ТЕХНИЧЕСКОЕ ЗАДАНИЕ
И
СТАНДАРТ

на выполнение работ по атаке на пиринговую платёжную систему “Биткойн”

Минск 2021

Содержание

1. Общие сведения

1.1.Полное наименование работы и ее условное обозначение

Полное наименование работы: атака на пиринговую платёжную систему “Биткойн”.
Условное обозначение работы: атака на Биткойн.

1.2. Исполнитель

Исполнителем проекта является Общество с ограниченной ответственностью “Элвис и Бурундуки”, именуемое в дальнейшем “Исполнитель”.

1.3. Заказчик

Заказчиком проекта является физическое лицо Чергинец Дмитрий Николаевич,гражданина Республики Беларусь, проживающая по адресу: г. Минск, пр. Независимости 4, паспорт: MP7778800 выдан Советским РУВД г.Минска 03.06.2018 г., именуемый в дальнейшем “Заказчик”.

1.4. Языки программирования проекта

Языки программирования, которые используются в проекте:

- Python 3.8;
- C++ 20;
- Wolfram Mathematica 12.3;

1.5. Программные библиотеки

Специальные программные библиотеки, которые используются в проекте:

- Python:
    - grequests и requests - асинхронное создание и получение веб-запросов;
    - bs4 - парсинг веб-сайтов;
    - hashlib - основные хеш-функции;
    - ecdsa - взаимодействие с Elliptic Curve Digital Signature Algorithm для создания приватных и открытых ключей;
    - base58 - форматирование контрольной суммы в адрес Биткойна.
- C++:
    - OpenSSL - криптографическая библиотека: используется для функций sha256 и ripemd160
    - secp256k1 - библиотека для работы с эллиптической кривой secp256k1: используется для генерации приватных и публичных Bitcoin ключей;
    - cpp-httplib - библиотека для работы с https запросами: используется для проверки сгенерированного адреса.
- Wolfram Mathematica: отсутствует.

1.6. Срок выполнения работы

Начало: со дня заключения технического задания с заказчиком.
Окончание: до 09.05.2021 включительно

1.7. Стоимость и порядок оплаты услуг Исполнителя

Заказчик оплачивает услуги Исполнителя:

- по факту их выполнения;
- в соответствии с нормативами правового акта, регулирующего текущую и итоговую аттестацию, установленным Министерством Республики Беларусь от 22.12.2003 года № 21-04-1/105;
- путем выставлением отметки всем членам команды Исполнителя в ведомости для отметок.

В случае, если Исполнитель окажет Заказчику технические услуги не в полном объеме, а также при расторжении данного Технического задания по инициативе Заказчика или отказе Заказчика от исполнения Технического задания, Заказчик производит оплату фактически оказанных технических услуг, подтвержденных документально.

1.8. Порядок предъявления заказчику результата работы

По завершении работы Исполнитель предъявляет на электронную почту Заказчика (cherginetsdn@gmail.com) ссылку на проект в информационной системе https://github.com. Заказчик изучает полученную документацию и, при наличии замечаний, в праве в течении трёх рабочих дней после предоставления ссылки на выполненные задания отправить замечания для корректировки работы.
В случае, если Заказчик не сообщает своих замечаний по работе в течении трёх рабочих дней после предоставления ссылки, проект считается завершённым и все последующие замечания будут не действительны.

1.9. Порядок разрешения споров и условия расторжения Технического задания и стандарта

Все споры и разногласия, которые могут возникнуть из настоящего Технического задания, должны разрешаться путем переговоров между Сторонами. В случае невозможности достичь соглашения путем переговоров, споры между сторонами разрешаются в соответствии с законодательством Республики Беларусь либо в следующих ситуациях:

- Техническое задание может быть расторгнут до истечения срока его действия по взаимному согласию Сторон.
- Техническое задание может быть расторгнут в одностороннем порядке в случаях определенных законодательством Республики Беларусь, а также в следующих случаях:
    - выявления обстоятельств, делающих невозможным совершение сделки;

- появления обстоятельств, при которых Исполнитель не вправе оказывать технические услуги Заказчику.

При расторжении Технического задания в одностороннем порядке инициатором расторжения высылается второй стороне уведомление не позднее, чем за 3 (три) рабочих дней до даты расторжения.

1.10. Обязанности Исполнителя

Исполнитель обязан:

- Организовать сбор документации, необходимых для проекта;
- Установить перечень лиц имеющих права в отношении выполнения проекта и информировать Заказчика о наличии таких лиц и их правах;
- Соблюдать конфиденциальность информации, полученной в процессе предоставления технических услуг Заказчику. Обязанность соблюдения конфиденциальности остается в силе после завершения отношений между Исполнителем и Заказчиком;
- Информировать Заказчика о ходе выполнения проекта. Предупреждать о возможных препятствиях и изменениях в процессе выполнения работы.

1.11. Обязанности Заказчика

Заказчик обязан:

- Ознакомиться с предоставленной Исполнителем документацией и Техническим заданием проекта;
- Обеспечить Исполнителя информацией и документами, необходимыми для выполнения им своих обязательств;
- Соблюдать конфиденциальность информации, полученной в процессе взаимодействия с Исполнителем , в том числе не разглашать содержание (условия) Технического задания. Обязанность соблюдения конфиденциальности остается в силе после завершения отношений между Исполнителем и Заказчиком;
- Оплатить услуги Исполнителя в соответствии с условиями Технического задания.
- Известить Исполнителя в письменной форме о намерении изменить условия Технического задания.

1.12. Ответственность сторон

- Стороны признают, что исполнение обязательств Исполнителем обусловлено волей и действиями Заказчика. Если Исполнитель не может выполнить условия Технического задания надлежащим образом не по своей вине, ответственность его не наступает.
- Исполнитель не несет ответственность за предоставление неверной информации должностными лицами других предприятий, учреждений, организаций и Заказчика.

- Стороны не несут ответственности за невозможность или просрочку исполнения обязательств по Техническому заданию, если в процессе работы выявятся обстоятельства, препятствующие совершению сделки
- В случае нарушения одной из Сторон своих обязательств, она выплачивает другой стороне в течение 3 (трех) рабочих дней с момента предъявления соответствующего требования, штрафную неустойку в размере двойной ставки от суммы, установленных Исполнителем и Заказчиком за оказание технического обслуживания
- В случае возникновения обстоятельств непреодолимой силы (форс-мажорных) обстоятельств, Стороны освобождаются от ответственности..

1.13. Защита работы

Защита проекта проходит в форме беседы Заказчиком с командой Исполнителя:

- директор/математик: Яблонская Анна Олеговна
- системный/бизнес-аналитик: Кирилло Дмитрий Евгеньевич
- программисты/тестировщики: Алексеев Александр Александрович
  Карлович Алексей Олегович
  Корбовский Никита Андреевич.

Дата защиты работы согласуется с Исполнителем и Заказчиком после предъявления на электронную почту Заказчика (cherginetsdn@gmail.com) ссылки на проект.

1.14. Дополнительные условия заключения сделки

- Техническое задание составлено в двух экземплярах, по одному для каждого лица:Исполнитель и Заказчик, именуемые в дальнейшем “Стороны”. Признание недействительным части Технического задания не влечет недействительности его в целом.
- Стороны свидетельствуют, что на момент подписания Технического задания Заказчик ознакомлен с документом, содержащим порядок выполнения алгоритма работы программы, а также получил все разъяснения по указанию услуги.
- Исполнитель за исполнение Технического задания назначает ответственным: директора Общества с ограниченной ответственностью “Элвис и Бурундуки” Яблонская Анна Олеговна, гражданка Республики Беларусь, проживающая по адресу: г. Минск, ул. Карла Маркса 38, паспорт: MP2223355 выдан Фрунзенским РУВД г.Минска 22.11.2012 г.

2. Цели и задачи проекта

2.1. Цели работы

- Поиск адресов, на каждом из которых хранится сумма биткоинов, большая порога L;
- Юридические аспекты правообладания биткоином: можно ли воровать чужие биткоины, подбирая ключ;

- Разработка алгоритма атаки на адреса с большими суммами путем перебора ключей;

2.2. Задачи работы

- Правовые аспекты взламывания аккаунта, на котором хранятся биткоины;
- Попытаться взломать аккаунт при помощи программ C++, Mathematica, Python;
- Оценить вероятность успешности атаки;
- Сравнить скорость работы данных программ.

3. Термины и определения

В настоящем техническом задании применяются следующие термины с соответствующими определениями:
Атака 51% – это захват системы, при котором мощность атакующего превышает всю остальную мощность системы минимум на 1%.
Биткойн - пиринговая платёжная система, использующая одноименную единицу для учёта операций.
Блокчейн - выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию.
Декрет № 8 «О развитии цифровой экономики» - декрет президента Республики Беларусь Александра Лукашенко, включающий меры по либерализации условий ведения предпринимательской деятельности в сфере информационных технологий, в частности, цифровой экономике.
Доказательство выполнения работы (англ. Proof-of-work, PoW) — принцип защиты сетевых систем от злоупотребления услугами, основанный на необходимости выполнения на стороне клиента некоторой достаточно длительной работы (нахождение решения задачи), результат которой легко и быстро проверяется на стороне сервера.
Доказательство доли владения (англ. Proof-of-stake, PoS) — метод защиты в криптовалютах, при котором вероятность формирования участником очередного блока в блокчейне пропорциональна доле, которую составляют принадлежащие этому участнику расчётные единицы данной криптовалюты от их общего количества.
Ключ - параметр, который управляет криптографическими операциями выработки и проверки электронной цифровой подписи, зашифрования и расшифрования, генерации псевдослучайных чисел и др.
Конфиденциальность - гарантия того, что сообщения доступны для использования только тем сторонам, которым они предназначены.
Личный ключ - ключ, который связан с конкретной стороной, не является общедоступным и используется в настоящем стандарте для выработки электронной цифровой подписи и для разбора токена ключа.
Открытый ключ - ключ, который строится по личному ключу, связан с конкретной стороной, может быть сделан общедоступным и используется в настоящем стандарте для проверки электронной цифровой подписи и для создания токена ключа.
Парсинг — сбор и систематизирование информации, размещенную на определенных сайтах, с помощью специальных программ, автоматизирующих процесс.
Подлинность - гарантия того, что сторона действительно является владельцем

(создателем, отправителем) определенного сообщения.
Секретный ключ - ключ, который связан с конкретными сторонами, не является общедоступным и используется в настоящем стандарте для генерации псевдослучайных чисел и для защиты других ключей.
Сообщение - двоичное слово конечной длины.
Смарт-контракт - компьютерный алгоритм, предназначенный для формирования, контроля и предоставления информации о владении чем-либо.
Токен ключа - сообщение, которое передается от одной стороны другой при транспорте ключа и представляет собой транспортируемый ключ в защищенной форме, а также данные, необходимые получателю для снятия защиты.
Транспорт ключа - конфиденциальная передача ключа от одной стороны другой.
Целостность - гарантия того, что сообщение не изменено при хранении или передаче.
Цифровая (электронная) валюта - электронные деньги, которые используются как альтернативная или дополнительная валюта.
Хэш-значение - двоичное слово фиксированной длины, которое определяется по сообщению без использования ключа и служит для контроля целостности сообщения и для представления сообщения в (необратимо) сжатой форме.
Хэширование - выработка хэш-значений.
ICO, Initial coin offering, (англ. - «первичное предложение [размещение] монет») — форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией.

4. Законность проекта

4.1. Законность проекта в Республике Беларусь

Законодательством Республики Беларуси установлены базовые правила отношений, связанных с применением технологии блокчейн, а также даны определения таким ключевым понятиям, как блокчейн, токены, криптовалюты, майнинг, смарт-контракты. То есть в Республике Беларусь узаконены биржи криптовалют, операторы обмена криптовалют, майнинг, смарт-контракт, блокчейн, токены после принятия Декрета № 8 «О развитии цифровой экономики», подписанным Президентом Республики Беларусь 21 декабря 2017 года. Это означает, что в Республики Беларусь сформировано полное правовое регулирование криптовалют,что делает последующие попытки взламывания личного кошелька пользователя незаконным в соответствии с законодательством Республики Беларусь.
В случае успешного выполнения проекта: взлом кошелька пользователя и перевода его средств на кошелёк нужного нам пользователя, к Заказчику и Исполнителю могут быть применены следующие статьи Уголовного кодекса Республики Беларусь:

- Статья 205. Кража (наказывается общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на срок от трех до двенадцати лет с конфискацией имущества);
- Статья 206. Грабеж (наказывается общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до четырех лет, или

лишением свободы на срок от трех до восьми лет с конфискацией имущества или без конфискации.);

- Статья 209. Мошенничество (наказываются общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на срок от трех до десяти лет с конфискацией имущества);
- Статья 212. Хищение путем использования компьютерной техники (наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или я лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения);
- Статья 215. Присвоение найденного имущества (наказывается общественными работами, или штрафом, или арестом на срок до трех месяцев);
- Статья 216. Причинение ущерба в значительном размере посредством извлечения имущественных выгод в результате обмана, злоупотребления доверием или путем модификации компьютерной информации при отсутствии признаков хищения (наказывается штрафом, или исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до пяти лет или лишением свободы на тот же срок);
- Статья 218. Умышленные уничтожение либо повреждение имущества (наказывается общественными работами, или штрафом, или исправительными работами на срок до двух лет, или арестом на срок до трех месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на срок от семи до двенадцати лет);
- Статья 219. Уничтожение либо повреждение имущества по неосторожности (наказывается исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет);
- Статья 235. Легализация («отмывание») материальных ценностей, приобретенных преступным путем (наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью со штрафом, или лишением свободы на срок от пяти до десяти лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью);
- Статья 236. Приобретение либо сбыт материальных ценностей, заведомо добытых преступным путем (наказывается штрафом, или исправительными работами на срок до двух лет, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на срок от двух до шести лет);
- Статья 254. Коммерческий шпионаж: похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну, с целью их разглашения либо незаконного использования (наказывается арестом на срок от двух до шести месяцев, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от одного года до пяти лет);
- Статья 285. Создание преступной организации либо участие в ней (1. Деятельность по созданию преступной организации либо руководство преступной организацией или входящими в нее структурными подразделениями

– наказываются лишением свободы на срок от пяти до тринадцати лет с конфискацией имущества или без конфискации.
2. Участие в преступной организации в любой иной форме – наказывается лишением свободы на срок от трех до семи лет с конфискацией имущества или без конфискации);

- Статья 288. Принуждение лица к участию в преступной деятельности (наказывается арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от двух до семи лет);
- Статья 349. Несанкционированный доступ к компьютерной информации (наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок);
- Статья 350. Модификация компьютерной информации (наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения);
- Статья 351. Компьютерный саботаж: умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от трех до десяти лет);
- Статья 352. Неправомерное завладение компьютерной информацией (наказывается общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок);
- Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (наказывается штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет);
- Статья 354. Разработка, использование либо распространение вредоносных программ (наказывается штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на срок от трех до десяти лет);
- Статья 355. Нарушение правил эксплуатации компьютерной системы или сети (наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок);

Можно заметить, что согласно Статьям 215, 349, 352 случайный подбор ключа не является законным методом овладения кошельком пользователя или цифровой

криптовалюты “Биткойн” и будет наказываться законом. Стоит отметить, что во всех странах мира существуют схожие законодательные Статьи на этот счет, а наказания за данные злодеяния применяются более строже.

Важно отметить, что существует вариант подбора ключа утерянного или забытого Биткойн кошелька, но в данном случае все тогда зависит от удачи хакера: если пользователь вспомнит приватный ключ от своего личного кошелька и увидит, что суммы не сходятся, то пользователь имеет полное право обратиться в суд за незаконное присвоение найденного имущества, несанкционированный доступ к компьютерной информации и неправомерное завладение компьютерной информацией. Причём, если с данного кошелька будут переведены Биткойны на другой кошелек пользователя, то человеку, совершившему незаконную передачу цифровых средств, грозит следующие статьи: грабёж, кража, хищение путем использования компьютерной техники. И шанс выигрыша в суде очень высок по этому делу у пользователя, которого взломали.

Из вышеприведённых фактов можно вынести следующий вывод: если хакер подобрал приватный ключ к затерянному Биткойн кошельку и при этом владелец кошелька не вспомнил свой ключ к кошельку, то он останется безнаказанным. Если пользователь все-таки вспомнил свой приватный ключ, то здесь есть два сценария развития событий: удастся узнать личность хакера или не удастся узнать. На данный момент, отследить последовательность перевода Биткойнов возможно. Существуют множество компаний, которые, используя свой алгоритм и комплекс данных, могут найти человека, которые перевел Биткойны на свой кошелек, если он даже использовал множество Биткойн кошельков. Но есть существенный минус того, что некоторые сервисы Биткойн кошельков не требуют идентификации пользователя, соответственно, узнать личность хакера становится практически нереально, так как они все используют VPN сервисы и узнать истинный IP делается невозможным. Если все-таки удастся узнать личность хакера, то владелец кошелька имеет полное право подать на него в суд и владелец, с вероятностью 99%, выиграет суд и хакеру придется вернуть все Биткойн средства, а также компенсацию за причиненный вред.

4.2. Законность проекта в других странах мира

Во многих странах уже дана правовая оценка криптовалюте и уже внесены поправки в Законодательство этих стран, установлены базовые правила отношений, связанных с применением технологии блокчейн, а также даны определения, связанные с цифровой экономикой и криптосистемой.
В ряде стран официально разрешены операции с криптовалютами. Обычно они рассматриваются как товар или инвестиционный актив и для целей налогообложения подчинены соответствующему законодательству.
В одних странах биткойны признают в качестве расчётной денежной единицы , в других биткойн является законным платёжным средством с налогом на покупку. В некоторых странах операции с биткойнами запрещены для банков, но разрешены для физических лиц, в определенных государствах на криптовалюты распространяются такие же правила, как и на иностранные валюты. Соответственно, любая попытка взламывания, незаконного перевода цифровой валюты на счет других пользователя и

изменение данных кошелька пользователя будет наказываться Законом стран, где совершенно преступление или в каком государстве пользователь был взломан.

5. Алгоритм компьютерной программы

5.1. Генерация приватного ключа

Вход: —.
Выход: priv$\in\mathbb{N}$ размером 32 байта, priv$\in${1, 2^{256}}.
Алгоритм:

1. Генерируем случайное число между 1 и p (p — целое число, порядок базовой точки G эллиптической кривой Secp256k1, константа(p≈2^{256})).
   priv = randomInt(1, p)

5.2. Генерация публичного ключа

Вход: priv (приватный ключ) $\in\mathbb{N}$ размером 32 байта, priv$\in${1, 2^{256}}.
Выход: pub$\in\mathbb{N}$ размером 65 байт.
Алгоритм:

1. Перемножаем priv и G (G — целое число размером 65 байт, базовая точка эллиптической кривой Secp256k1, константа).
   *pub = priv*G*

G = “04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8” (в 16-ой форме).

5.3. Генерация адреса

Вход: pub (публичный ключ) $\in\mathbb{N}$ размером 65 байта.
Выход: address— строка в формате base58.
Алгоритм:

1. Переводим pub в 16-ую форму записи.
   pub = pub.hex()
2. Хешируем pub с помощью SHA-256.
   pub = pub.SHA-256()
3. Хешируем pub с помощью RIPEMD-160 и получаем число размером 20 байт
   *pub = pub.*RIPEMD-160*()*
4. Добавляем в начале network ID byte и сохраняем во временную переменную temp
   temp= “0x00” + pub
5. Дважды хешируем temp с помощью SHA-256, сохраняя результат в pub.
   pub = temp.SHA-256()
   pub = pub.SHA-256()
6. Берем первые четыре байта из полученного числа и приписываем их к temp. Получаем наш адрес размером 25 байт.
   temp += pub(1:4)

7. Преобразуем результат в строку base58
   address = temp.base58()

6. Вероятность успешной атаки на Биткойн

6.1. Вероятность взлома при помощи используемых программ

- Python:$1 * 10^{-62}$ %;
- C++: $1 * 10^{-45}$ %;
- Wolfram Mathematica: $1 * 10^{-90}$ %.

Исходя из этих данных можно сделать следующий вывод: шансов на взлом Биткойн кошелька при помощи используемых нами программ нет.

6.2. Теоретическая вероятность взлома Биткойн кошелька

Технически, подобрать приватный ключ и получить доступ к криптовалюте возможно. Однако это займет немало времени. По подсчетам специалистов, на взлом простого, старого биткойн-кошелька с помощью видеокарт среднего класса при скорости в 600 MK/s для подбора ключа уйдет около 385934935200739541752907479121 92 лет.

Компания Google в сентября 2019 года создало квантовый суперкомпьютер, который смог за 3 минуты и 20 секунд выполнить расчеты, на которые самому мощному компьютеру из существующих потребовалось бы 10 тысяч лет. Но специалисты в области криптографии заявили, что квантовое превосходство, которое представил Google, демонстрирует практическую применимость квантовых компьютеров к определенным классам задач. Они утверждают, что это совершенно другой класс проблем, не имеющий к взлому криптографии никакого отношения

Многие авторитетные издания в области блокчейна также считают, что прорыв Google ничего не значит, ведь их изобретение относится к простейшим квантовым вычислениям, и здесь даже не может идти и речи о взломе криптографических алгоритмов. По их словам, они не знают, возможна ли эволюция квантовых компьютеров: вероятно, добавление новых кубитов приведет к экспоненциальному росту стоимости.

Взамен перебора приватного ключа, хакеры пользуются именно кражей приватных ключей с сервисов или устройств пользователей. Зная тот самый заветный приватный ключ, определить публичный адрес и получить доступ к хранилищу проще простого.

Заключение Технического задания и стандарта

Дата заключения Технического задания и стандарта: 04.05.2021
С условиями, требованиями, выполнениями и алгоритмом Технического задания и стандарта Исполнитель и Заказчик ознакомлены и согласны:

М.П. _____
Исполнитель
Яблонская Анна Олеговна

М.П._____
Заказчик
Чергинец Дмитрий Николаевич