УДК 343 **Юридические науки**

Милаева Майя Юрьевна, *к. ю. н., доцент, кафедра «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация*

Чихутова Дарья Денисовна, *студент 2-ого курса кафедра «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация*

ПРОБЛЕМА ПРАВОВОГО РЕГУЛИРОВАНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В СФЕРЕ КРИПТОВАЛЮТЫ В РОССИИ

Аннотация: В данной работе будет рассмотрены проблемы, которые возникают в сфере уголовного права в связи с отсутствием законодательного регулирования в сфере криптовалюты, причины влияния ее на платежные системы, будет подробно рассмотрено и разъяснено, почему преступления, связанные с криптовалютой на 2022 год нельзя отнести ни в одну статью УК РФ.

На основе статистических данных будут составлены и проанализированы криминологические портреты преступников, совершающих преступления в данной сфере, а также выявлены основные способы похищения криптовалют.

На основе вышеперечисленного будет составлена и предложена статья для уголовного кодекса Российской Федерации.

Ключевые слова: Уголовный кодекс РФ, преступления в сфере компьютерной информации, криптовалюта, компьютерная безопасность, раздел 28 УК РФ «Преступления в сфере компьютерной информации».

Annotation: In this paper, the problems that arise in the field of criminal law due to the lack of legislative regulation in the field of cryptocurrency, the reasons for its influence on payment systems will be considered in detail and explained why crimes related to cryptocurrency for 2022 cannot be attributed to any article of the

Criminal Code of the Russian Federation.

Based on statistical data, criminological portraits of criminals committing crimes in this area will be compiled and analyzed, as well as the main methods of stealing cryptocurrencies will be identified.

Based on the above, an article for the Criminal Code of the Russian Federation will be compiled and proposed.

Key words: Criminal Code of the Russian Federation, prevalence in the field of computer information, cryptocurrency, computer security, section 28 of the Criminal Code of the Russian Federation "Crimes in the field of computer information".

Введение.

Рассмотрим понятие компьютерной безопасности.

Из неофициальных источников: это раздел информационной безопасности, характеризующий невозможность возникновения ущерба компьютера, превышающего величину приемлемого ущерба для него от всех выявленных и изученных источников его отказов в определенных условиях работы и на заданном интервале времени. То есть это защита цифровой информации в сети Интернет.

Еще одно определение, которое понадобится - киберпреступление. Официального определения нет, поэтому сформулируем самостоятельно. Киберпреступление - любое преступление в сфере компьютерной информации, а правонарушитель в сфере компьютерной безопасности - хакер.

Статистические данные о преступности в сфере компьютерной безопасности в России

Согласно статистике сайта cdep.ru за последние 2 года (2020-2022) наблюдается рост преступлений по статьям 272-274.1 УК РФ (Раздел 28 Преступления в сфере компьютерной безопасности) [7]. В 2020 году было зарегистрировано 137 осужденных по данным статьям, а в 2021 году было зарегистрировано уже 225 осуждённых по данным статьям. Особенно резкий

скачок был зарегистрирован в 2022 году, за первое полугодие которого по данному разделу был осужден 131 человек. Это связано с появлениями новых технологий и пандемией, прошедшей в 2020-2021 годах.

Года	Количество преступлений
2012	280
2013	268
2014	218
2015	235
2016	185
2017	203
2018	129
2019	165
2020	137
2021	225
2022(1 полугодие)	131

Таблица 1 – Сравнительная таблица количества преступлений в различные года по статьям 272-274.1 УК РФ

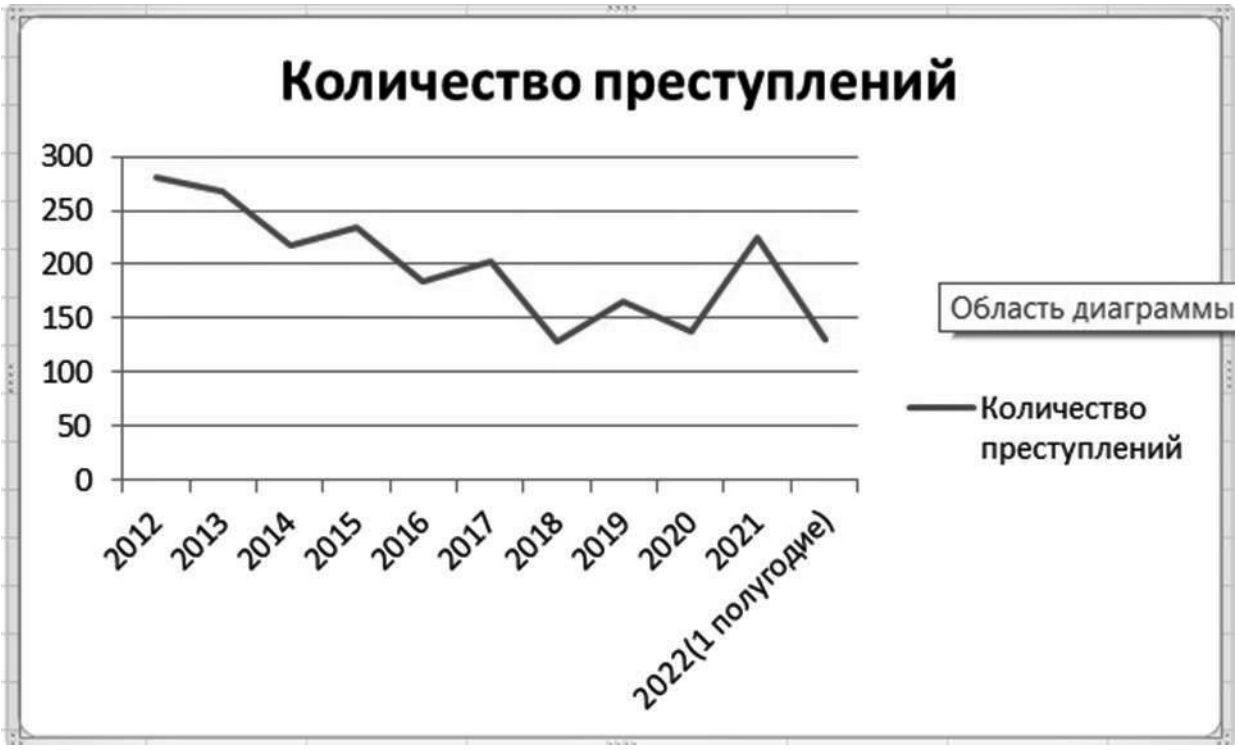

Рис.[1] – Диаграмма количеств преступлений в различные года по статьям 272-274.1 УК РФ

Наглядно посмотреть количество преступлений в 2012-2022 года можно посмотреть на рис. [1]. Раздел 28 («Преступления в сфере компьютерной безопасности») был добавлен в 2011 году, но по нему статистики нет, однако стоит обратить внимание на количество преступлений, совершенных в 2012 году, оно максимально за десятилетие. Можно заметить также постепенный спад преступности в данной области в 2012-2019 и резкий подъем в 2020-2022.

Это показывает актуальность темы компьютерной безопасности в уголовном праве в 2022 году. В данной работе будет рассмотрена компьютерная безопасность в сфере криптовалюты, регулирования которой, по мнению автора, не хватает в УК РФ [13].

Основная часть.

Для начала стоит внести ясность в понятие криптовалюта. Криптовалюта - это единица учета децентрализованной платежной системы [12]. Эта система представляет собой записи о транзакциях, которые хранятся на компьютерах по всему миру. У данной валюты нет физического эквивалента, но ее можно конвертировать в любые денежные единицы и обратно. В гражданском законодательстве ее регулирует закон “О цифровой валюте”, который говорит о том, что на территории РФ ее можно покупать и продавать, но при этом важно фиксировать все транзакции для налоговой службы, перед которой необходимо отчитываться за прибыль от сделки с криптовалютой [4].

При этом на территории России она не платежеспособна. Согласно этому же закону «запрещено использование цифровых финансовых активов и утилитарных прав для оплаты товаров и услуг на территории Российской Федерации».

На данный момент нет статьи в Уголовном кодексе РФ, которая вводит наказание за преступления, связанные с цифровыми финансовыми активами, по причине политики государства по укреплению единственной платежеспособной валюты в РФ – рубля, а также по причине того, что криптовалюта - явление относительно новое. Она была создана в 2009, но распространение получила лишь в 2017 году, с появлением биткоина.

По мнению автора, стоит внести статью под номером 272.1 в Уголовный кодекс РФ о цифровой финансовой валюте, так как официально, она разрешена на территории государства, с нее можно получать прибыль и она является одним из связующих звеньев в развитии отношений между Россией и других государств.

Сразу появляется вопрос, почему же нельзя применять для квалификации содержимого статьи, которые уже есть в уголовном кодексе? Тут рассмотрим подробно. Отметим статьи, которые могут, на первый взгляд, регулировать обращение криптовалюты.

К ним относятся:

1. Статья 272 УК РФ «Неправомерный доступ к компьютерной информации» в совокупности со статьей 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

2. Статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации».

3. Статья 159.3 УК РФ «Мошенничество с использованием электронных средств платежа».

4. Статья 158 УК РФ «Кража».

Теперь последовательно разберем каждый из них.

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации» в совокупности со статьей 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».

Криптовалюту можно рассматривать как компьютерную информацию, потому что, как уже было сказано выше, это не платежная система, а лишь запись о транзакциях, которые можно копировать и изымать как и любую другую компьютерную информацию. Чтобы изъять данную «информацию» понадобиться вредоносная компьютерная программа, которая предусмотрена статьей 273 УК РФ. На первый взгляд, получается совокупность преступлений с минимальным наказанием в 2 месяца и максимальным в 6 лет.

И здесь можно заметить первое несоответствие. Криптовалюту можно

перевести в денежную единицу, а значит это еще и денежное хищение. То есть срок должен быть больше, потому что даже при краже с использованием электронных денежных средств назначено наказание до 6 лет со штрафом либо с ограничением свободы, либо без такового. Но хищение криптовалюты создает уязвимость в системе. Это может вызвать негативные последствия для других пользователей, не связанных с преступником или жертвой. Также сумма похищенной криптовалюты, по данным аналитической компании в сфере цифровых активов Chainalysis, чаще всего бывает не менее 1 млн, что эквивалентно краже в особо крупном размере [11].

Отсюда становится понятно, что статья 158 УК РФ «Кража» в данном случае тоже не подходит, потому что максимальное наказание за похищение криптовалюты по данной статье будет меньше, чем стоило бы дать, учитывая ущерб, который может быть принесен, как владельцу сбережений, так и платформе.

Статьи 159.3 УК РФ и 159.6 УК РФ не подходят, потому что не все преступления связанные с криптовалютой, происходят из-за человеческого фактора, а официальное определение мошенничества, которое дано в уголовном кодексе Российской Федерации: мошенничество - хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием.

Таким образом, приходим к выводу, что преступления, связанные с криптовалютой нельзя отнести ни в одну статью уголовного кодекса Российской Федерации, имеющейся на 2022 год.

По мнению автора, ее стоит добавить. Во-первых, по данным аналитической компании в сфере цифровых активов Chainalysis, с января по июль 2022 года киберпреступники украли криптовалюту на 1,9 млн. долларов, что почти на 60% больше, чем за тот же период годом ранее [11].

Во-вторых, государству выгодно ввести уголовное наказание за хищение криптовалюты. Так как в таком случае, больше людей в России будут в нее вкладываться, что создаст дополнительные источники дохода с помощью

налогов. Стоит отметить, что не в небольшом количестве стран сейчас регулируется криптовалюта, то есть ее регулирование подтолкнет иностранных инвесторов вкладываться в криптовалюту и регистрировать платформы для нее именно здесь. Это может поднять как экономический уровень страны, так и показать прогрессивность России относительно других стран [2].

Исходя из сказанного выше, можно понять, что добавить статью стоит в главу 28 «Преступления в сфере компьютерной информации», так как в данном случае криптовалюта выступает в роли особого рода компьютерной информации, которую можно перевести в денежный эквивалент. При том, что хищение происходит с использованием компьютерных систем. В частности, статью стоит добавить под номером 272.1 УК РФ. Здесь стоит сделать упор именно на неправомерный доступ к компьютерной информации.

Для того чтобы составить статью нужно для начала составить криминологический портрет преступника.

Криминологический портрет хакера

Хакерами чаще всего являются мужчины (65%) с высшим техническим образованием (60%) или студенты [5]. Замкнуты и общаются только через компьютер на английском языке с добавлением других символов. В среднем в возрасте от 17 до 26 лет. Не имеют судимости и живут в городской среде [9].

94% не имеют психических отклонений, оставшиеся 6% имеют психические отклонения, не исключающие вменяемость [3]. Невменяемых, согласно статистике, среди киберпреступников нет [1].

Это означает, что единственное, что объединяет киберпреступников - навыки в технической сфере и программировании. Это значит, что специальный субъект в данном случае не нужен.

Таким образом, были определены субъект преступления, номер статьи, куда будут внесены изменения, и рассмотрены схожие статьи, которые могут послужить основой для законодательного регулирования криптовалюты. Приступаем к формулированию самой статьи.

Начать следует с официальной статистики того, каким образом данные

преступления совершаются чаще всего. Для этого возвращаемся к данным аналитической компании в сфере цифровых активов Chainalysis [11].

Один из самых популярных способов, это мошенничество, но оно попадает под статьи 159, 159.3, 159.6 УК РФ, поэтому далее будут рассмотрены случаи, не включающие данный состав преступления.

Самый популярный на данный момент способ похищения криптовалюты - взлом бирж, на которых она хранится. В 2022 году этот способ обогнал даже фишинговые рассылки (рассылки сообщений, в которые встроена вредоносная программа), уточняет Chainalysis [11]. Из наиболее ярких примеров можно выделить два крупных хищения, произошедших в первую неделю августа 2022 года. Хакеры взломали блокчейн-проект Solana(блокчейн-цифровая база данных информации, которая отражает все совершенные транзакции) и украли криптовалюту с 7700 кошельков клиентов, а также блокчейн-мост Nomad(протокол, соединяющий два блокчейна и позволяющий взаимодействовать между ними), который делает переводы между сетями. В результате взлома злоумышленники украли криптовалюту на 200 млн долларов [6; 8; 10].

Такие взломы происходят из-за того, что многие биржи хранят приватные ключи для кошельков пользователей, изначальное предназначение которых восстановлять доступ при утраченном пароле и блокировка подозрительных счетов.

Это значит, что здесь имеет место 272 и 158 статьи УК РФ, в совокупности здесь можно дать максимально 10 лет. Но это также создает уязвимость в системе, поэтому считаю, что 10 лет должно быть минимальным наказанием, а максимальным 15. Стоит добавить, что здесь нет смысла в штрафе в качестве наказания. Как уже было сказано выше, хищение криптовалюты происходит в особо крупном размере, а штраф должен быть больше, чем похищенная сумма. Это может также вызвать проблему с эквивалентом суммы в заработную плату или иной доход осуждения за определенный срок.

Есть много других менее популярных способов взлома, о которых рассказывает основатель торгового терминала для криптовалют Letit Рустам Буркеев [10]. К примеру, внесение изменений в смарт-контракт или использование исходных багов в них, для выведения средств. Взлом облачных хранилищ и заражение компьютера жертвы вирусом, который подменяет адрес получателя при отправке монет.

Можно заметить некоторое сходство. Во многих требуется вредоносное программное обеспечение, человеческий фактор или программное обеспечение изначально должно иметь баг, также их объединяет то, что после некоторых взломов на компьютере жертвы может появиться уязвимость. Это, разумеется, и будет основой для назначения наказания.

Случай, при котором на компьютере жертвы появляется уязвимость или потерю важных данных, нужно вынести отдельной частью. К примеру, если попытка взлома включает в себя троян, который удаляет антивирус или просто замедление работы устройства.

Также отдельной частью, стоит вынести случаи, когда взлом производится группой людей по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а также случаи, которые повлекли за собой тяжкие последствия или создали угрозу их наступления. Под этим в данном случае подразумевается не вышеупомянутый случай с удалением данных или созданием уязвимостей, а более серьезные последствия, такие как полная остановка платформы в связи с ее не функциональностью.

Таким образом, можно переходить к формулированию статьи.

Статья 272.1 УК РФ. Хищение криптовалюты

1. Хищение криптовалюты,-

Наказывается лишением свободы на срок до 4 лет с ограничением свободы на срок до одного года либо без такового.

2. То же деяние, которое повлекло за собой уязвимость устройства или системы или потерю данных,-

наказывается лишением свободы до 6 лет с ограничением свободы на срок до двух лет либо без такового.

3.. То же деяние, совершенное в особо крупном размере,-

Наказывается до 12 лет лишения свободы с ограничением свободы на срок до двух лет либо без такового.

4. То же деяние, предусмотренное первой, второй или третьей настоящей статьи, если оно повлекло тяжкие последствия или угрозу их наступления,-

Наказывается до 15 лет лишения свободы с ограничением свободы на срок до двух лет либо без такового.

Примечание: 1. Под криптовалютой понимается единица учета децентрализованной платежной системы, которая может быть конвертирована в любые денежные единицы и обратно.

2. Под уязвимостью понимается недостаток в системе, используя который, можно намеренно нарушить её целостность и вызвать неправильную работу.

3.Под особо крупным размером понимается сумма больше 1 миллиона рублей.

Заключение.

За последние два года в России возросло количество киберпреступлений, появились новые виды компьютерных преступлений. Одно из них было рассмотрено в данной работе. Согласно официальной статистике аналитической компании в сфере цифровых активов Chainalysis хищение криптовалюты - популярное явление, которое набирает обороты с каждым годом. С 2021 года количество этих преступлений выросло на 60%. Чаще всего данные преступления совершают мужчины, живущие в городах, в возрасте от 17 до 26 лет и имеющие техническое образование. Самыми популярными способами хищения криптовалют является взлом бирж и мошенничество. В итоге работы была предложена редакция новой статьи.

Библиографический список:

1. Введенская О.Ю. Характеристика личности интернет-преступников // Вестник Краснодарского университета МВД России. 2015.№ 4. С. 116-118.

2. Карасёва М.Ю. Понятие свободы личности как объекта уголовно-правовой охраны// Гуманитарный вестник. 2012. № 2 (2). С. 1 // Международный журнал прикладных и фундаментальных исследований. 2016. № 10-4. С. 665-667.

3. Карасёва М.Ю. Проблемы уголовной ответственности за незаконное помещение в психиатрический стационар // Международный журнал прикладных и фундаментальных исследований. 2016. №10-4. С. 665-667.

4. Компьютерная справочная правовая система России (электронный ресурс). URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 16.11.2022).

5. Милаева М.Ю. Современный взгляд на криминологический портрет серийного убийцы // E-Scio. 2019. №7 (34). С. 519-525.

6. Образовательный портал компании Binance (электронный ресурс). URL: https://academy.binance.com/ru/articles/what-s-a-blockchain-bridge (дата обращения: 16.11.2022).

7. Портал правовой статистики судебного департамента при Верховном суде Российской Федерации (электронный ресурс) URL: http://www.cdep.ru/?id=79 (дата обращения 16.11.2022).

8. Портал финансового супермаркета и информационного агентства Banki.ru (электронный ресурс). URL: https://www.banki.ru/news/daytheme/?id=10975614 (дата обращения 16.11.2022).

9. Пучков О.А. «Социально-криминологический портрет хакера: концептуальный образ» Вопросы российского и международного права. 2020. Том 10. № 3А. С. 60-71.

10. Сайт американского финансово-экономического журнала Forbes(электронный ресурс). URL: https://www.forbes.ru/investicii/475171-samoe-opasnoe-zveno-sam-celovek-kak-voruut-kriptovalutu-i-mozno-li-ee-vernut (дата обращения: 16.11.2022).

11. Сайт аналитической компании в сфере цифровых активов Chainalysis (электронный ресурс). URL: https://blog.chainalysis.com/reports/crypto-crime-midyear-update-2022/ (дата обращения 16.11.2022).

12. Сайт интернет-издания о бизнесе, стартапах, инновациях, маркетинге и технологиях vc.ru (электронный ресурс). URL: https://vc.ru/u/1188077-mine-exchange/437781-chto-takoe-kriptovalyuta-obyasnyaem-prostymi-slovami (дата обращения 16.11.2022).

13. Уголовный кодекс Российской Федерации от 13.12.1996 №63- ФЗ (ред. От 24.03.2022) (с изм. и доп. вступ. в силу с 01.04.2022) - Москва: ПРОСПЕКТ,2022-384с.