УДК 351.822+336.74 DOI: 10.37468/2307-1400-2022-1-63-81

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Зайцев Александр Константинович[1]
Матвеев Владимир Владимирович[1]

[1] Санкт-Петербургский государственный экономический университет, Санкт-Петербург, Россия

АННОТАЦИЯ

В статье представлены существующие угрозы и вызовы, исходящие от террористических организаций, включающие увеличение числа террористических актов с участием террористов-одиночек, вовлечение молодежи, миграцию, контрабанду, использование компьютерных игр и криптовалюты. Детально рассмотрена угроза использования криптовалюты в деятельности террористических организаций. Вместе с тем описаны возможности «Прозрачного блокчейна» для отслеживания подозрительных трансакций Росфинмониторингом, среди которых отслеживание цепочки перемещения цифровых финансовых активов, оценка вероятности связи криптовалютных кошельков с потенциально противоправной деятельностью, мониторинг поведения участников криптовалютных рынков с целью идентификации лиц, замешанных в нарушении закона. Также в статье выявлены пробелы в нормативно-правовой базе по регулированию цифровых финансовых активов. Так, выявлено отсутствие требований к минимальному порогу сумм, подлежащих обязательному контролю государства в целях противодействия ОД/ФТ и полное отсутствие регулирования деятельности майнеров, т.е. лиц, осуществляющих выпуск криптовалют, а также самого процесса выпуска цифровых валют. Сделан вывод о необходимости доработки законодательного регулирования криптовалюты и информационных систем, осуществляющих ее оборот, а также о необходимости развития технических средств регулирования и отслеживания криптовалютных операций Росфинмониторингом для наиболее эффективного осуществления государственного контроля за оборотом криптовалютных активов и препятствованию использования криптовалюты как механизма финансирования терроризма.

Ключевые слова: криптовалюта, криптотрансакции, блокчейн, финансирование терроризма, Федеральная служба по финансовому мониторингу Российской Федерации, противодействие легализации (отмыванию) доходов и финансированию терроризма, «Прозрачный блокчейн», финансовая безопасность, цифровые финансовые активы.

ECONOMIC CRIMES USING DIGITAL TECHNOLOGIES

Zaitcev A. K.[1]
Matveev V.V.[1]

[1] St. Petersburg State University of Economics, St. Petersburg, Russia

ABSTRACT

The article presents the existing threats and challenges posed by terrorist organizations, including an increase in the number of terrorist attacks involving lone terrorists, the involvement of young people, migration, smuggling, the use of computer games and cryptocurrencies. The threat of using cryptocurrency in the activities of terrorist organizations is considered in detail. At the same time, the possibilities of the Transparent Blockchain for tracking suspicious transactions by Rosfinmonitoring are described, including tracking the chain of movement of digital financial assets, assessing the likelihood of cryptocurrency wallets being associated with potentially illegal activities, monitoring the behavior of cryptocurrency market participants in order to identify persons involved in violating the law. The article also identified gaps in the regulatory framework for the regulation of digital financial assets. Thus, the absence of requirements for the minimum threshold of amounts subject to mandatory state control in order to combat ML/TF and the complete absence of regulation of the activities of miners, i.e. persons issuing cryptocurrencies, as well as the process of issuing digital currencies. It is concluded that it is necessary to refine the legislative regulation of cryptocurrency and information systems that carry out its circulation and also it is concluded that it is necessary to develop technical means for regulating and tracking cryptocurrency transactions by Rosfinmonitoring for the most effective implementation of state control over the circulation of cryptocurrency assets and preventing the use of cryptocurrency as a mechanism for financing terrorism.

Keywords: cryptocurrency, cryptotransactions, blockchain, financing terrorism, Federal Financial Monitoring Service of the Russian Federation, counteraction to legalization (laundering) of incomes and financing of terrorism, «Transparent Blockchain», financial security, digital financial assets.

Активное развитие цифровых технологий в последнее время оказывает влияние на все сферы общественной жизни и все сектора мировой экономической системы, в том числе на управление кредитно-финансовой системы. Первоначально это активная тенденция перевода наличных денег в электронные, а затем создание принципиально новых – цифровых денег.

С учетом краха глобальной кредитно-финансовой системы, основанной на расчетах в долларах Федеральной Резервной Системы (неверно называемых долларами США) и ориентированной на таргетирование уровня инфляции, а фактически на поддержание уровня прибыли владельцев финансовых инструментов, появилась необходимость создания новых фиатных денег – цифровой валюты, которые еще называют криптовалютой.

Появление и сверхбыстрое распространение цифровых денег стало привлекательным инструментом для собственников преступных капиталов, так как цифровые деньги позволили создать новые механизмы для легализации доходов, полученных преступным путем [1].

В связи с этим перед Федеральной службой по финансовому мониторингу (Росфинмониторинг), которая является федеральным органом исполнительной власти, осуществляющим функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, стоит новая задача по разработке мер противодействия распространению операций по переводу доходов, полученных нелегально, в цифровые деньги [2].

Для анализа происходящих процессов в данной предметной области необходимо указать основные понятия.

1. *Легализация денежных средств* – совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретенными другими лицами преступным путем, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом.

2. *Отмывание денег* – это процесс, в котором полученное имущество, приобретенное или аккумулируемое вследствие незаконной деятельности, перемещается или скрывается для того, чтобы прервать преступную цепочку.

Основные направления киберпреступлений, в которых используются криптовалюты:

– отмывание денег;
– вымогательство;
– даркнет-рынки;
– мошеннические схемы;
– кража;
– финансирование терроризма и экстремизма [3].

Структура источников получения денег преступным путем представлена на рисунке 1.

Этапы отмывания денежных доходов, полученных преступным путем

С учетом того, что до недавнего времени в Российской Федерации преимущественно использовались наличные деньги, то преступники чаще всего использовали старые, наиболее безопасные для них схемы отмывки по принципу «из рук в руки». Широко известна трехфазная схема отмывания денег, полученных преступным путем, представленная на рисунке 2.

Этап 1. Размещение денежных средств

Этап размещения состоит в непосредственном перемещении наличных денежных средств в мобильные финансовые инструменты. При этом, как правило, место получения преступных доходов и место их размещения территориально удалены друг от друга. Этап размещения крупных сумм наличности является самым слабым звеном в процессе отмывания денег. Незаконно полученные деньги легко могут быть выявлены на этом этапе. Размещение в криптовалюте может происходить по трем направлениям, которые отображены на рисунке 3. OTC – аббревиатура с английского Overthecounter, что означает «поверх прилавка», это сделка с любым финансовым инструментом, совершенная продавцом и покупателем за пределами рынка, то есть напрямую. Таким образом, OTC платформы отличаются от бирж:

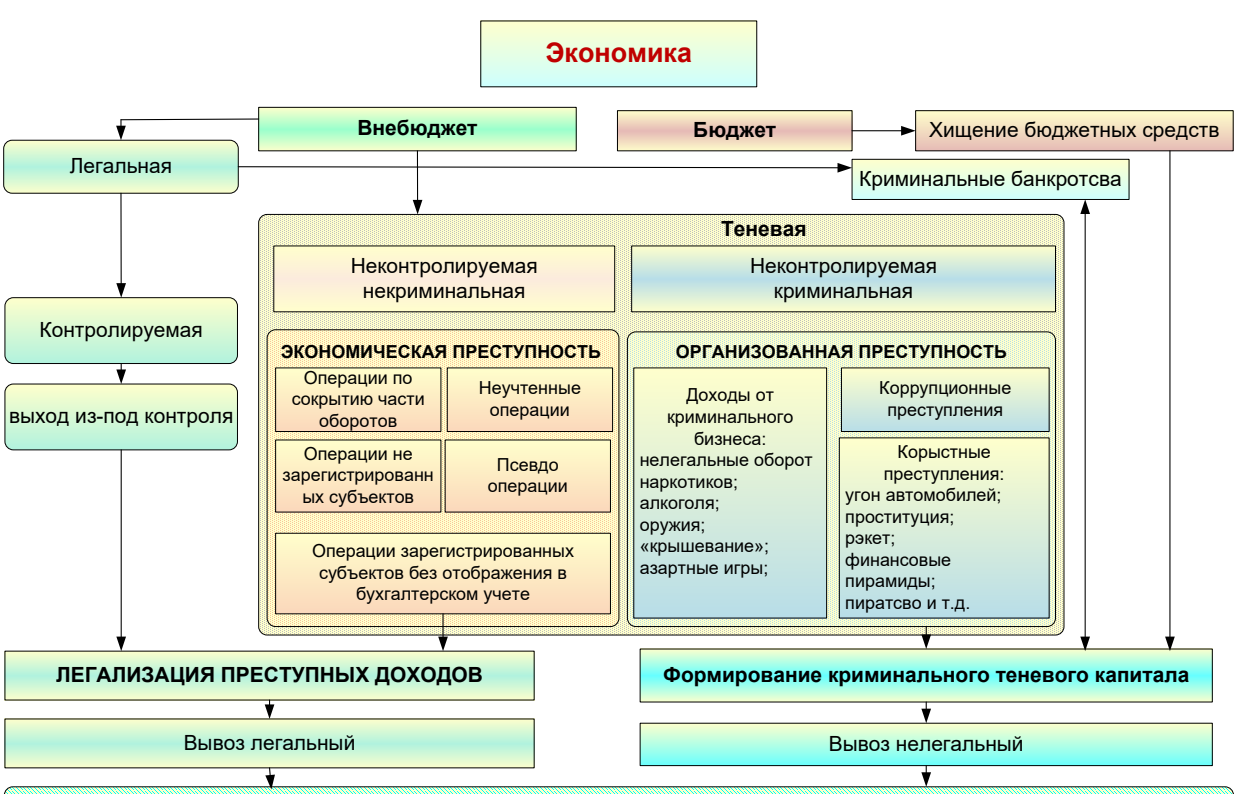

Рисунок 1 – Источники получения денежных доходов преступным путем

1 **Размещение денежных средств** - процесс, в результате которого денежные средства поступают в финансовую систему того или иного государства, например, путем размещения денежных средств во вклады, путем приобретения ценных бумаг за наличный расчет, покупки доли бизнеса. Данный этап наиболее опасный для «отмывателей», т.к. именно здесь прослеживается четкая связь между доходом и совершенным преступлением.

2 **Расслоение (оборот, перемешивание, смешивание) денежных средств -** процесс, в ходе которого фактическим владельцем или его доверенным лицом совершается значительное количество операций с целью отдалить денежные средства от первоначального источника. Главная задача «отмывателя» - нивелировать связь между источником получения денежных средств и самими денежными средствами. «Отмывателю» особенно важно получить денежные средства из организации с хорошей деловой репутацией.

3 **Интеграция** - процесс, в результате которого размещенные **денежные средства или имущество возвращаются в легальную экономику**, например в виде приобретения недвижимости, драгоценностей, иных предметов роскоши.

Рисунок 2 – Трехфазная модель отмывания денежных доходов полученных преступным путем

– большей ликвидностью;
– большими порогами лимитов (максимальные суммы операций значительно больше);
– меньшими временными издержками.

При совершении OTC-сделки происходит обмен различными суммами денег, в том числе и крупными, на криптовалюту на определенных платформах. Поиск покупателей может занять некоторое количество времени, однако данные издержки не будут весомыми, потому что на OTC платформе ежедневно возникает множество предложений по сделкам различных масштабов.

При прямом переводе денег в криптовалюту многие биржи просят идентифицировать личность, то есть пользователю поступает запрос пройти процедуру «KYC». Чтобы избежать раскрытия личности преступники либо находят более конфиденциальную криптовалюту, которая не требует авторизации, либо при выполнении процедуры «Know Your Customer» предоставляют ложные паспортные данные, найденные в сети Интернет.

Одним из способов размещения денег в криптовалюте являются многочисленные незначительные начисления на разные счета, то есть пользователь создает несколько активных аккаунтов и начисляет на них максимально допустимую сумму, при которой не нужна идентификация.

Этап 2. Перемещение доходов

Этап перемещения доходов, полученных преступным путем, представляет собой отрыв незаконных доходов от их источников путем сложной цепи финансовых операций, направленных на маскировку проверяемого следа этих доходов. На данном этапе происходят многочисленные операции с криптовалютой, чтобы запутать денежные потоки. Два основных способа перемещения денежных средств в криптовалюте представлены на рисунке 4.

Опыт стран, входящих в ФАТФ (Группа разработки финансовых мер по борьбе с отмыванием денег – Financial Action Task Force, FATF) указывает на то, что существуют способы сопоставления криптовалютных трансакций и кошельков с их владельцами [4].

Чтобы скрыть свое происхождение, преступники прибегают к таким инструментам, как тумблеры и миксеры, которые смешивают в произвольном порядке операции по криптовалюте, что в значительной степени снижает возможность раскрытия преступления.

Тумблеры (tumbler) – это сервисы, в которые владелец может перевести свои деньги и, заплатив комиссию, получить совершенно другие счета в криптовалюте, которые с ним никак не будут связаны [5].

Миксер – это трансакции перемешивания, в которых сайт принимает криптовалюту множества человек, затем использует алгоритмы для смешивания и отправляет биткоины по разным кошелькам.

В системе блокчейна существует криптои-

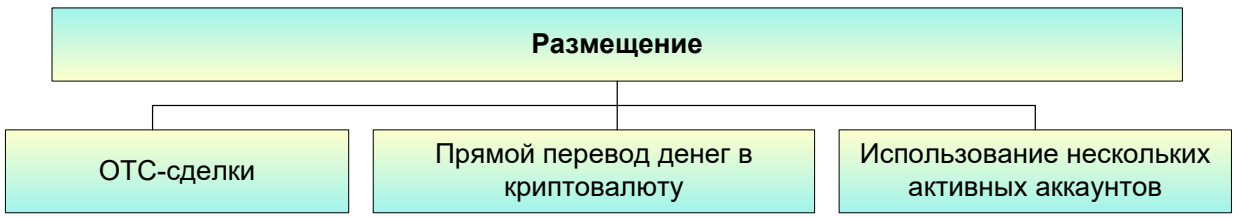

Рисунок 3 – Варианты размещения средств в криптовалюте

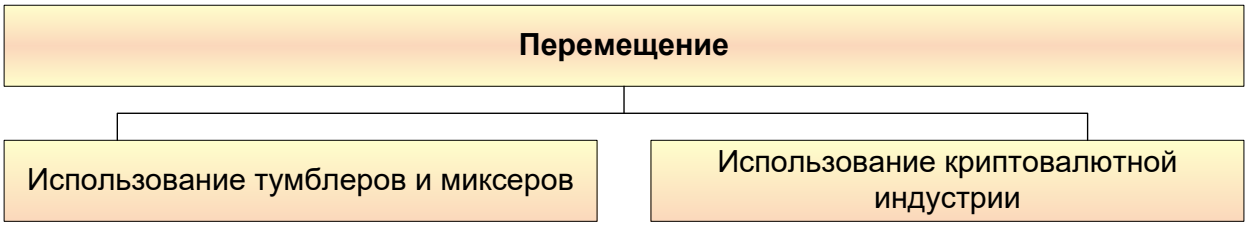

Рисунок 4 – Способы перемещения денежных средств в криптовалюте

гральная индустрия, в которой злоумышленники переводят криптовалюту на игровую платформу, делают незначительные ставки и выводят обратно. Данный способ позволяет замаскировать схему по отмыванию денег. Более того, существует возможность выполнения трансакций через TOR[1], которые чаще всего невозможно отследить в связи с тем, что сложно определить реальный IP-адрес [6].

Этап 3. Вывод «чистых» денег

Третий этап заключается в выведении уже «чистых» денег из системы блокчейна. Этап интеграции заключается в легализации, направленной непосредственно на придание видимости законности преступно полученных денежных доходов. Преимущественно преступники используют OTC-сделки, указанные на этапе Размещения. Происходит поиск клиента, который желает приобрести значительную сумму криптовалюты. После обмена «криптовалюта – наличные или безналичные деньги» установить происхождение денег практически невозможно.

Представленная трехфазовая модель является наиболее распространенной среди преступников для легализации доходов. Указанные три стадии могут осуществляться одновременно или частично накладываться друг на друга. Это зависит от имеющегося механизма легализации и от требований, предъявляемых преступной организацией.

Классификация криптовалют

Основными видами криптовалют в настоящее время являются следующие: биткойн, лайткоин, эфир, нэм, дэш, рипл, монеро и другие. Одной из самых распространенных криптовалют является биткоин. На него приходится большая часть финансовых операций с криптовалютами. Статистика продаж криптовалюты указывает, что биткоин занимает приблизительно треть всего рынка. Структура объёма операций в различных криптовалютах представлена на рисунке 5.

Несмотря на то, что в 2020 году уровень преступности в криптовалютной сфере снизился, тем не менее злоумышленники проявляют высокую заинтересованность к криптовалюте с учетом

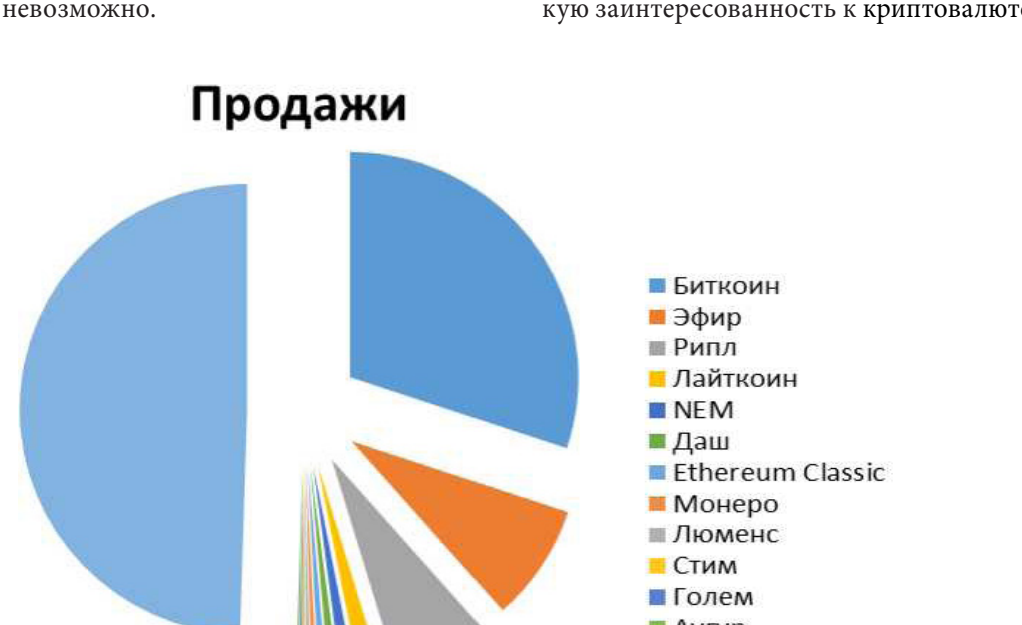

Рисунок 5 – Объем операций в криптовалютах

1 Tor (сокр. от англ. The Onion Router) – свободное и открытое программное обеспечение для реализации анонимного сетевого соединения. С помощью Tor пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счёт использования распределённой сети серверов – узлов.

анонимности ее природы и легкостью, с которой пользователи могут отправлять средства по всему миру. Динамика участвующих в криминальных криптовалютных трансакциях сумм за 2017-2020 годы отображена на рисунке 6.

В 2021 г. доля криптовалют, связанных с криминалом, составила более $10 млрд переводов (или 0,34% от всего объема криптовалютных трансакций). Хотя эти цифры в 2 раза ниже, чем в 2019 г. ($21,4 млрд или 2,1%), но общая активность преступной деятельности за период с 2019 по 2021 гг. с использованием криптовалют возросла почти втрое.

Так, например, Chainalysis[2], представляя свою статистику, напоминает о том, что на момент представления отчета выявлены далеко не все факты криминала, так как появляется дополнительное количество адресов, связанных с криминалом [7].

Использование модели ICO для отмывания доходов

ICO (Initial Coin Offering) – это относительно новая форма инвестирования, появление которой связано со становлением криптовалют. ICO, представляя собой форму привлечения инвестиций для криптовалютных проектов, не имеет под собой никакой регулятивной базы. Благодаря этому инициатором первичного монетного размещения может выступать любое юридическое и физическое лицо. При этом никаких аудитов и проверок проект не проходит. Почти все работы ведутся в режиме онлайн.

Использование ICO платформ является совершенно новой схемой легализации денежных средств, которая возникла с появлением криптовалюты и токенов [8].

Токен – это единица учёта, не являющаяся криптовалютой, предназначенная для представления цифрового баланса в некотором активе. Иными словами - выполняющая функцию «заменителя ценных бумаг» в цифровом мире [9].

ICO – форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалюты, полученных разовой или ускоренной эмиссией. Данная операция разрабатывалась изначально для наибольшего

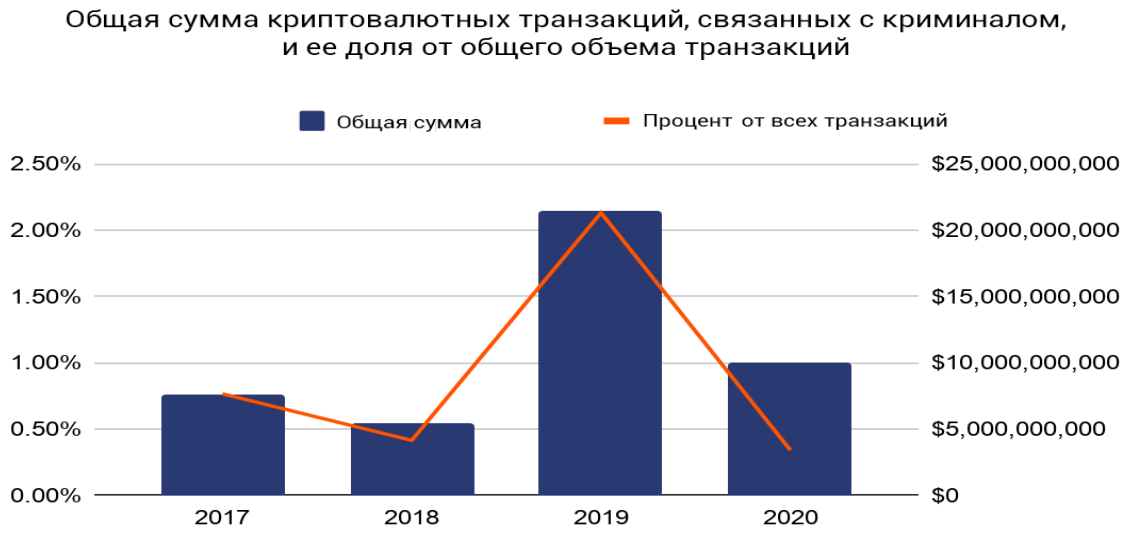

Рисунок 6 – Общая сумма криптовалютных трансакций, связанных с криминалом, и ее доля от общего числа трансакций

2 Chainalysis – это компания, занимающаяся анализом блокчейнов. Она предоставляет данные, программное обеспечение и проводит исследования для государственных учреждений, бирж, финансовых учреждений, страховых компаний и компаний по кибербезопасности в более чем 50 странах. Платформа данных компании позволяет проводить расследования, поддерживает инструменты соблюдения нормативных требований и управления рисками, которые использовались для раскрытия самых громких кибер-уголовных дел в мире и безопасного расширения доступа потребителей к криптовалюте.

привлечения инвестиционного внимания к той или иной монете. Однако, мошенники узнали о подобной платформе и стали использовать ее в качестве новой модели легализации денежных средств.

Через схему ICO проходят много операций, в том числе с целью отмывания доходов. Данный сценарий осуществим только при условии, что обменные площадки не сотрудничают с правоохранительными органами. Схема использования модели ICO представлена на рисунке 7.

В данной системе участвуют два игрока. Один, например, инвестор, который приобретает токены для дальнейшей их выгодной реализации, и второй – владелец «грязных» денег. Участники сделки не знают друг друга, первый стремится подороже продать, а второй заинтересован в приобретении токенов и поэтому зачастую предлагает самый выгодный курс. После чего злоумышленник производит обмен специальной валюты на любой площадке.

Использование программ-вымогателей

Программы-вымогатели – это тип вредоносного программного обеспечения (ПО), которое блокирует доступ к устройству или системе жертвы, а затем требует выполнения определенных условий в обмен на восстановление доступа законного владельца устройства / системы.

Программы-вымогатели могут быть доставлены в систему несколькими способами: от вложений электронной почты и фишинговых ссылок до неожиданных надстроек и, казалось бы, законного программного обеспечения.

Злоумышленники также используют тактику социальной инженерии, изображая из себя сотрудников правоохранительных органов, которые требуют штрафов за наличие пиратского программного обеспечения или незаконных материалов на их компьютерах.

Программы-вымогатели обычно нацелены на ценные файлы, такие как финансовые документы, важные программы и личные фотографии, и шифруют или удаляют их файлы из резервных копий.

Это часто делается с использованием симметричного или асимметричного алгоритма шифрования, который позволяет программе-вымогателю сгенерировать ключ шифрования и предложить его жертве в обмен на что-то, обычно это какой-то платеж.

Чаще всего жертвы программ-вымогателей не знают о взломе до тех пор, пока им не предъявляется экранная записка о выкупе, которая предупреждает их об атаке.

Эта записка обычно грозит отказом в доступе до тех пор, пока не будет выплачен выкуп. Сумма выкупа указывается, и иногда требуется оплата в криптовалюте из-за конфиденциальности и удобства платежных сетей с блокчейном.

После выполнения условий злоумышленник обычно отправляет жертве ключ дешифрования или напрямую расшифровывает зараженное устройство / систему, чтобы законный пользо-

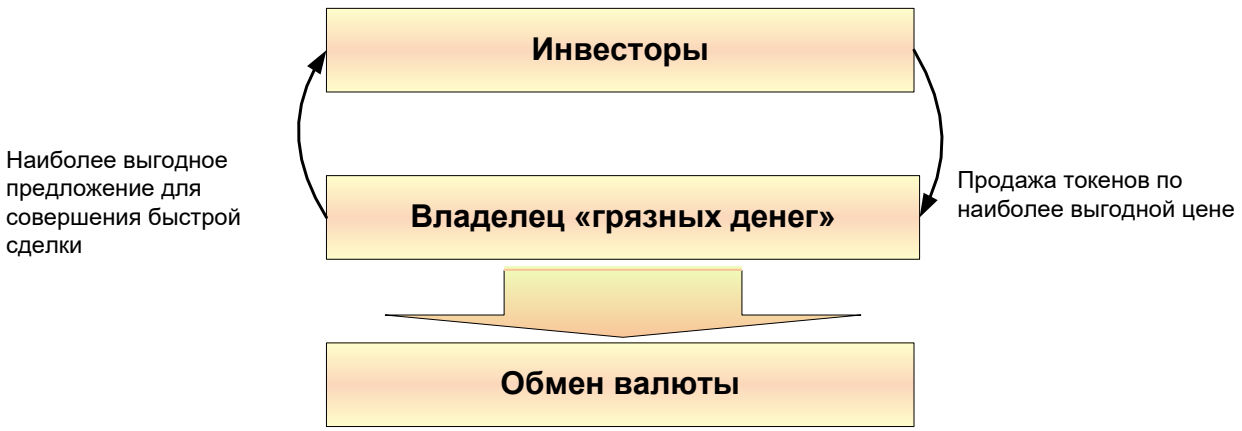

Рисунок 7 – Схема использования модели ICO

ватель мог восстановить контроль над своей системой.

Программы-вымогатели – это серьезная растущая проблема кибербезопасности как для государственного, так и для частного секторов. Только вскрытые платежи злоумышленников-вымогателей с 2019 по 2021 год выросли на 337%. Общий объем платежей криптовалюты вырос на сумму более 400 миллионов долларов. Это по самым низким оценкам на основе вскрытых платежей. Тенденция увеличения таких платежей с каждым годом все возрастает и не показывает признаков замедления.

Платежи программ-вымогателей могут создать риск санкций для организаций-жертв и компаний, которые помогают им осуществлять платежи. По данным Chainalysis, 13% известных платежей программ-вымогателей в 2021 году сопряжены с санкционным риском.

В 2021 году средний размер платежа составил 54.000 долларов США. Это отчасти связано с тем, что злоумышленники-вымогатели более эффективно атакуют более крупные организации с помощью незаконных сторонних поставщиков, которые продают им хакерские инструменты, украденные данные и другие активы для проведения более успешных атак. На рисунке 8 отображена динамика общей суммы криптовалюты, полученной адресами программ-вымогателей за 2016-2021 годы [10].

Увеличение количества программ-вымогателей, начиная с 2020 года, было вызвано рядом новых штаммов, получающих большие суммы от жертв, а также несколькими ранее существовавшими штаммами, увеличивающими доходы. На рисунке 9 представлены топ-10 штаммов программ-вымогателей по доходам в период с 2014 по 2021 годы.

Штаммы программ-вымогателей не работают стабильно, даже из месяца в месяц. Они постоянно мигрируют.

Количество активных в течение года штаммов может создать впечатление, что существует несколько отдельных групп, осуществляющих атаки программ-вымогателей. Но это может быть обманчивым впечатлением. Так, многие штаммы функционируют на Модели RaaS (Модель программы-вымогателя как услуги), в которой злоумышленники, известные как партнеры, «арендуют» использование определенного штамма программы-вымогателя у его создателей или администраторов, которые в обмен получают

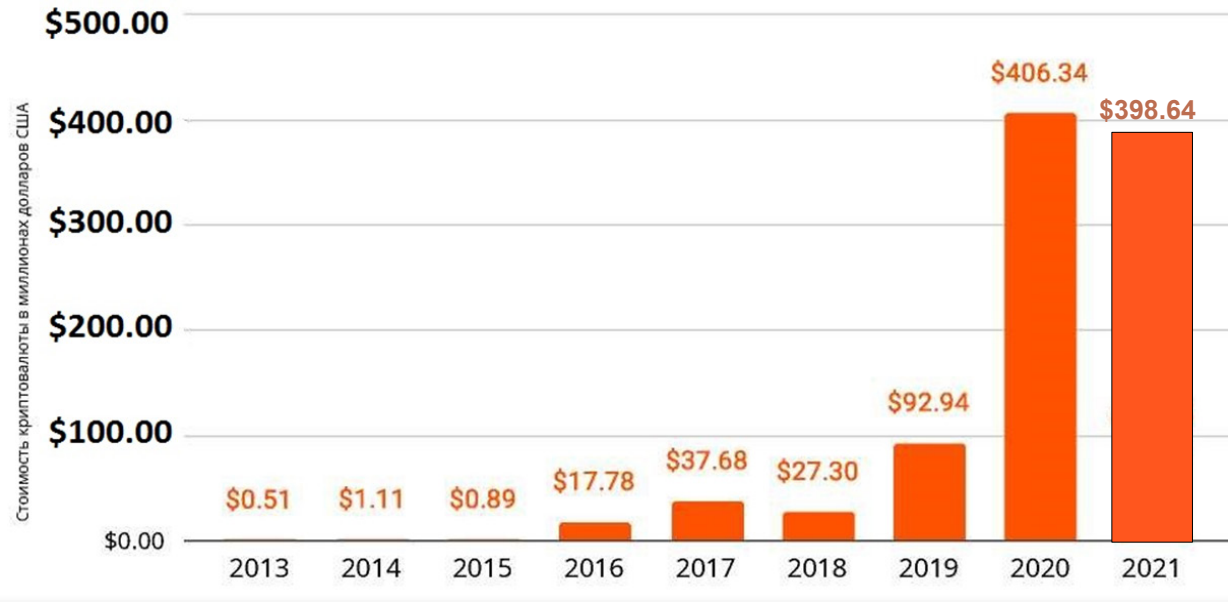

Рисунок 8 – Общая стоимость криптовалюты, полученная адресами программ-вымогателей 2016-2021гг. (Включены валюты: BCH, BTC, ETH, USDT)

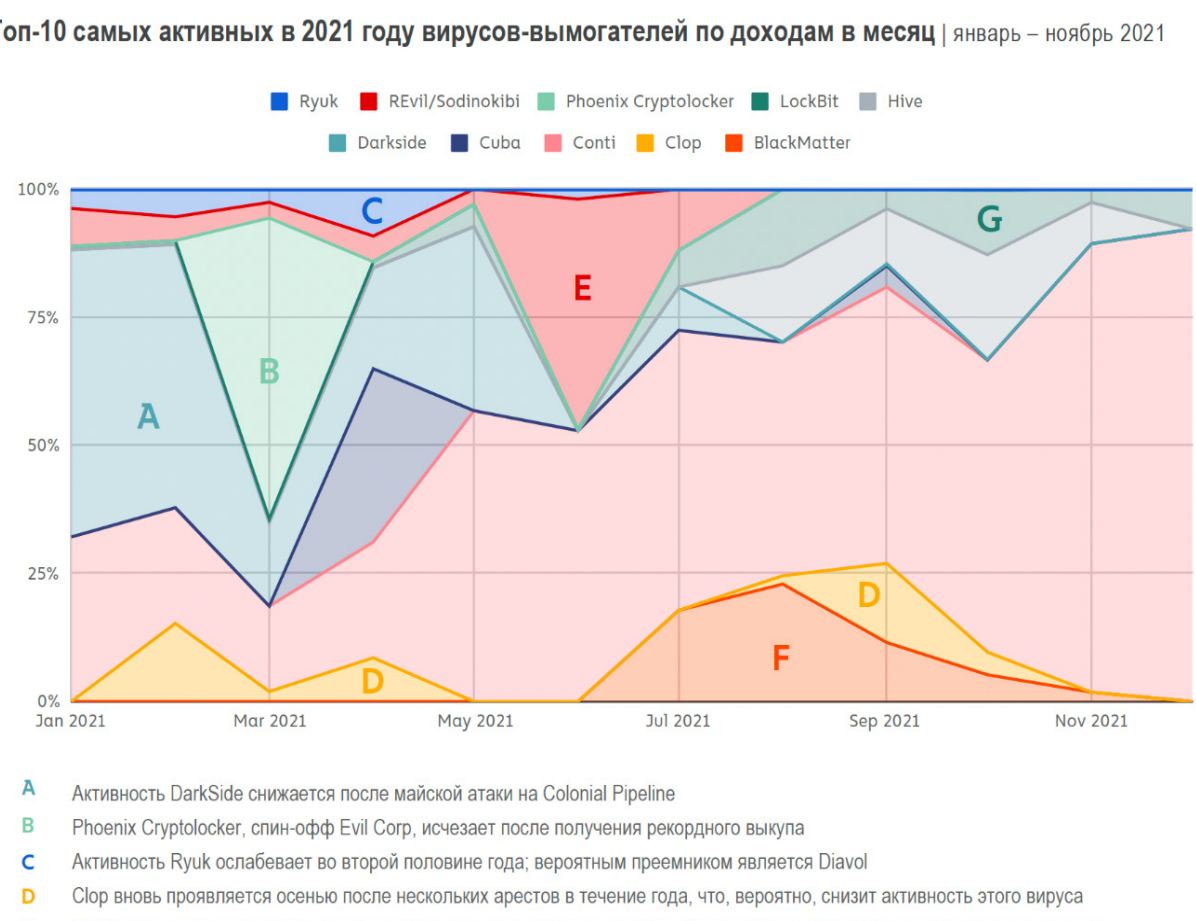

Рисунок 9 – Топ-10 самых активных в 2021 г. программ-вымогателей по доходам в месяц (январь – ноябрь 2021 г.)

часть денег от каждой успешной атаки, которую проводят партнеры.

Многие филиалы RaaS мигрируют между штаммами, предполагая, что экосистема программ-вымогателей меньше, чем может показаться на первый взгляд. Кроме того, многие исследователи кибербезопасности считают, что некоторые из самых крупных штаммов могут даже иметь одних и тех же создателей и администраторов, которые публично закрывают операции одного штамма, прежде чем просто выпустить новый, очень похожий штамм под новым именем. С помощью анализа блокчейна можно установить некоторые из этих связей, проанализировав, как адреса, связанные с различными штаммами программ-вымогателей, взаимодействуют друг с другом.

На рисунке 10 графически структурированы основные направления средств из кошельков программ-вымогателей. Первое и самое распространённое направление – обмен. От второго направления и дальше по порядку в каждом столбце соответственно: игровая платформа, безымянные сервисы, юрисдикции с высоким риском, незаконные адресы, смешивание и другие направления.

Программа-вымогатель: Netwalker («Сетевой странник» или «Сетевой бродяга»)

ФАТФ объявил скоординированные действия международных правоохранительных органов по уничтожению вируса-вымогателя Netwalker. В том числе изъятие почти полумиллиона долларов в криптовалюте, отключение темного

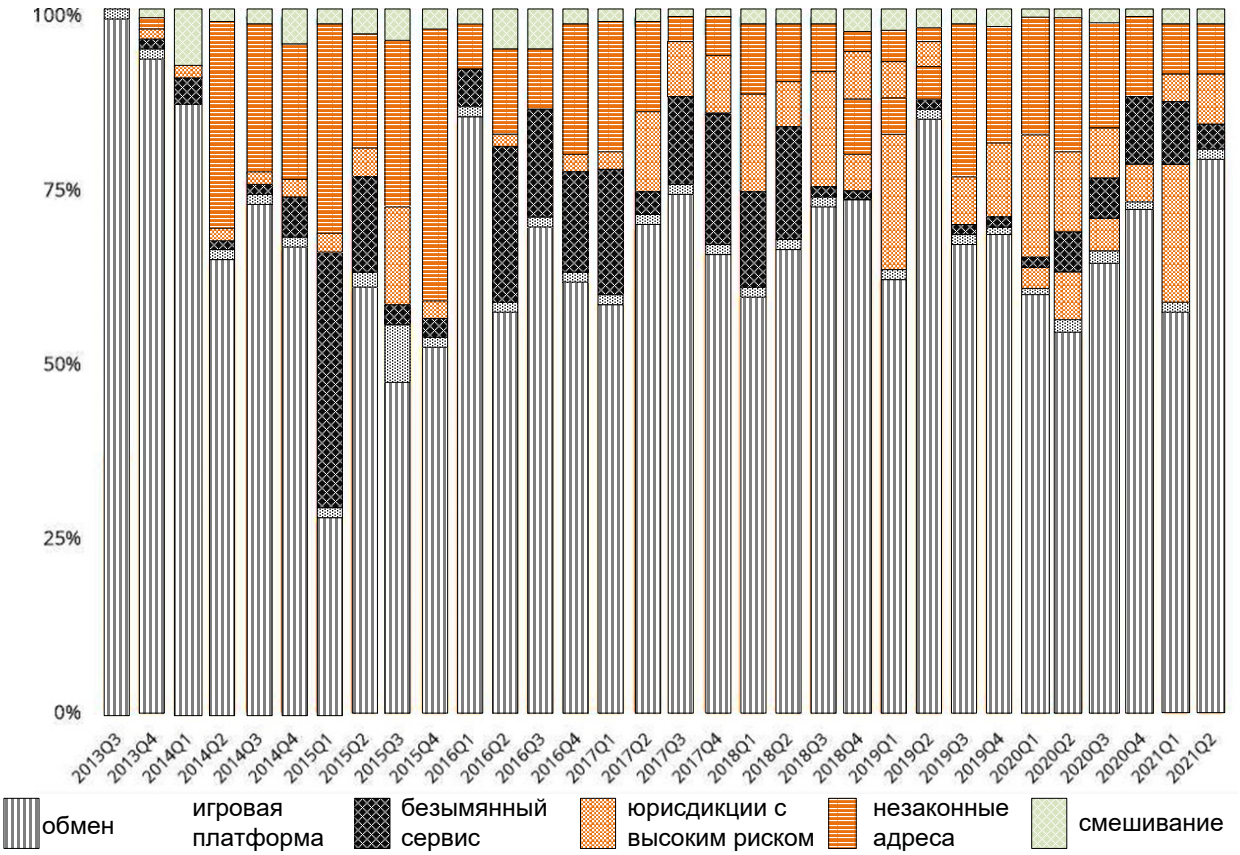

Рисунок 10 – Направление средств, покидающих кошельки программ-вымогателей (2013-2021 гг.)

веб-ресурса, используемого для связи с жертвами вируса-вымогателя Netwalker, и арест гражданина Канады Себастьяна Вашона – Desjardins, который получил десятки миллионов долларов, действуя в качестве партнера Netwalker [11].

Этот случай подчеркивает изощренность, с которой работал Netwalker, глобальное влияние атак программ-вымогателей и значительные средства, которые злоумышленники-вымогатели крадут у своих жертв.

Анализ блокчейна говорит о штамме программы-вымогателя Netwalker, что позволяет выделить конкретные элементы расследования, чтобы показать, как правоохранительным органам удалось отследить незаконные средства.

Как и многие штаммы, Netwalker работает на RaaS модели, в котором злоумышленники, известные как аффилированные лица, «арендуют» использование определенного штамма программ-вымогателей у его создателей или администраторов, которые в обмен получают часть денег от каждой успешной атаки, проводимой аффилированными лицами. RaaS привел к большему количеству атак, что еще больше усложнило количественную оценку полного финансового воздействия. Но тенденция ясна: ни одна другая категория преступлений, связанных с криптовалютой, не имела более высоких темпов роста, чем программы-вымогатели в 2020 году.

Netwalker был лидером среди программ-вымогателей по доходам в 2021 году, наряду с Ryuk, Maze, Doppelpaymer и Sodinokibi. Компания Chainalysis отследила выкуп Netwalker на сумму около 94 миллионов долларов, причем платежи были произведены еще в 2018 году. В середине 2020 года компания набрала обороты, увеличив средний размер выкупа до 33.000 долларов в прошлом году по сравнению с 7.000 долларов в 2019 году.

На рисунке 11 графические выделены «жертвы» программы-вымогателя «Netwalker» по странам.

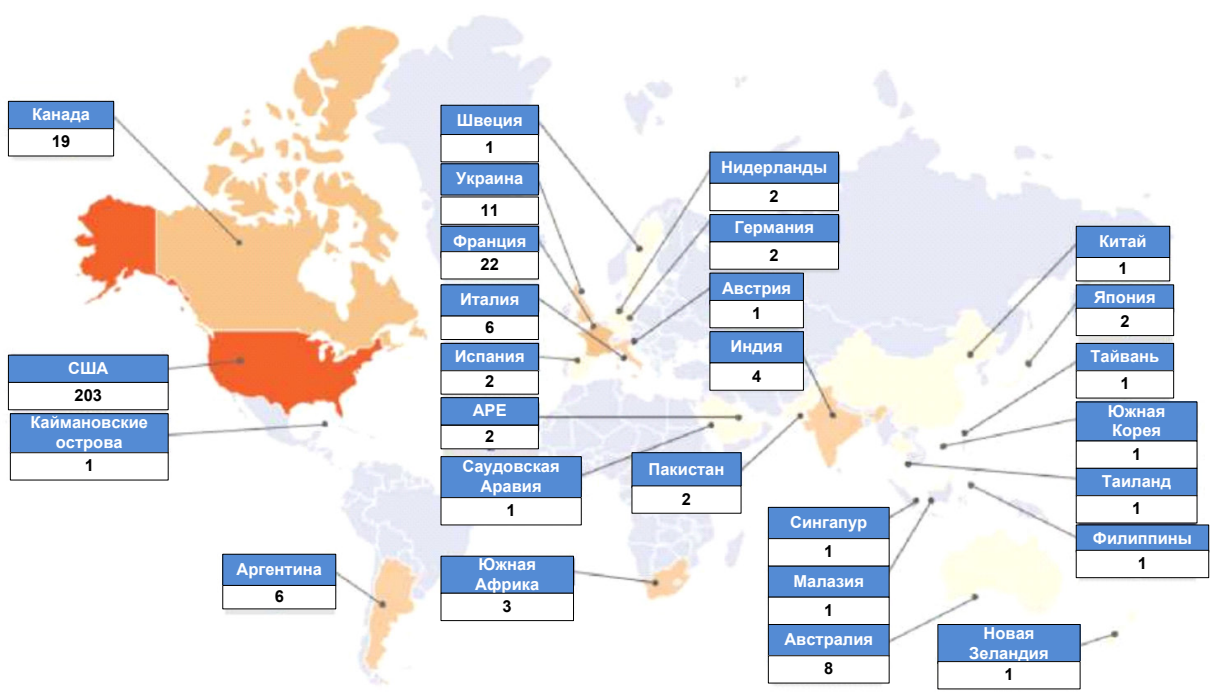

Рисунок 11 – Жертвы Netwalker по всему миру

Как правило, доходы от атак Netwalker получают четыре роли: вероятный администратор или разработчик (8-10%), партнер (76-80%) и две комиссионные роли (2,5-5% каждая). Партнер, такой как Vachon-Desjardins, обычно отвечает за получение доступа к сети жертвы и развертывание вредоносного ПО. Также бывают случаи, когда на один кошелек поступает 100% платежа, который, как мы полагаем, принадлежит администратору Netwalker и указывает на то, что он или она также может быть непосредственно причастен к некоторым атакам.

На рисунке 12 схематично изображен процесс типичного перевода средств с адреса для выплаты выкупа различным участникам программы-вымогателя «Netwalker» [12].

На рисунке 13 в виде диаграммы приведены примеры аффилированных штаммов RaaS.

Анализ блокчейна показывает, что на самом деле было менее 20 уникальных филиалов. Некоторые из этих филиалов редко развертывали Netwalker. Некоторые перешли на другие штаммы RaaS, и можно утверждать, что некоторые филиалы получали платежи от других вариантов.

Администратор Netwalker, известный на форумах даркнета под ником «Bugatti», в мае 2020 года разместил на форуме объявление о поиске дополнительных русскоязычных аффилиатов по мере «освобождения» вакансий, что подтверждает оценку перехода аффилиатов на другие штаммы.

Анализ блокчейна также может показать, что действующие лица программ-вымогателей платят за услуги, необходимые им для ведения преступного бизнеса. Например, участники Netwalker заплатили за хостинг облачного хранилища криптовалютой, которая, вероятно, использовалась для размещения украденных данных жертвы для дальнейшего вымогательства.

Действительно, Netwalker активизировал свои усилия по вымогательству, не только заблокировав жертвам доступ к их данным, но и украв их. Прежде чем шифровать компьютерные файлы в сети жертвы, субъекты Netwalker начали красть данные и автоматически публиковать данные жертвы

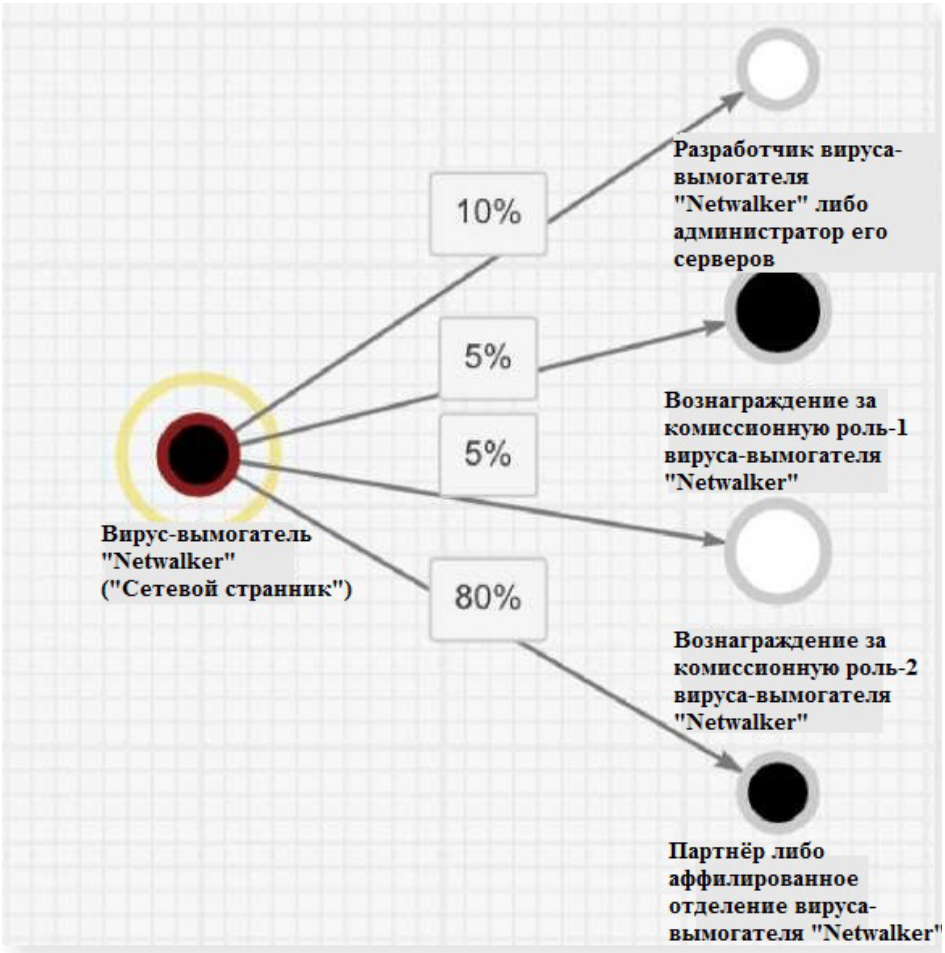

Рисунок 12 – Типичный перевод средств с адреса для выплаты выкупа различным участникам Netwalker

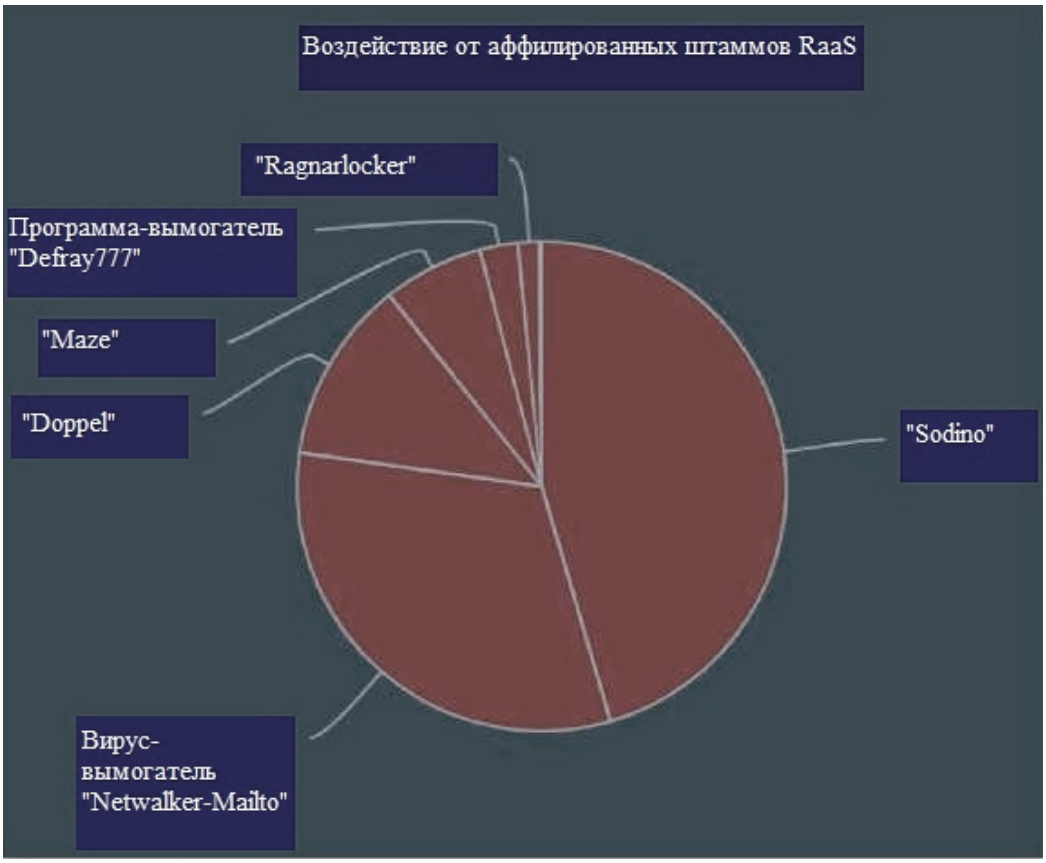

Рисунок 13 – Аффилированные штаммы RaaS

на сайте утечки, если выкуп не был уплачен в срок, что является еще одной растущей тенденцией среди нескольких штаммов программ- вымогателей. На рисунке 14 схематично представлена публикация данных жертвы на сайте утечки [13].

Помимо Netwalker, Vachon-Desjardins участвовал в развертывании других штаммов RaaS, таких как Sodinokibi, Suncrypt и Ragnarlocker. Видно, как партнеры со временем переходят на другие штаммы. Кроме того, администратор Netwalker Bugatti перечислил подтверждение предыдущего опыта взлома в качестве необходимого условия для того, чтобы стать партнером Netwalker, поэтому было бы разумно, чтобы такие партнеры, как Vachon-Desjardins, имели послужной список.

На рисунке 15 отображены филиалы программы-вымогателя «Netwalker», которые

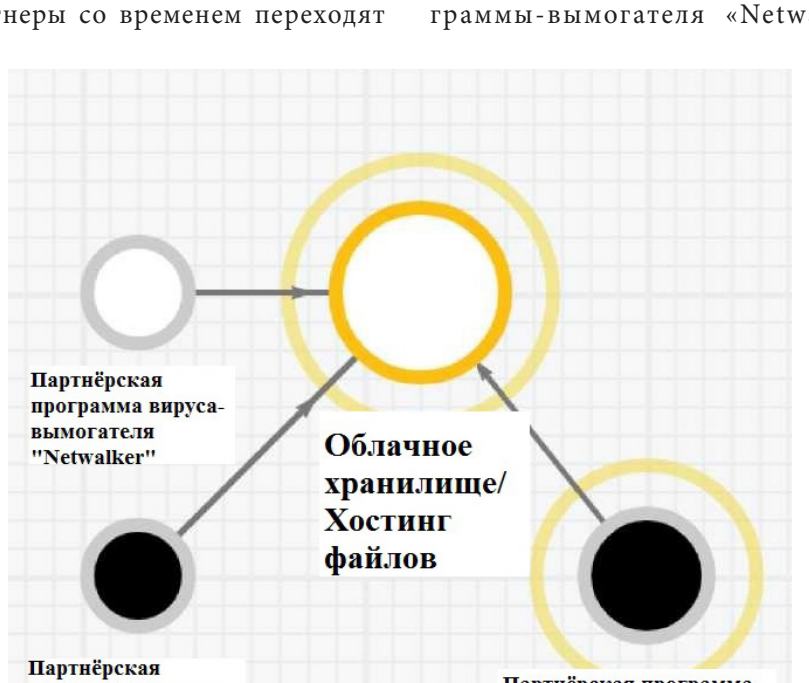

Рисунок 14 – Публикация данных жертвы на сайте утечки

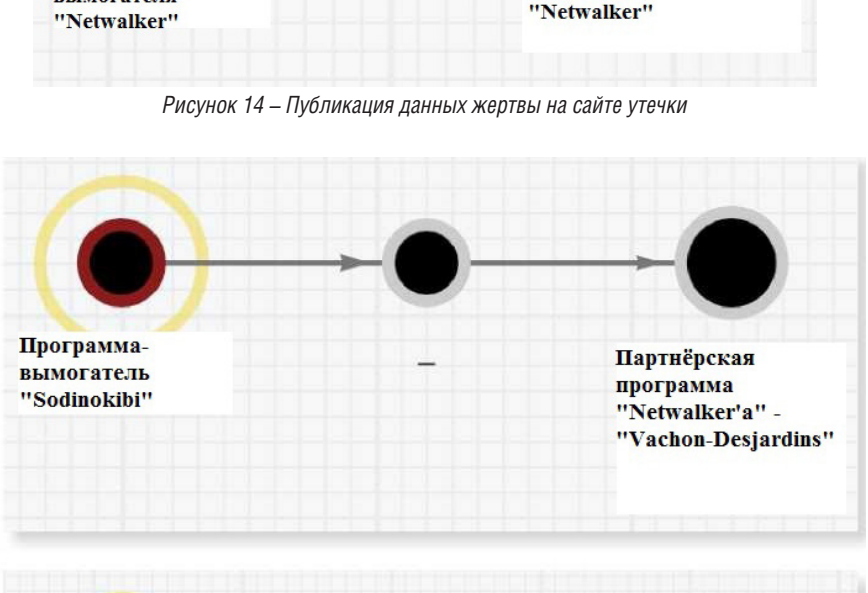

Рисунок 15 – Филиалы Netwalker, подверженные воздействию штаммов программ-вымогателей Sodinokibi и Ragnar Locker

подвергаются воздействию штаммов программ-вымогателей Sodinokibi и Ragnar Locker.

Партнерское дублирование является важным явлением, которое контролирующие органы должны понимать в борьбе с программами-вымогателями, поскольку оно предполагает относительно небольшое количество злоумышленников, создающих проблему, несмотря на множество штаммов, активных в любой момент времени. Исследование показывает, что небольшая группа адресов служебных депозитов получает большую часть средств, украденных в результате атак программ-вымогателей. Правоохранительные органы могут значительно снизить активность программ-вымогателей, нарушив работу относительно небольшой группы злоумышленников и поставщиков услуг по отмыванию денег.

Увеличение размеров платежей за выкуп совпадает с увеличением платежей с адресов программ-вымогателей на другие незаконные адреса, связанные со вспомогательными службами программ-вымогателей. Под незаконными сторонними услугами понимается ряд провайдеров, некоторые из которых явно действуют как преступники, которые могут помочь киберпреступникам проводить более масштабные и эффективные атаки.

1. Инфраструктура как поставщик услуг. Злоумышленникам-вымогателям нужна киберинфраструктура, такая как:
   - пуленепробиваемый веб-хостинг;
   - службы регистрации доменов;
   - ботнеты;
   - прокси-службы;
   - службы электронной почты для проведения атак.

Кроме того, многие полагаются на облачный хостинг и другие формы инфраструктуры для проведения атак по краже данных, что относится к новой стратегии, в которой злоумышленники-вымогатели сливают данные, украденные у жертв, чтобы добиться более быстрых и крупных платежей.

2. Хакерские инструменты и провайдеры доступа. Злоумышленники с программами-вымогателями могут приобретать сетевой доступ к жертвам, которые уже были скомпрометированы в рамках схемы, известной как «Доступ как услуга». Другие будут покупать инструменты, которые помогут им самим проникнуть в сети жертв. Одним из примеров являются наборы эксплойтов. Наборы эксплойтов сканируют уязвимости, чтобы закрепиться в сети или развернуть полезную нагрузку, такую как программы-вымогатели. Эти эксплойты позволяют злоумышленникам-вымогателям преследовать более крупные организации с более развитой кибербезопасностью, которые обычно могут позволить себе более высокие выкупы, чем менее сложные организации. Другим примером может служить вредоносное ПО как услуга, позволяющая киберпреступникам брать в аренду программное обеспечение для более эффективного распространения программ-вымогателей.

3. Магазины мошенников. Мошеннические магазины также играют важную роль в операциях с программами-вымогателями. Мошеннические магазины — это подмножество рынков даркнета, которые продают украденные данные, включая пароли и личную информацию (PII) для многих людей, и даже скомпрометированные учетные данные RDP, используемые для получения доступа к сети жертвы. Подобно эксплойтам и доступу, описанным выше, эта информация может помочь злоумышленникам-вымогателям проникнуть в компьютерные сети жертв.

4. Услуги после атаки. Некоторые программы-вымогатели и RaaS применяют расширенные методы вымогательства, такие как найм подпольных колл-центров для прямого вызова жертв и наслоение DDoS-атак на жертв, отказывающихся платить, вероятно, арендованных через поставщиков DDoS-as-a-Service. Администраторы программ-вымогателей даже платят наемным работникам, чтобы помочь жертвам в процессе выплаты выкупа, в том числе профессиональным переговорщикам.

До 2020 года на незаконные сторонние сервисы редко приходилось более 3% средств, отправленных с адресов программ-вымогателей.

С тех пор они значительно увеличились, часто составляя до 9% расходов. С 2021 года общая сумма средств, отправленных с адресов программ-вымогателей, значительно увеличилась, а это означает, что эти цифры отражают значительное увеличение долларов, потраченных на незаконные услуги злоумышленниками программ-вымогателей.

Все эти сторонние поставщики позволяют злоумышленникам-вымогателям более эффективно атаковать более крупные организации, и их растущее использование может быть одной из причин более высоких выплат выкупа, которые мы наблюдаем с 2020 года. Анализ блокчейна показывает, что эти незаконные поставщики услуг стали связующим звеном экосистемы программ-вымогателей. На рисунке 16 показано, как различные типы провайдеров в совокупности связывают самые распространенные штаммы программ-вымогателей на основе истории транзакций криптовалюты.

На рисунке 17 показано, как несколько штаммов программ-вымогателей отправляют средства популярному пуленепробиваемому хостинг-провайдеру.

На рисунке 18 видно, как другие штаммы взаимодействуют с двумя поставщиками вредоносных программ как услуг.

Если злоумышленники с программами-вымогателями по-прежнему будут иметь доступ к передовой инфраструктуре и инструментам, предоставляемым сторонними поставщиками, мы ожидаем, что размеры платежей за выкуп будут продолжать расти. Правоохранительные органы и криптовалютные компании должны работать вместе, чтобы уничтожить не только самих злоумышленников, но и поставщиков инструментов, облегчающих атаки [14].

Тенденция 2021 года: российские программы-вымогатели

Многие штаммы программ-вымогателей связаны с находящимися под санкциями киберпреступными группами, базирующимися в том числе в России или связанными с ней. Такими как печально известная Evil Corp, руководство

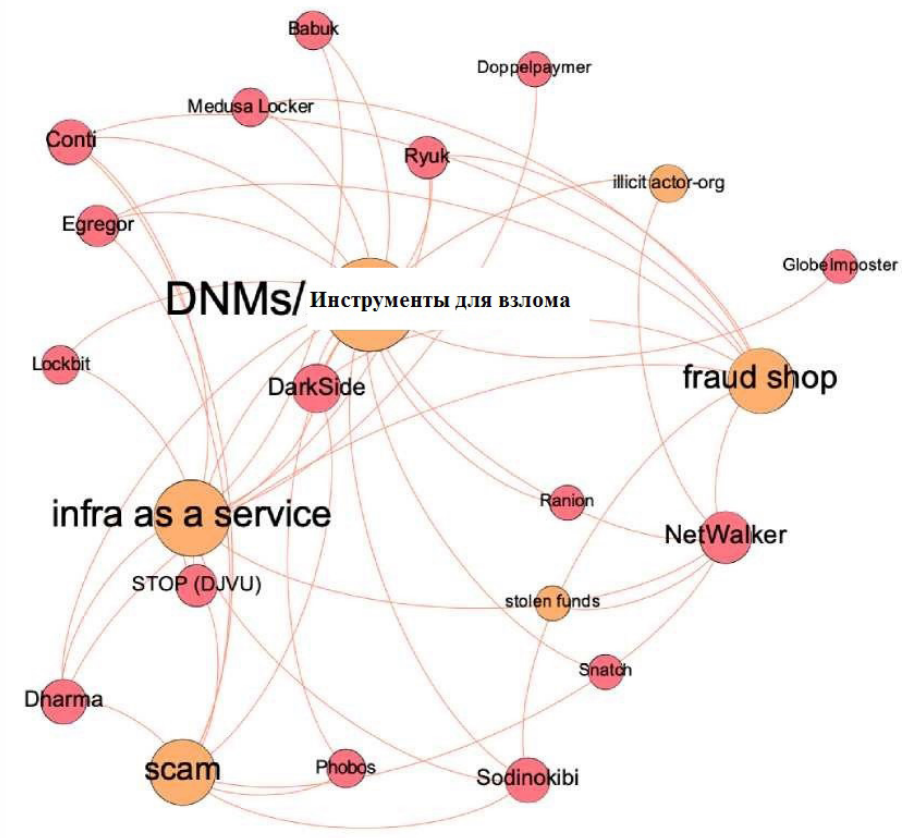

Рисунок 16 – Связь распространенных штаммов программ-вымогателей с различными типами провайдеров

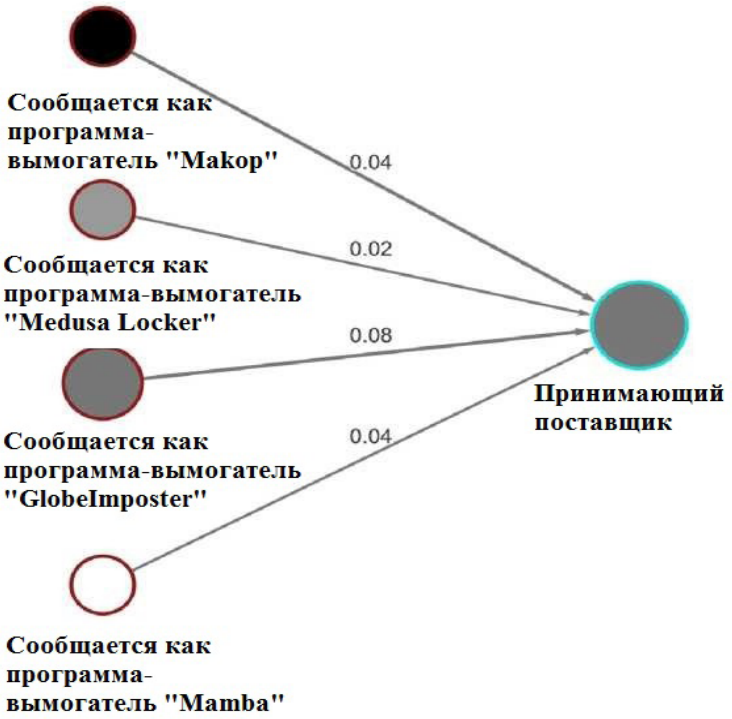

Рисунок 17 – Процесс взаимодействия штаммов программ-вымогателей с хостинг-провайдером

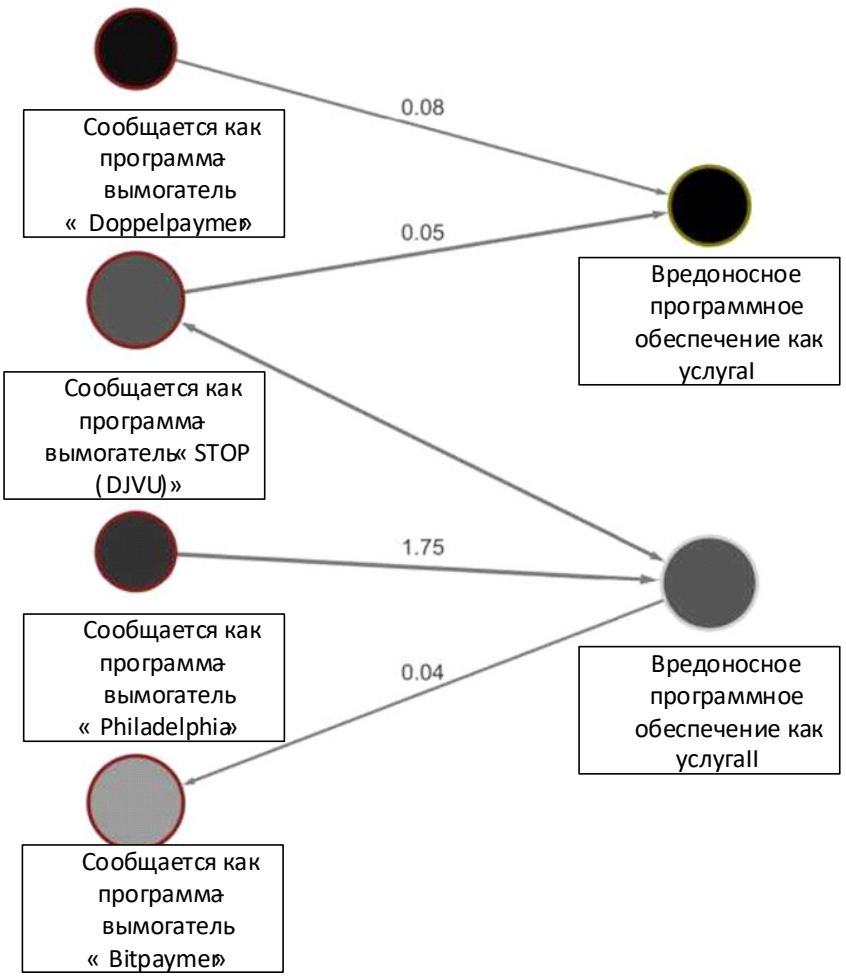

Рисунок 18 – Процесс взаимодействия штаммов программ-вымогателей с поставщиками вредоносных программ

которой, как сообщается, связано с российскими пользователями криптовалюты. Киберпреступники, связанные с Россией и другими русскоязычными странами Содружества Независимых Государств (СНГ) являются одними из самых многочисленных в мире. Российские сервисы получили больше криптовалюты с незаконных адресов, чем в любой другой стране, что позволяет предположить, что связанные с Россией киберпреступники были крупнейшими финансовыми бенефициарами от преступлений, связанных с криптовалютой. Большая часть этой деятельности была управляемой с российского рынка даркнета, который помимо наркотиков продает украденные данные, которые могут быть полезны злоумышленникам-вымогателям.

В 2021 году штаммы программ-вымогателей, связанные с Россией и другими странами СНГ, будут составлять большую долю в общей активности программ-вымогателей. На рисунке 19 показана сравнивая активность в 2020 и 2021 годах для двух категорий штаммов программ-вымогателей:

– штаммы, связанные с Evil Corp;
– штаммы с кодом, предотвращающим шифрование, если программа-вымогатель обнаруживает, что операционная система жертвы находится в стране СНГ. Обычно можно предположить, что эти штаммы возникли в России или других странах СНГ.

Цифры ясны: в совокупности на эти штаммы программ-вымогателей приходится большая активность в 2021 году по сравнению с 2020 годом. На рисунке 20 показан общий объем активности двух программ-вымогателей, на которую приходится десять самых активных программ-вымогателей в 2020 и 2021 годах. Хотя такой график и исключает многие отдельные штаммы, он все же отражает большую часть активности за оба года.

В 2020 году примерно 86% изученных доходов от программ-вымогателей можно отнести к штаммам программ-вымогателей, которые либо связаны с Evil Corp, либо предназначены для избегания стран СНГ. Пока в 2021 году этот показатель составляет 92%. Данные о программах-вымогателях конкретно свидетельствуют о том, что анализ блокчейна, а также сотрудничество с другими фирмами в индустрии криптовалюты будут иметь решающее значение для борьбы с киберпреступностью.

В качестве вывода можно утверждать, что нельзя недооценивать важность более полного и стандартизированного сбора информации в ходе расследований программ-вымогателей, незави-

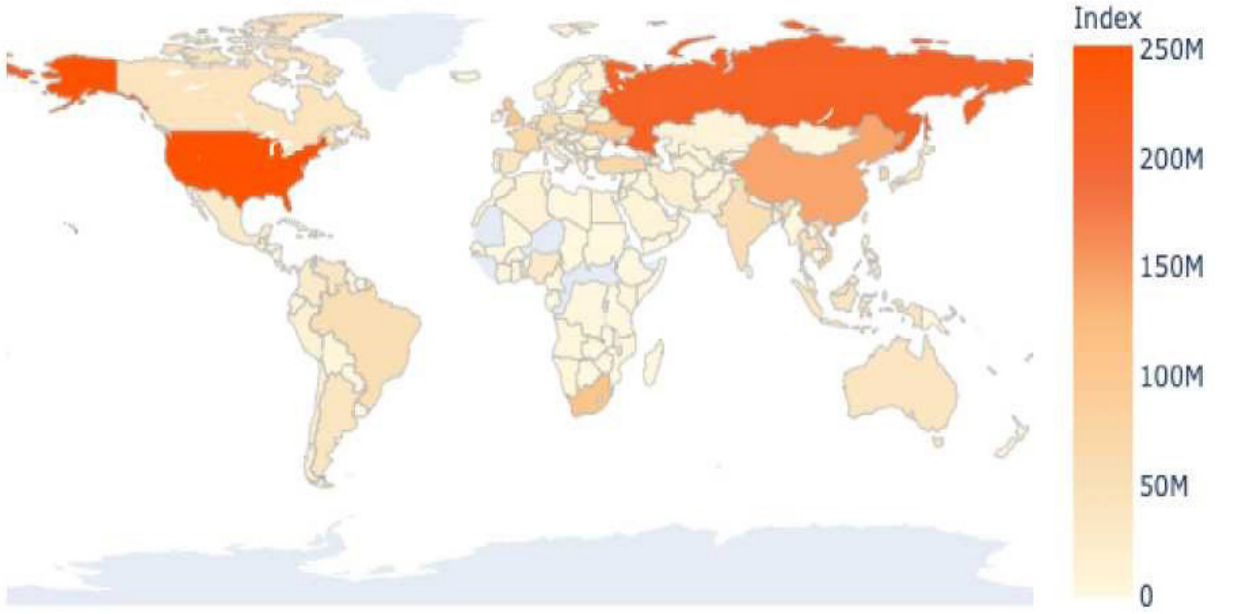

Рисунок 19 – Сравнительная активность для двух категорий штампов в странах СНГ

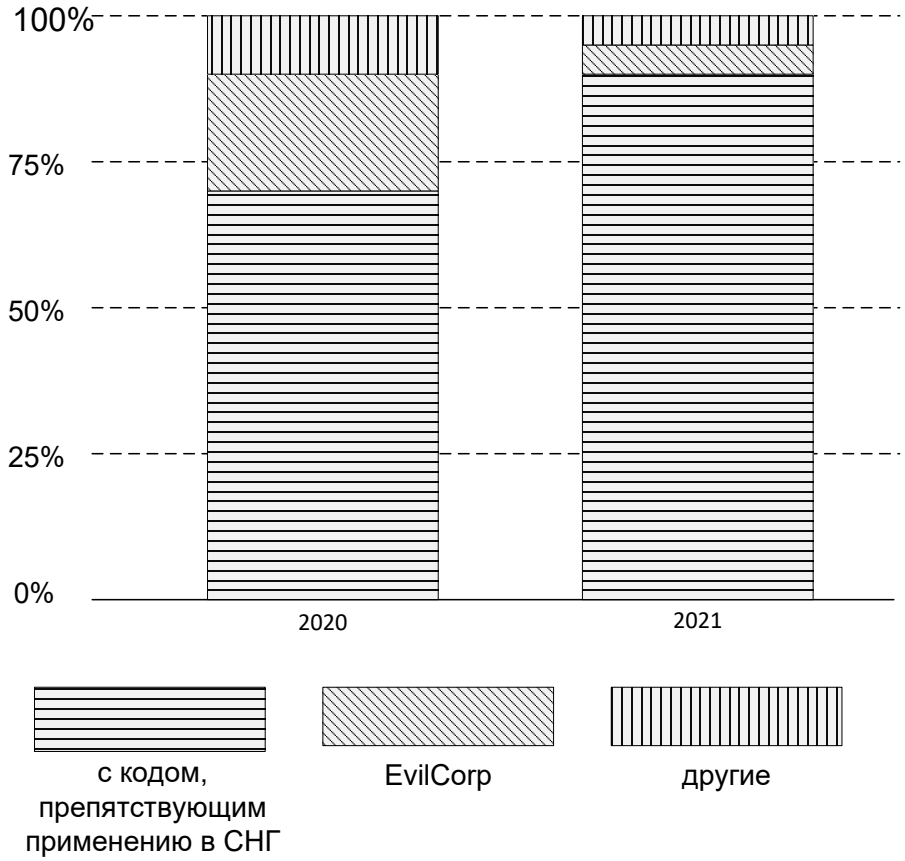

Рисунок 20 – Доля доходов от программ-вымогателей: 2020 г. и 2021 г.

симо от того, предоставлена ли она жертвами или собрана правоохранительными органами. Это может потребовать от Росфинмониторинга и правоохранительных структур, банковского сектора и местных органов власти устранить юридические барьеры и, возможно, создать стимулы для организаций государственного и частного секторов, чтобы они могли сообщать об инцидентах с программами-вымогателями, не опасаясь дополнительных убытков. Программа-вымогатель – это преступление, которое может угрожать каждому аспекту нашей жизни, от инфраструктуры и торговли до угроз национальной безопасности. И в то время, как некоторые утверждают, что природа криптовалюты облегчает преступления программ-вымогателей, ее природа также способствует беспрецедентной прозрачности, которая приносит огромную пользу в системе денежных трансакций и облегчает работу правоохранительным органам.

Список литературы

1. *Кирьянова Д. А.* Криптовалюта: угроза финансовой безопасности РФ // Сборник статей международной практической конференции «Проблемы обеспечения финансовой безопасности и эффективности экономических систем в XXI в.». – СПб: Санкт-Петербургский университет технологий управления и экономики, 2017. – С. 262-268.

2. Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ УК РФ Статья 174: [принят 13.06.1996] – [ред. от 09.03.2022]. - 2022.

3. *Шашкова А.В.* Международная и национальная практика противодействия коррупции и отмыванию незаконных доходов: практика корпоративного управления: учебное пособие. – М.: Аспект Пресс, 2014. – ISBN 978-5-75670755-7.

4. ФАТФ. Руководящие документы. Внесение изменений в стандарты ФАТФ и заявление ФАТФ по виртуальным активам. – 2018.

[Электронный ресурс] – URL: http://www.fedsfm.ru/documents/international-fatf (дата обращения: 07.03.2022).

5. *Allison I.* Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering [Электронный ресурс] / I. Allison. - 2015 - Retrieved 17 May 2015. – URL: https://www.ibtimes.co.uk/bitcoin-tumbler- business-covering-tracks-world-cryptocurrency- laundering-1487480 (дата обращения: 28.02.2022).

6. The Cryptocurrency Tumblers: Risks, Legality and Oversight [Электронный ресурс]. – 2017. URL: https://papers.ssrn.com/sol3/papers.cfm?abstr act_id=3080361 (дата обращения: 25.02.2022).

7. Отчет компании CipherTrace за 3 квартал 2018 года [Электронный ресурс]. - 2018. URL: https://ciphertrace.com (дата обращения: 03.03.2022).

8. Миксер криптовалют: лучший способ сохранить анонимность биткоина [Электронный ресурс]. – 2018. URL: CryptoFox.ru (дата обращения: 27.02.2022).

9. Что такое токен? [Электронный ресурс]. – 2017. URL: https://forklog.com/chto-takoe-token/ (дата обращения: 01.03.2022).

10. USA. Laws. Internal revenue code USA: [passed 1926] – 2018.

11. ФАТФ/ОЭСР. Руководящие документы. Руководство ФАТФ Криминализация финансирования терроризма (рекомендация 5) [Электронный ресурс] – С. 5-53. – 2016. URL: www.fatf-gafi.org (дата обращения: 04.03.2022).

12. Cryptocurrencies by Market Capitalization [Электронный ресурс]. URL: COINMARKETCAP.COM (дата обращения: 06.03.2022).

13. Cryptocurrency Anti-Money Laundering Report 2018 Q2 // Report-AML-20180703, 2018. – P. 1-13.

14. Reuters. T Annual Report 2017 [Электронный ресурс] / T. Reuters. – March 16. 2018. URL: https://annual-report.thomsonreuters.com/downloads/annual- report-2017-thomson-reuters.pdf (дата обращения: 02.03.2022).

Статья поступила в редакцию 11 марта 2022 г.
Принята к публикации 29 марта 2022 г.

Ссылка для цитирования: Зайцев А. К., Матвеев В. В. Экономические преступления с использованием цифровых технологий // Национальная безопасность и стратегическое планирование. 2022. № 1(37). С. 63-81. DOI: https://doi.org/10.37468/2307-1400-2022-1-63-81

Сведения об авторах:

ЗАЙЦЕВ АЛЕКСАНДР КОНСТАНТИНОВИЧ – *аспирант Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург*
e-mail: alexanderzaitsev619@gmail.com

МАТВЕЕВ ВЛАДИМИР ВЛАДИМИРОВИЧ – *доктор технических наук, кандидат экономических наук, профессор, профессор кафедры экономической безопасности Санкт-Петербургского государственного экономического университета, первый вице-президент Петровской академии наук и искусств, действительный член Академии военных наук, г. Санкт-Петербург*
e-mail: 070355mvv@ gmail.com