

**Инструкция по генерации запроса и получению сертификата
электронной подписи в личном кабинете для АРМ на macOS и Linux**

Листов 12

Оглавление

I.	Работа с заявкой в личном кабинете.....	3
II.	Установка расширения TrustPlugin для браузера	4
III.	Установка приложения TrustPlugin на macOS.....	4
IV.	Установка приложения TrustPlugin на Linux	6
V.	Генерация запроса на сертификат с использованием СКЗИ КриптоПро CSP на macOS	8
VI.	Генерация запроса на сертификат с использованием СКЗИ КриптоПро CSP на Linux	10
VII.	Установка сертификата через личный кабинет.....	12

Внимание! Перед тем как работать с электронной подписью на macOS или Linux, ознакомьтесь с требованиями к рабочему месту.

I. Работа с заявкой в личном кабинете

После создания заявки на получение услуги удостоверяющего центра (Рисунок 1) вы можете создать запрос на выпуск сертификата. Для этого выполните следующие действия:

Список заявок						
Всего 2 заявки						
Номер	Клиент	Дата подачи	Точка выдачи	Стоимость	Статус	Сертификат
...	...	27.10.2021	77 - АО "ИнфоТeKC Интернет Траст", г. Москва	7950	Ожидание оплаты	запроса на сертификат

Рисунок 1

- Перейдите в личный кабинет АО «ИИТ» по ссылке iitrust.lk¹ и введите логин и пароль в соответствующие поля.
- После обработки заявки счёт отправляется на электронную почту (статусы заявки «Проверка данных» и «Ожидает оплату»). После поступления оплаты статус заявки изменится на «Ожидание запроса на сертификат».
- В списке заявок выберите заявку в статусе «Ожидание запроса на сертификат» и нажмите на её строчку/номер. Если ранее на рабочем месте не был установлен TrustPlugin для браузера, то необходимо установить его.

¹ Если вы пользуетесь корпоративным личным кабинетом, используйте соответствующую ссылку для своего домена.

II. Установка расширения TrustPlugin для браузера

Внимание! Если у вас macOS, то для работы плагина в браузере Safari требуются дополнительные настройки, поэтому рекомендуется использовать браузеры Google Chrome, Chromium GOST, Mozilla Firefox, Яндекс.Браузер.

1. Откройте страницу расширения в интернет-магазине браузера, пройдя по ссылке https://iitrust.ru/get_iit_plugin_for_my_os

Для Яндекс.Браузера актуальную версию расширения установите из [магазина приложений Google Chrome](#).

Нажмите кнопку **Установить/Добавить**. Примеры для Google Chrome и Mozilla Firefox на рисунке 2.

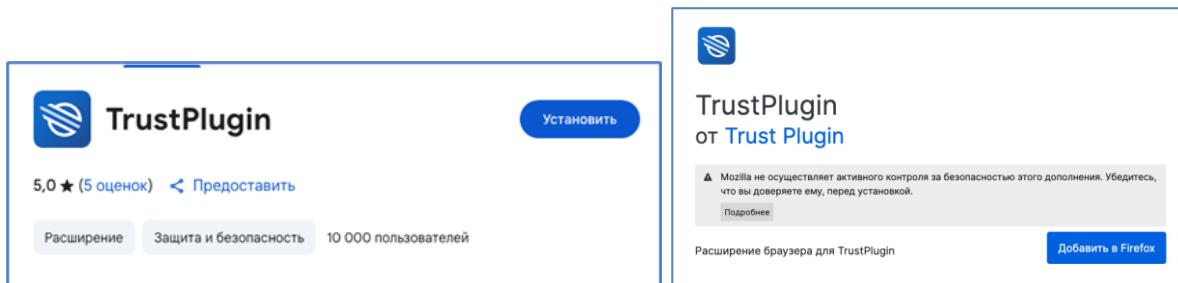


Рисунок 2

2. Подтвердите установку расширения, нажав на кнопку **Установить расширение/Добавить** во всплывающем диалоговом окне браузера (Рисунок 3).

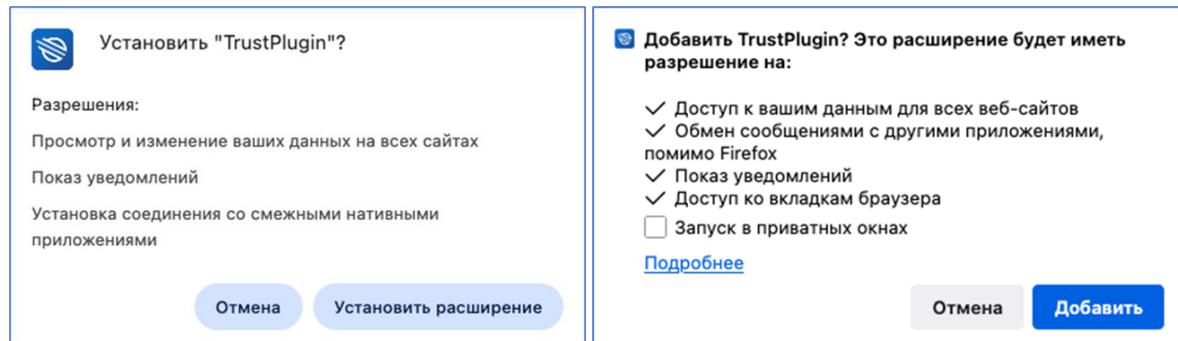


Рисунок 3

III. Установка приложения TrustPlugin на macOS

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если работаете в macOS.

- Загрузите актуальную версию TrustPlugin из личного кабинета (Рисунок 4) или по ссылке: <https://plugin.iitrust.ru/api/downloads/trustplugin-macos.pkg>

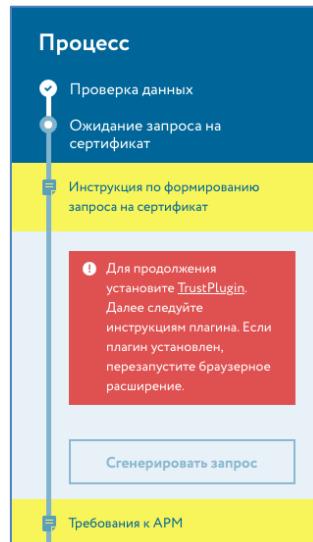


Рисунок 4

- Перейдите в директорию **Загрузки** (или в другую директорию, в которую вы сохранили дистрибутив).
- Правой кнопкой мыши нажмите на файле **trustplugin-macos.pkg** и выберите **Открыть** (Рисунок 5).

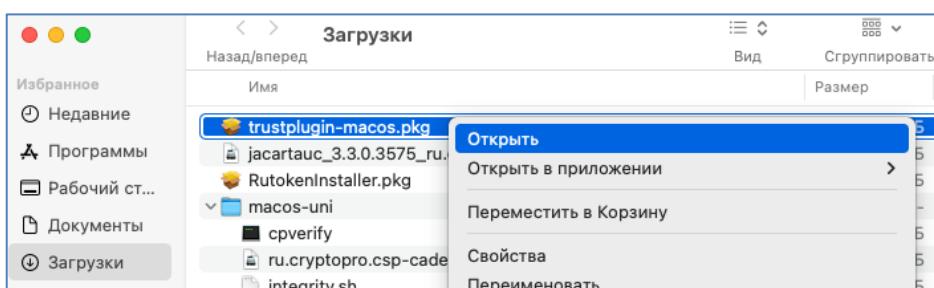


Рисунок 5

- У вас должно появиться окно с предупреждением «macOS не удается проверить разработчика «trustplugin-macos.pkg». Вы действительно хотите открыть этот файл?» (Рисунок 6). Необходимо нажать кнопку **Открыть**.

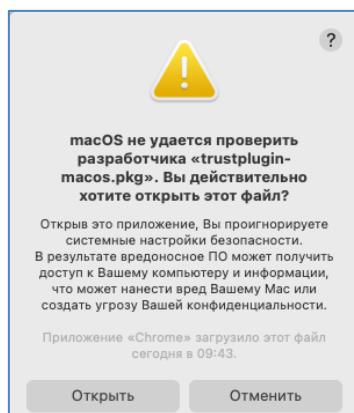


Рисунок 6

Если в текущем окне нет кнопки Открыть, то необходимо выполнить следующие действия:

- нажать на символ Apple в левом верхнем углу экрана;
- открыть Системные настройки (System Preferences);
- перейти в Конфиденциальность и безопасность (Privacy & Security);
- в правой части окна в разделе Безопасность нажмите кнопку «Все равно открыть» (Open Anyway) рядом с названием заблокированного приложения.

5. В открывшемся окне мастера установки TrustPlugin пройдите по всем этапам установки, нажимая кнопку Продолжить. В процессе установки потребуется принять лицензионное соглашение и ввести пароль администратора (Рисунок 7).

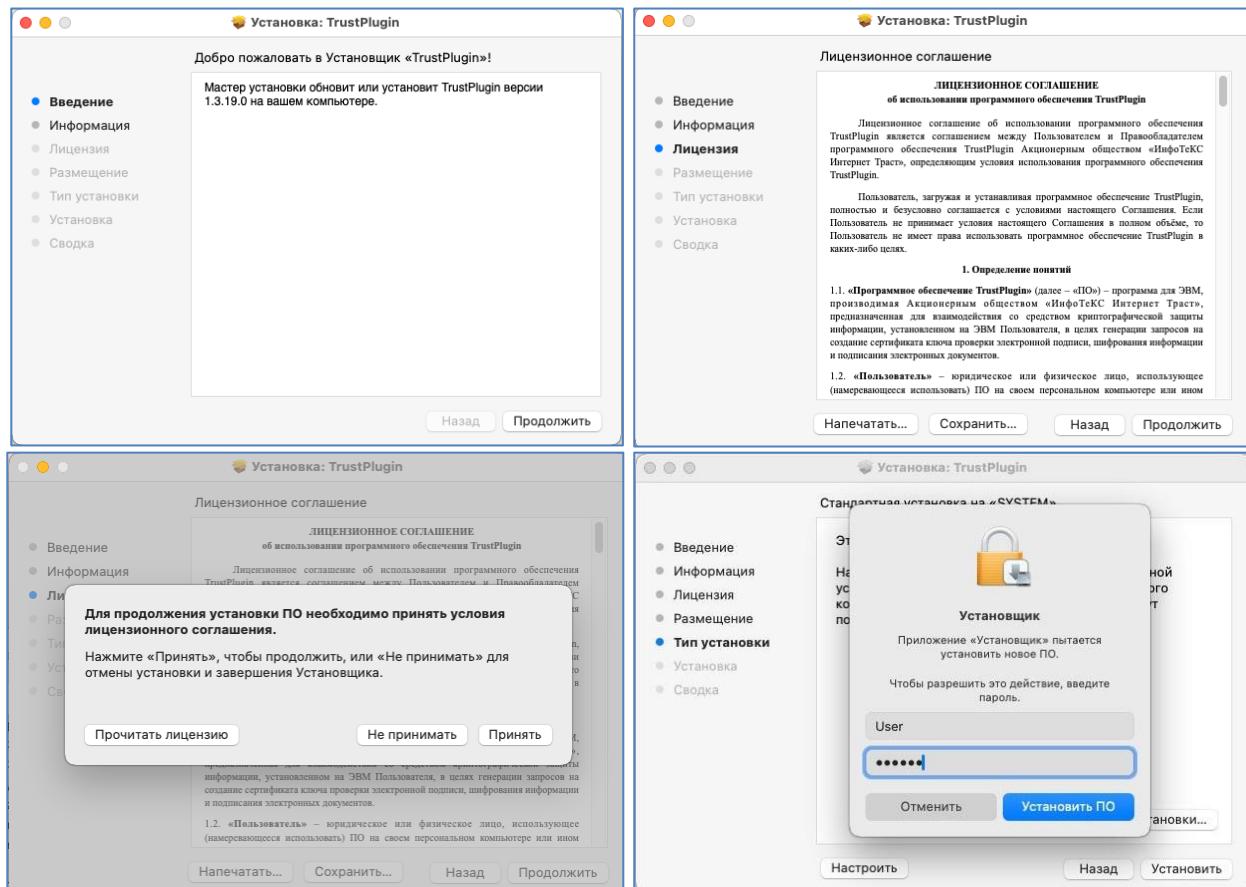


Рисунок 7

6. После завершения установки, убедитесь, что в трее (верхний-правый угол экрана) появилась иконка TrustPlugin (Рисунок 8).



Рисунок 8

Если иконки нет, запустите приложение TrustPlugin вручную через LaunchPad или из раздела Программы в Finder.

IV. Установка приложения TrustPlugin на Linux

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если работаете в Linux.

1. Загрузите подходящую версию shell-инсталлятора TrustPlugin из личного кабинета (Рисунок 9) или по ссылкам:

- Для DEB (Astra Linux, Debian): <https://plugin.iitrust.ru/api/downloads/trustplugin-linux-debian.deb.sh>
- Для RPM (Alt Linux, RedOS): <https://plugin.iitrust.ru/api/downloads/trustplugin-alt-redos.rpm.sh>

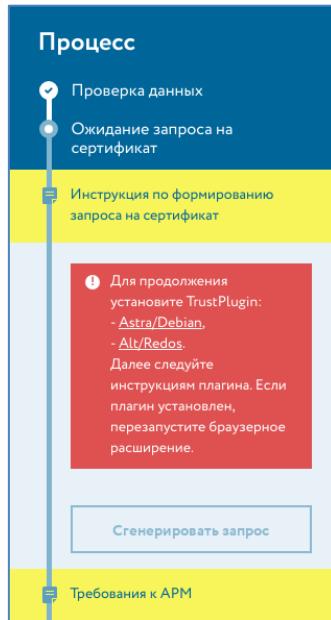


Рисунок 9

2. Откройте терминал, в терминале перейдите в каталог с загруженным Shell-инсталлятором плагина.

Пример команды:

```
cd /home/${UserName}/Загрузки
```

где \${UserName} - имя учетной записи.

3. Установите флаг исполняемости файла:

Команда для DEB:

```
chmod ugo+x ./trustplugin-linux-debian.deb.sh
```

Команда для RPM:

```
chmod ugo+x ./trustplugin-alt-redos.rpm.sh
```

4. Выполните установку плагина отправив команду **trustplugin-linux-debian.deb.sh**, либо **trustplugin-alt-redos.rpm.sh**, в зависимости от загруженного инсталлятора.

Внимание! Установку необходимо выполнять с правами суперпользователя. Для этого перед командой запуска скрипта нужно указать параметр sudo.

Команда для DEB:

```
sudo ./trustplugin-linux-debian.deb.sh --with-token-support
```

Команда для RPM:

```
sudo ./trustplugin-alt-redos.rpm.sh
```

V. Генерация запроса на сертификат с использованием СКЗИ КриптоПро CSP на macOS

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если работаете в macOS.

Внимание! Для генерации запроса на сертификат необходимо наличие установленного ГОСТ СКЗИ (криптопровайдера) КриптоПро CSP, либо токена с аппаратным ГОСТ СКЗИ (Рисунок 10).

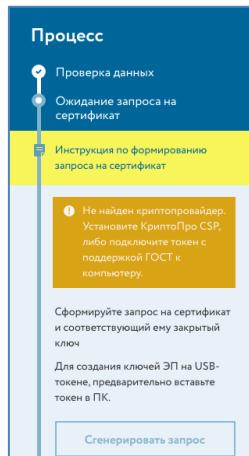


Рисунок 10

1. В личном кабинете на странице заявки нажмите кнопку **Сгенерировать запрос** (Рисунок 11).

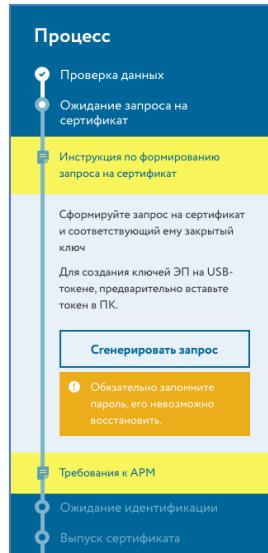


Рисунок 11

2. В окне выбора ключевого носителя **CryptoPro CSP** укажите место хранения контейнера ключей. В данном примере указан жесткий диск (Рисунок 12).

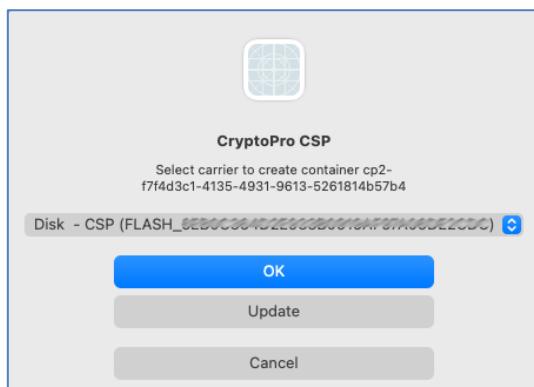


Рисунок 12

Внимание! Не удаляйте контейнер с закрытым ключом! В случае удаления, контейнер с закрытым ключом невозможно восстановить.

3. Появится окно **CryptoPro CSP random number generator**. Перемещайте указатель мыши или нажимайте различные клавиши для генерации случайной последовательности (Рисунок 13).



Рисунок 13

4. В окне **Authentication – CryptoPro CSP** введите пароль и его подтверждение (Рисунок 14).



Рисунок 14

Внимание! Обязательно запомните введённый пароль. В случае если пароль будет утерян (забыт), доступ к ключевой информации будет невозможен, что приведёт к внеплановой смене ключевого дистрибутива.

Ваша заявка получит статус «Ожидает идентификацию». Необходимо собрать комплект документов и посетить точку выдачи, дополнительная информация будет отправлена на электронную почту.

Как только заявка пройдёт идентификацию и сертификат будет издан, статус изменится на «Ожидает завершения». Агент в своем личном кабинете нажмёт кнопку **Завершить**, после чего вы сможете установить сертификат.

VI. Генерация запроса на сертификат с использованием СКЗИ КриптоПро CSP на Linux

Внимание! Данный пункт инструкции следует использовать, ТОЛЬКО если работаете в Linux.

Внимание! Для генерации запроса на сертификат необходимо наличие установленного ГОСТ СКЗИ (криптопровайдера) КриптоПро CSP, либо токена с аппаратным ГОСТ СКЗИ (Рисунок 15).

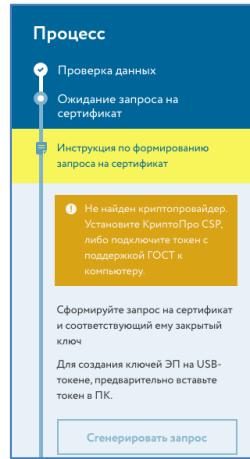


Рисунок 15

1. В личном кабинете нажмите кнопку **Сгенерировать запрос** (Рисунок 16).

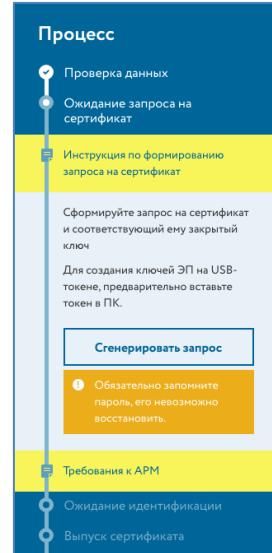


Рисунок 16

2. В окне выбора ключевого носителя КриптоПро CSP укажите место хранения контейнера ключей. В данном примере указан жесткий диск (Рисунок 17).

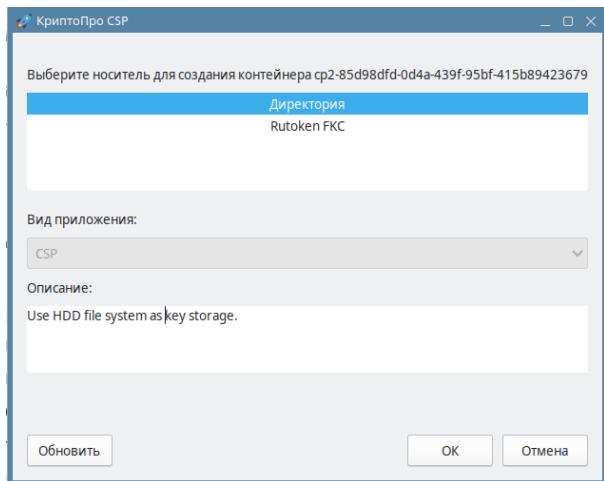


Рисунок 17

Внимание! Не удаляйте контейнер с закрытым ключом! В случае удаления, контейнер с закрытым ключом невозможно восстановить.

- Появится окно электронной рулетки. Перемещайте указатель мыши или нажимайте различные клавиши для генерации случайной последовательности (Рисунок 18).

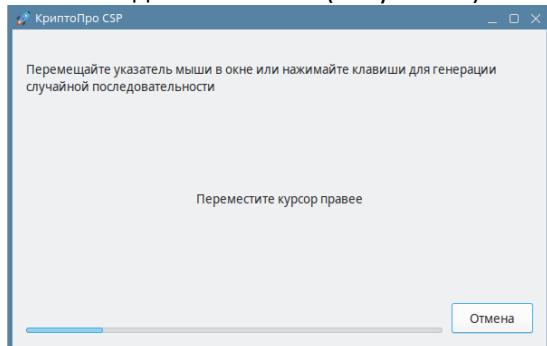


Рисунок 18

- В окне Аутентификация – КриптоПро CSP введите пароль и его подтверждение (Рисунок 19).

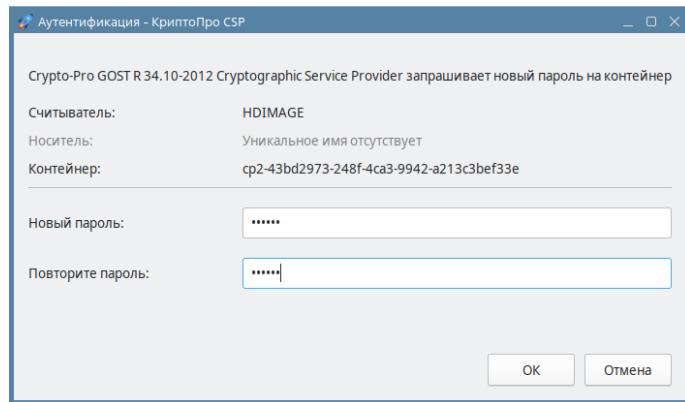


Рисунок 19

Внимание! Обязательно запомните введённый пароль. В случае если пароль будет утерян (забыт), доступ к ключевой информации будет невозможен, что приведёт к внеплановой смене ключевого дистрибутива.

Ваша заявка получит статус «Ожидает идентификацию». Необходимо собрать комплект документов и посетить точку выдачи, дополнительная информация будет отправлена на электронную почту. Как только заявка пройдёт идентификацию и сертификат будет издан, статус изменится на «Ожидает завершения». Агент в своем личном кабинете нажмёт кнопку **Завершить**, после чего вы сможете установить сертификат.

VII. Установка сертификата через личный кабинет

- Перейдите в личный кабинет по ссылке [iitrust.lk²](#) и введите логин и пароль в соответствующие поля.
- В списке заявок выберите заявку в статусе «Завершена» и нажмите на её номер/строчку. На странице заявки нажмите кнопку **Установить**. Сертификат будет успешно установлен в контейнер (Рисунок 20).

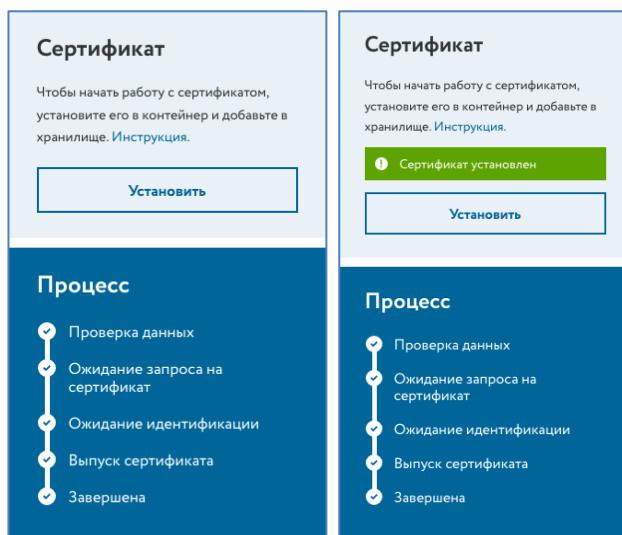


Рисунок 20

При запросе пароля введите его или пин-код от носителя, примеры окон для macOS и Linux на рисунке 21.

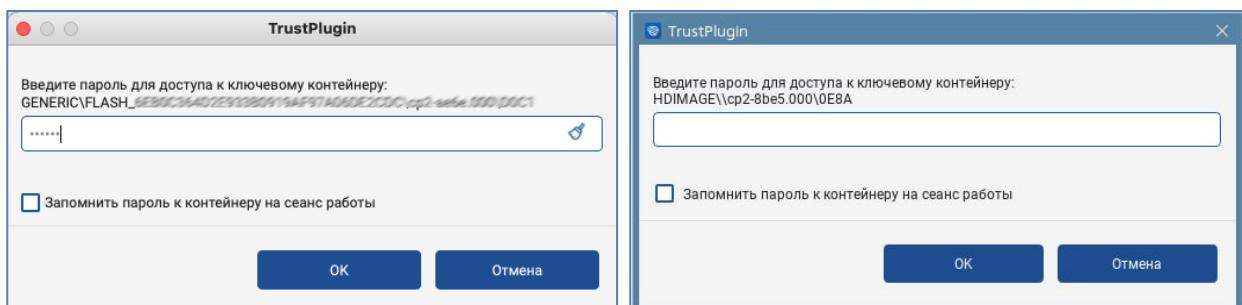


Рисунок 21

² Если вы пользуетесь корпоративным личным кабинетом, используйте соответствующую ссылку для своего домена.