки входа в систему и т.д.
- Учетные записи, относящиеся к субъектам, которые, как можно предположить, больше не ведут активной деятельности в данной юрисдикции (например, учетная запись иностранного студента, проданная после завершения обучения).
- IP-адреса или GPS-координаты, происходящие из юрисдикций с высоким риском отмывания денег.
- Использование виртуальных частных сетей (VPN), компрометирующих устройств (например, IOT-устройств) и хостинговых компаний, которые могут маскировать IP-адрес пользователя.
- Использование нескольких IP-адресов или электронных устройств, связанных с одной учетной записью в Интернете.
- Один статический IP-адрес или электронное устройство, связанное с несколькими учетными записями разных владельцев учетных записей.
- Доступ к учетной записи через порты компьютера, используемые такими приложениями, как Team Viewer и т.п., что не позволяет увидеть истинное устройство и местоположение.
- Учетные записи, работающие с чрезмерно быстрыми нажатиями клавиш или навигацией, свидетельствующими о возможном управлении ботом.

Негативная информация о владельце счета

- Наличие существенных и поддающихся проверке негативных новостей о клиенте или контрагентах, например, счет, принадлежащий известной или предполагаемой предыдущей жертве мошенничества, мула или похищения личности.
- Сообщение о мошенничестве или отзыв из заочного учреждения или других сторонних баз данных о мошенничестве.
- Наличие запросов на отзыв электронных переводов.
- Наличие неблагоприятной информации, предоставленной ПФР или правоохранительными органами о лицах, участвующих в операции.

Транзакции ВА

- Отправка/получение больших объемов или частое использование низких сумм ВА на адреса нехостинговых кошельков; или адреса, связанные с даркнет-площадками, платформами для размещения материалов о сексуальном насилии над детьми, площадками для продажи вредоносных программ, группами вымогателей, сервисами микширования/тумблирования, юрисдикциями высокого риска, игорными сайтами и мошенниками.
- Превышение суточных лимитов пополнения счета в биткоин-банкоматах.
- Отсутствие документов, подтверждающих происхождение ВА или средств, конвертированных в криптоактивы.

- Переводы ВА на кошельки, связанные с незаконной деятельностью в даркве-бе (например, терроризм, детская порнография, наркотики и т.д.).
- Транзакции с использованием более чем одного типа ВА, особенно тех, которые обеспечивают повышенную анонимность.
- Аномальная транзакционная активность ВА с кошельков, связанных с пиринговыми платформами, не имеющая логического объяснения.

Другие

- Несоответствие номера счета и имени владельца счета.
- Пользователь виден по телефону или в сопровождении физического лица через систему видеонаблюдения, его инструктируют или наставляют во время совершения операции.
- Компании-бенефициары управляют Интернет-сайтами, предоставляющими торговые/инвестиционные услуги, во многих случаях не авторизованными или не включенными в перечень национального надзорного органа.

Приложение 2: использование синергетического эффекта от мер по борьбе с мошенничеством и ПОД/ФТ

В данном Приложении собраны примеры того, как финансовые регуляторы наряду с мерами контроля в области ПОД/ФТ применяют требования по борьбе с мошенничеством, некоторые из которых направлены против возможности преступников регистрировать, получать доступ и контролировать счета мулов удаленно. К ним относятся различные меры, связанные с проверкой клиентов и мониторингом операций.

Эти меры контроля могут быть полезны для ФУ, ПУВА и других финансовых и платежных организаций.

- Внедрение строгих процессов «Знай своего клиента» (ЗСК) или «Знай свой бизнес» (Know-Your-Business), использование биометрических характеристик в процессе регистрации и т.д., а также идентификация одного мобильного или защищенного устройства для подтверждения подлинности банковских операций в Интернете (другие устройства блокируются или подвергаются усиленным мерам по снижению рисков).
- Период ожидания при первом подключении услуг интернет-банкинга или защищенных устройств (т.е. полный набор банковских услуг не становится доступным сразу после открытия), ограничение количества или стоимости финансовых операций клиента.
- Разработка определения ожидаемых операций (количество операций, суммы, типы контрагентов, страны-участники) для выявления подозрительных операций, а также ужесточение правил выявления мошенничества и триггеров для упреждающего блокирования незаконных операций.
- Использование сервисов «верификации получателя», позволяющих отправителю/плательщику/должнику платежного поручения проверить соответствие имени бенефициара/получателя/кредитора, указанного в платежных сообщениях, имени владельца счета.
- Сокращение общения с клиентами по электронной почте и в социальных сетях до информирования общего характера с явным указанием на недопустимость обмена идентификационными и персональными данными с ФУ/ПУВА по электронной почте.
- Добавление программ распознавания голоса и искусственного интеллекта в общение с клиентами для обеспечения их подлинной идентификации.
- Требование использования механизмов многофакторной аутентификации при проверке клиента, а также при проведении финансовых операций, добавлении или активации бенефициаров с использованием различных каналов.
- Удостоверение личности пользователя при удаленной настройке и предотвращение получения преступниками доступа к нескольким счетам с использованием информации о счетах денежных мулов или жертв за счет:
    - Повышения надежности процесса идентификации клиента с помощью тестов на «живость» (т.е. обеспечение живого и подлинного человека), в том числе, если при проверке «живости» человек подвергается социальной инженерии;

  - Мониторинга IP-адресов, используемых для подключения к сайтам банковских услуг в режиме онлайн и т.д., в том числе для выявления использования средств удаленного доступа и атаки «человек в браузере».

- Расширение типов данных, которые собирают и анализируют подотчетные организации о клиентах, включая, например, номера мобильных телефонов, IP-адреса, GPS-координаты, идентификаторы устройств и т.д. В целях предотвращения мошенничества ФУ могут повторять такую идентификацию, используя риск-ориентированный подход (например, проводить такие проверки при обнаружении аномального поведения).
- Внедрение системы мониторинга операций в режиме реального времени, основанной на оценке рисков, для оперативного выявления, расследования и, при необходимости, информирования о подозрительных операциях. Сложность системы мониторинга должна быть соизмерима с объемом и характером операций, обрабатываемых ФУ.

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

INTERPOL

FATF

www.egmontgroup.org | www.interpol.int | www.fatf-gafi.org

Ноябрь 2023

Незаконные финансовые потоки от кибермошенничества

В данном отчете анализируются методы, используемые для кибермошенничества, его связь с другими преступлениями и то, как преступники могут использовать уязвимые места в новых технологиях. В отчете приводятся примеры национальных оперативных мер и стратегий, которые доказали свою эффективность в борьбе с мошенничеством с использованием кибертехнологий. В отчете также указаны индикаторы риска и эффективные требования и меры контроля в области борьбы с мошенничеством, которые могут помочь организациям государственного и частного секторов обнаружить и предотвратить мошенничество с использованием кибертехнологий и связанное с ним отмывание денег.