

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

СОЗ «ТАЙГА»

Версия документа: 1.02 от 22.03.2026

Код: HMA-001-USER-GUIDE

г. Москва, 2026 г.

СОДЕРЖАНИЕ

1. Термины и сокращения.....	6
2. Введение	8
2.1. Назначение приложения	8
2.2. Целевая аудитория.....	8
2.3. Ключевые преимущества	8
2.3.1. Примечание	9
3. Начало работы.....	10
3.1. Требования к браузерам и устройствам.....	10
3.1.1. Поддерживаемые браузеры.....	10
3.1.2. Устройства.....	10
3.1.3. Технические требования	10
3.2. Получение доступа.....	11
3.2.1. Анонимный доступ к сервису	11
Как получить доступ:	11
3.2.2. Регистрация и аутентификация через учетную запись.....	11
Как получить доступ:	11
3.2.3. Аутентификация через LDAP	12
Как получить доступ:	12
4. Сценарии использования.....	13
4.1. Сценарий 1: Создание и чтение записки	13
Откройте главную страницу	13
Введите содержимое записки.....	14
Настройте записку	14
Создайте записку.....	15
Дополнительные действия.....	16
4.2. Сценарий 2. Прикрепление файлов к записке.....	17
Откройте главную страницу	17
Включите возможность прикрепления файлов.....	18
Добавьте нужные файлы	18
Прикрепите изображение / ссылку на файл к тексту записки.....	19
Зашифруйте и отправьте записку	23
4.3. Сценарий 3. Дополнительная защита ссылок	23

4.3.1. Вариант 1: Защита паролем	23
Создайте записку.....	23
Активируйте защиту паролем	23
Скопируйте ссылку.....	25
4.3.2. Вариант 2: Защита сертификатом	25
Подготовьте сертификат	25
Активируйте защиту сертификатом.....	25
Укажите получателя	26
Получите зашифрованную ссылку	27
Скопируйте ссылку.....	27
4.4. Сценарий 4. Создание записки с разметкой Markdown.....	28
4.4.1. Подготовка.....	28
Откройте страницу создания записки	28
Введите содержимое записки.....	29
Введите текст с разметкой.....	30
4.4.2. Заголовки.....	30
4.4.3. Параграфы и перенос строк	31
4.4.4. Списки	31
Нумерованный.....	32
Маркированный.....	32
4.4.5. Блоки кода.....	33
4.4.6. Цитаты	34
4.4.7. Ссылки и изображения.....	34
Ссылка.....	34
Прикрепленное изображение	35
Прикрепленный файл.....	35
4.4.8. Горизонтальная линия	35
4.4.9. Экспорт в PDF / Печать записки.....	36
4.4.10. Клавиши быстрого доступа	36
4.5. Сценарий 5: Создание ключа и отправка сертификата.....	37
4.5.1. Цель.....	37
4.5.2. Управление ключами	37
4.5.3. U2F / FIDO токены.....	39
Особенности.....	39

Создание.....	39
Создание ключа на текущем устройстве.....	44
Поделиться сертификатом.....	46
4.5.4. Рутокен.....	51
Особенности.....	51
Создание.....	52
Поделиться сертификатом.....	55
4.5.5. Мнемоника.....	56
Особенности.....	56
Создание.....	57
Управление существующей мнемоникой.....	58
Поделиться сертификатом.....	58
4.6. Сценарий 6: Чтение записки.....	59
4.6.1. Получение ссылку на записку.....	59
4.6.2. Вариант 1. Ссылка без дополнительной защиты.....	59
4.6.3. Вариант 2. Ссылка защищенная паролем.....	60
4.6.4. Вариант 3. Ссылка защищенная сертификатом.....	61
Рутокен.....	62
FIDO / U2F токен.....	65
Мнемоника.....	68
4.6.5. Вариант 4. Неполная ссылка.....	70
4.7. Сценарий 7: Управление сертификатами. Экспорт/импорт (для хранилища сертификатов).....	70
4.7.1. Экспорт сертификатов.....	70
4.7.2. Импорт сертификатов.....	71
4.7.3. Удаление сертификатов.....	72
5. Интерфейс и основные функции.....	73
5.1. Главная страница (Создание записок).....	73
5.1.1. Элементы управления:.....	73
5.2. Страница управления сертификатами.....	75
5.2.1. Элементы управления:.....	75
5.3. Страница создания ключей.....	77
5.3.1. Элементы управления:.....	77
5.4. Страница создания ссылки.....	80
5.4.1. Элементы управления:.....	80

5.5. Страница чтения записок.....	80
5.5.1. Элементы управления:	81
6. Поддержка.....	84
6.1. Контакты.....	84

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

СОЗ «ТАЙГА» — Сервис обмена записками «Тайга», защищённое решение для одноразовой передачи конфиденциальных сообщений с использованием криптографических методов.

Записка — Зашифрованное сообщение (текстовое и/или содержащее файлы), созданное пользователем и доступное по уникальной ссылке. Может быть одноразовой или многоразовой, с ограниченным временем жизни.

Ключ шифрования — Криптографический ключ, используемый для шифрования/расшифровки содержимого записки. Генерируется на стороне клиента и не передаётся на сервер.

Открытый ключ — Публичная часть криптопары (ключ-пара), необходимая другим пользователям для зашифрования данных, предназначенных именно вам. Из открытого ключа невозможно восстановить закрытый.

Закрытый ключ — Секретная часть криптопары, необходимая только владельцу для расшифровки сообщений, зашифрованных его открытым ключом. Должен храниться в надёжном месте (на токене, в мнемонике или защищённой области браузера).

Сертификат — Файл или объект, содержащий открытый ключ и метаданные (имя владельца, срок действия, цифровая подпись удостоверяющего центра). Используется для шифрования/подписи в соответствии со стандартом CMS (P 1323565.1.025-2019).

ГОСТ 34.11-2018 (Стрибог) — Российский криптографический стандарт хэширования, используемый в СОЗ «Тайга» для генерации ключей и контрольных сумм.

ГОСТ 34.12-2018 (Кузнечик) — Российский блочный шифр, рекомендованный для защиты информации, применяется в СОЗ «Тайга» как основной алгоритм шифрования по умолчанию.

AES — Стандарт симметричного шифрования (Advanced Encryption Standard), используется в режимах, требующих повышенной совместимости или многоступенчатого шифрования.

XOR — Простейший метод побитового шифрования; в СОЗ «Тайга» применяется только для небольших текстов при «Усиленном» режиме защиты (ключ $\geq$ длины сообщения).

CMS (Cryptographic Message Syntax) — Стандарт (RFC 5652) для шифрования и подписи сообщений, реализован в СОЗ «Тайга» в соответствии с Р 1323565.1.025-2019.

PoW CAPTCHA — Доказательство работы (Proof-of-Work), используемое вместо визуальной капчи для защиты от спама и автоматических запросов при создании записок.

U2F / FIDO — Протоколы аутентификации (Universal Second Factor / Fast Identity Online), позволяющие использовать аппаратные токены (Рутокен U2F, YubiKey и др.) для безопасного хранения ключей и расшифровки записок.

Rutoken — Аппаратный крип토폰 (Рутокен ЭЦП 2.0/3.0, Lite, MFA), используемый для хранения закрытых ключей и выполнения операций шифрования/расшифровки.

Мнемоника — Человеческочитаемая последовательность слов (обычно 12 или 24), кодирующая закрытый ключ. Предоставляет удобный способ резервного копирования без использования сторонних программ.

PBKDF2 (Password-Based Key Derivation Function 2) — Алгоритм получения криптографического ключа из пароля, используемый в СОЗ «Тайга» с ГОСТ 34.11-2018 и динамическими итерациями для усиления защиты против offline атак.

Markdown — Легковесный язык разметки, поддерживаемый редактором СОЗ «Тайга», позволяющий форматировать текст (заголовки, списки, код, цитаты).

Web Crypto API / WebAuthn API — Современные JavaScript-интерфейсы браузера для работы с криптографией и аутентификацией по FIDO2.

Сервисный ключ — Ключ, созданный сервисом на внешнем носителе (Rutoken/U2F) или в хранилище браузера, используется исключительно для работы с СОЗ «Тайга» и не влияет на другие сертификаты/ключи на устройстве.

Доверенный сертификат — Сертификат, добавленный администратором системы в глобальный список доверенных. Такие сертификаты защищены от перезаписи при импорте и не могут быть удалены пользователями.

2. ВВЕДЕНИЕ

2.1. Назначение приложения

Сервис обмена записками «Тайга» (СОЗ «Тайга») — это сервис для безопасной передачи и хранения конфиденциальных сообщений с использованием одноразового чтения. Приложение позволяет создавать зашифрованные записки, которые могут быть прочитаны только один раз и после этого автоматически удаляются из системы.

Сервис реализует следующие основные функции:

- Создание зашифрованных сообщений с различными методами шифрования (ГОСТ 34.11-2018, AES, XOR)
- Управление доступом к данным через многофакторную аутентификацию (Rutoken, FIDO, мнемонические фразы)
- Добавление файлов и использование Markdown для форматирования текста
- Настройка времени жизни записки — автоматическое удаление после прочтения или по заданному сроку

2.2. Целевая аудитория

Тайга подойдёт для широкого круга пользователей, например:

- **Юристы и консультанты**, которые обмениваются чувствительными данными с клиентами
- **Команды разработчиков** и IT-специалисты, нуждающиеся в защищенном обмене технической информацией
- **Менеджеры проектов**, контролирующие доступ к важным данным (пароли, схемы архитектуры)
- **Техническая поддержка**, при передаче доступов, одноразовых паролей.
- **Любые пользователи**, стремящиеся обеспечить конфиденциальность своих сообщений

2.3. Ключевые преимущества

1. **Конфиденциальность данных** — все сообщения шифруются на стороне клиента по российским криптографическим стандартам (ГОСТ 34.12-2018), исключая возможность перехвата или расшифровки.

2. **Одноразовое использование** — записка может быть прочитана только один раз, после чего автоматически удаляется. Это гарантирует, что конфиденциальная информация не останется в системе.
3. **Многофункциональность** — поддержка текстовых записок, файлов и сертификатного шифрования позволяет использовать приложение для различных сценариев передачи данных.
4. **Удобный интерфейс** — простая навигация через основные функции (создание, просмотр, удаление) без необходимости установки дополнительного программного обеспечения.
5. **Защита от спама** — использование PoW CAPTCHA при создании сообщений снижает риск автоматических запросов и несанкционированного доступа.

2.3.1. Примечание

В основе приложения используется JavaScript-библиотека WellspringJS, реализующая криптографические функции согласно российским стандартам.

3. НАЧАЛО РАБОТЫ

3.1. Требования к браузерам и устройствам

3.1.1. Поддерживаемые браузеры

- Google Chrome (версия 80+)
- Mozilla Firefox (версия 75+)
- Safari (версия 13+)
- Microsoft Edge (версия 80+)

Примечание:

Для функций криптографии и работы с Rutoken требуется поддержка Web Crypto API и JavaScript ES6+

3.1.2. Устройства

- **Компьютер** — полный функционал, рекомендуется для основных операций
- **Мобильные устройства (iOS/Android)** — адаптированная верстка, ограниченный функционал

Примечание:

На мобильных устройствах некоторые функции могут быть менее удобны — например, переключение между разделами требует дополнительного тапа

Примечание:

На мобильных устройствах скорости шифрования могут быть ниже чем на компьютерах из-за особенностей процессоров.

3.1.3. Технические требования

- Браузеры должны поддерживать JavaScript, HTML5 и WebAuthn API
- Для Rutoken устройств требуется:
 - Установленный плагин в браузере

3.2. Получение доступа

3.2.1. Анонимный доступ к сервису

Если администратор включил анонимный доступ к сервису, вы можете получить доступ к функционалу без регистрации и входа в систему.

Как получить доступ:

1. Откройте веб-браузер и перейдите на главную страницу сервиса (например, <https://taiga.ru>).
2. Вы увидите форму создания зашифрованной записки.
3. Заполните необходимые поля:
 - Введите текст записки
 - Прикрепите файлы (не более 10 МБ на файл)
4. Нажмите "Создать записку".
5. Система сгенерирует уникальный URL с встроенным зашифрованным ключом и ID записки.
6. Перешлите полученный URL получателю для доступа к записке.

3.2.2. Регистрация и аутентификация через учетную запись

Если администратор разрешил регистрацию пользователей, вы можете создать учетную запись для доступа к расширенным функциям сервиса.

Как получить доступ:

1. Перейдите на страницу логина (/login).
2. Нажмите кнопку "Зарегистрироваться"
3. Заполните форму регистрации:
 - Укажите имя
 - Введите электронную почту
 - Установите пароль (минимум 12 символов)
4. После успешной регистрации войдите в систему через страницу входа (/login), используя вашу электронную почту и пароль.
5. После успешного входа вы получите доступ к:

- Созданию зашифрованных записок с настройками шифрования
- Управлению своими записками
- Настройке параметров доступа к запискам
- Импорту/экспорту сертификатов для дополнительной защиты

3.2.3. Аутентификация через LDAP

Если администратор настроил интеграцию с LDAP-сервером (например, Active Directory), вы можете войти в систему, используя учетные данные вашей организации.

Как получить доступ:

1. Перейдите на страницу входа (/login).
2. Введите свой логин и пароль, используя учетные данные вашей организации.
3. Сервис проверит ваши учетные данные через LDAP-сервер.
4. После успешной аутентификации вы получите доступ к сервису без необходимости создания отдельной учетной записи.

4. СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

4.1. Сценарий 1: Создание и чтение записки

После открытия сервиса в браузере вы окажетесь на главной странице приложения **Тайга**. Здесь вы можете создать свою первую записку, воспользовавшись удобным интерфейсом.

Откройте главную страницу

После авторизации вы попадёте на экран создания новой записки. Этот экран содержит все необходимые инструменты для шифрования, добавления файлов и выбора метода защиты данных.

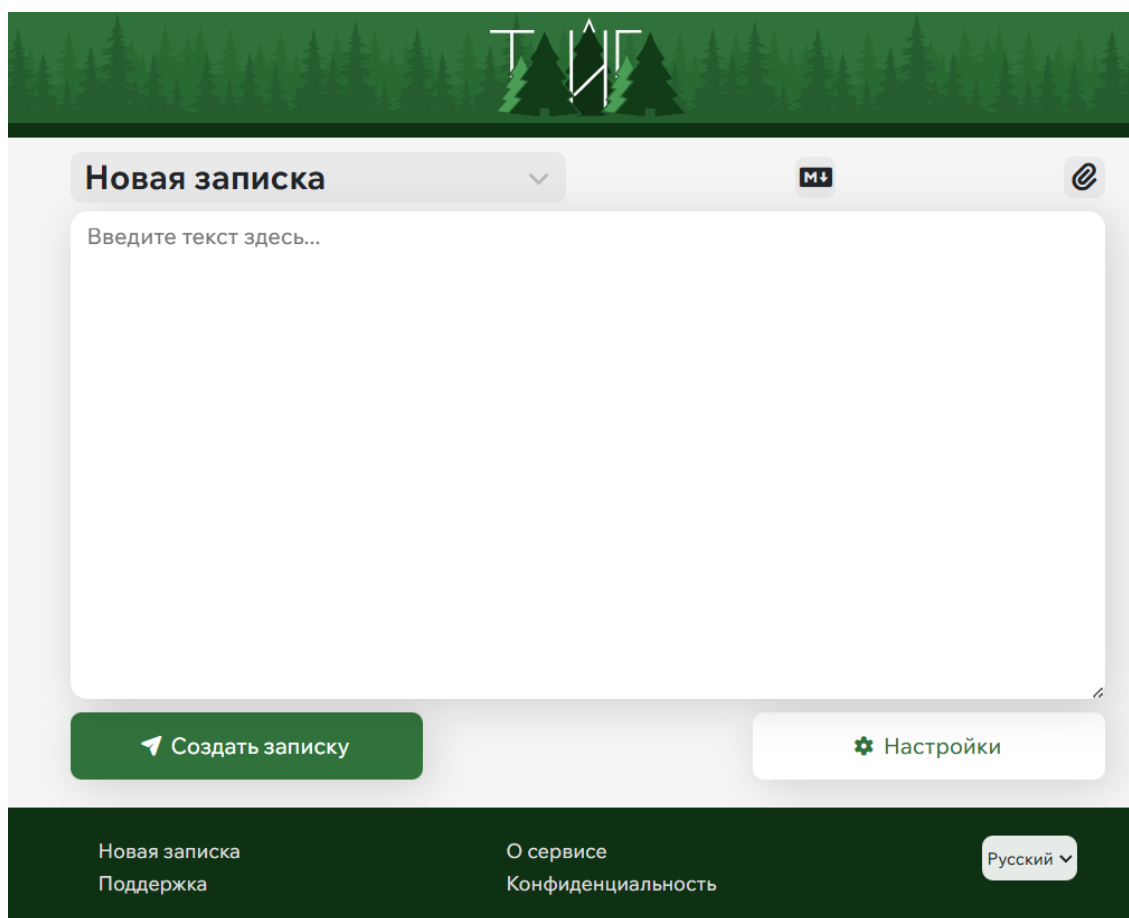


Рисунок 1 — Главная страница

Введите содержимое записки

В центральной части экрана расположен блок **ввода текста**. Здесь можно написать обычный текст или использовать Markdown для форматирования. Для включения Markdown

разметки нажмите «  ».

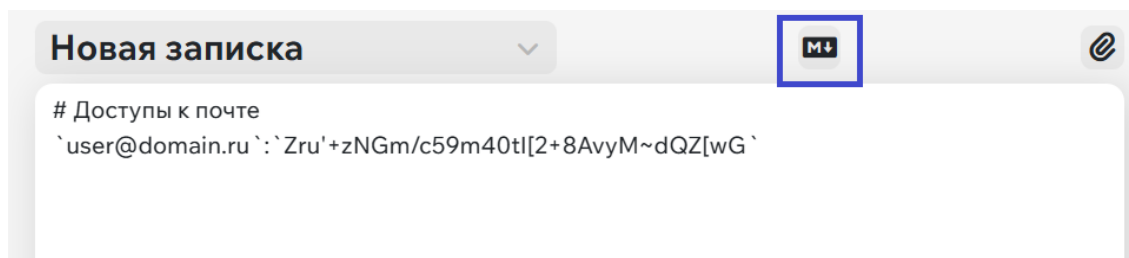


Рисунок 2 — Кнопка для включения Markdown разметки

При включенном Markdown можно включить предпросмотр нажав на иконку «  ».

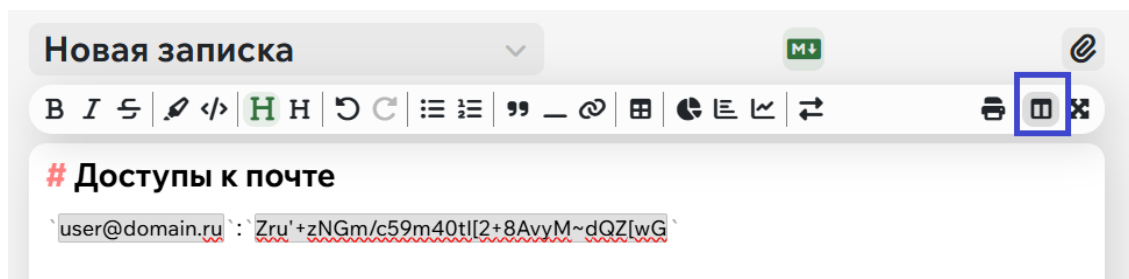


Рисунок 3 — Кнопка для включения предпросмотра Markdown разметки

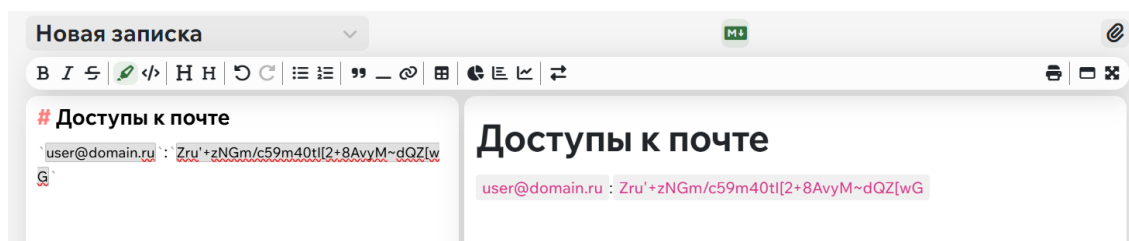


Рисунок 4 — Включенный предпросмотр

Настройте записку

Для большинства сценариев достаточно стандартных настроек, но вы можете настроить записку под себя, для этого откройте блок «**Настройки**»



Рисунок 5 — Кнопка для открытия настроек

В открывшемся поле:

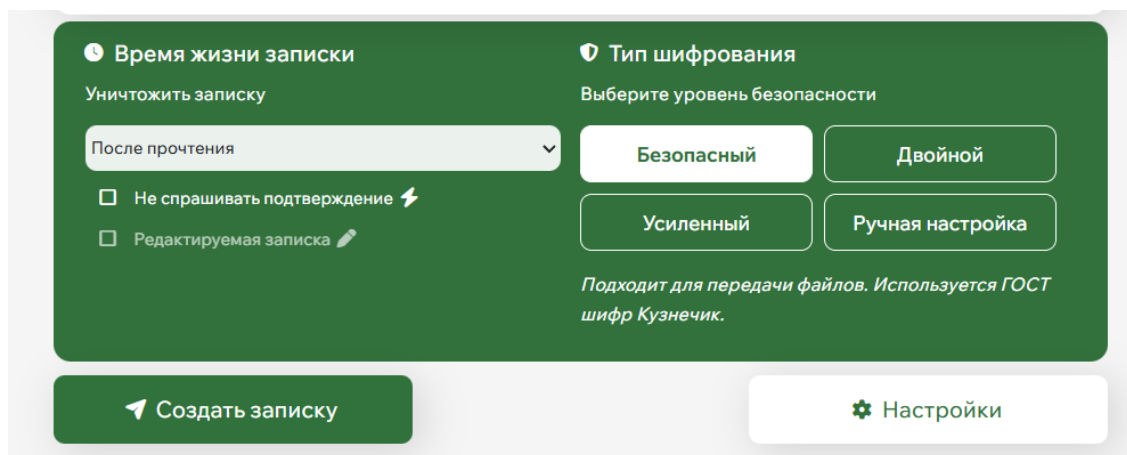


Рисунок 6 — Меню настроек записки

Время жизни записки. Выберите, как долго ваша записка будет доступна:

- **После прочтения** (по умолчанию). Удалится сразу после прочтения, одноразовая.
- **15 минут, 1 час, 7 дней** и т.д.

Метод шифрования. Здесь можно выбрать уровень защиты:

- **Простое:** автоматический выбор режима шифра Кузнечик. (рекомендуется по умолчанию).
- **Двойное / Максимальное:** более высокий уровень защиты. Сначала сообщение шифруется шифром Кузнечик, затем AES
- **Усиленный:** записка шифруется с помощью XOR, ключ больше или равен длине записки. Режим подходит только для небольших текстов.
- **Ручная настройка:** позволяет выбрать конкретные параметры шифрования.

Создайте записку

Нажмите кнопку «Создать записку».

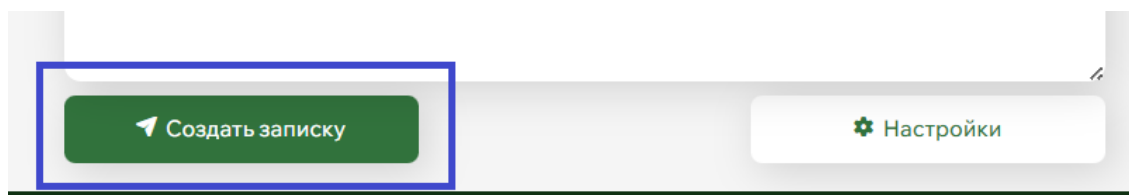


Рисунок 7 — Кнопка для создания записки

После успешного создания появится ссылка на вашу записку.

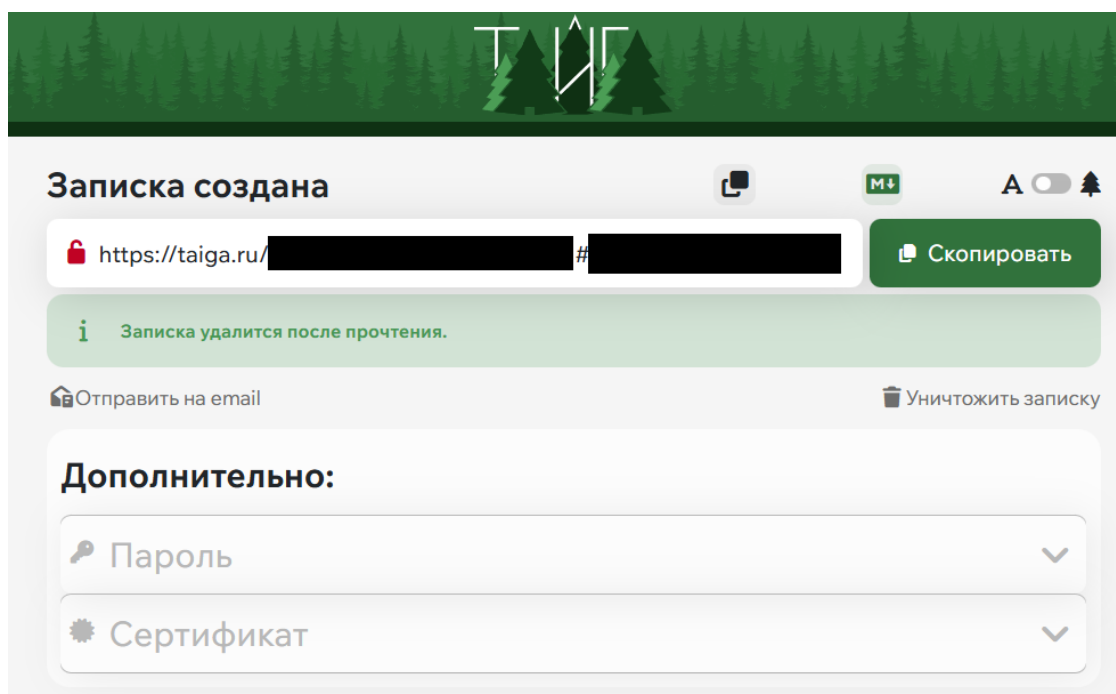


Рисунок 8 — Страница со ссылкой на записку

Важно:

Отправьте эту ссылку получателю, она не будет отображаться снова.

Дополнительные действия

После создания записки доступны дополнительные действия:

- **Дублировать записку** – возвращает на странице редактирования, с ранее заполненной запиской. Позволяет поправить текст и создать ещё одну записку.
- **Копировать ссылку** - чтобы передать её другому человеку.
- **Удалить сейчас** - немедленно удалить запись (необратимо).
- **Зашифровать дополнительно.** Если вы хотите дополнительно зашифровать ключ в ссылке – используйте:

- Пароль
- Импортированные или доверенные сертификаты

4.2. Сценарий 2. Прикрепление файлов к записке

Прикрепление файлов к защищённой записке — удобный способ передачи документов, изображений или других данных вместе с текстом сообщения. Эта функция поддерживается как на этапе создания записки, так и при её редактировании.

Откройте главную страницу

После авторизации вы попадёте на экран создания новой записки. Этот экран содержит все необходимые инструменты для шифрования, добавления файлов и выбора метода защиты данных.

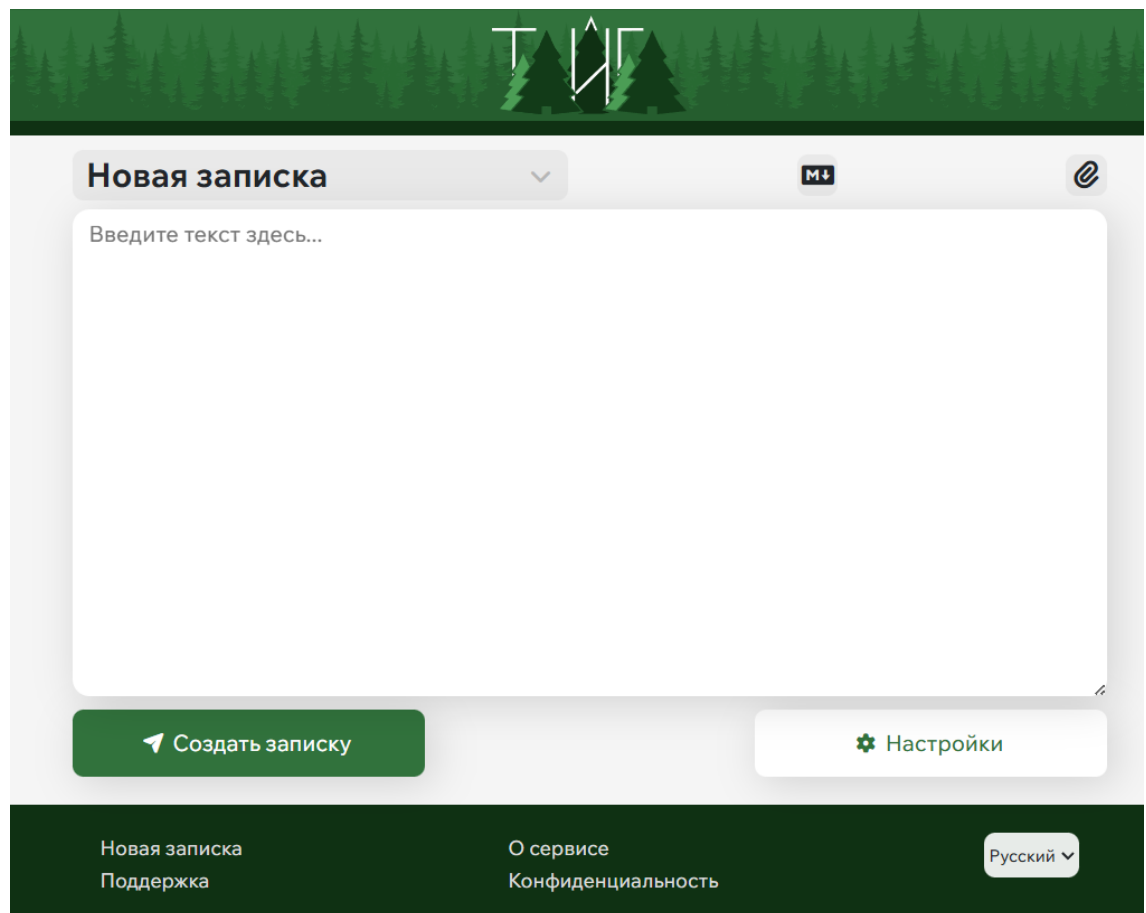


Рисунок 9 — Главная страница

Включите возможность прикрепления файлов

Найдите чекбокс «  » (в интерфейсе он отмечен иконкой скрепки).

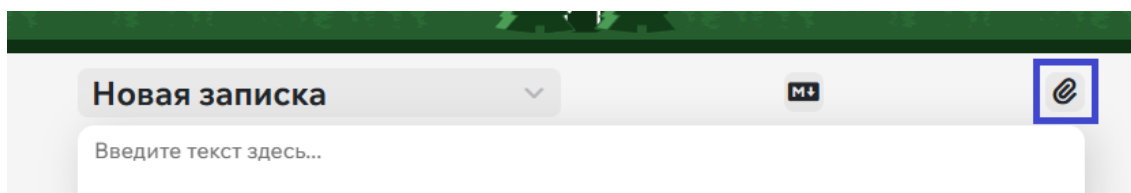


Рисунок 10 — Кнопка прикрепления файлов в интерфейсе

После этого появится специальный элемент управления для выбора файлов.

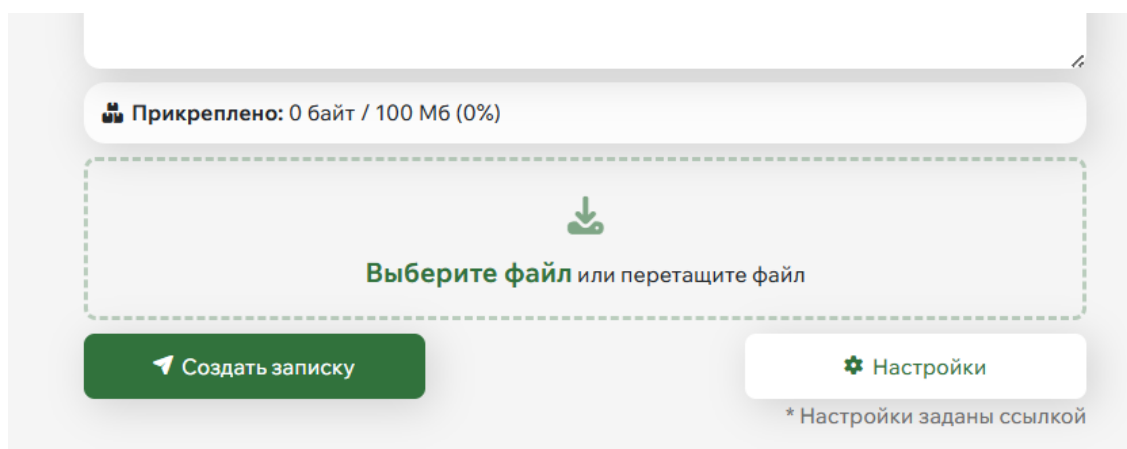


Рисунок 11 — Область выбора файлов

Добавьте нужные файлы

Перетащите файлы в выделенную зону, либо нажмите на кнопку выбора файла и выберите их через проводник.

Прикрепленные файлы отображаются как карточки с полями:

- Имя
- Размер (с указанием в удобных единицах: КВ, МВ)
- Возможность удалить файл перед отправкой
- Возможность вставить ссылку на файл внутри записки

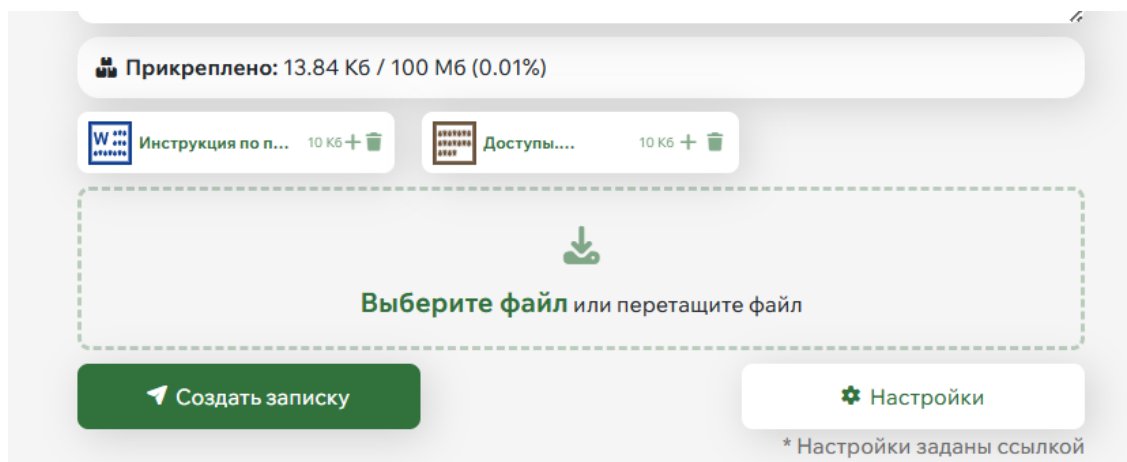


Рисунок 12 — Прикрепленные файлы к записке

Примечание:

Файлы сжимаются перед отправкой.

Примечание:

Прикрепленные файлы шифруются аналогично содержимому записки и не хранятся на сервере в открытом виде.

Прикрепите изображение / ссылку на файл к тексту записки

Выберите в записке место куда хотите добавить файл

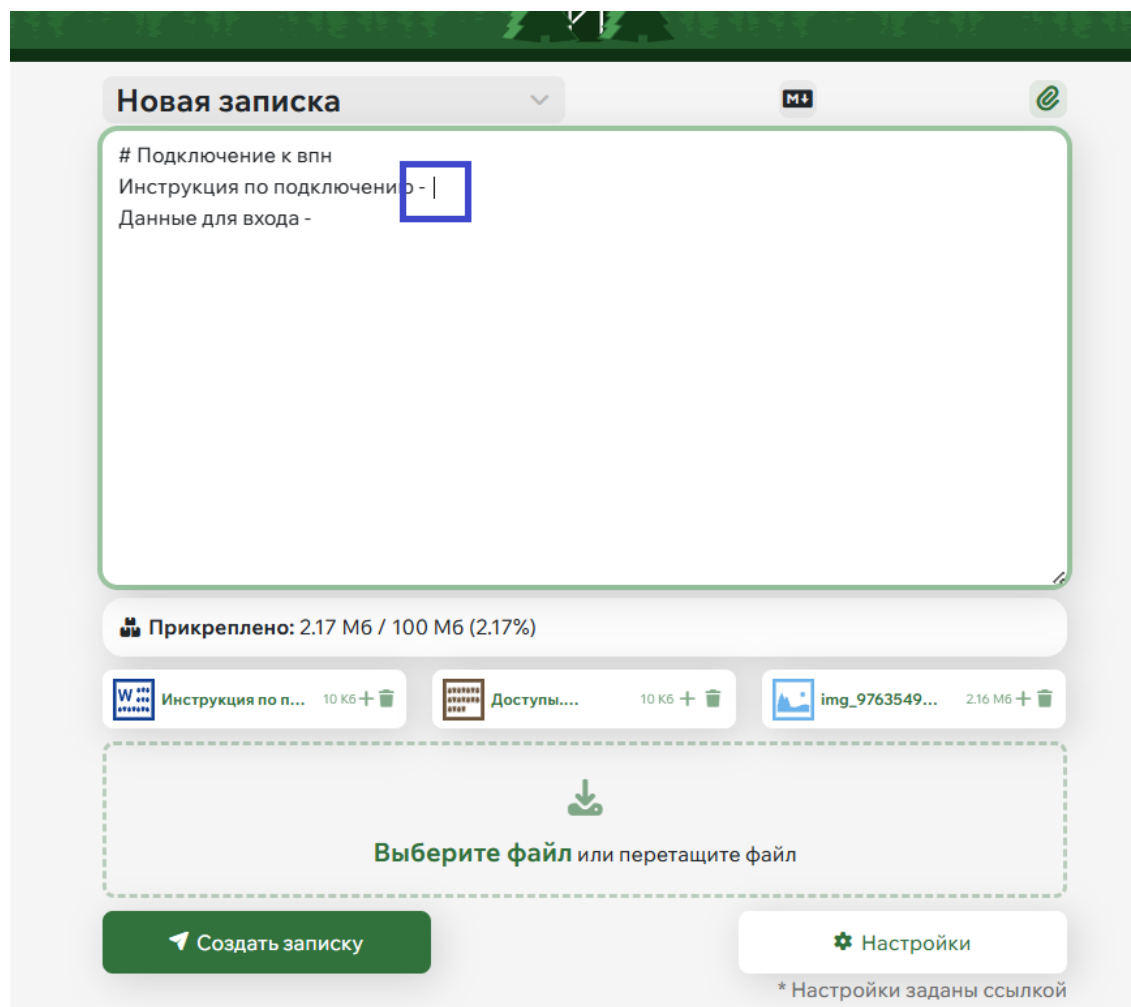


Рисунок 13 — Выбор места в записке для прикрепления файла

Нажмите на иконку «**+**» рядом с файлом, который хотите добавить в текст записки.

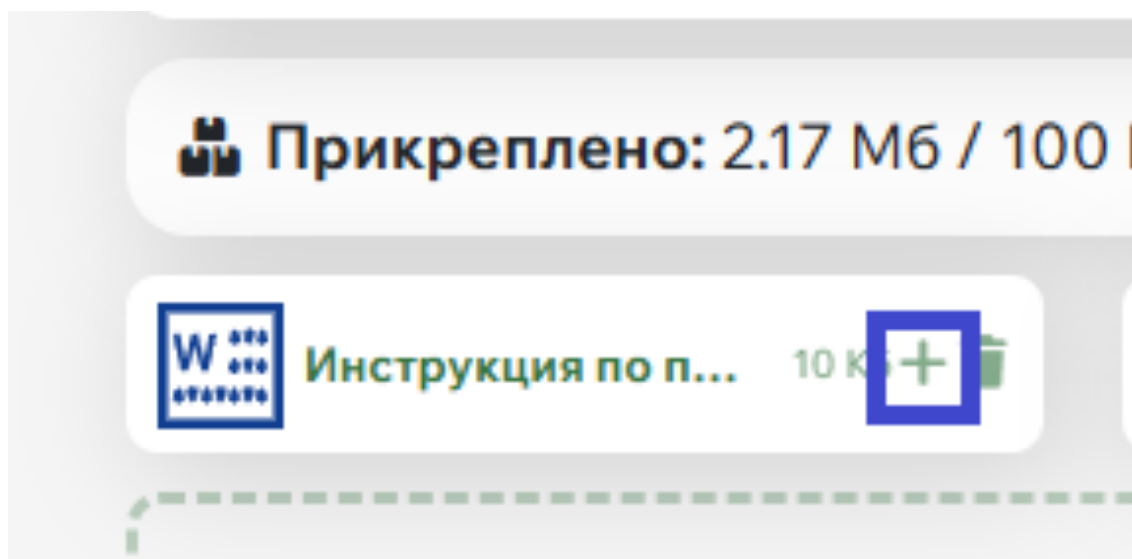


Рисунок 14 — Кнопка добавления ссылки на файл в записку

Ссылка на файл добавится в текст и откроется предпросмотр Markdown разметки

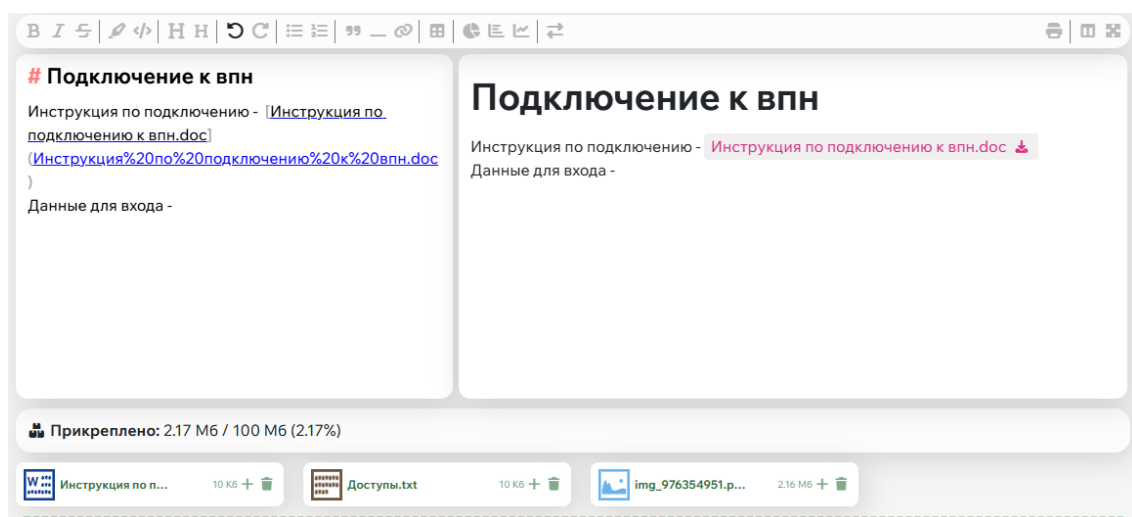


Рисунок 15 — предпросмотр записки с прикрепленной ссылкой на файл

При добавлении изображений через « + » они будут прикреплены к записке через предпросмотр

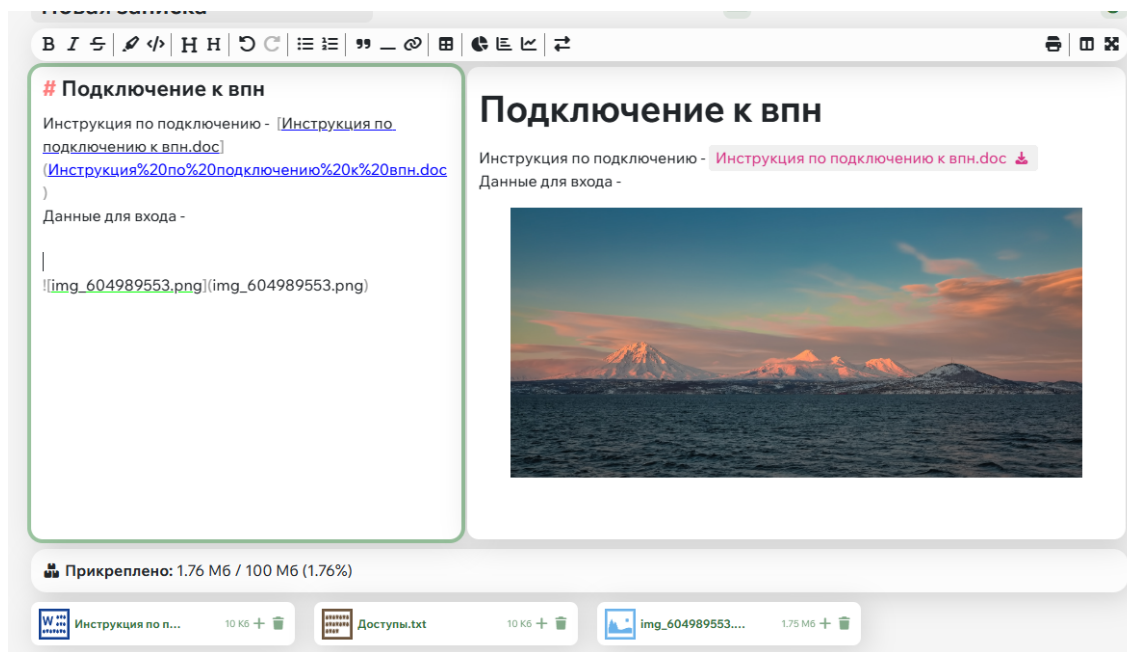


Рисунок 16 — предпросмотр записки с прикрепленной картинкой

Если необходимо добавить ссылку на скачивание картинки уберите восклицательный знак в начале строки

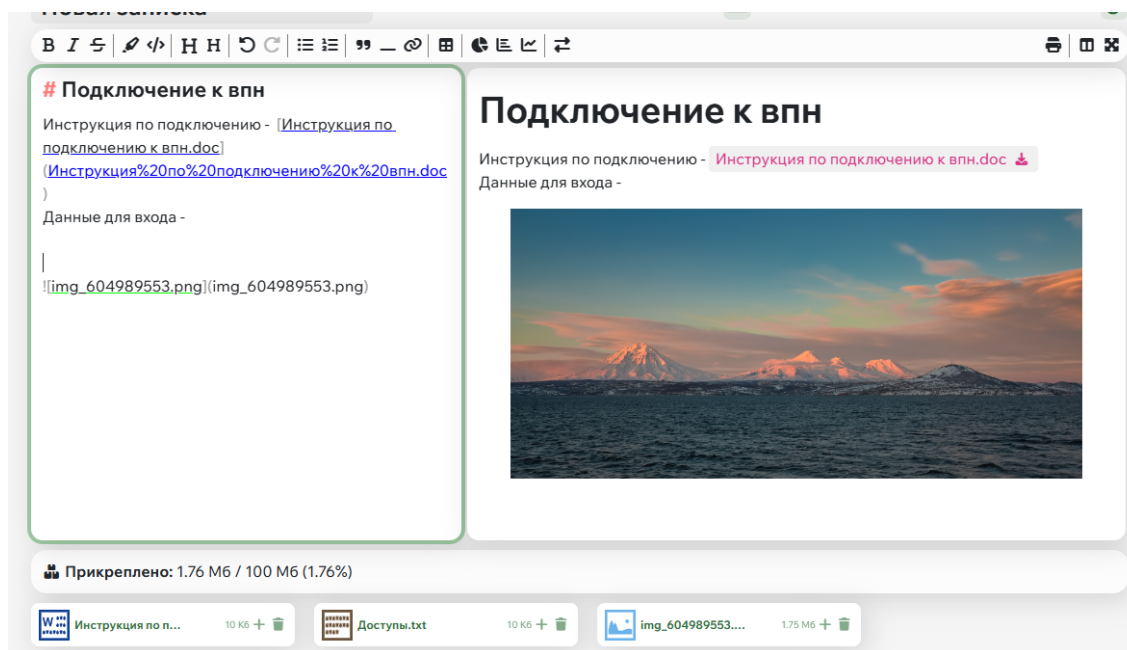


Рисунок 17 — предпросмотр записки с прикрепленной картинкой в виде файла

Для удаления файла из записки нажмите иконку «  ».

Зашифруйте и отправьте записку

Когда всё готово:

1. Нажмите **«Создать записку»**, файлы будут сжаты и встроены в зашифрованное сообщение.
2. Ссылка для доступа к записке автоматически генерируется после успешного создания.

Примечание:

Используйте множественный выбор (Ctrl / Cmd + клик), чтобы добавить сразу несколько файлов.

Примечание:

Если объём данных превышает допустимый лимит, появится уведомление об ошибке: «Слишком большой размер прикрепленных файлов»

4.3. Сценарий 3. Дополнительная защита ссылок

Эта инструкция поможет дополнительно защитить созданную вами ссылку (с ключом) с помощью **пароля** или **сертификата**, чтобы только пользователи, для которых предназначена ссылка могли получить доступ. Это особенно полезно при передаче конфиденциальной информации через внешние каналы связи.

4.3.1. Вариант 1: Защита паролем

Создайте записку

Перейдите на главную страницу, добавьте текст или файл и нажмите кнопку **«Создать записку»**.

Активируйте защиту паролем

Нажмите на кнопку **«Пароль»** во вкладке **«Дополнительно»**.

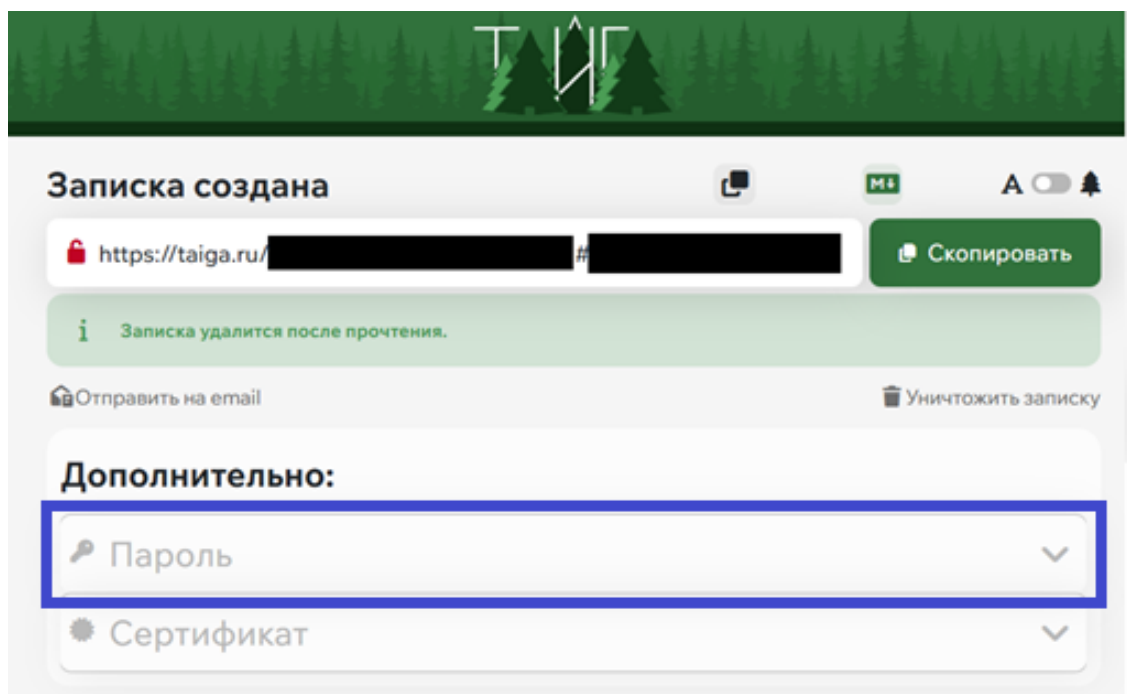


Рисунок 18 — Страница с ссылкой на записку. Вкладка «Пароль»

Введите ваш пароль в соответствующее поле.

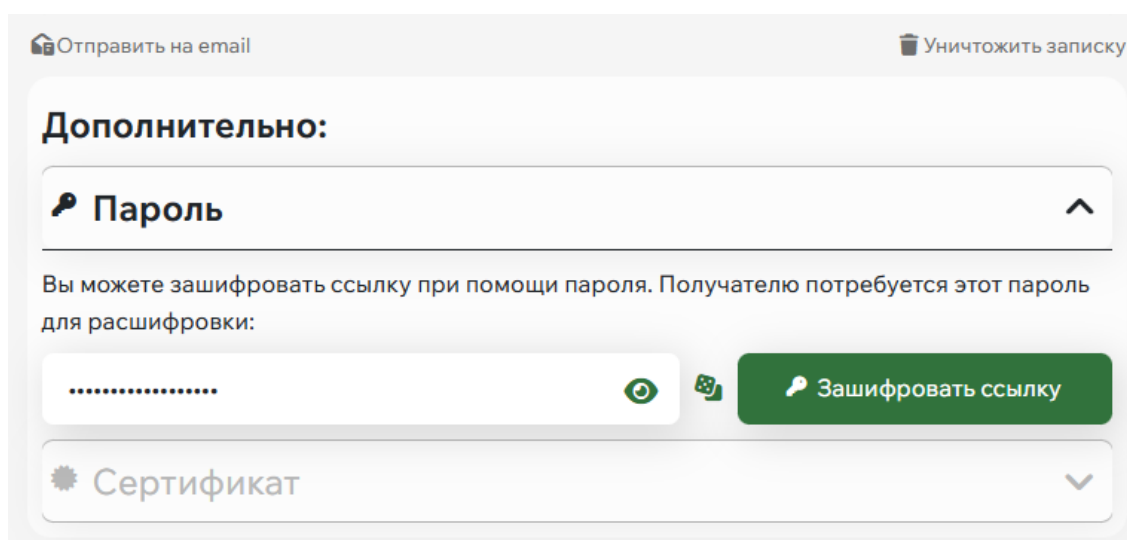


Рисунок 19 — Открытая вкладка с установкой пароля на записку

Для генерации пароля нажмите на кнопку «»

Скопируйте ссылку.

После подтверждения будет создана безопасная ссылка — она будет помечена иконкой «  » и содержать зашифрованный ключ, доступный только при знании пароля. Таким образом, что перехват ссылки не даёт доступа к тексту записки и шифротексту.

Примечание:

Рекомендуем передавать пароль отдельно от ссылки, через другой канал связи.

Примечание:

Вы можете создать несколько ссылок на одну и ту же записку с разными паролями. Для этого достаточно ввести другой пароль, при этом первая ссылка будет расшифровываться только первым паролем, а вторая только вторым. Шифрование паролем происходит в браузере пользователя.

4.3.2. Вариант 2: Защита сертификатом

Подготовьте сертификат

- Убедитесь, что у вас есть действующий ГОСТ или RSA-сертификат получателя, или, что сертификат получателя есть среди доверенных.
- Сертификат должен быть загружен в локальное хранилище браузера — см. инструкцию по импорту сертификатов.

Примечание:

Если у Вас нет сертификата получателя - попросите получателя прислать сертификат.

Активируйте защиту сертификатом

Нажмите на кнопку «Сертификат» во вкладке «Дополнительно».

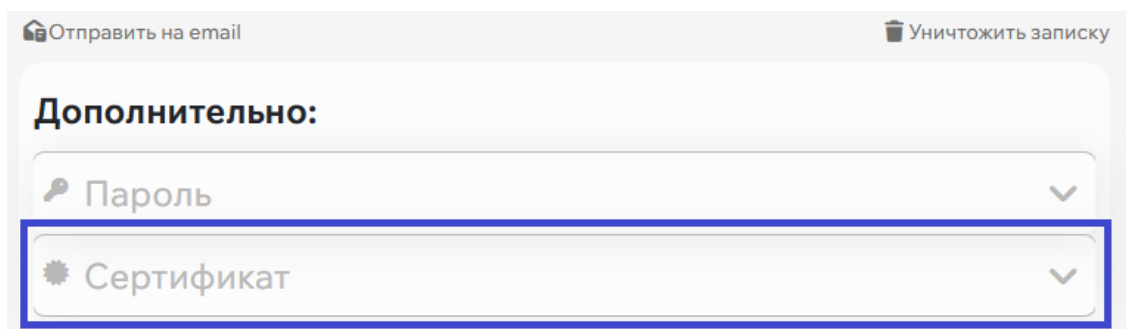


Рисунок 20 — Страница с ссылкой на записку. Вкладка Сертификат

Укажите получателя

- Выберите нужный сертификат из выпадающего списка.

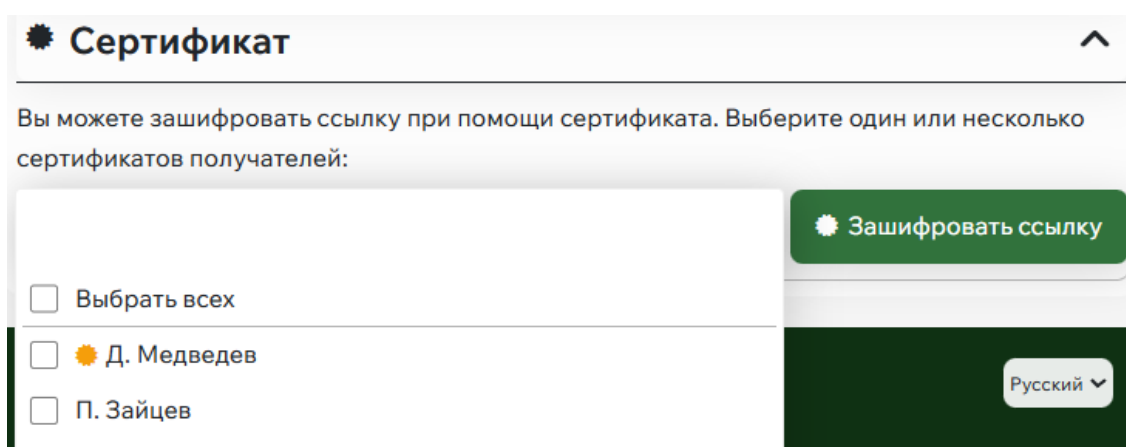


Рисунок 21 — Выбор сертификатов получателей из списка

- Можно выбрать несколько, если требуется отправить одному или нескольким пользователям.
- При необходимости можно нажать на «  » рядом с именем получателя, чтобы убрать его из получателей

Дополнительно:

🔑 Пароль ▾

⚙ Сертификат ▴

Вы можете зашифровать ссылку при помощи сертификата. Выберите один или несколько сертификатов получателей:

⚙ Д. Медведев ✕ П. Зайцев ✕ ▾

⚙ Зашифровать ссылку

Рисунок 22 — Сформированный список получателей

Примечание:

Ссылка шифруется и обновляется прямо в браузере, без отправки на сервер. Вы можете сколько угодно раз менять получателей, для каждого набора получателей будет генерироваться своя ссылка. После выбора получателей скопируйте полученную ссылку.

Получите зашифрованную ссылку

Система автоматически зашифрует ключ записки с помощью открытого ключа выбранного сертификата. Получатель сможет расшифровать данные только при наличии своего закрытого ключа.

Скопируйте ссылку.

После подтверждения будет создана безопасная ссылка — она будет помечена иконкой «  » и содержать зашифрованный ключ, доступный только при наличии закрытого ключа от сертификата. Таким образом, что перехват ссылки не даёт доступа к тексту записки и шифротексту.

Примечание:

Отправителю для зашифрования сертификатами, ключи которых находятся на Rutoken дополнительные расширения на устройстве не требуются. У получателя для расшифрования должен быть установлено расширение Рутокен плагин.

Примечание:

Вы можете создать несколько ссылок на одну и ту же записку с разными связками сертификатов. Для этого достаточно изменить получателей, при этом первая ссылка будет расшифровываться только ключами от первых сертификатов, а вторая только от вторых. Шифрование паролем происходит в браузере пользователя.

4.4. Сценарий 4. Создание записки с разметкой Markdown.

Сервис «Тайга» позволяет создавать защищённые одноразовые записки, поддерживая использование текста с форматированием — это реализуется через **Markdown-разметку**. Ниже приведена пошаговая инструкция, как создать свою первую записку с Markdown и примеры основных элементов разметки.

4.4.1. Подготовка

Откройте страницу создания записки

Откройте главную страницу сервиса «Тайга». Вы увидите интерфейс для ввода новой записки.

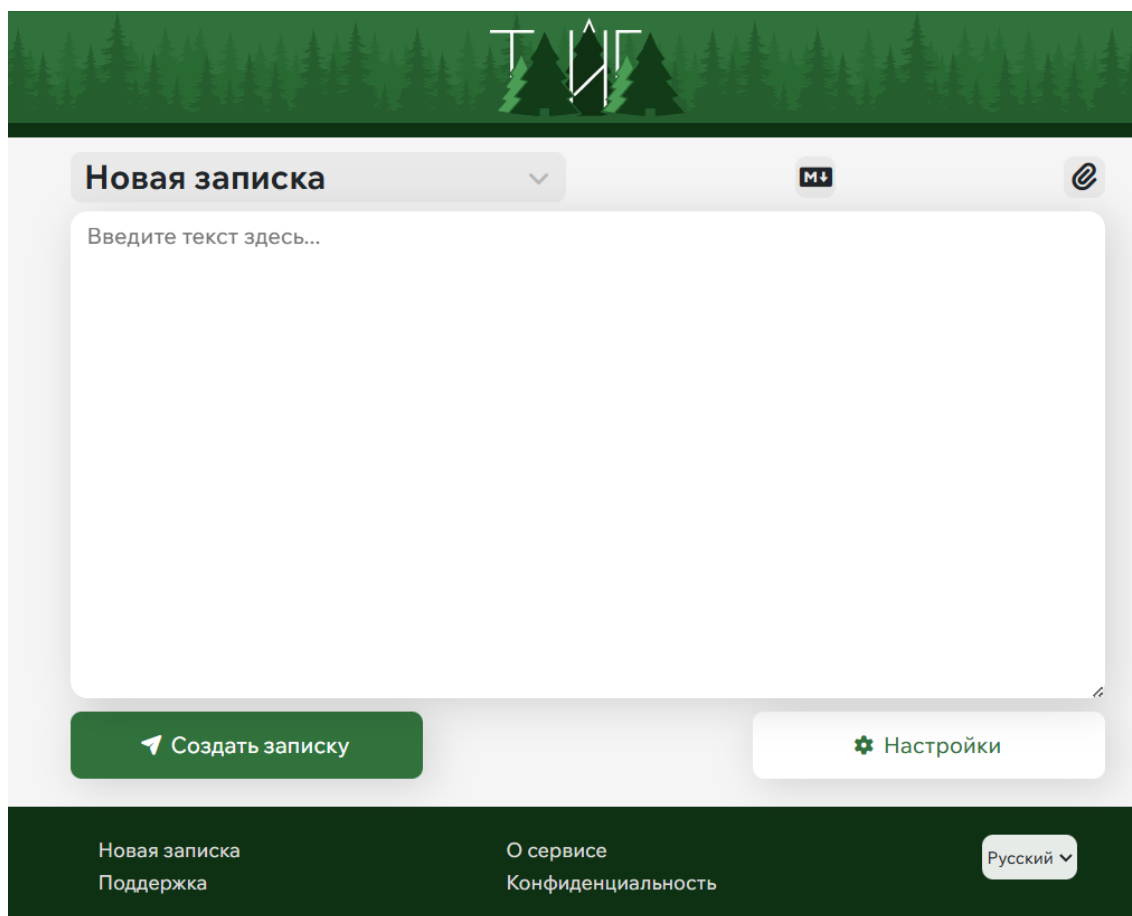


Рисунок 23 — Главная страница

Введите содержимое записки

В центральной части экрана расположен блок **ввода текста**. Здесь можно написать обычный текст или использовать Markdown для форматирования. Для **включения**

Markdown разметки нажмите «».

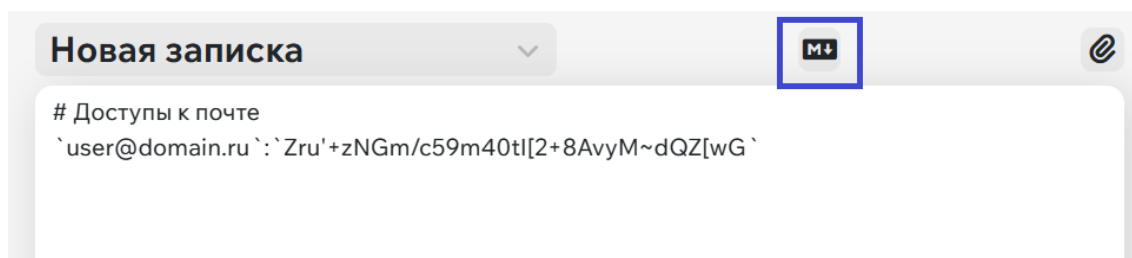


Рисунок 24 — Кнопка для включения Markdown разметки

При включенном Markdown можно включить **предпросмотр** нажав на иконку «».

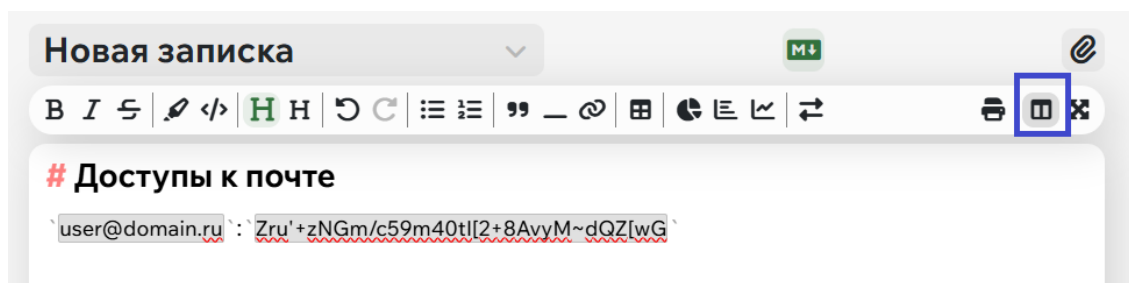


Рисунок 25 — Кнопка для включения предпросмотра Markdown разметки

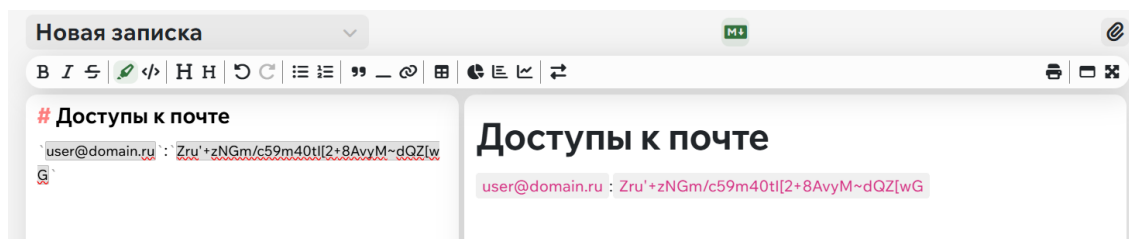


Рисунок 26 — Включенный предпросмотр

Введите текст с разметкой

В поле для ввода можно использовать любой из следующих элементов форматирования:

4.4.2. Заголовки

Заголовки **первого** и **второго** уровня можно активировать с помощью кнопок « **H** » и « **H** » на панели управления запиской.

```
# Главный заголовок
## Подзаголовок второго уровня
### Третий уровень и т.д.
#### Четвертый уровень
##### Пятый уровень
##### Шестой уровень
```

Текст

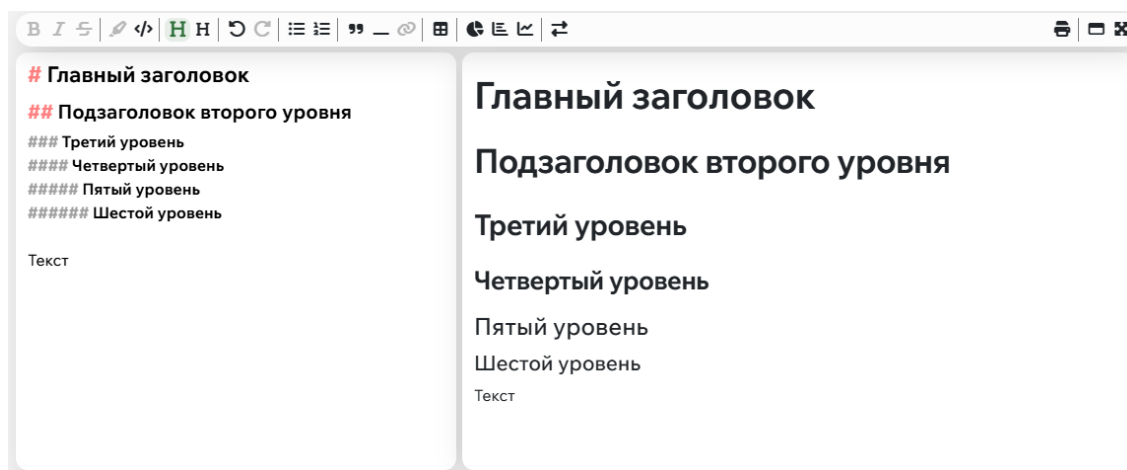


Рисунок 27 — Пример текстового поля с заголовками

4.4.3. Параграфы и перенос строк

Просто начните новую строку, чтобы сделать абзац. Для принудительного перевода строки внутри одного параграфа используйте два пробела в конце строки.

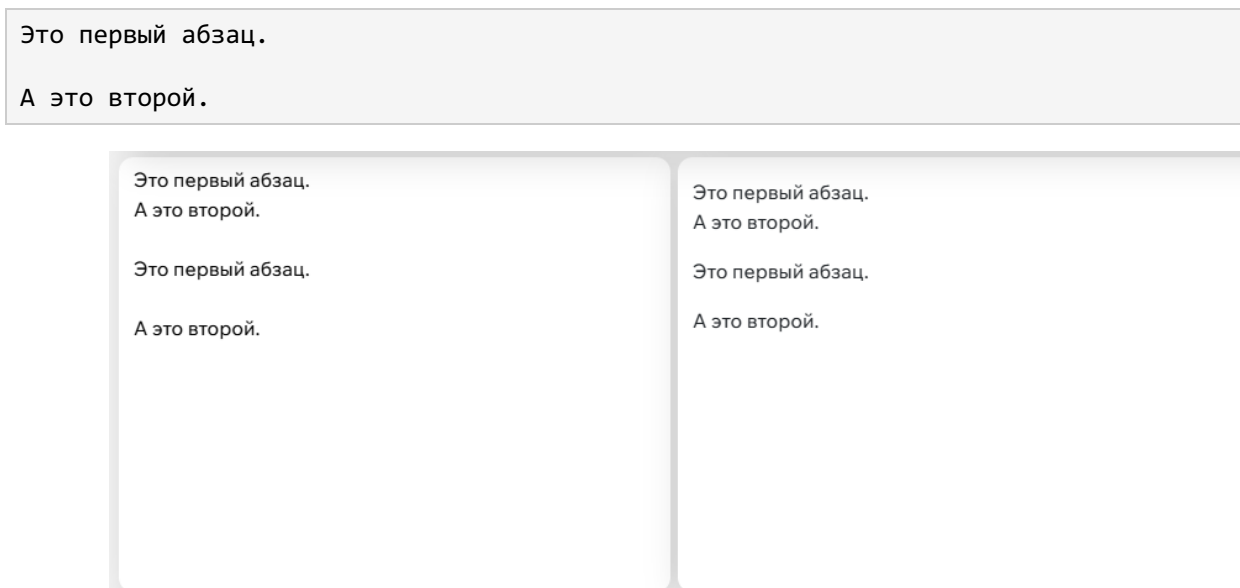


Рисунок 28 — Пример текстового поля с абзацами

4.4.4. Списки

Списки можно создать с помощью кнопок на панели управления запиской. Для создания **нумерованного списка** нажмите «», для создания **маркированного списка** нажмите «».

Нумерованный

Обычный нумерованный список задается через 1. или 1)

1. Первый пункт
2. Второй пункт
3. Третий пункт

Возможна автонумерация списка:

1. Первый пункт
1. Второй пункт
1. Третий пункт

Маркированный

Маркированный список задается - или *, для подпунктов нужно добавить перед символом два пробела.

- Пункт один
- Пункт два
- Подпункт

Список №1: 1. Первый пункт 2) Второй пункт 3. Третий пункт Список №2: 1. Первый пункт 1. Второй пункт 1. Третий пункт Пункты - Пункт один - Пункт два - Подпункт	Список №1: 1. Первый пункт 2. Второй пункт 3. Третий пункт Список №2: 1. Первый пункт 2. Второй пункт 3. Третий пункт Пункты • Пункт один • Пункт два ◦ Подпункт
---	--

Рисунок 29 — Нумерованный и маркированный списки

4.4.5. Блоки кода

Особенность блоков кода состоит в том, что при клике на по блоку содержимое копируется в буфер обмена.

Блоки кода можно создать с помощью кнопок на панели управления запиской. Для создания **однострочного блока кода** выделите текст и нажмите «  », для создания **многострочного блока кода** выделите текст и нажмите «  »

Для однострочного кода используются обратные кавычки:

```
`console.log('Hello, world!')`  
  
`Пароль`
```

Для многострочного блока кода используйте три обратных апострофа. Если блок содержит код - напишите code у открывающих обратных апострофов для автоопределения языка или укажите язык кода:

```
```javascript  
function test() {
 return true;
}
```  
  
```code  
function test() {
 return true;
}
```
```

Если блок не содержит код - просто заключите текст в тройные обратные апострофы:

```
```  
Любой текст
в несколько строк, который
можно скопировать
```
```

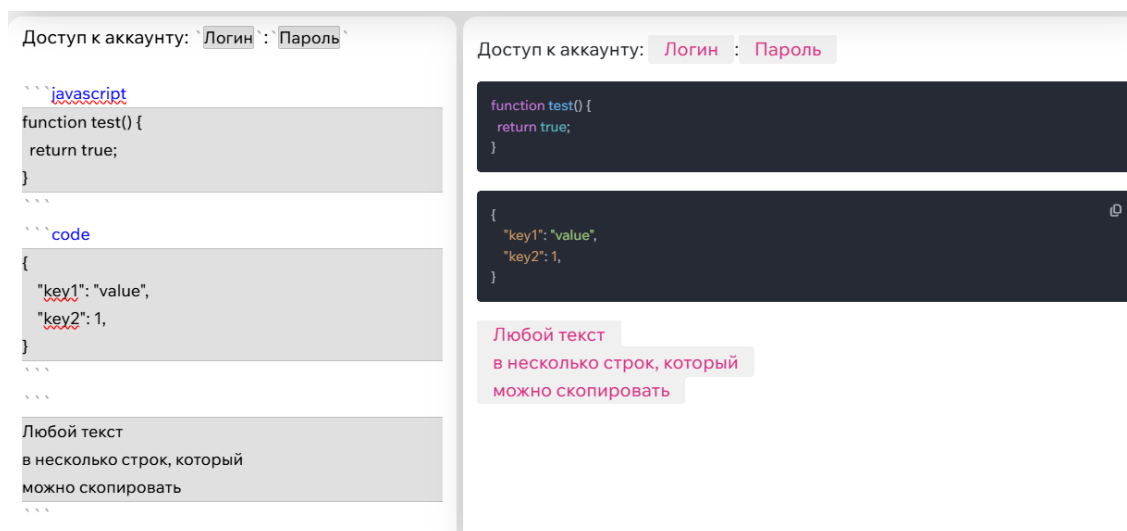


Рисунок 30 — Однострочные и многострочные блоки кода

4.4.6. Цитаты

Для создания **цитаты** выделите текст и нажмите « ” ».

Для ручного добавления используйте символ > в начале строки:

> Лес – прекрасное выражение силы природы и самый ясный образчик ее совершенства.
> *Паустовский К. Г.*

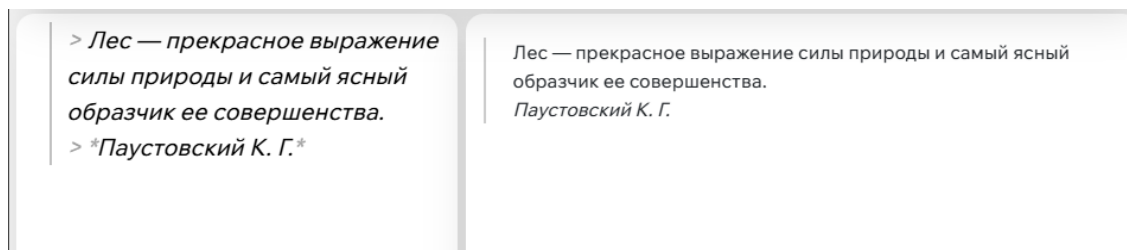


Рисунок 31 — Пример использования цитат в тексте

4.4.7. Ссылки и изображения

К записке можно прикрепить **ссылки** выделите текст и нажмите « 🔗 », после чего во всплывающем окне введите url ссылки.

Ссылка

[Текст ссылки](https://example.com)

Прикрепленное изображение

Для создания предпросмотра прикрепленного изображения напишите

```

```

Прикрепленный файл

Для создания ссылки загрузки прикрепленного файла напишите

```
[текст ссылки](ссылка_на_прикрепленный_файл.png)
```

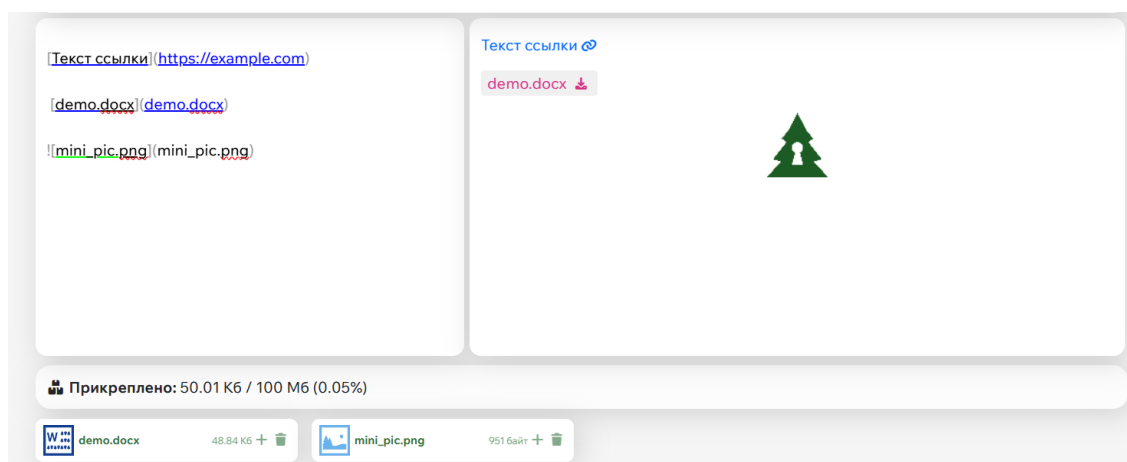


Рисунок 32 — Пример прикрепления внешних ссылок, ссылки на прикрепленные файлы, предпросмотр прикрепленных изображений

4.4.8. Горизонтальная линия

В записке можно создать **разрыв страницы**, для этого нажмите « — ».

Или напишите вручную

```
***
```

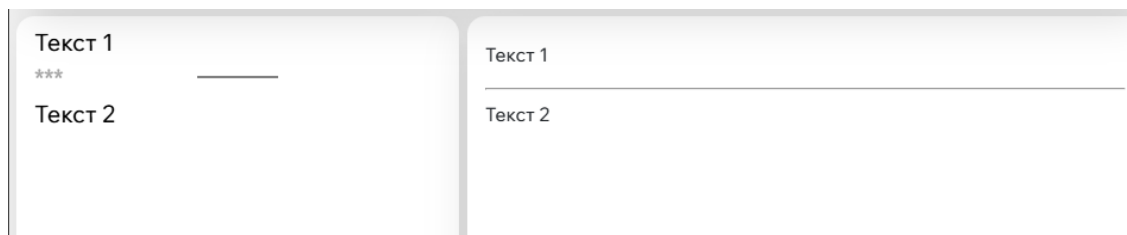


Рисунок 33 — Пример написания разрыва страницы

4.4.9. Экспорт в PDF / Печать записки

Если вы хотите распечатать записку:

1. Нажмите кнопку «  » в правом верхнем углу редактора.
2. Браузер предложит стандартный диалог печати. Среди принтеров будет "Сохранить как PDF"

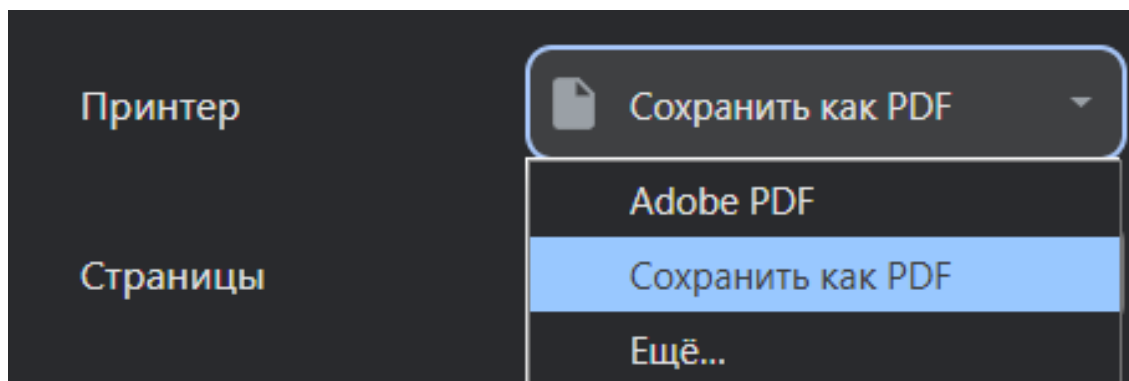


Рисунок 34 — Список принтеров после нажатия на кнопку печати

4.4.10. Клавиши быстрого доступа

Таблица 1

| Комбинация клавиш | Действие |
|-------------------|--------------------------|
| Ctrl + B | Жирный текст |
| Ctrl + I | Курсив |
| Ctrl + D | Зачеркнутый текст |
| Ctrl + K | Однострочный блок кода |
| Ctrl + E | Многострочный блок кода |
| Ctrl + Shift + H | Заголовок первого уровня |
| Ctrl + H | Заголовок второго уровня |
| Ctrl + U | Маркированный список |
| Ctrl + O | Нумерованный список |
| Ctrl + Q | Цитата |

| | |
|---------------------|-------------------------------------|
| Ctrl + R | Разрыв страницы |
| Ctrl + L | Ссылка |
| Alt + P | Печать / Экспорт в PDF |
| F9 | Предпросмотр |
| F11 | Развернуть поле ввода на весь экран |
| Ctrl + M | Вкл./выкл. режима Markdown |
| Ctrl + Enter | Отправка записки |

4.5. Сценарий 5: Создание ключа и отправка сертификата.

4.5.1. Цель

Создать ключ, сгенерировать на его основе сертификат, а затем поделиться этим сертификатом с получателем.

4.5.2. Управление ключами

Откройте управление ключами

Перейдите на главную страницу приложения, нажмите на выпадающий список **"Новая записка"** и выберите **"Мои ключи"**

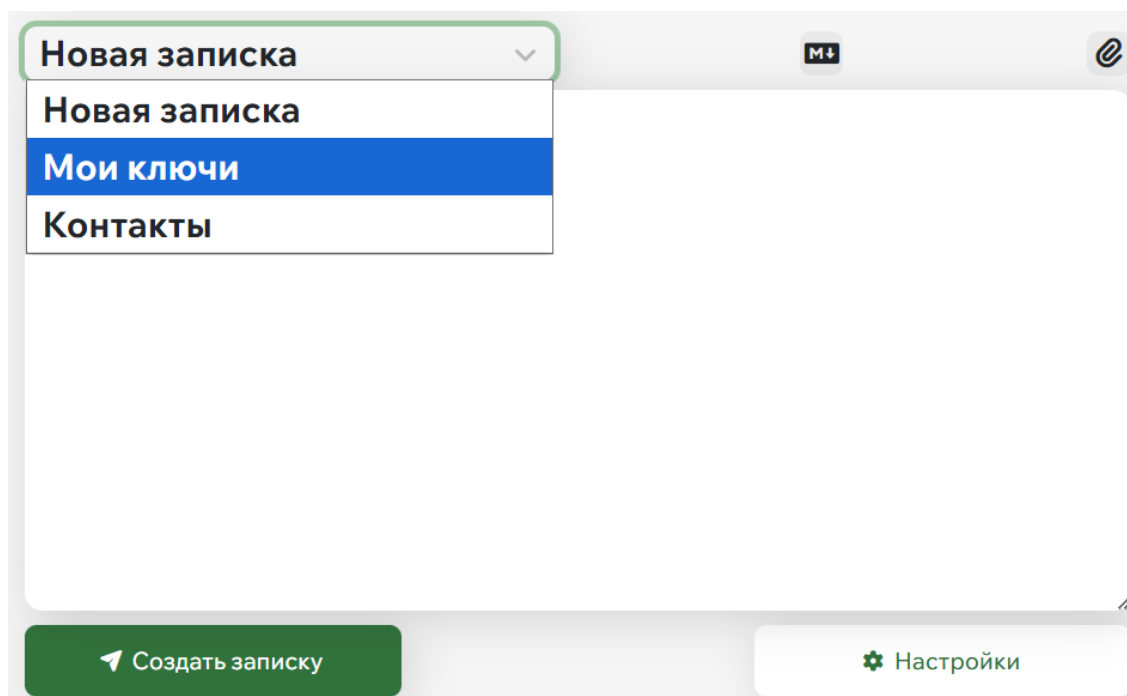


Рисунок 35 — Открытие страницы управления ключами

После этого откроется интерфейс с выбором способов хранения ключа.

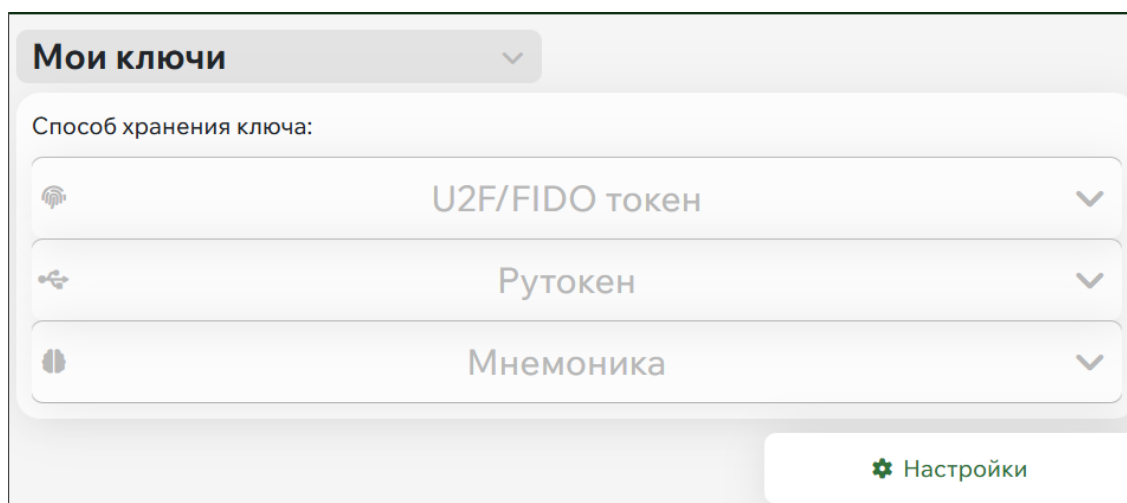


Рисунок 36 — Управление ключами. Выбор способа хранения закрытого ключа

Справка:

Сервис "Тайга" позволяет дополнительно шифровать ссылки с помощью сертификатов. Для шифрования используется стандарт CMS (Р 1323565.1.025-2019), особенность стандарта состоит в том, что для зашифрования сообщения отправителю

необходим открытый ключ получателя, для расшифрования получателю нужен закрытый ключ.

Тайга предоставляет несколько способов для хранения закрытых ключей, далее рассмотрим их все.

4.5.3. U2F / FIDO токены

Особенности

Для работы необходимо одно из устройств устройство:

- Рутокен MFA
- Рутокен U2F
- Yubikey 5
- и других токенов с поддержкой u2f.

Для работы не нужны программы, только современный браузер.

Расшифрование с помощью FIDO ключа может происходить как с ноутбуков, так и с телефонов, планшетов.

Создание

Для создания ключа откройте раздел "U2F / FIDO".



Рисунок 37 — Меню управления токеном

Из-за особенностей протокола мы не можем получить список ключей, если вы ранее не создавали ключ, то нажмите кнопку **"Новый ключ"**.

Откроется всплывающее окно с выбором устройства:

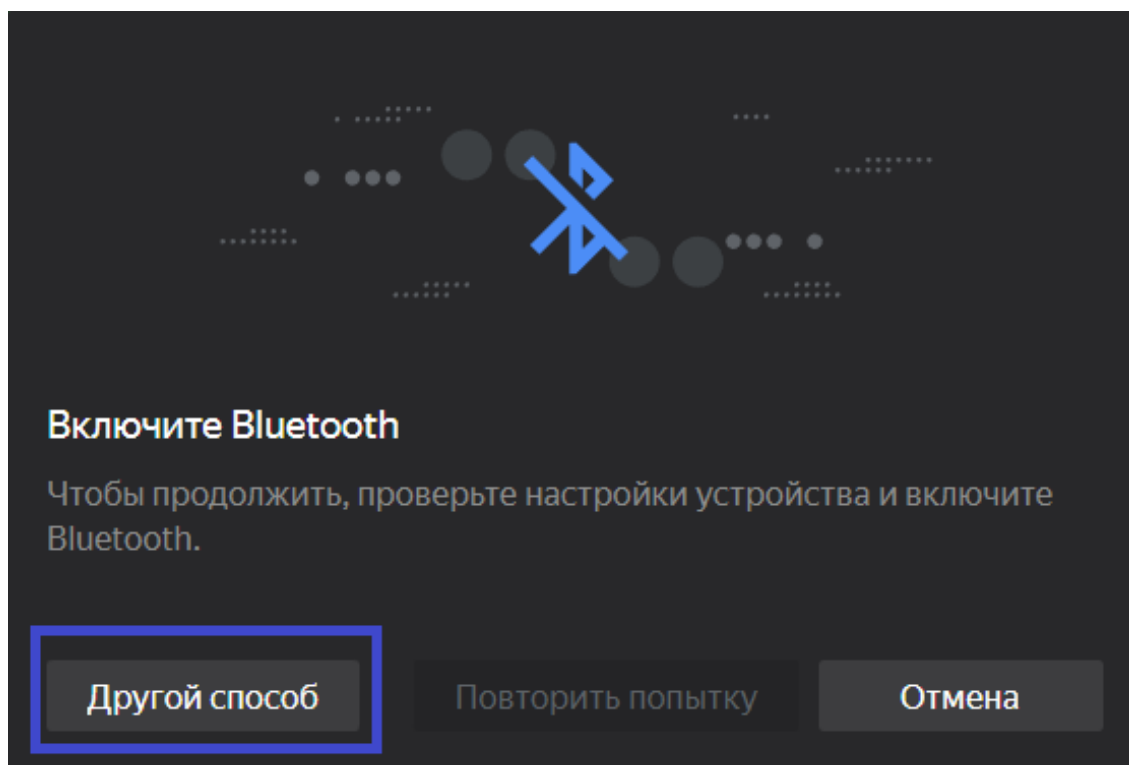


Рисунок 38 — Всплывающее окно, нажмите "Другой способ"

Примечание:

Окно может отличаться от представленного на экране в зависимости от ОС и настроек. Если необходимо - нажмите "Отмена" или "Другой способ", для того чтобы вернуться к окну выбора где сохранить ключ.

В открывшемся окне выберите внешний электронный ключ

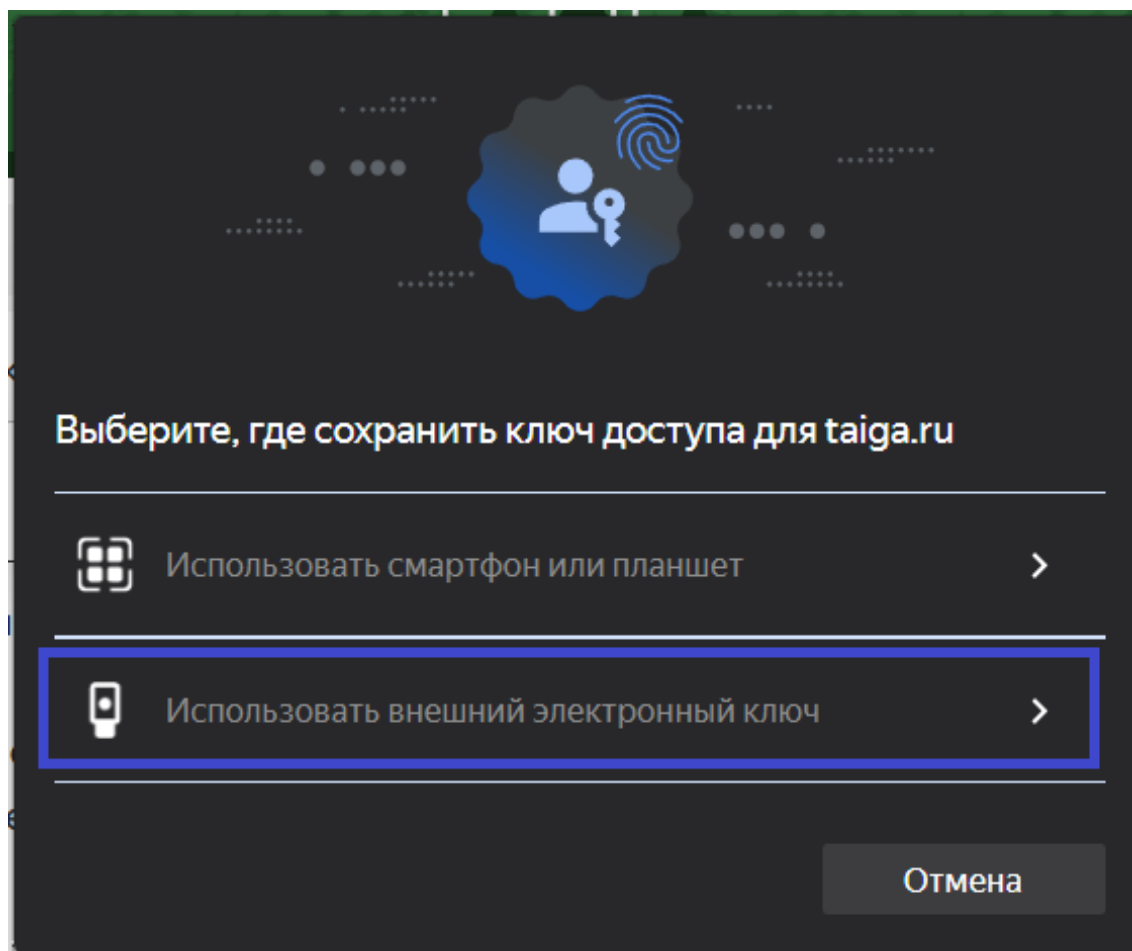


Рисунок 39 — Всплывающее окно, нажмите "Внешний электронный ключ"

Выберите "ОК", чтобы разрешить добавить ключ

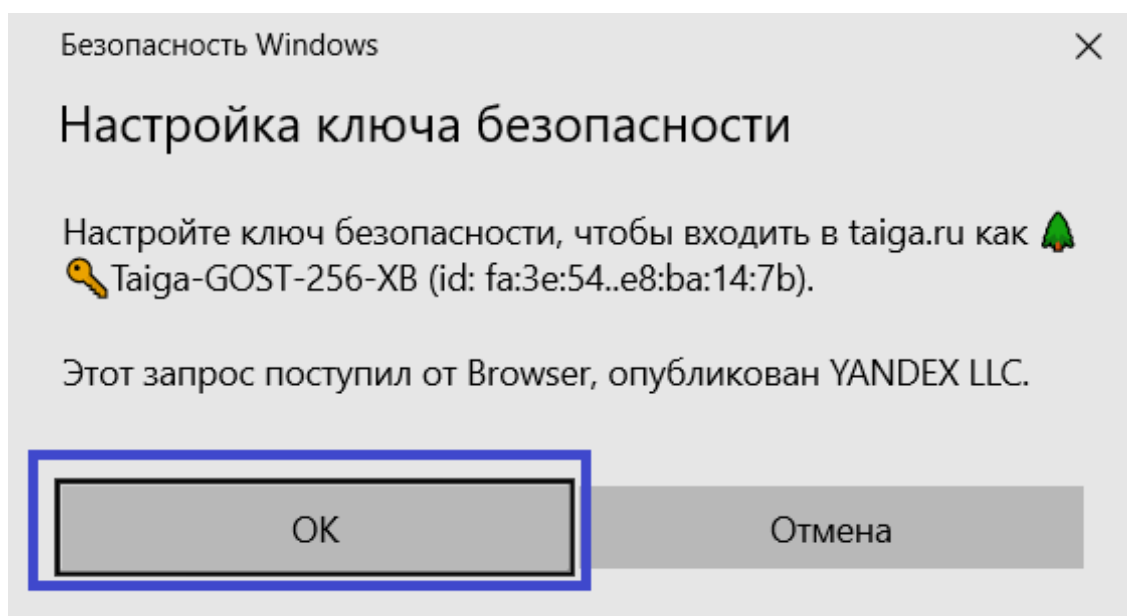


Рисунок 40 — Всплывающее окно, нажмите "OK"

Выберите "OK", чтобы разрешить добавить ключ

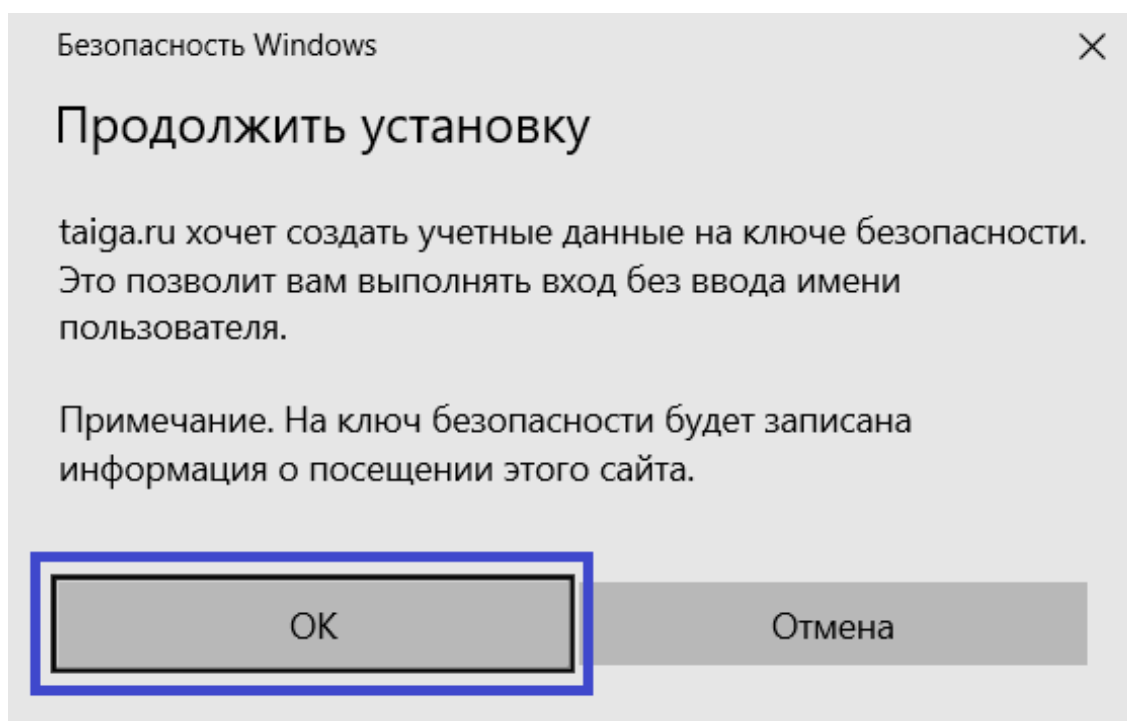


Рисунок 41 — Всплывающее окно, нажмите "OK"

Введите ПИН-код и нажмите "OK"

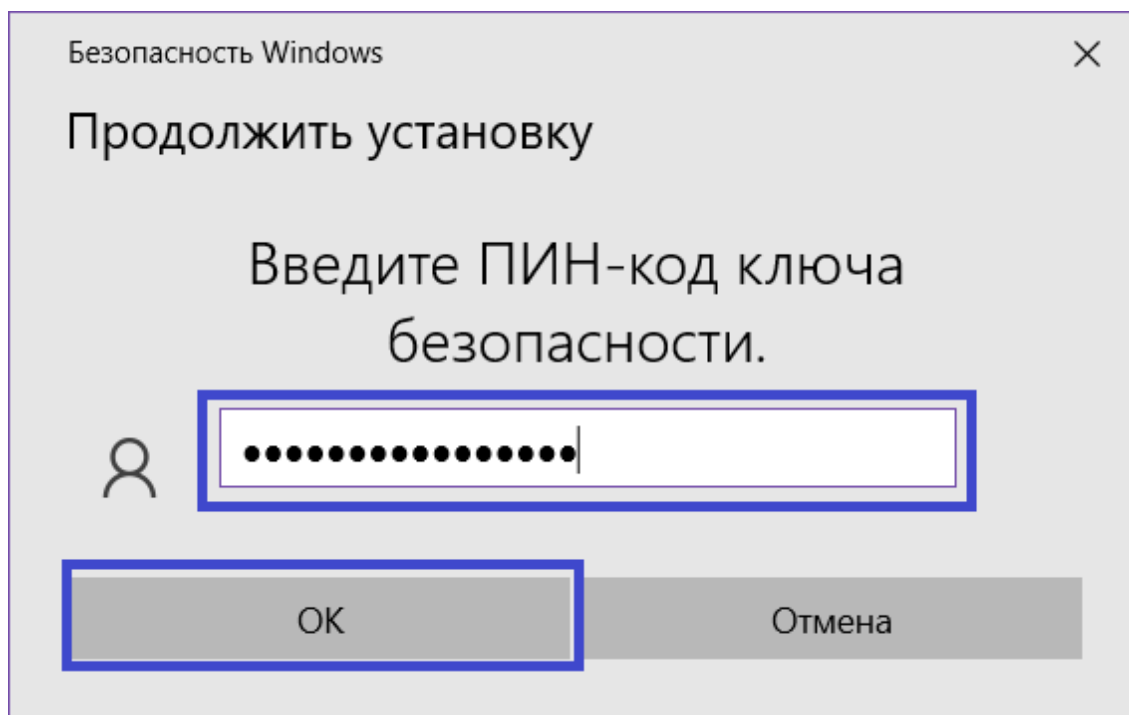


Рисунок 42 — Всплывающее окно, нажмите "ОК"

Коснитесь кнопки на ключе

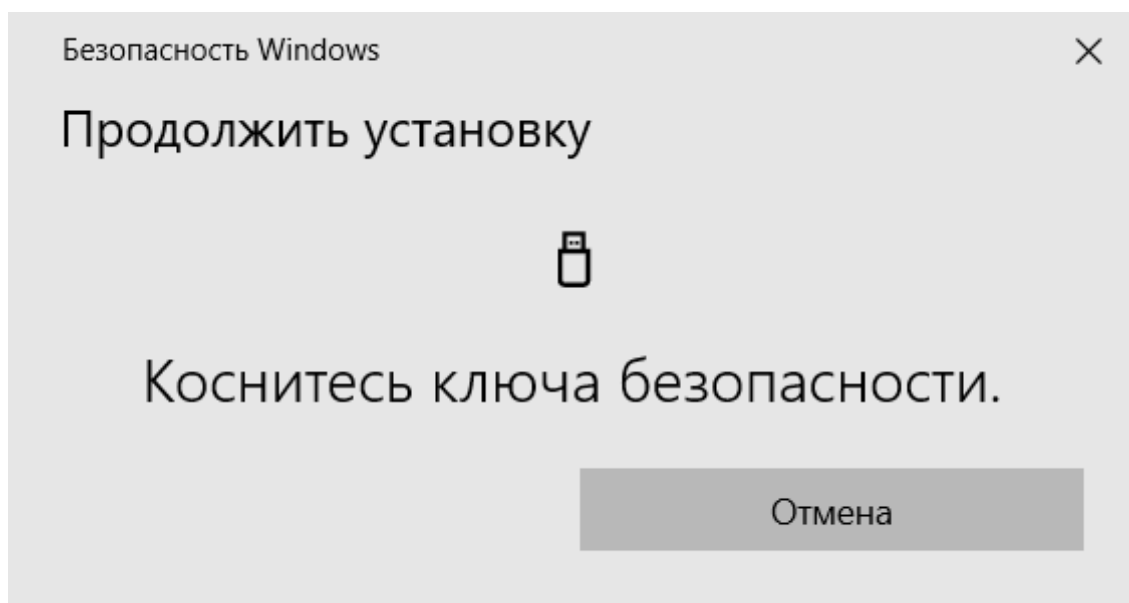


Рисунок 43 — Коснитесь ключа безопасности

После этого ключ будет успешно создан на устройстве.

Примечание:

*Из-за особенностей протокола U2F мы используем дополнительные поля ключа, доступ к которым защищен пин-кодом как место для хранения ключа, однако, ключи из U2F / FIDO токенов **могут быть извлекаемы** при знании пин-кода, это стоит учитывать в модели рисков.*

Создание ключа на текущем устройстве

Если администратор сервера включил настройку "Разрешить хранить FIDO / U2F ключи на устройстве пользователя", то пользователи могут сохранять ключи не только на внешних устройствах (токены/телефоны), но и на текущем устройстве с помощью встроенных в ОС средств хранения ключей.

Для создания ключа откройте раздел "U2F / FIDO".



Рисунок 44 — Меню управления токеном

Из-за особенностей протокола мы не можем получить список ключей, если вы ранее не создавали ключ, то нажмите кнопку "**Новый ключ**".

Откроется всплывающее окно с выбором устройства:

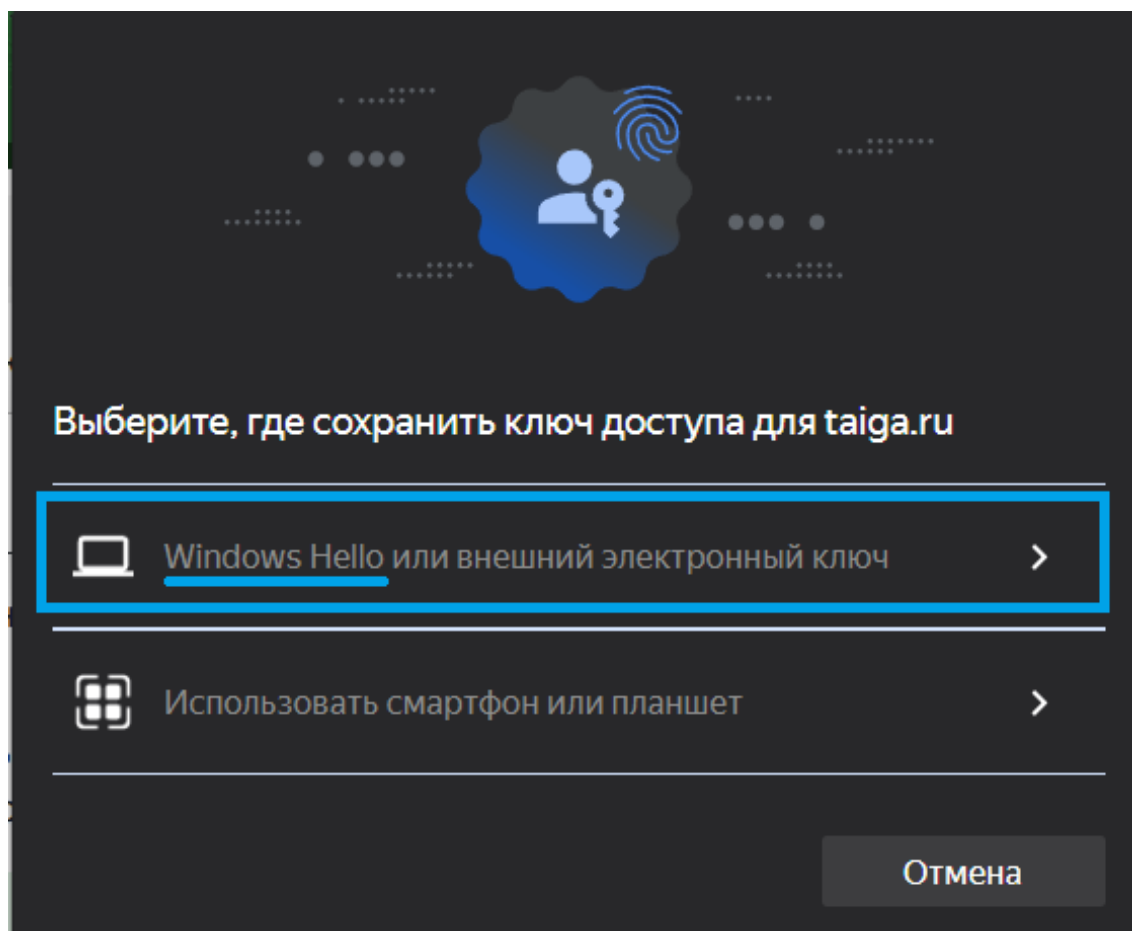


Рисунок 45 — Всплывающее окно, нажмите "Windows Hello"

Введите пин-код или пароль от текущего устройства:

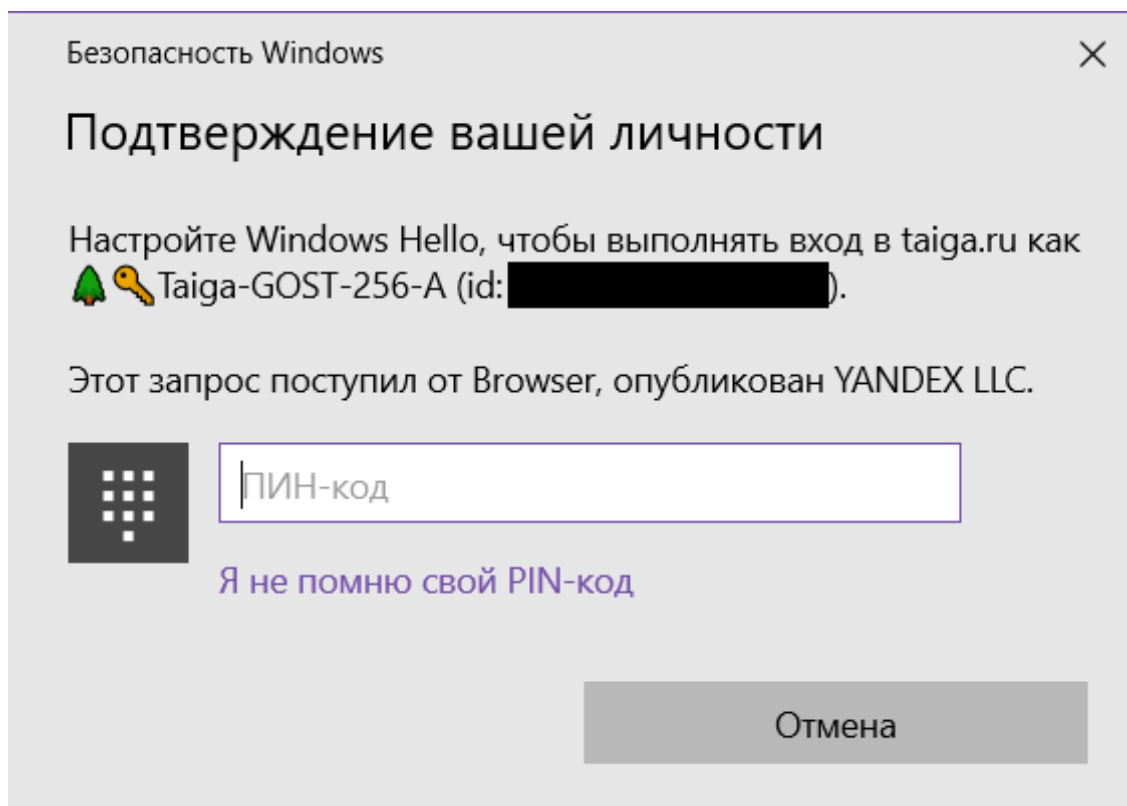


Рисунок 46 — Всплывающее окно с вводом пин-кода

Если ключ создан успешно, то будет выведено уведомление



Рисунок 47 — Всплывающее окно с вводом пин-кода

Поделиться сертификатом

1. Чтобы поделиться сертификатом нажмите кнопку «  ».
2. В открывшемся всплывающем окне укажите ваше имя, это имя будет предложено получателю при сохранении сертификата в хранилище. Значение по умолчанию: **Аноним.**

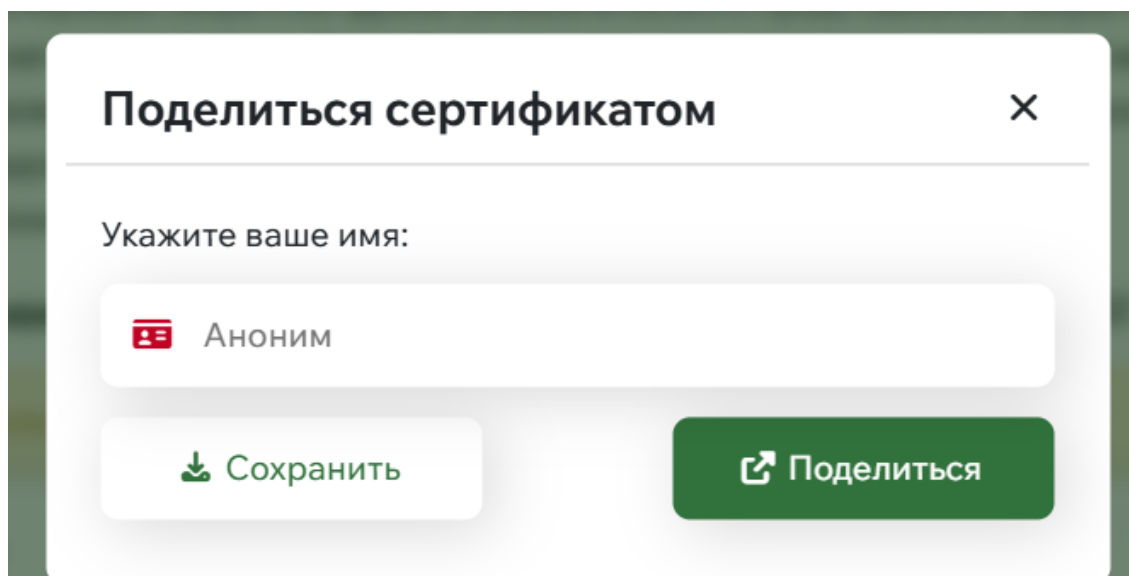


Рисунок 48 — Поделиться сертификатом. Поле указания имени

3. Вы можете:

- нажать кнопку **"Поделиться"**. Будет создана записка содержащая ваш сертификат. Время жизни записки - **7 дней**.
- сохранить сертификат в файл .json и передать его получателю.

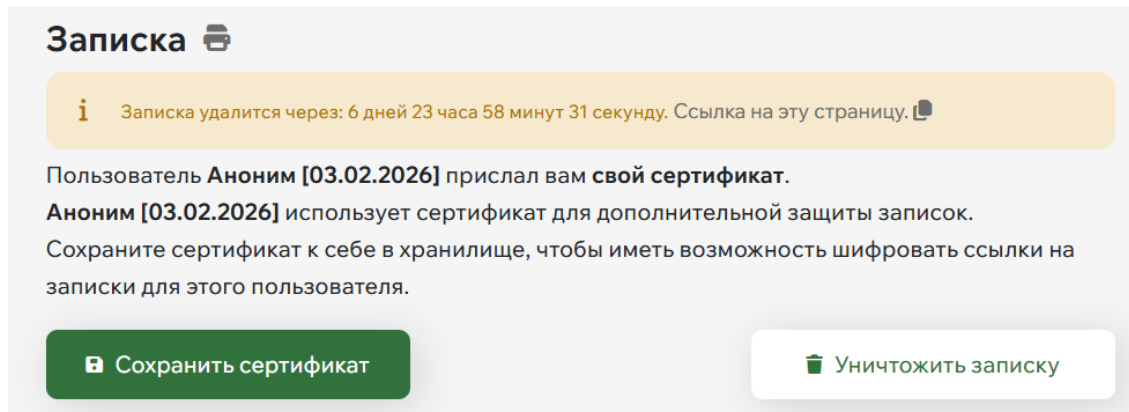


Рисунок 49 — Пример записки, содержащей сертификат

4. После нажатия на любую из кнопок пункта 3) откроется всплывающее окно в котором нужно ввести ПИН-код токена

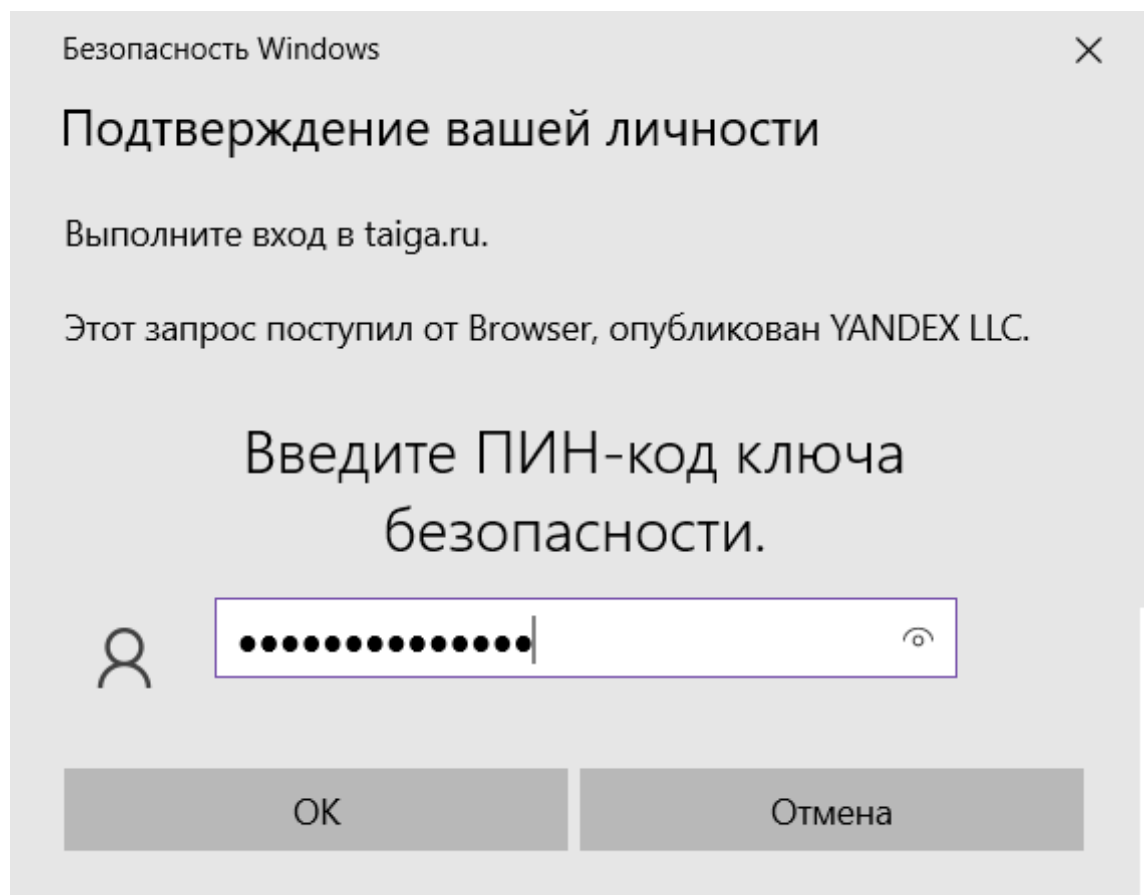


Рисунок 50 — Ввод пин-кода

5. Коснитесь кнопки на ключе

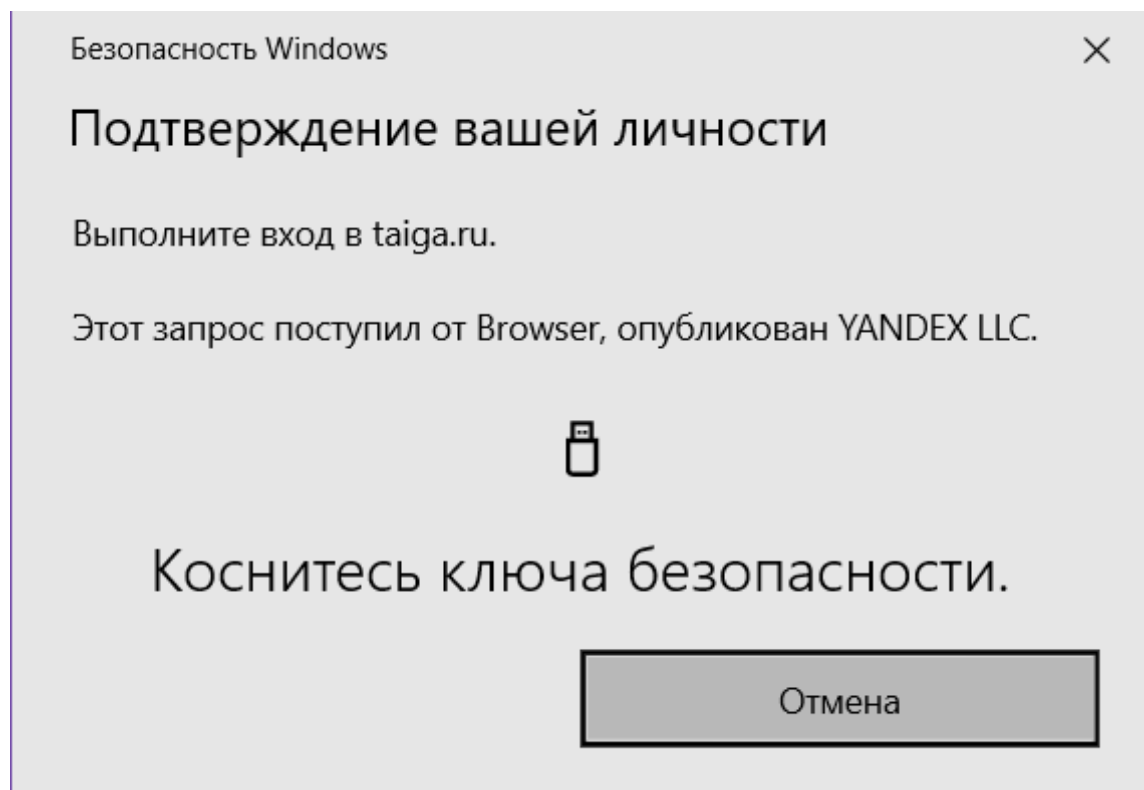


Рисунок 51 — Коснитесь ключа безопасности

6. Если на токене несколько ключей - выберите тот, которым хотите поделиться и нажмите "ОК"

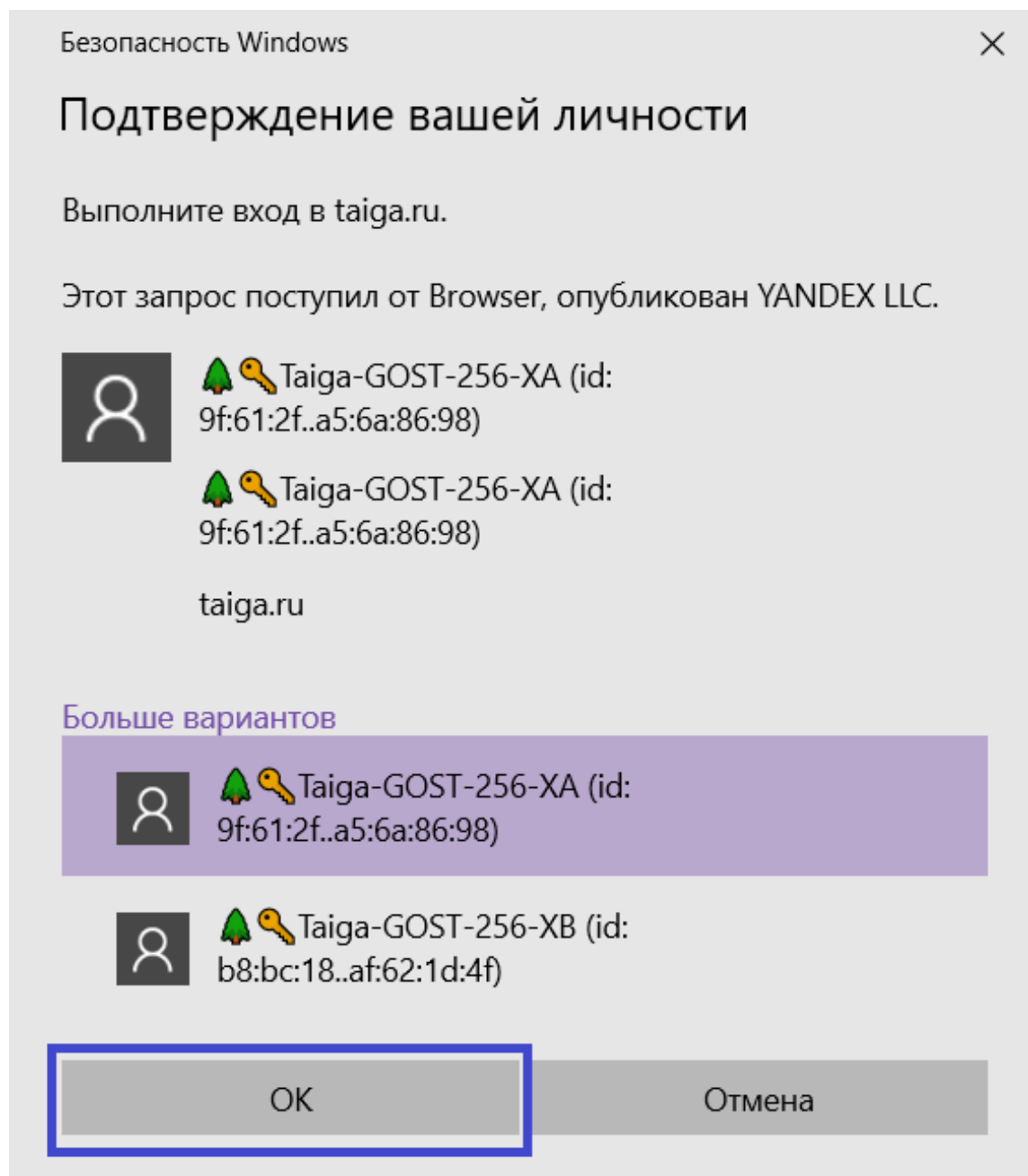


Рисунок 52 — Коснитесь ключа безопасности

Примечание:

Если при попытке **поделиться** ключом возникает ошибка как на скриншоте ниже, то скорее всего на токене не созданы ключи. Если данная ошибка возникает при создании ключа - используйте другой ключ.

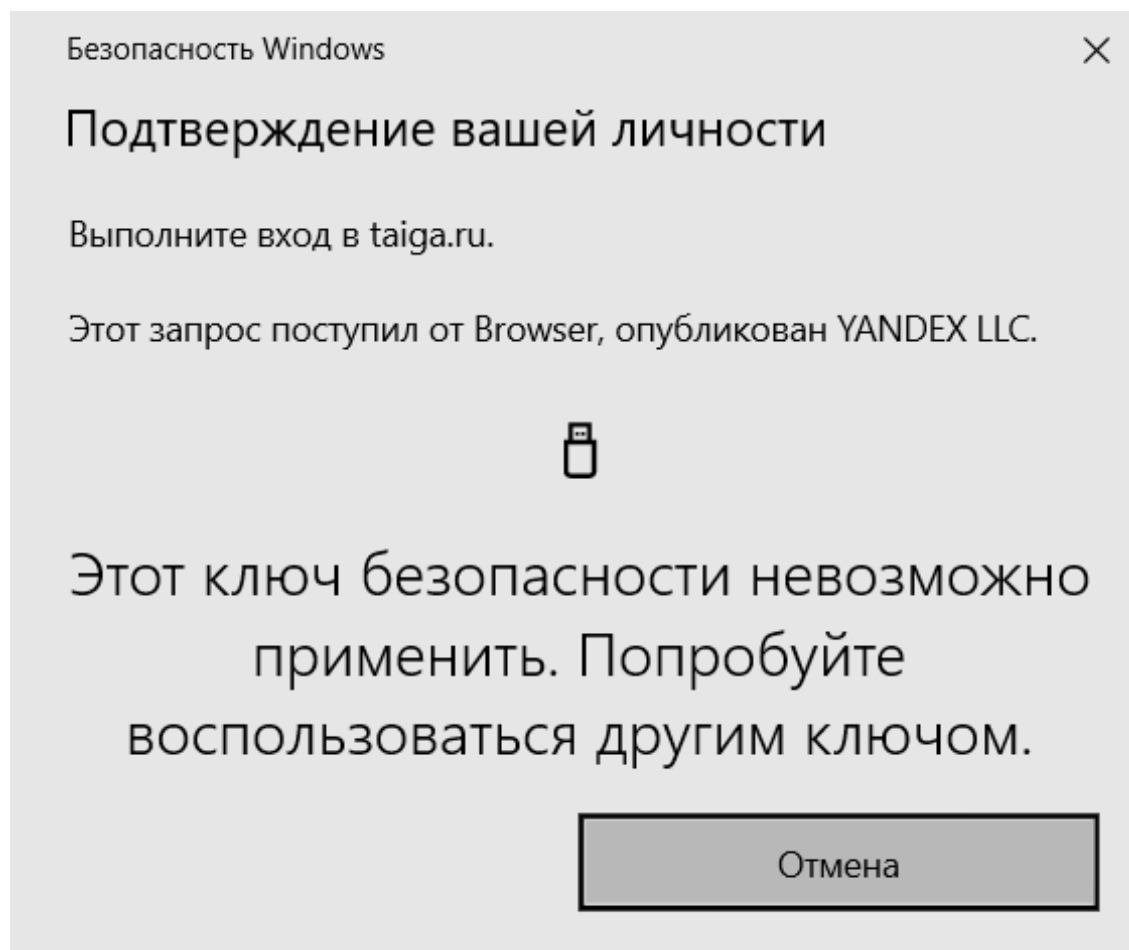


Рисунок 53 — Пример ошибки

4.5.4. Рутокен

Особенности

Для работы необходимо одно из устройств устройство:

- Рутокен ЭЦП 2.0
 - Рутокен ЭЦП 3.0
 - Рутокен Lite
- (Тесты на других устройствах Рутокен не проводились)

Для работы необходим "Адаптер Рутокен Плагин", можно установить расширение можно с [официального сайта Рутокен](#).

Расшифрование работает только с компьютера, так как требует установленный "Адаптер Рутокен Плагин".

Примечание:

*Рутокен Lite всегда отображается с предупреждением, это сделано намеренно и не влияет на работу. Связано такое решение с тем, что версия Lite не имеет физической возможности шифровать данные. В качестве компромиса, из-за распространенности Lite версии, мы используем защищенное хранилище бинарных данных на токене для хранения ключа. Однако, ключи из Lite версии **могут быть извлекаемы** при знании пин-кода, это стоит учитывать в модели рисков.*

Создание

Для создания ключа откройте раздел "Рутокен". Если вы видите уведомление, о том, что расширение "Адаптер Рутокен Плагин" не установлено, то скачайте и установите его, а затем обновите страницу.

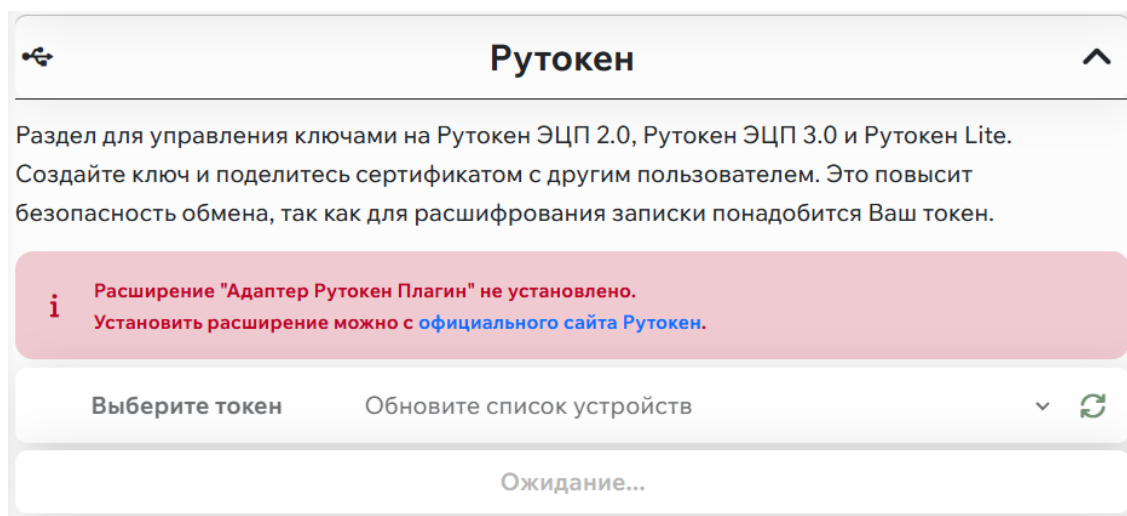


Рисунок 54 — Ошибка: Расширение "Адаптер Рутокен Плагин" не установлено

Если отображается фраза "Подключите устройство..." значит расширение установлено, но устройства не подключены

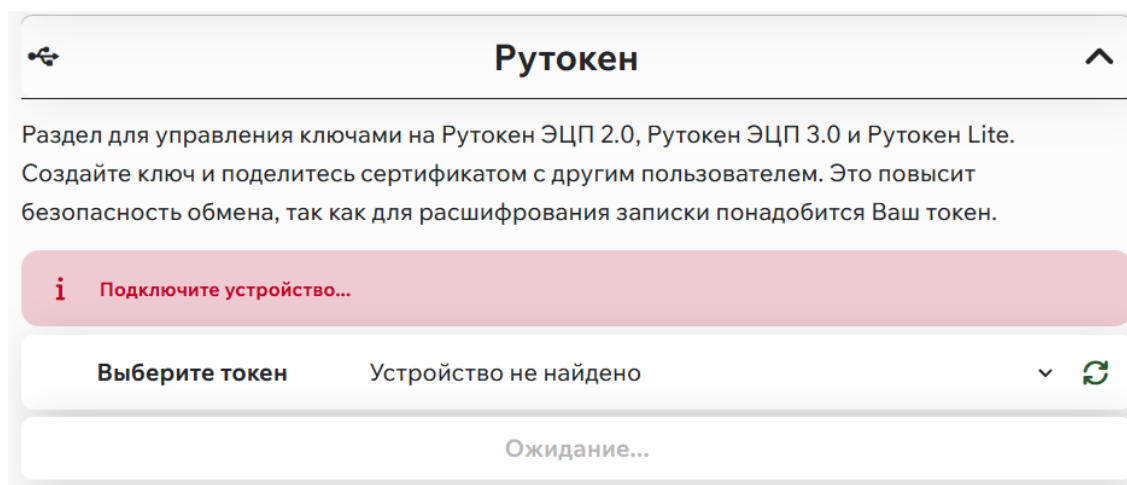


Рисунок 55 — Ожидание устройств

Если после подключения устройства оно не появилось, то нажмите кнопку «  » и выберите устройство из подключенных

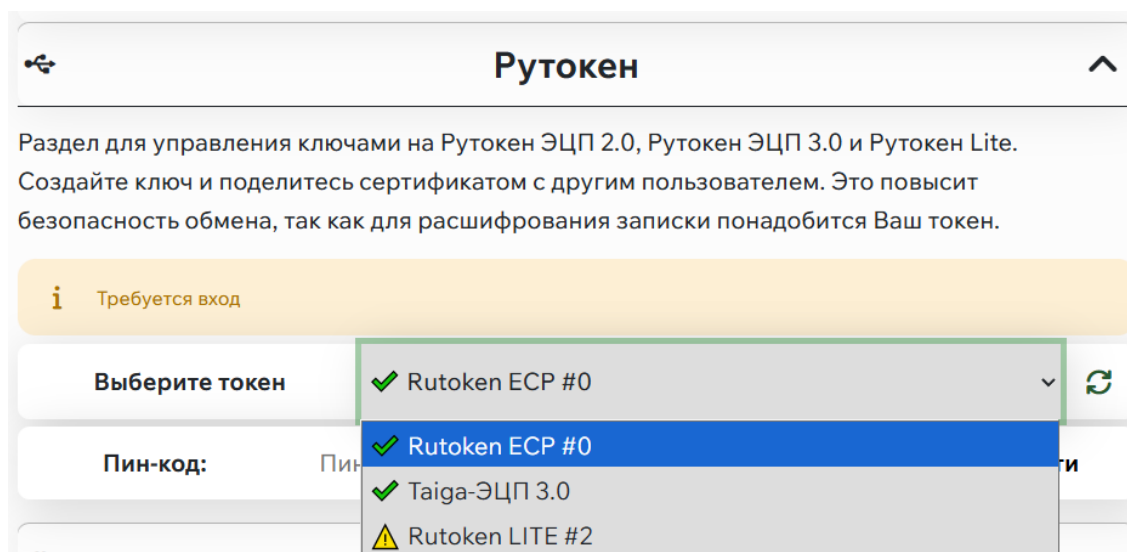


Рисунок 56 — Выбор устройства

И затем введите пин-код от токена

Рутокен

Раздел для управления ключами на Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0 и Рутокен Lite. Создайте ключ и поделитесь сертификатом с другим пользователем. Это повысит безопасность обмена, так как для расшифровки записки понадобится Ваш токен.

Требуется вход

Выберите токен ✓ Taiga-ЭЦП 3.0

Пин-код: **Войти**

Рисунок 57 — Введите пин-код токена

После успешной авторизации откроется меню управления токеном. При первом заходе отобразится одна кнопка "Новый ключ". В разделе "Расширенные настройки" можно настроить длину ключа.

Чтобы создать ключ для сервиса нажмите "Новый ключ".

Примечание:

Для сервиса на токене генерируются отдельные ключи. При очистке токена удаляются только ключи связанные с сервисом тайга. Другие ключи на токене не будут затронуты

Выберите токен ⚠ Rutoken LITE #2

Выйти

+
Новый ключ

> Расширенные настройки

Рисунок 58 — Меню управления токеном. На токене отсутствуют ключи

После создания ключа в управлении токеном будут две кнопки:

- **"Очистить токен"** - при нажатии на неё все сервисные ключи и сертификаты тайги будут удалены с токена. Ваши ключи и сертификаты затронуты не будут.
- **"Поделиться"** - для отправки вашего сертификата.

В меню "Расширенные настройки" можно создать несколько ключей и сертификатов, выбрать сертификат которым хотите поделиться, а так же удалить какой-то один ключ.

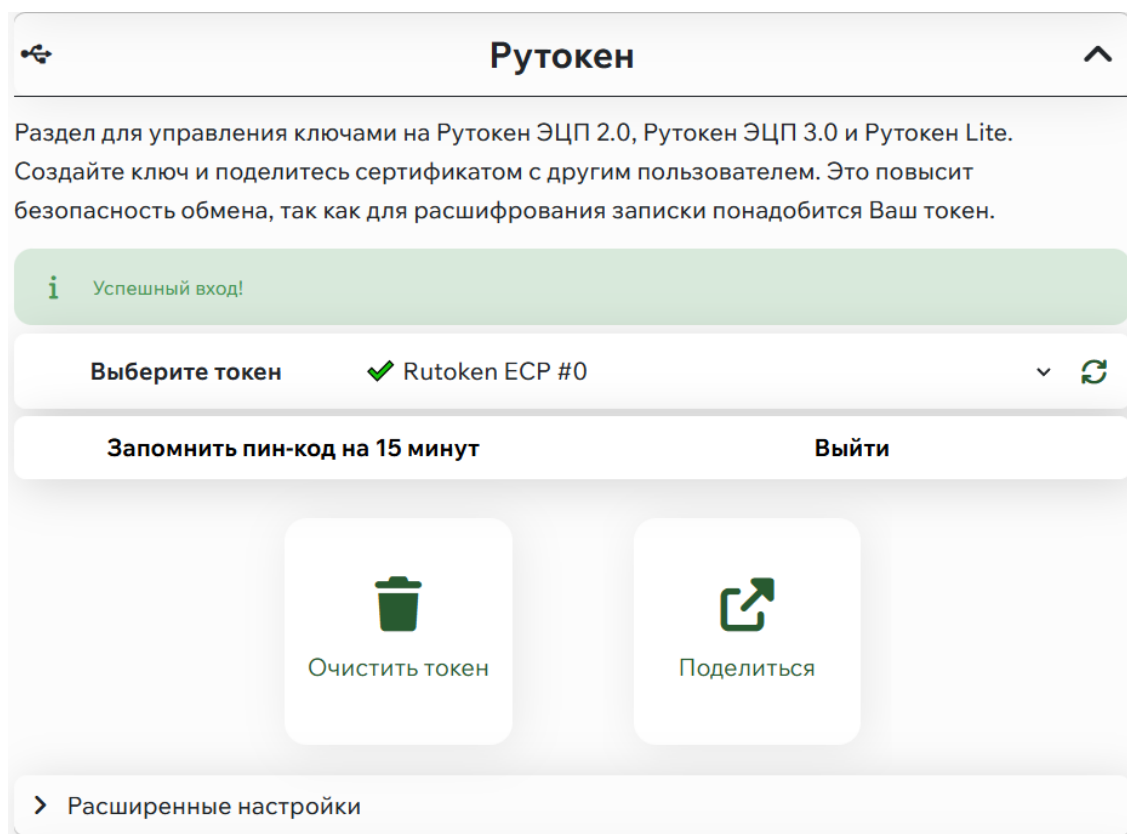


Рисунок 59 — Меню управления токеном

Поделиться сертификатом

1. Чтобы поделиться сертификатом нажмите кнопку «  ».
2. В открывшемся всплывающем окне укажите ваше имя, это имя будет предложено получателю при сохранении сертификата в хранилище. Значение по умолчанию: **Аноним**.

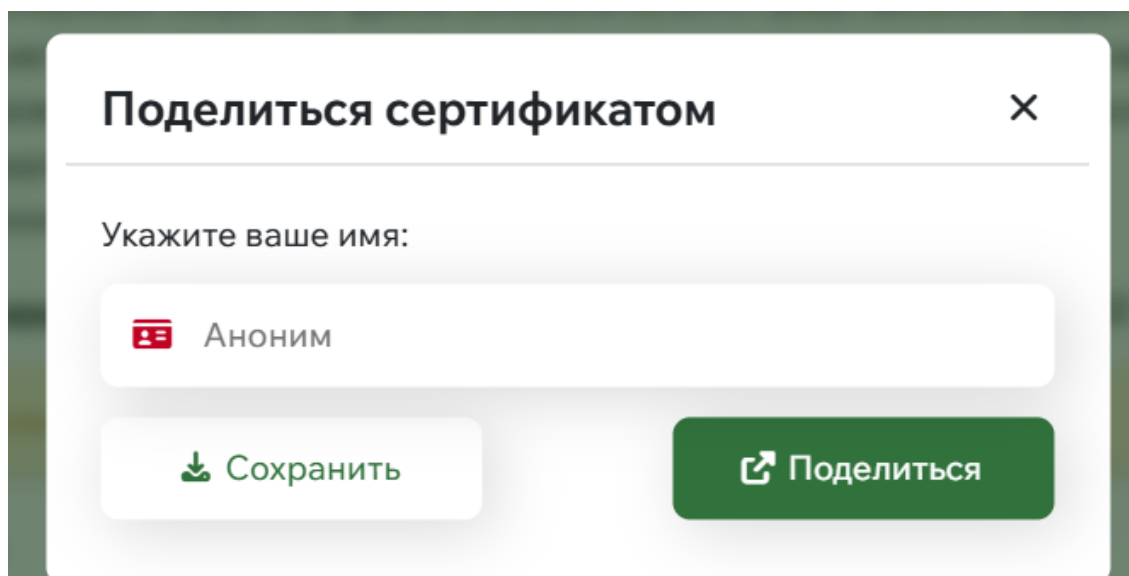


Рисунок 60 — Поделиться сертификатом. Поле указания имени

3. После этого вы можете:

- нажать кнопку **"Поделиться"**. Будет создана записка содержащая ваш сертификат. Время жизни записки - **7 дней**.
- сохранить сертификат в файл .json и передать его получателю.

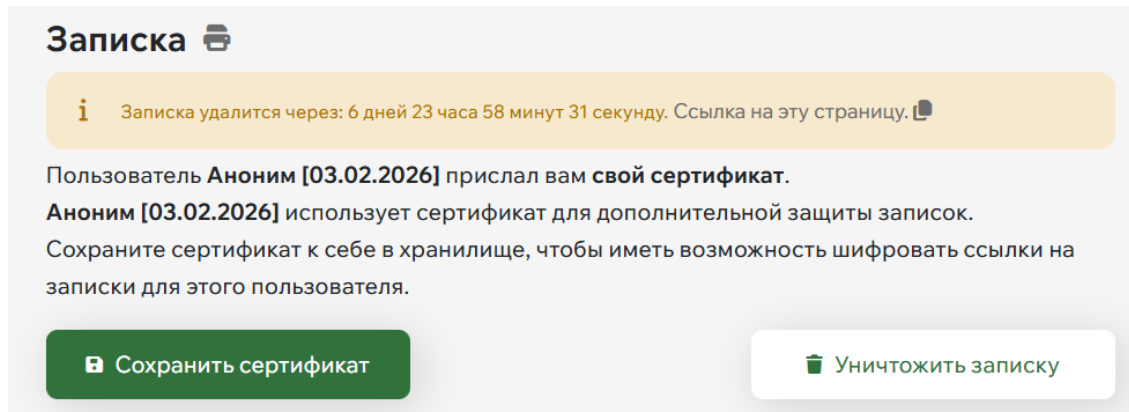


Рисунок 61 — Пример записки, содержащей сертификат

4.5.5. Мнемоника

Особенности

Мнемоника - это набор легко запоминающихся слов, используемый для кодирования и сохранения приватных ключей.

После создания сертификата мнемонику невозможно изменить — только удаление старого сертификата и создание заново.

Примечание:

Разглашение мнемоники позволит злоумышленнику расшифровывать записки.

Держите фразу в секрете, храните её локально или используйте средства для хранения паролей.

Для работы не нужны дополнительные устройства и программы.

Расшифрование с помощью мнемоники может происходить как с ноутбуков, так и с телефонов, планшетов.

Создание

Для создания мнемоники откройте раздел "Мнемоника" и нажмите кнопку «». После этого будет сгенерирована случайная фраза.

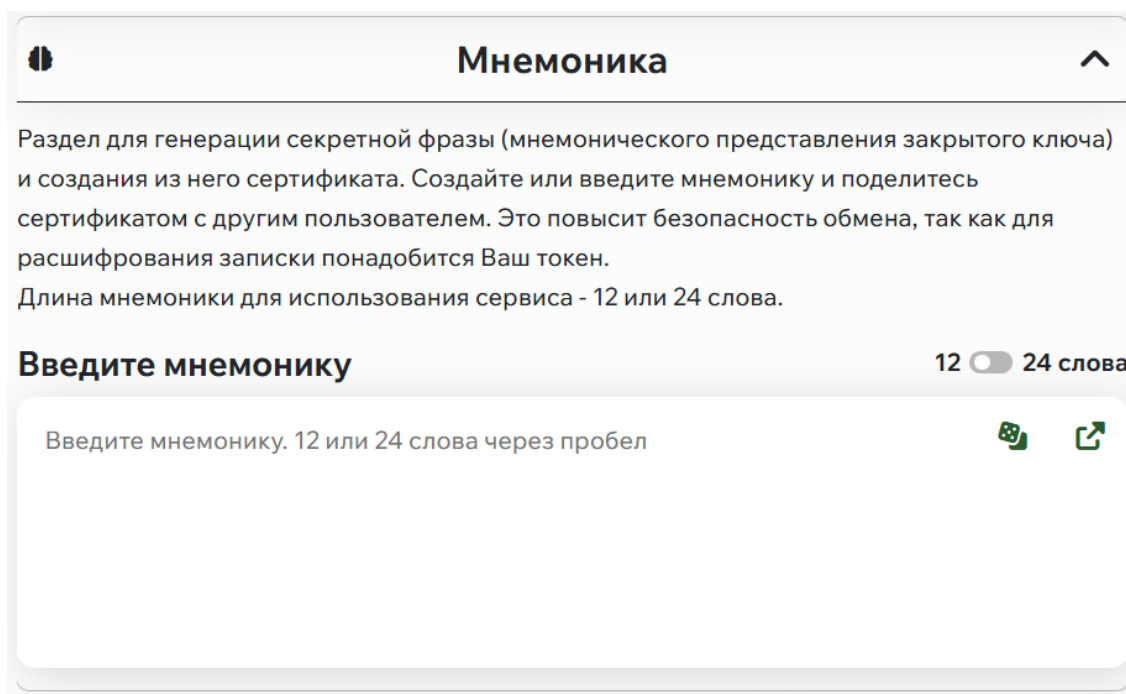


Рисунок 62 — Способ хранения ключа: Мнемоника

Вы можете повторно нажать кнопку «», чтобы получить новую случайную последовательность слов, а так же использовать переключатель « 12 24 слова» для изменения длины мнемоники.

Управление существующей мнемоникой

В поле ввода мнемоники можете ввести ранее сохраненную мнемонику, подсказки помогут исправить ошибки при вводе.

Поделиться сертификатом

1. Чтобы поделиться сертификатом нажмите кнопку «».
2. В открывшемся всплывающем окне укажите ваше имя, это имя будет предложено получателю при сохранении сертификата в хранилище. Значение по умолчанию: **Аноним**.

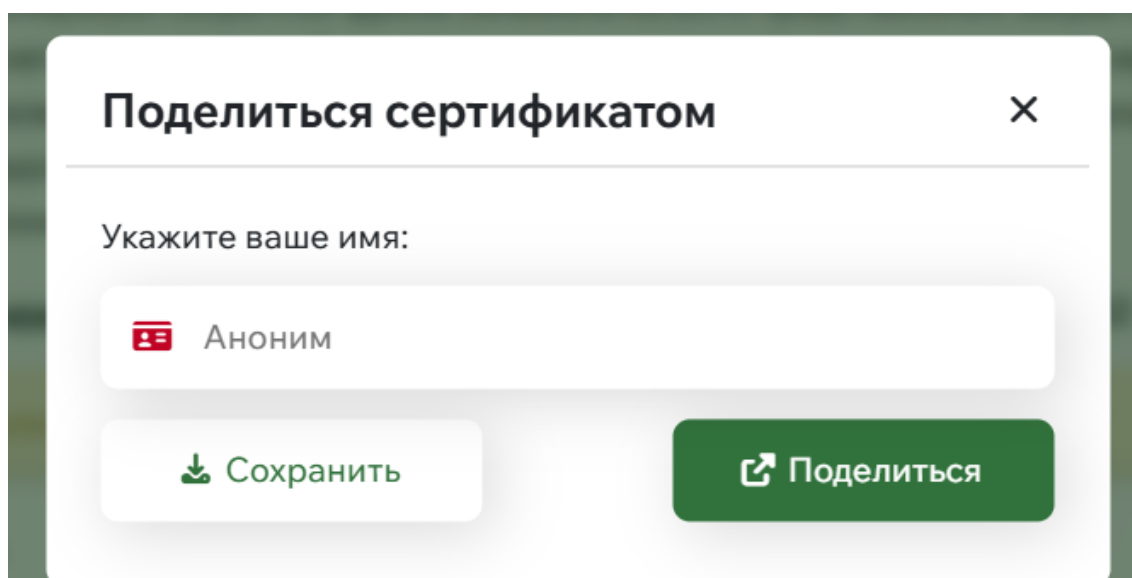


Рисунок 63 — Поделиться сертификатом. Поле указания имени

3. После этого вы можете:
 - нажать кнопку "**Поделиться**". Будет создана записка содержащая ваш сертификат. Время жизни записки - **7 дней**.
 - сохранить сертификат в файл .json и передать его получателю.

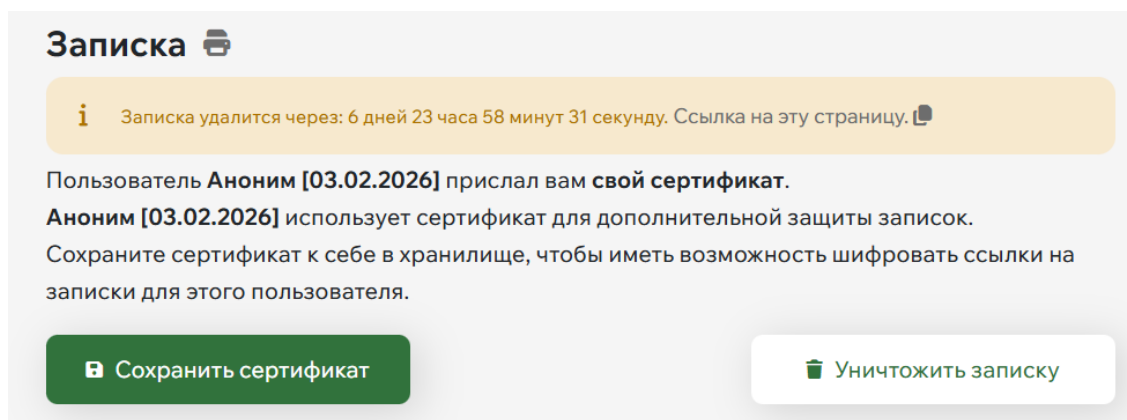


Рисунок 64 — Пример записки, содержащей сертификат

4.6. Сценарий 6: Чтение записки

4.6.1. Получение ссылки на записку

После создания записки, отправитель направляет Вам уникальную ссылку для её доступа к записке. Ссылка содержит ключ, необходимый для расшифровки содержимого. Откройте ссылку в вашем браузере.

4.6.2. Вариант 1. Ссылка без дополнительной защиты

Если ссылка была создана без дополнительной защиты, то либо записка будет открыта сразу, либо вы увидите окно

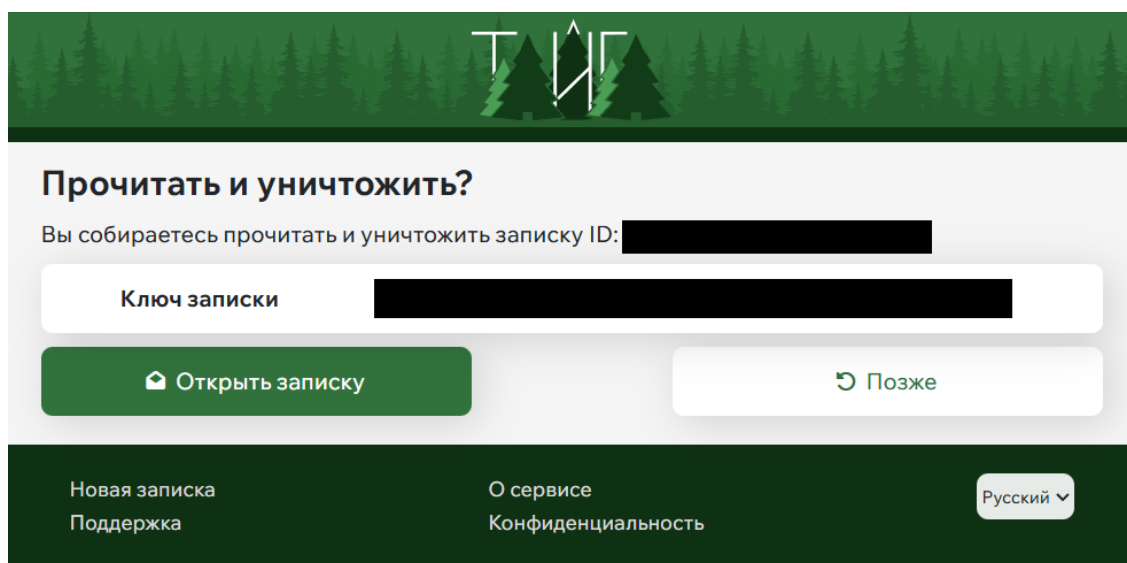


Рисунок 65 — Открытие одноразовой записки без дополнительной защиты

После нажатия на кнопку **"Открыть записку"** она будет показана Вам и удалена с сервера, при нажатии на **"Позже"** вас вернёт на главную страницу, а записка не будет прочитана и удалена.

Многоразовые записки открываются сразу, без этого окна.

4.6.3. Вариант 2. Ссылка защищенная паролем

Система автоматически определит, что записка зашифрована паролем. Появится окно с инпутом для ввода пароля. Вы должны ввести тот же пароль, который использовался при создании записи. Система использует PBKDF2 (P 50.1.111-2016) на хэш-функции ГОСТ 34.11-2018 (Стрибог) для генерации ключей из пароля.

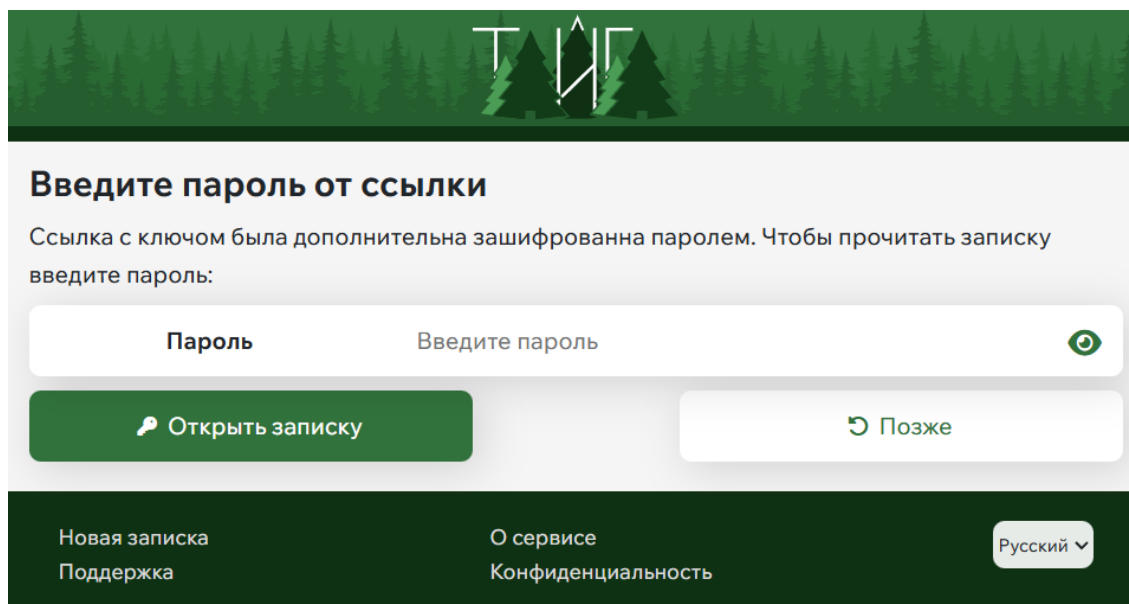
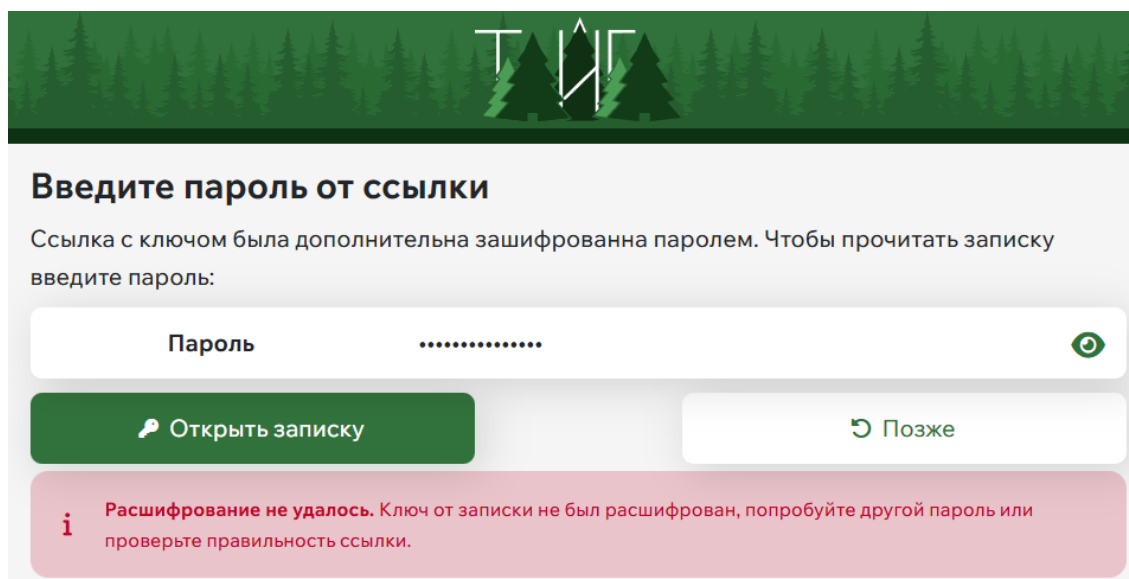
The screenshot shows a web interface for opening a password-protected note. At the top is a green header with a forest background and the letters 'ТИГ' in white. Below the header, the main content area has a light gray background. It starts with the title 'Введите пароль от ссылки' in bold. Below the title is a message: 'Ссылка с ключом была дополнительно зашифрована паролем. Чтобы прочитать записку введите пароль:'. There is a large white input field with the placeholder text 'Введите пароль' and a green eye icon on the right. Below the input field are two buttons: a green button with a key icon and the text 'Открыть записку', and a white button with a circular arrow icon and the text 'Позже'. At the bottom of the interface is a dark green footer bar. It contains links 'Новая записка' and 'Поддержка' on the left, 'О сервисе' and 'Конфиденциальность' in the center, and a language selector 'Русский' with a dropdown arrow on the right.

Рисунок 66 — Открытие записки защищенной паролем. Страница с вводом пароля

Введите пароль в соответствующее поле. Нажмите кнопку **"Открыть записку"**.

Если пароль верный, содержимое записки будет отображено на экране. Если пароль неверен — система покажет ошибку:



Введите пароль от ссылки

Ссылка с ключом была дополнительно зашифрована паролем. Чтобы прочитать записку введите пароль:

Пароль



 Открыть записку

 Позже

 **Расшифрование не удалось.** Ключ от записки не был расшифрован, попробуйте другой пароль или проверьте правильность ссылки.

Рисунок 67 — Сообщение об ошибке при неправильном пароле

Если вы ввели неверный пароль, можно повторить попытку. Введите правильный пароль и снова нажмите кнопку "Открыть записку".

Примечание:

Пароль не может быть пустым.

Примечание:

Для расшифровки необходим точный пароль, указанный при создании записи.

4.6.4. Вариант 3. Ссылка защищенная сертификатом

Система автоматически определит, что записка сертификатом. Появится окно с выбором места хранения ключа.

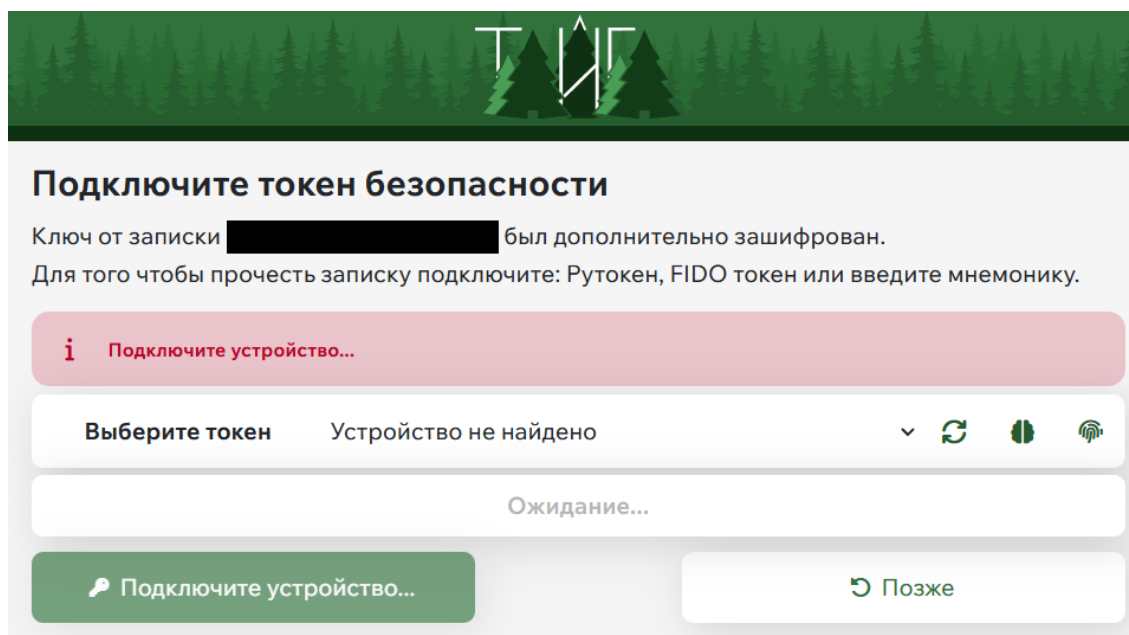


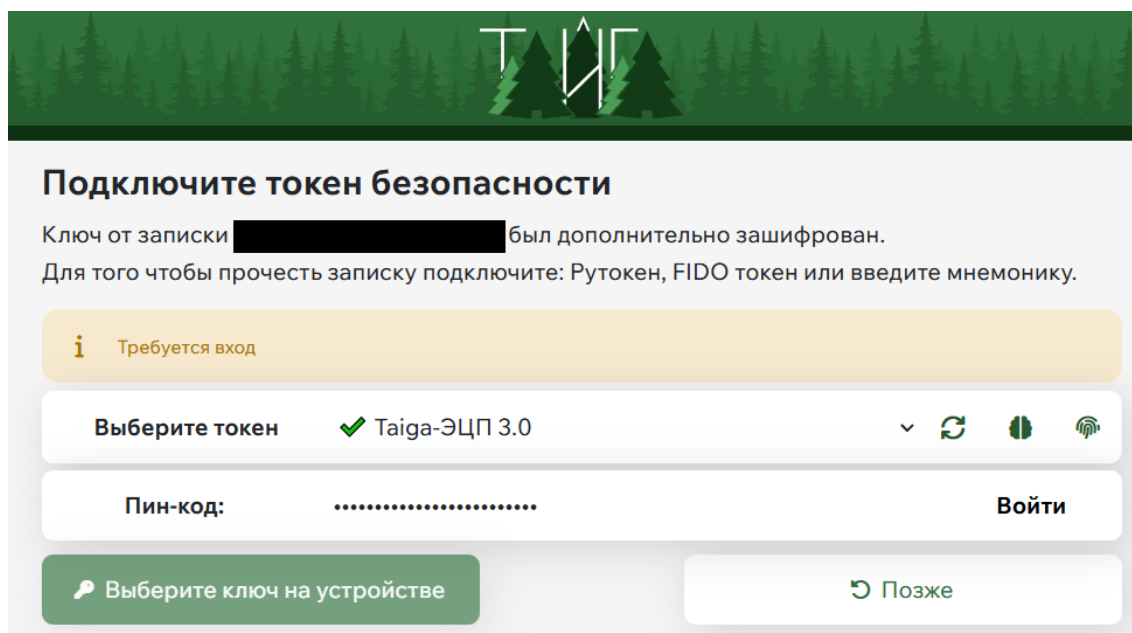
Рисунок 68 — Открытие записки защищенной сертификатом

В зависимости от способа хранения закрытого ключа, рассмотрим варианты расшифрования

Рутокен

Если ваш ключ хранится на Рутокен Lite или Рутокен ЭЦП, то подключите ключ к компьютеру и нажмите «  » для обновления подключенных устройств.

Введите пин-код в соответствующее поле и нажмите **"Войти"**.



Подключите токен безопасности

Ключ от записки [redacted] был дополнительно зашифрован.
Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

i Требуется вход

Выберите токен ✓ Taiga-ЭЦП 3.0

Пин-код: **Войти**

Выберите ключ на устройстве Позже

Рисунок 69 — Открытие записки защищенной сертификатом. Ввод пин-кода от Рутокен

Выберите сервисный ключ среди обнаруженных на устройстве и нажмите **"Использовать этот ключ"**. Или, нажмите **"Попробовать все ключи"**, чтобы попробовать все обнаруженные сервисные ключи.

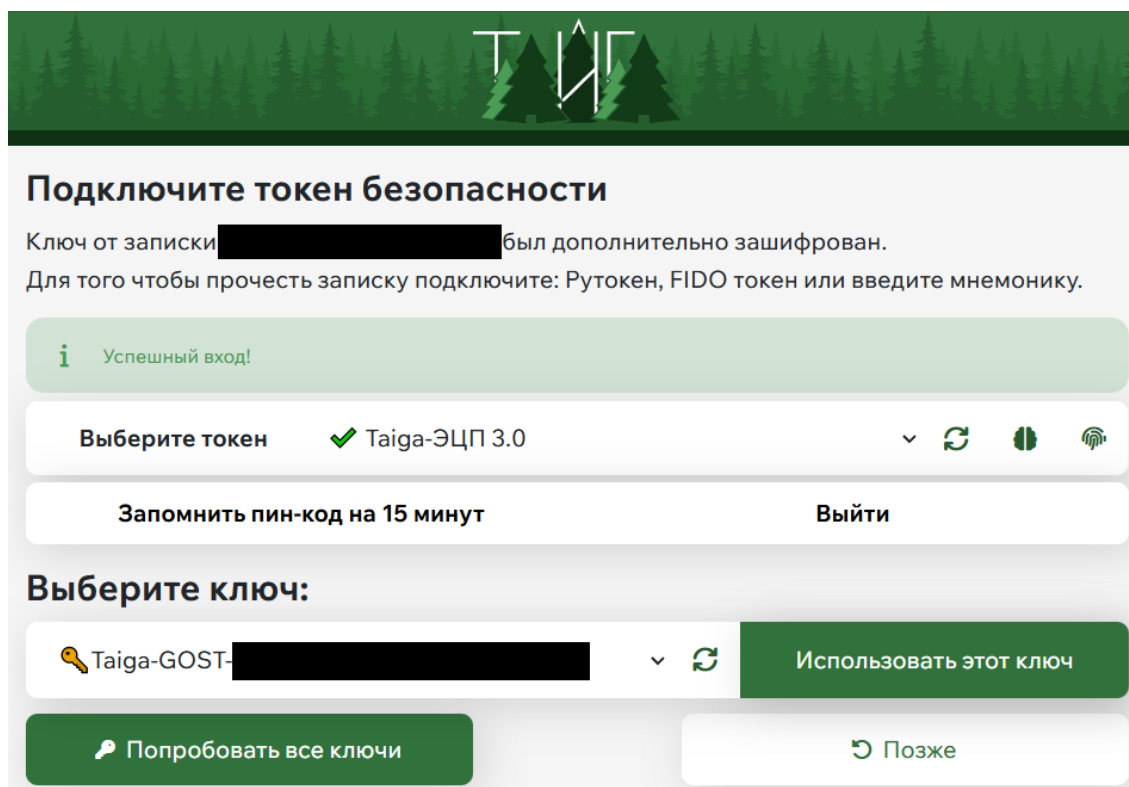


Рисунок 70 — Открытие записки защищенной сертификатом. Выбор ключа на устройстве Рутокен

Если ключ подходит для расшифрования записки, то записка будет отображена на экране. В случае, если ни один ключ не подошёл, то будет выведена ошибка **"Расшифрование не удалось"**. Попробуйте использовать ключ с другого носителя или обратитесь к получателю.

Подключите токен безопасности

Ключ от записки [REDACTED] был дополнительно зашифрован.
Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

 Успешный вход!

Выберите токен

✓ Taiga-ЭЦП 3.0

▼ ↺ 🔒 🖨

Запомнить пин-код на 15 минут

Выйти

Выберите ключ:

 Taiga-GOST-[REDACTED]

▼ ↺

Использовать этот ключ

 Попробовать все ключи

↺ Позже

 **Расшифрование не удалось.** Ключ от записки не был расшифрован, попробуйте другой ключ или токен.

Рисунок 71 — Открытие записки защищенной сертификатом. Расшифрование не удалось

FIDO / U2F токен

Если ваш ключ хранится на токене Рутокен MFA, Рутокен Nano, Рутокен U2F, Yubikey или ином устройстве FIDO / U2F, то подключите ключ к компьютеру и нажмите «».

Откроется окно ввода пин-кода, введите пин-код и нажмите "ОК".

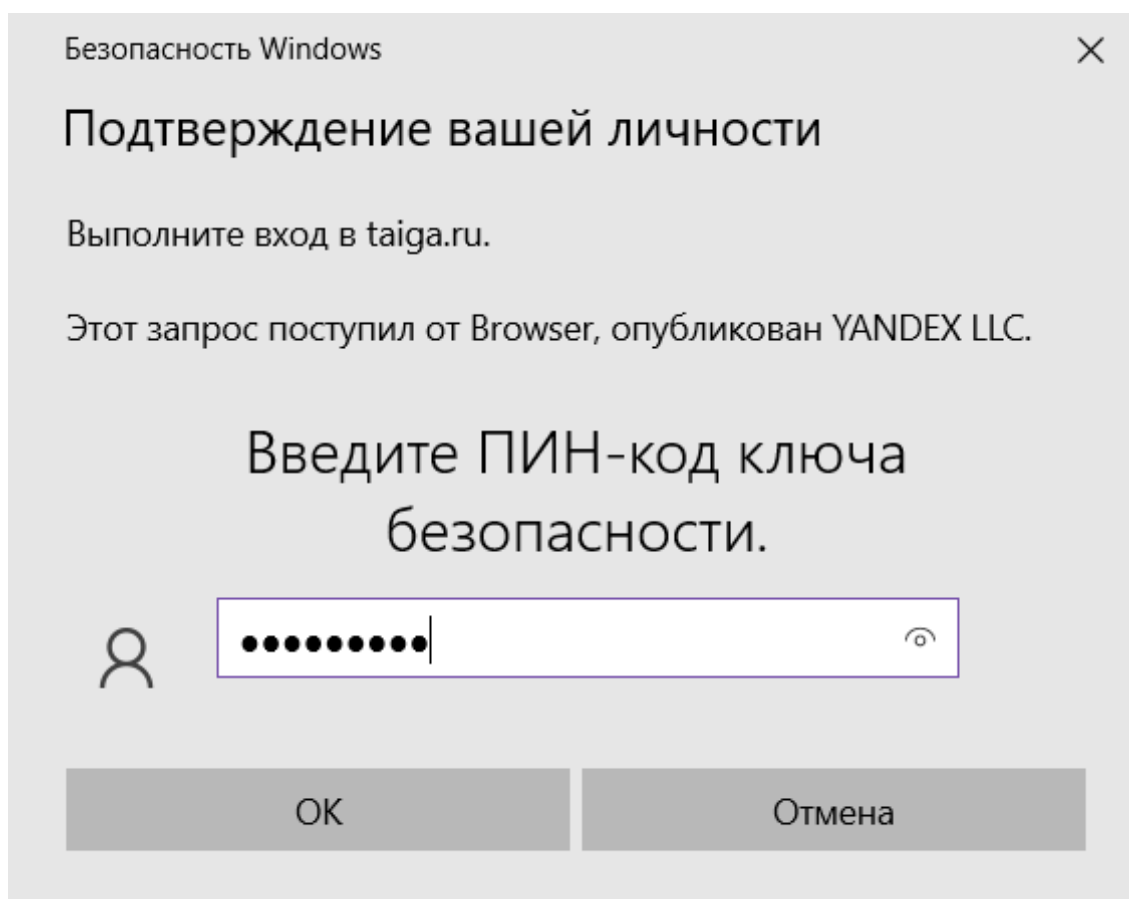


Рисунок 72 — Открытие записки защищенной сертификатом. Ввод пин-кода на FIDO ключе
Коснитесь кнопки на ключе безопасности.

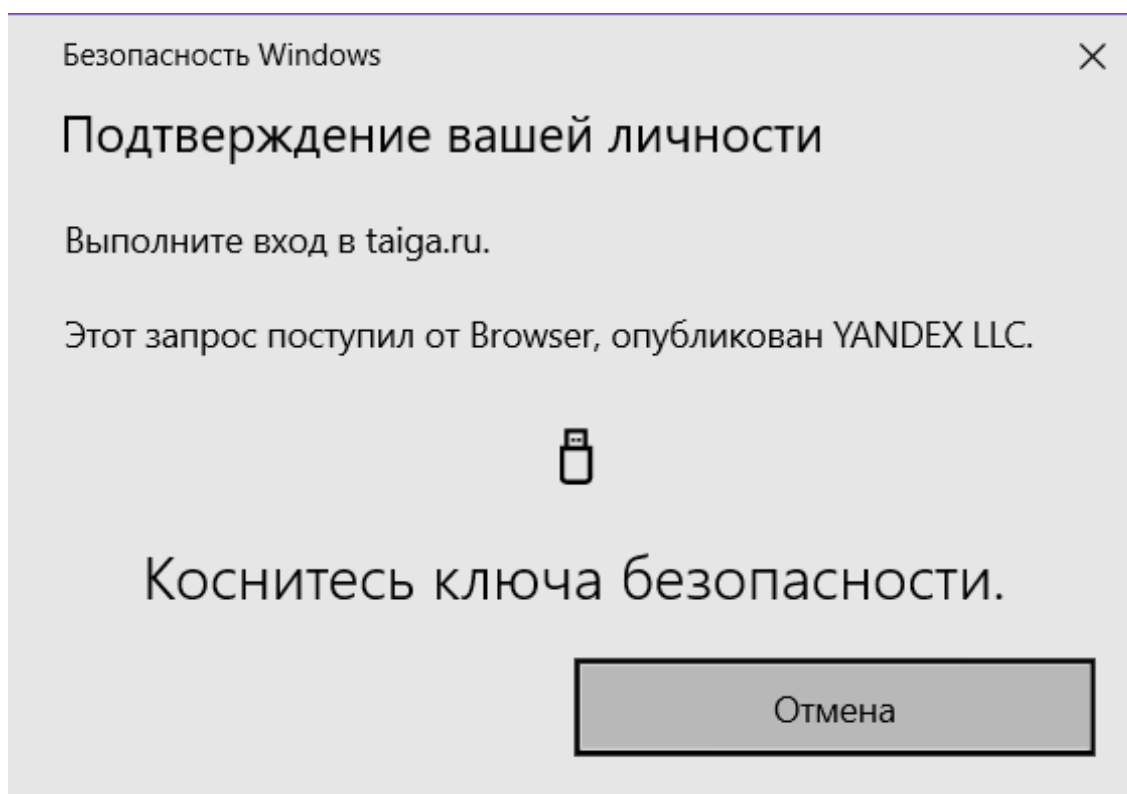


Рисунок 73 — Открытие записки защищенной сертификатом. Коснитесь ключа безопасности

Если у вас несколько ключей на токене - выберите ключ которым хотите расшифровать. Если ключ подходит для расшифрования записки, то записка будет отображена на экране. В случае, если ключ не подошёл, то будет выведена ошибка **"Расшифрование не удалось"**. Попробуйте использовать ключ с другого носителя или обратитесь к получателю.

Подключите токен безопасности

Ключ от записки [REDACTED] был дополнительно зашифрован.
Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

 Подключите устройство...

Выберите токен Устройство не найдено    

Ожидание...

 Подключите устройство...  Позже

 Расшифрование не удалось. Ключ от записки не был расшифрован, попробуйте другой ключ или токен.

Рисунок 74 — Открытие записки защищенной сертификатом. Расшифрование не удалось

Мнемоника

Если ваш ключ хранится в виде мнемоники, то нажмите «  ». Откроется поле ввода мнемоники. Введите свою мнемонику, следуя подсказкам.

Подключите токен безопасности

Ключ от записки [REDACTED] был дополнительно зашифрован.
Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

Введите мнемонику 

 Подключите устройство...  Позже

Рисунок 75 — Открытие записки защищенной сертификатом. Ввод мнемоники

После ввода мнемоники нажмите **"Использовать мнемонику"**. Если ключ подходит для расшифрования записки, то записка будет отображена на экране.

Введите мнемонику

Ключ от записки [REDACTED] был дополнительно зашифрован.
 Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

| | | | |
|---------------|---------------|---------------|---------------|
| 01 [REDACTED] | 02 [REDACTED] | 03 [REDACTED] | 04 [REDACTED] |
| 05 [REDACTED] | 06 [REDACTED] | 07 [REDACTED] | 08 [REDACTED] |
| 09 [REDACTED] | 10 [REDACTED] | 11 [REDACTED] | 12 [REDACTED] |



 **Использовать мнемонику**  **Позже**

Рисунок 76 — Открытие записки защищенной сертификатом. Ввод мнемоники

В случае, если ключ не подошёл, то будет выведена ошибка **"Расшифрование не удалось"**. Попробуйте использовать другой ключ, ключ с другого носителя или обратитесь к получателю.

Введите мнемонику

Ключ от записки [REDACTED] был дополнительно зашифрован.
 Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

| | | | |
|---------------|---------------|---------------|---------------|
| 01 [REDACTED] | 02 [REDACTED] | 03 [REDACTED] | 04 [REDACTED] |
| 05 [REDACTED] | 06 [REDACTED] | 07 [REDACTED] | 08 [REDACTED] |
| 09 [REDACTED] | 10 [REDACTED] | 11 [REDACTED] | 12 [REDACTED] |



 **Использовать мнемонику**  **Позже**

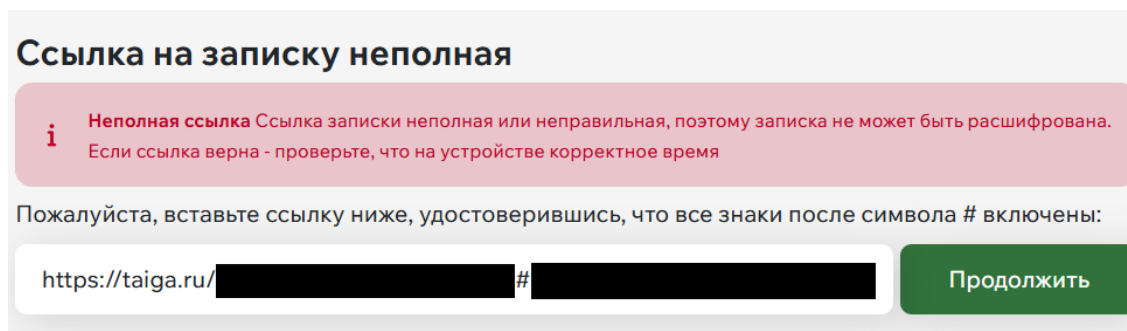
 **Расшифрование не удалось.** Ключ от записки не был расшифрован, попробуйте другой ключ или токен.

Рисунок 77 — Открытие записки защищенной сертификатом. Расшифрование не удалось

Чтобы вернуться к выбору ключа на рутокене и FIDO ключе нажмите «  ».

4.6.5. Вариант 4. Неполная ссылка

Если ключ в записке не подходит по какой-то причине или нарушена целостность ссылки будет выведено окно с повторным вводом ссылки. Проверьте, что ссылка скопирована корректно и вставьте её в соответствующее поле и нажмите **"Продолжить"**.



The screenshot shows a dialog box titled "Ссылка на записку неполная" (Link to the note is incomplete). It contains an information icon (i) and a red message: "Неполная ссылка Ссылка записки неполная или неправильная, поэтому записка не может быть расшифрована. Если ссылка верна - проверьте, что на устройстве корректное время" (Incomplete link. The link to the note is incomplete or incorrect, so the note cannot be decrypted. If the link is correct - check that the time on the device is correct). Below the message, it says "Пожалуйста, вставьте ссылку ниже, удостоверившись, что все знаки после символа # включены:" (Please paste the link below, ensuring that all signs after the # symbol are included:). There is a text input field containing "https://taiga.ru/" followed by a blacked-out section and a "#", and another blacked-out section after the "#". To the right of the input field is a green button labeled "Продолжить" (Continue).

Рисунок 78 — Неполная ссылка на записку

4.7. Сценарий 7: Управление сертификатами. Экспорт/импорт (для хранилища сертификатов).

4.7.1. Экспорт сертификатов

В приложении "Тайга" вы можете экспортировать все сохранённые сертификаты в один JSON-файл для резервного копирования или передачи между устройствами. Процесс полностью локальный и не требует подключения к серверу.

Откройте страницу управления сертификатами, для этого перейдите в раздел "Контакты" через меню слева.

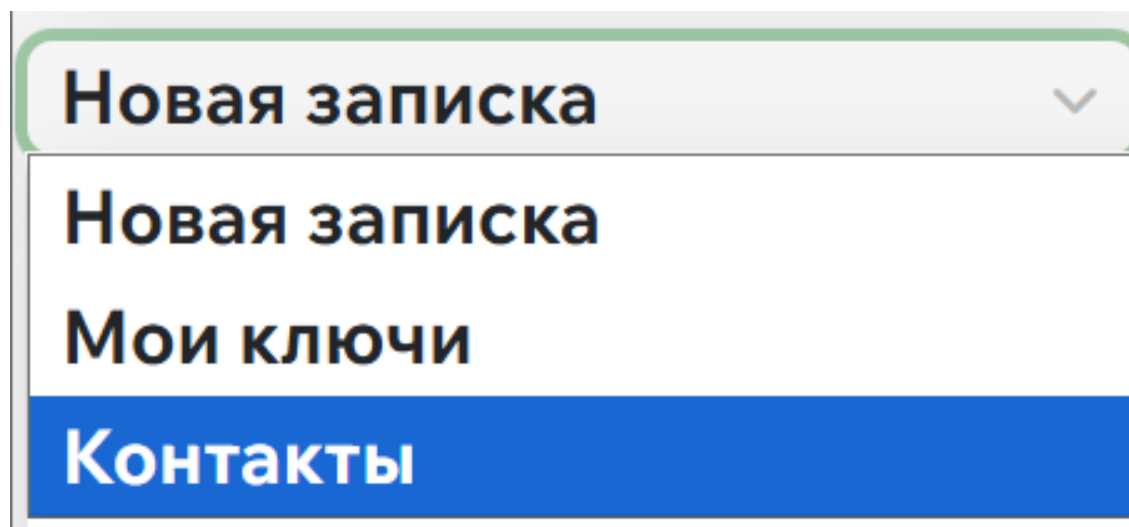


Рисунок 79 — Меню контакты

На странице контактов найдите кнопку с иконкой «» (расположена в правом верхнем углу или на карточке соответствующего сертификата) и нажмите её.

Система автоматически подготовит JSON-файл с данными всех сертификатов и предложит его скачать на вашем устройстве.

Примечание:

Экспортированный файл содержит все метаданные сертификатов (имя, PEM-формат). Файл сохраняется локально в браузере и не передается на сервер.

4.7.2. Импорт сертификатов

Импорт позволяет добавить сертификаты из внешнего JSON-файла, уже сохраненного на вашем устройстве. Система проверяет корректность данных перед добавлением в локальное хранилище.

Откройте страницу управления сертификатами, для этого перейдите в раздел "Контакты" через меню слева.

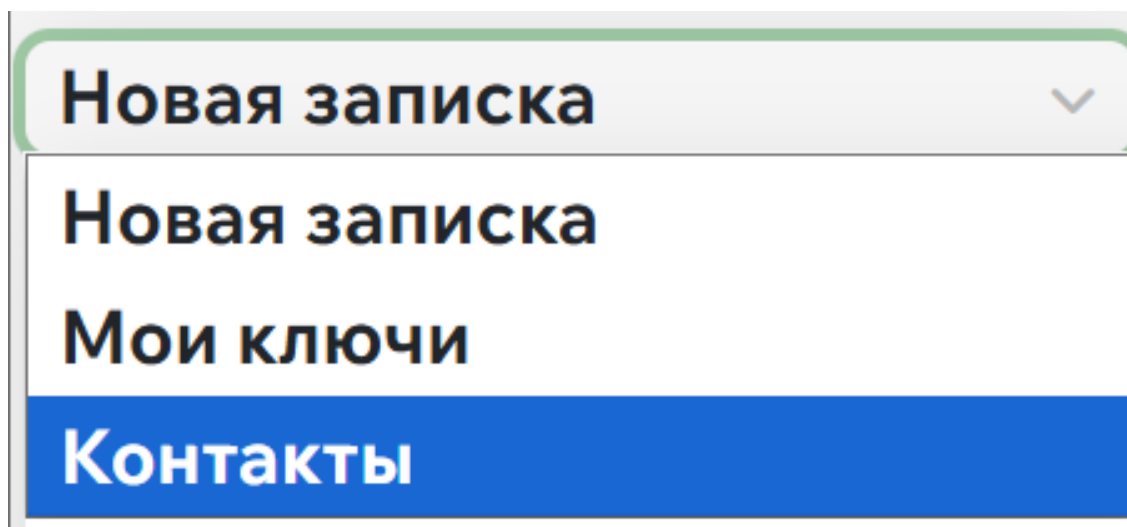


Рисунок 80 — Меню контакты

На странице контактов найдите кнопку с иконкой «  » (расположена в правом верхнем углу) и нажмите её.

Откроется диалог выбора файлов — выберите JSON-файл с сертификатами. Система проверит структуру файла и импортирует новые сертификаты. После завершения вы увидите обновлённый список сертификатов в интерфейсе.

Примечание:

Импорт возможен только из файлов в формате JSON. Если существуют сертификаты с повторяющимися именами, то будут сохранены оба варианта.

Примечание:

Существуют доверенные сертификаты, такие сертификаты задаёт администратор системы. Помечаются они иконкой «  ». При попытке импортировать сертификат с именем доверенного при следующем заходе он будет перезаписан на тот, который был задан администратором.

4.7.3. Удаление сертификатов

Вы можете удалить один или все сертификаты из хранилища нажав на кнопку «  » справа на верху или на карточке соответствующего сертификата.

5. ИНТЕРФЕЙС И ОСНОВНЫЕ ФУНКЦИИ

5.1. Главная страница (Создание записок)

Главная страница — это основной интерфейс для создания защищённых записок с различными способами шифрования. Пользователь может выбрать тип записки: текст, ключ или сертификат и настроить параметры безопасности.

5.1.1. Элементы управления:

- **Выбор типа записки:**
 - Выпадающий список с опциями: "Новая записка", "Мои ключи", "Контакты".
 - В зависимости от выбранного типа, появляются соответствующие страницы.

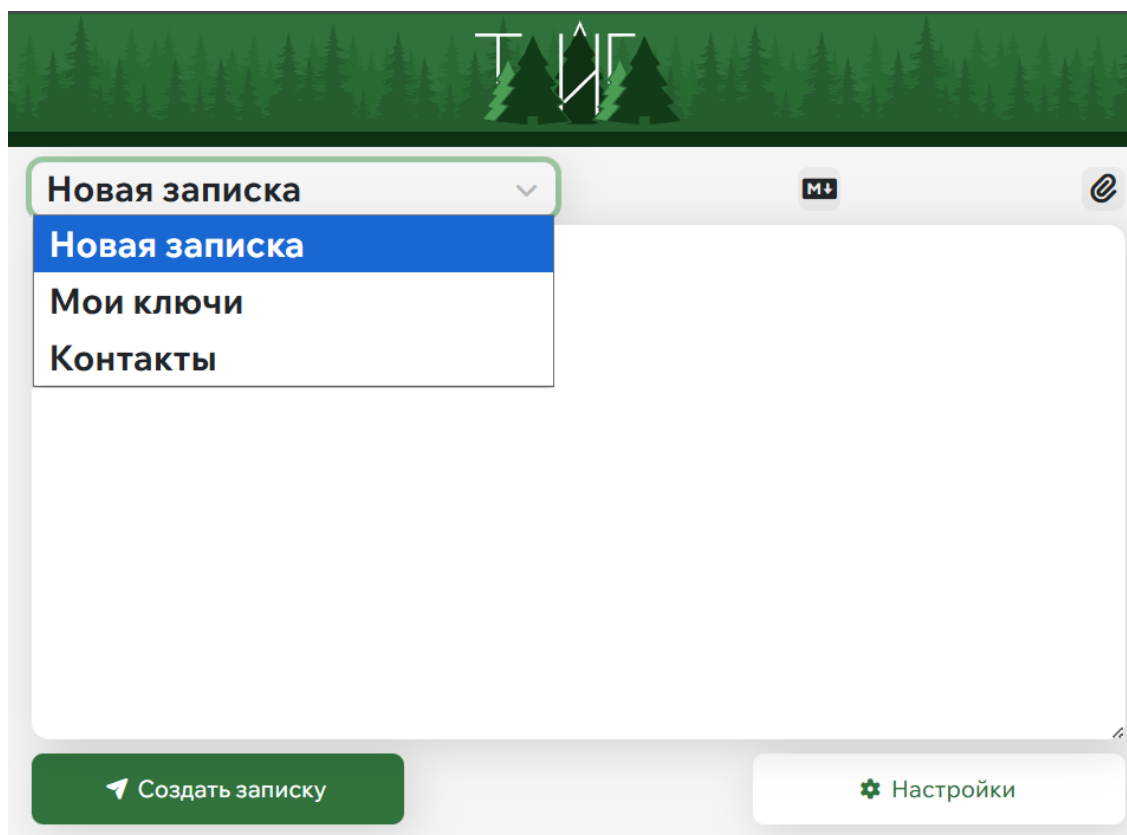


Рисунок 81 — Главная страница с выпадающим меню выбора типа записки

- **Markdown форматирование:**



- Чекбокс с эмодзи «» в правом верхнем углу для переключения режима.
- TinyMDE редактор поддерживает таблицы, код блоки и графики.

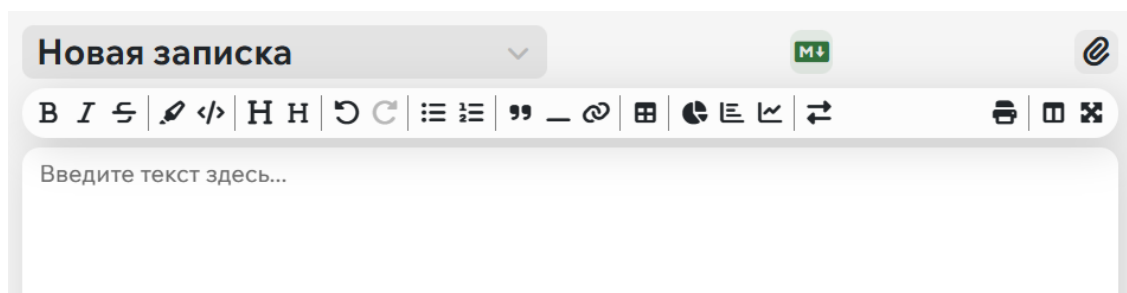


Рисунок 82 — Активированный Markdown режим с предпросмотром

- **Добавление файлов:**

- Чекбокс «  » для активации загрузки.
- Дроп-зона с индикатором выбора файлов.
- Список выбранных файлов отображается под полем ввода.

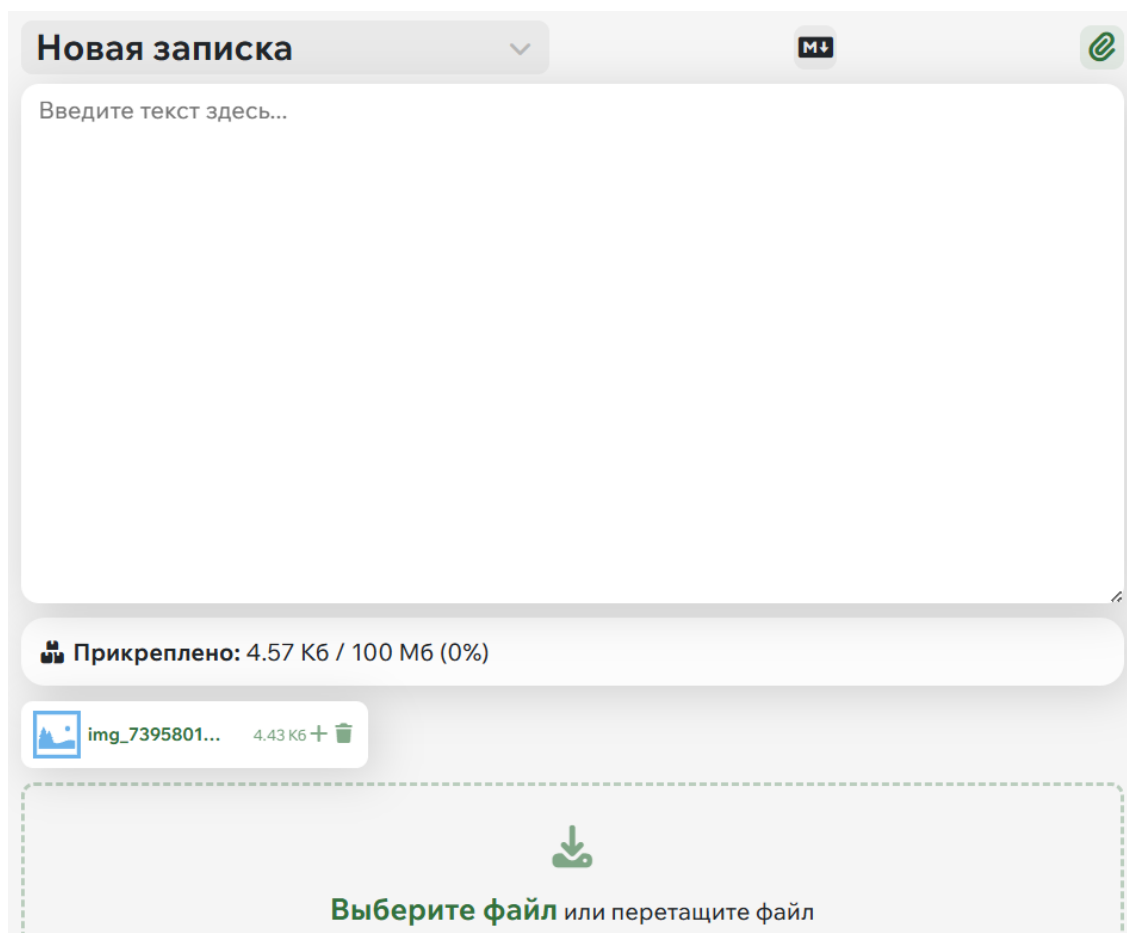


Рисунок 83 — Область загрузки файлов с дроп-зоной

- **Настройка записки:**

- Выпадающий список с опциями: "Удалить после прочтения", "15 минут", "24 часа" и др.
- Чекбокс для отключения запроса подтверждения удаления.
- Тип шифрования

Рисунок 84 — Параметры времени жизни с выбранным сроком

- **Кнопка создания записки:**
 - Зеленая кнопка "Создать записку" в левом нижнем углу формы.
 - При нажатии начинается процесс шифрования и генерации ссылки.

5.2. Страница управления сертификатами

Страница позволяет управлять локальными и защищёнными сертификатами. Основные функции: импорт, экспорт, удаление и переименование.

5.2.1. Элементы управления:

- **Список сертификатов:**
 - Таблица отображает все сохранённые сертификаты.
 - Цветовая кодировка различает локальные и подтвержденные администратором сертификаты.

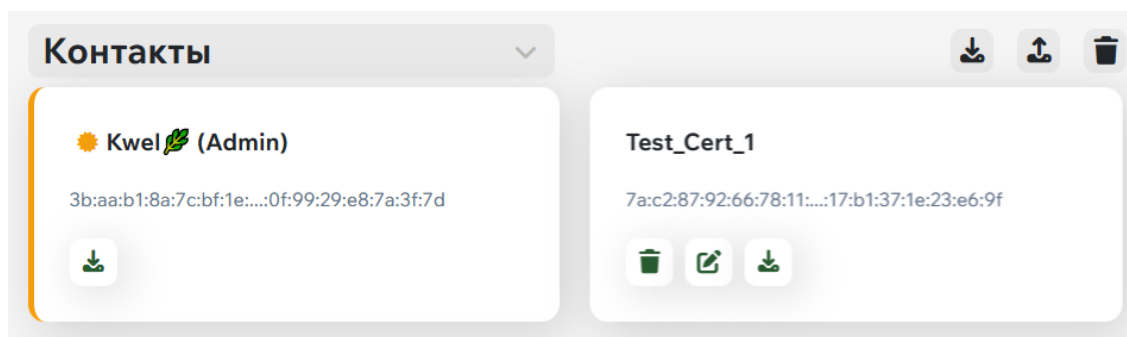


Рисунок 85 — Список сертификатов с цветовой кодировкой

- **Кнопки управления:**

- "Экспорт" — создать JSON файл со всеми сертификатами.
- "Импорт" — загрузить сертификаты из файла.
- "Удалить всё" — очистить список.



Рисунок 86 — Панель управления сертификатами с кнопками

- **Действия с конкретным сертификатом:**

- Кнопка "Удалить" доступна только для не подтвержденных сертификатов.
- Кнопка "Переименовать" — открывает модальное окно, доступна только для не подтвержденных сертификатов.
- Кнопка "Экспорт".

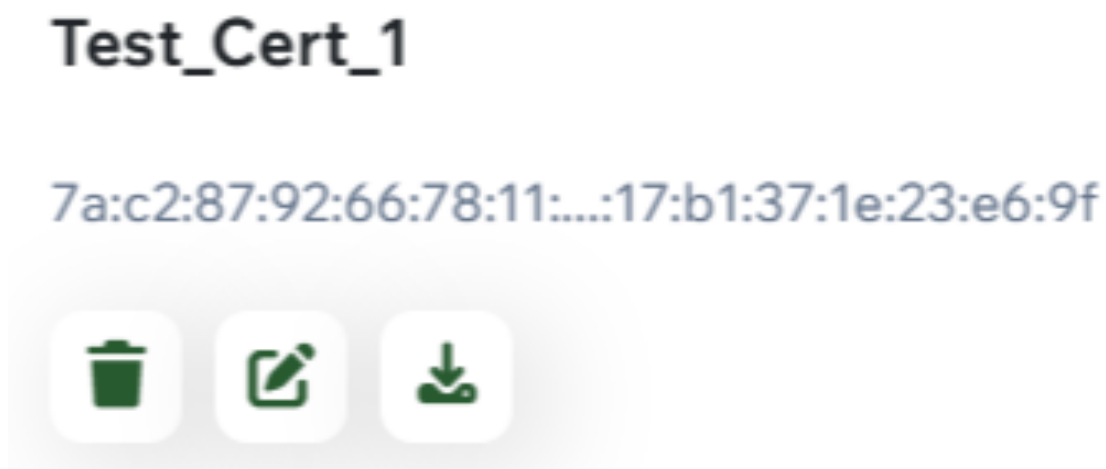


Рисунок 87 — Панель управления отдельным сертификатом

5.3. Страница создания ключей

Интерфейс для генерации и управления ключами хранищимися по методам FIDO, Rutoken или мнемонической фразы.

5.3.1. Элементы управления:

- **Выбор способа хранения ключа:**
 - Выпадающий список с опциями: FIDO, Rutoken, Mnemonic.

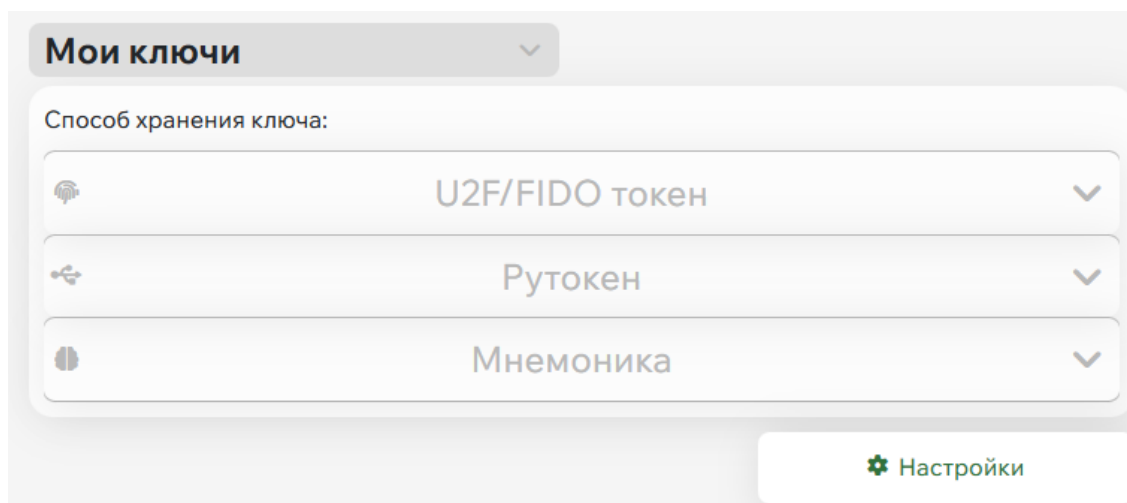


Рисунок 88 — Выбор метода хранения ключа

- **Генерация и хранение ключа:**



Рисунок 89 — Способ создания и хранения ключа: FIDO / U2F ключ

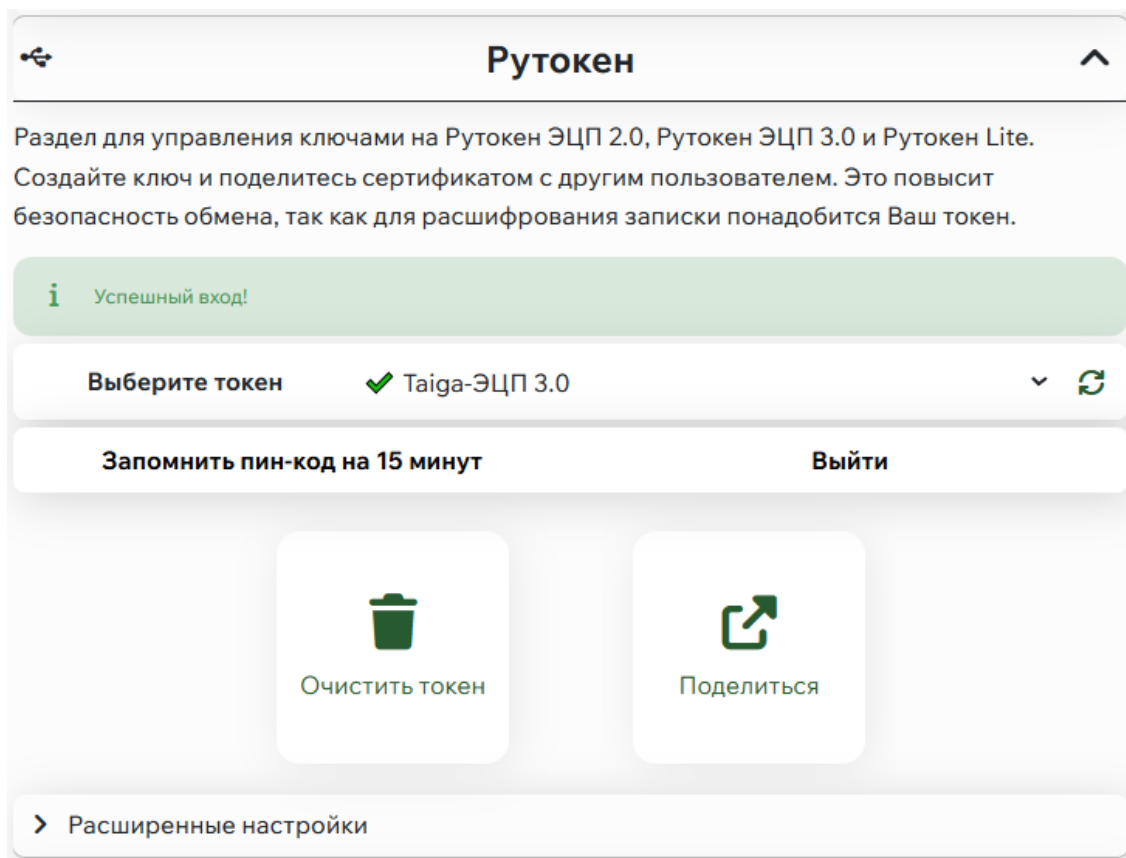


Рисунок 90 — Способ создания и хранения ключа: Рутокен



Мнемоника



Раздел для генерации секретной фразы (мнемонического представления закрытого ключа) и создания из него сертификата. Создайте или введите мнемонику и поделитесь сертификатом с другим пользователем. Это повысит безопасность обмена, так как для расшифровки записки понадобится Ваш токен.

Длина мнемоники для использования сервиса - 12 или 24 слова.

Введите мнемонику12 ☐ 24 слова

Введите мнемонику. 12 или 24 слова через пробел



Рисунок 91 — Способ создания и хранения ключа: мнемоника

- **Модальное окно:**

- После создания появляется окно с полем имени сертификата.
- Кнопки "Сохранить" и "Поделиться" для передачи данных.

Поделиться сертификатом



Укажите ваше имя для получателя:



 **Сохранить**

 **Поделиться**

Рисунок 92 — Модальное окно: поделиться сертификатом

5.4. Страница создания ссылки

Просмотр защищённой записки через уникальную ссылку. Доступ осуществляется с использованием пароля, сертификата или устройства.

5.4.1. Элементы управления:

- **Управление ссылкой:**
 - Дублировать записку
 - Включить Markdown при чтении записки по умолчанию
 - Изменить вид ссылки
 - Отправить ссылку по email
 - Прочитать записку / уничтожить записку
 - Скопировать ссылку
 - Дополнительная защита паролем
 - Дополнительная защита сертификатом

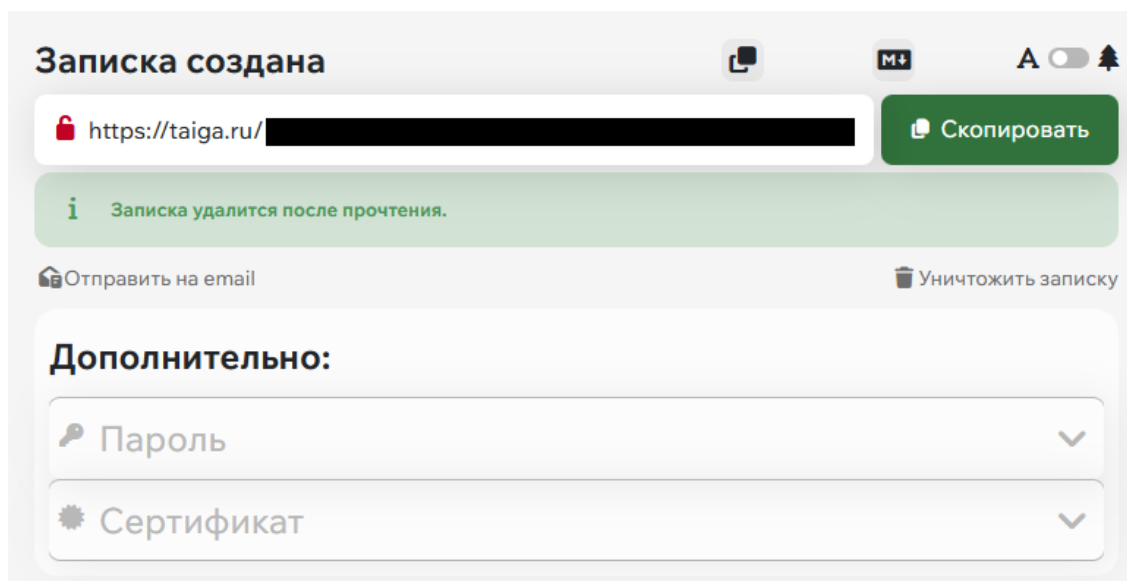


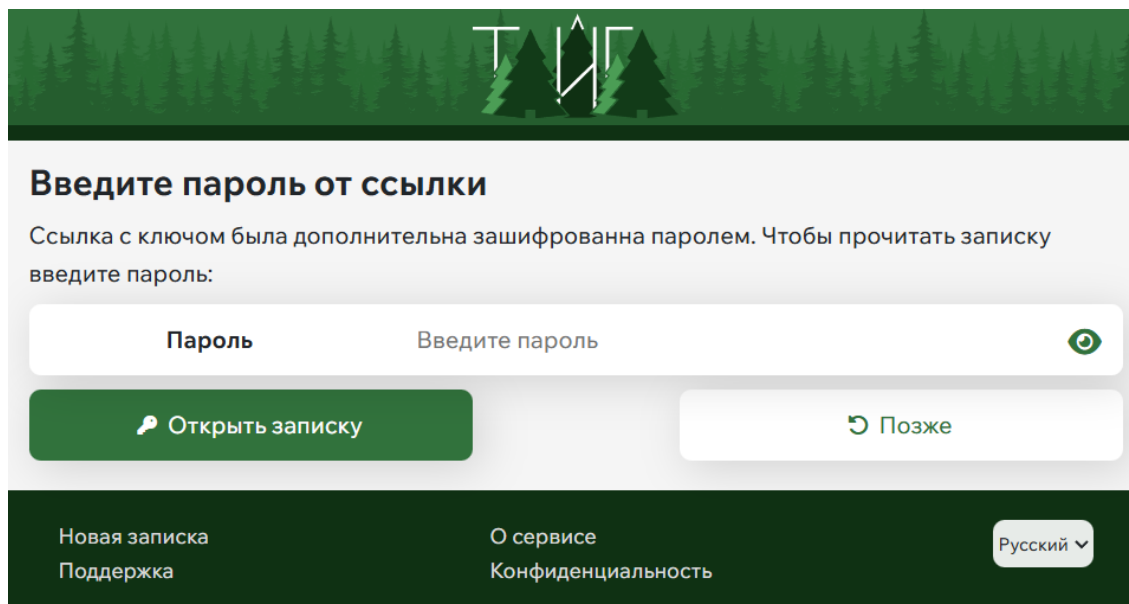
Рисунок 93 — Страница с ссылкой на записку

5.5. Страница чтения записок

Просмотр защищённой записки через уникальную ссылку. Доступ осуществляется с использованием пароля, сертификата или устройства.

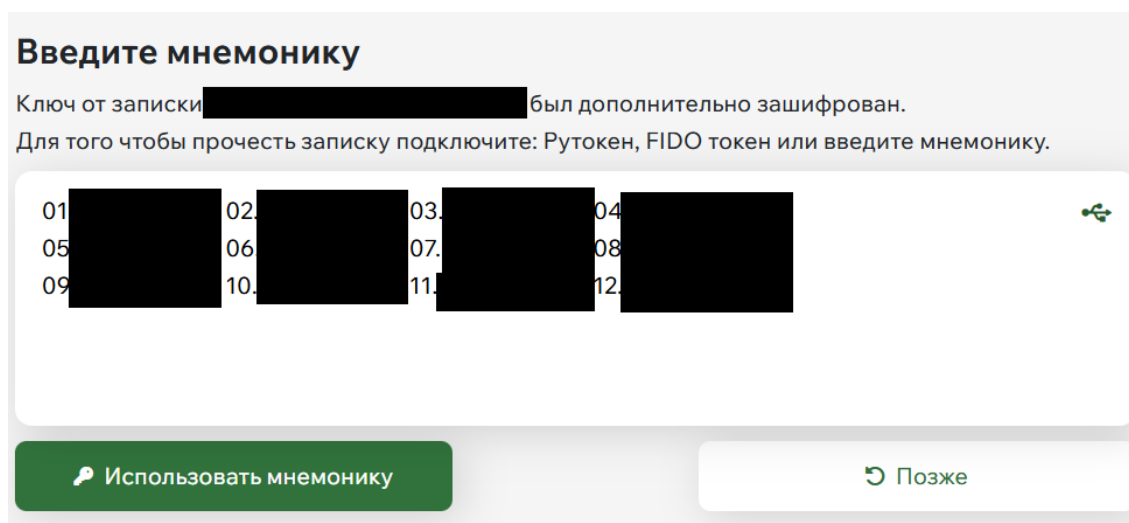
5.5.1. Элементы управления:

- **Расшифровка:**
 - Поле ввода пароля для расшифрования по паролю.
 - Список сертификатов для выбора.



The screenshot shows a web interface with a green header featuring a forest background and the letters 'ТИГ'. Below the header, the title 'Введите пароль от ссылки' (Enter password from link) is displayed. A message states: 'Ссылка с ключом была дополнительно зашифрована паролем. Чтобы прочитать записку введите пароль:' (The link with the key was additionally encrypted with a password. To read the note, enter the password:). There is a password input field with the placeholder 'Введите пароль' and a toggle icon on the right. Below the input field are two buttons: a green 'Открыть записку' (Open note) button and a white 'Позже' (Later) button. At the bottom, there is a dark green footer with links for 'Новая записка' (New note), 'Поддержка' (Support), 'О сервисе' (About service), and 'Конфиденциальность' (Privacy), along with a language selector set to 'Русский'.

Рисунок 94 — Открытие записки защищенной паролем. Страница с вводом пароля



The screenshot shows a web interface with the title 'Введите мнемонику' (Enter mnemonic). A message states: 'Ключ от записки [REDACTED] был дополнительно зашифрован. Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.' (The key from the note [REDACTED] was additionally encrypted. To read the note, connect: Рутокен, FIDO token or enter the mnemonic.). Below the message is a grid of 12 input fields for the mnemonic, arranged in 3 rows and 4 columns, with labels 01 through 12. A share icon is on the right. At the bottom, there are two buttons: a green 'Использовать мнемонику' (Use mnemonic) button and a white 'Позже' (Later) button.

Рисунок 95 — Открытие записки защищенной сертификатом. Ввод мнемоники

Подключите токен безопасности

Ключ от записки [redacted] был дополнительно зашифрован.
Для того чтобы прочесть записку подключите: Рутокен, FIDO токен или введите мнемонику.

Требуется вход

Выберите токен **✓ Taiga-ЭЦП 3.0**

Пин-код: **Войти**

Выберите ключ на устройстве **Позже**

Рисунок 96 — Открытие записки защищенной сертификатом. Ввод пин-кода от Рутокен

- **Управление запиской:**
 - Кнопка "Копировать ссылку".
 - Кнопка "Удалить сейчас".

Записка

Записка удалится через: 14 минут 57 секунд. Ссылка на эту страницу.

1231

Скопировать текст **Уничтожить записку**

Рисунок 97 — Чтение многократной записки

6. ПОДДЕРЖКА

6.1. Контакты

E-mail: support@taiga.ru

Телеграм: https://t.me/taiga_help_chat

По ним можно:

- Получить техническую помощь
- Отправить баг-репорты
- Связаться с командой разработчиков