



**ПРОГРАММНЫЙ КОМПЛЕКС
«СИСТЕМА КОНТРОЛЯ ДЕЙСТВИЙ ПОСТАВЩИКОВ ИТ-УСЛУГ
«НОВЫЕ ТЕХНОЛОГИИ»
Версия: 2.3.3**

**Портал доступа
Руководство пользователя**

RU.33654484.0001-04 90 02

Листов 43

СОДЕРЖАНИЕ

1 Назначение и область применения Портала доступа.....	4
2 Требования к пользователю Портала доступа.....	5
3 Начало работы.....	6
3.1 Вход.....	6
3.2 Описание интерфейса пользователя.....	7
4 Основы работы.....	8
4.1 Подсистема Персональные сейфы.....	8
5 Избранное.....	10
5.1 Добавление группы.....	11
5.2 Редактирование названия и описания группы.....	13
5.3 Удаление группы и профиля доступа.....	13
5.4 Добавление профилей доступа в Избранное	13
6 Все профили доступа.....	15
6.1 Кастомизация содержимого файлов авторизации.....	17
7 Секреты.....	18
7.1 Дерево сейфов.....	18
7.1.1 Создание нового сейфа.....	21
7.1.2 Вскрытие сейфа.....	23
7.1.3 Добавление секрета.....	23
7.1.4 Установка пломбы.....	25
7.1.5 Изменение пломбы.....	26
7.1.6 Редактирование сейфа.....	27
7.1.7 Удаление сейфа.....	27
7.2 Карточка сейфа.....	28
7.2.1 Доступ к сейфу.....	29
7.2.2 Добавление нового секрета.....	33
7.2.3 Копирование пароля из секрета.....	34
7.2.4 Копирование API-ключа из секрета.....	34
7.2.5 Копирование секрета в другой сейф.....	35
7.2.6 Удаление секрета.....	35
7.3 Карточка секрета.....	36
7.3.1 Просмотр карточки секрета.....	36
7.3.2 Редактирование секрета.....	37
8 Условные обозначения.....	39
Перечень сокращений.....	40
Перечень рисунков.....	41

Перечень таблиц.....	42
История изменений.....	43

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ ПОРТАЛА ДОСТУПА

Портал доступа – это подсистема СКДПУ НТ, предоставляющая пользователю возможность входа через единый веб-интерфейс на различные целевые системы, подключенные к различным шлюзам доступа в сети.

Также Портал доступа предоставляет функциональность, реализованную в подсистеме Персональный сейф, которая позволяет хранить аутентификационные данные пользователя, не связанные с целевыми устройствами и называемые секреты (см. [раздел 7](#)).

Портал доступа объединяет в одном списке все разрешенные в политиках доступных шлюзов доступа пользователю ресурсы.

2 ТРЕБОВАНИЯ К ПОЛЬЗОВАТЕЛЮ ПОРТАЛА ДОСТУПА

Пользователь Портала доступа должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы (веб-интерфейсами).

3 НАЧАЛО РАБОТЫ

3.1 Вход

Для получения доступа к функциональным возможностям веб-интерфейса Портала доступа необходимо:

- Шаг 1. Открыть веб-браузер и в адресной строке ввести адрес сервера Портала доступа, а также соответствующий порт через двоеточие.
- Шаг 2. В соответствующие поля следует ввести логин (1) и пароль (2). Обратите внимание, ваш пароль будет скрыт символами (•••••) для безопасности.

ВНИМАНИЕ: доступ к этой системе разрешён только авторизованным пользователям. Любая попытка получить доступ к этой системе без авторизации или остаться в системе обманным путём будет преследоваться по закону. Все авторизованные пользователи уведомлены и признают, что их действия могут записываться, сохраняться и проверяться.

ПОРТАЛ ДОСТУПА

Введите логин и пароль

Логин (1)

Пароль (2)

ВОЙТИ

© 2017–2025 ООО «АйТи БАСТИОН»

- Шаг 3. Нажать на кнопку **Войти**. Если для входа пользователя настроена двухфакторная авторизация, то будет предложено ввести второй фактор.

В случае успешной авторизации пользователь переходит в раздел веб-интерфейса Портала доступа, иначе будет выведено стандартное сообщение о невозможности авторизации.



В случае истечения лицензии отображается сообщение об истечении срока лицензии.



На Портале доступа действует контроль времени неактивности. По умолчанию период неактивности (отсутствия любых действий в интерфейсе) составляет пять минут, по истечении которых сеанс пользователя будет завершен.

3.2 Описание интерфейса пользователя

При успешной авторизации загружается основной веб-интерфейс Портала доступа. Окно веб-интерфейса содержит вкладки: **Избранное**, **Все профили доступа**, **Секреты**. По умолчанию после успешного входа происходит загрузка вкладки **Все профили доступа**.

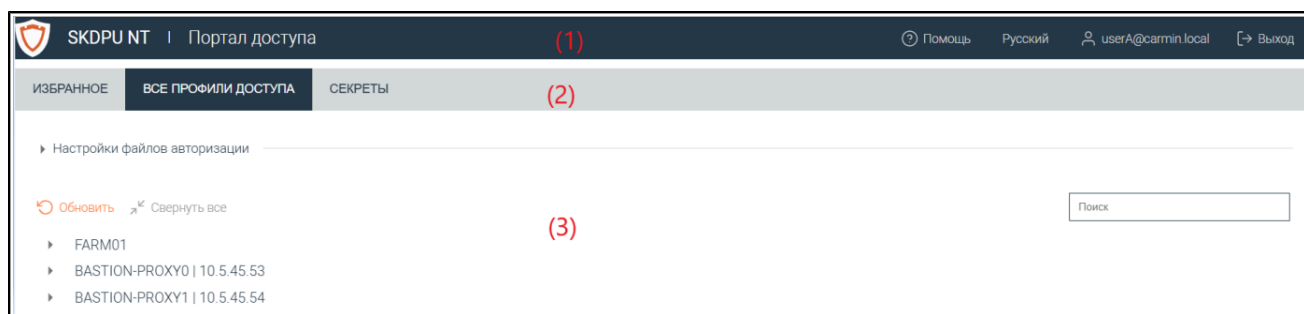


Рисунок 1 – Главная страница

Рабочая область окна содержит следующие структурные элементы:

- (1) – заголовок окна;
- (2) – область доступных вкладок;
- (3) – основная область, куда загружается содержимое активной вкладки.

В заголовке окна веб-интерфейса независимо от выбранной вкладки содержится:



- кнопка **Помощь** открывает окно **Помощь** в новой вкладке браузера;
- кнопка **Русский** меняет язык интерфейса для текущего сеанса пользователя;
- кнопка отображает аккаунт текущего пользователя;
- кнопка **Выход** закрывает текущую сессию пользователя и открывает страницу авторизации.

4 ОСНОВЫ РАБОТЫ

4.1 Подсистема Персональные сейфы

Система предоставляет возможность хранить и обмениваться различными секретами между пользователями. Данная функциональность реализована в рамках подсистемы Персональные сейфы и для пользователя доступна через интерфейс подсистемы Портал доступа.

Подсистема Персональные сейфы позволяет организовать в рамках системы одно или несколько выделенных хранилищ секретов и предоставлять к ним доступ для пользователей. Администраторы СКДПУ НТ не имеют доступа к персональным сейфам пользователей.

Система в качестве секретов может обрабатывать:

- логины и пароли;
- API-ключи (токены);
- Ключи SSH

и прикреплять файлы любых форматов ограниченного размера.

Система поддерживает для пользователя возможность организации личного хранилища секретов по следующим типам объектов:

- Личные сейфы (private) – один или несколько контейнеров с записями о секретах, которые пользователь использует только сам;
- Публичные сейфы (shared by me) – один или несколько контейнеров с записями о секретах, к которым пользователь может предоставить доступ для других пользователей системы на просмотр списка секретов, на чтение и редактирование секретов, настраиваемо;
- Доступные сейфы (shared with me) – один или несколько контейнеров с записями о секретах, к которым пользователю предоставили доступ другие пользователи.



Если пользователь работает с персональными сейфами в нескольких экземплярах Портала доступа, развернутых на разных узлах или на одном узле, то при создании сейфов в одном из экземпляров, он увидит их в остальных, только если экземпляры Порталов доступа настроены на одно и то же хранилище секретов (см. [раздел 7.2.1.1](#) и [раздел 7.2.1.2](#)).

Также при работе двух пользователей с разными экземплярами Портала доступа при расшаривании сейфов одним из пользователей второй должен иметь доступ к этому экземпляру Портала доступа, чтобы принять приглашение на доступ. В дальнейшем он может пользоваться любым доступным ему экземпляром Портала доступа, настроенным на то же самое хранилище секретов (см. [раздел 7.2.1.3](#)).

Записи в хранилищах всегда хранятся закодированными, аналогично другим секретам в рамках системы. Для большей защиты своих секретов пользователь может устанавливать для сейфа дополнительный пароль ("пломбу") и менять его при необходимости. Заданное значение пломбы

используется для кодирования сейфа на стороне клиента (браузера). Закрытие сейфа пломбой закрывает возможность доступа к секретам сейфа со стороны системы хранения. Дополнительный слой безопасности потребует дополнительных операций для доступа к секретам и может выполняться медленнее, чем для сейфов без пломбы. Рекомендуемое количество секретов в сейфе не более 200. Технически создать больше можно, но работа системы будет замедлена.

Подсистема предоставляет следующие базовые возможности:

- создавать личные сейфы и сейфы с возможностью предоставления доступа (см. [раздел 7.1.1](#));
- сохранять свои секреты в сейфы для безопасного хранения (см. [раздел 7.1.3](#));
- при добавлении записей о паролях следовать заданной в системе политике паролей;
- вести историю изменений записи и при необходимости получать доступ к предыдущим значениям в рамках настроек функционала;
- ставить на сейф дополнительную защиту-пароль, именуемую "пломбой", и менять ее при необходимости (см. [раздел 7.1.4](#));
- редактировать и удалять свои сейфы (см. [раздел 7.1.6](#) и [раздел 7.1.7](#));
- переносить свои секреты между своими сейфами (см. [раздел 7.2.5](#));
- копировать данные секретов, включая API-ключи, и скачивать SSH-ключи (см. [раздел 7.3.1](#));
- настраивать типы доступа к сейфам и давать другим пользователям доступ к своим секретам посредством формирования ссылки на доступ и отправки ее другому пользователю по защищенному каналу вне системы. При этом действуют ограничения на время действия ссылки и доступа к сейфу. отозвать доступ к сейфу у другого пользователя путем удаления этого доступа (см. [раздел 7.2.1](#));
- получать доступ к секретам других пользователей и взаимодействовать с ними в пределах типа доступа (см. [раздел 7.3](#));
- импортировать свои секреты из KeePass версии 2.x.

5 ИЗБРАННОЕ

На данной вкладке пользователь имеет возможность сформировать удобные для себя группы профилей доступа (см. [рисунок 2](#)).

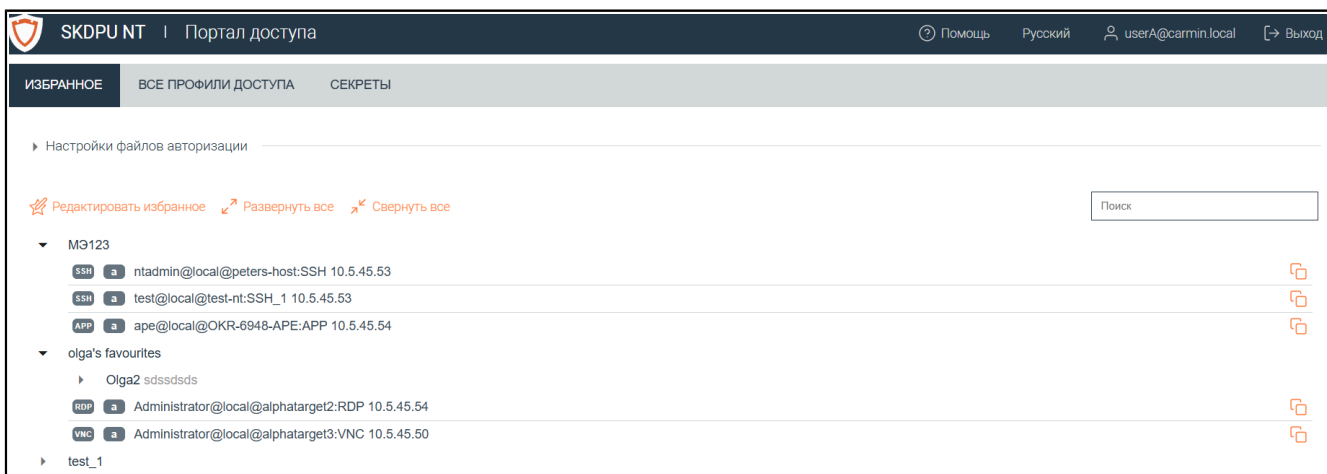


Рисунок 2 – Страница **Избранное**

Основные элементы управления:

- Кнопки **Свернуть все** и **Развернуть все**. Неактивны при отсутствии на странице хотя бы одной группы.
- Кнопка **Редактировать избранное** переводит страницу в режим изменения состава избранного, при этом маркеры типа профиля доступа и протокола профиля доступа, наименование профиля доступа отображаются в режиме редактирования неактивными, строки недоступны для нажатия и не реагируют на наведение.

Поиск при вводе каждого последующего символа отображает только строки и группы, содержащие данную подстроку (отрабатывается с задержкой в 1 сек).







На вкладке **Избранное** поиск будет только среди профилей доступа, которые входят в избранные группы.

Наведение курсора мыши на некоторые элементы вызывает всплывающие подсказки (см. [таблица 1](#)):

Таблица 1 – Соответствие подсказок элементам веб-интерфейса

Элемент	Подсказка
маркер i	Вход в интерактивном режиме
маркер am	Вход с текущей учетной записью пользователя
маркер a	Вход с указанием целевой учетной записи
кнопка	Скопировать в буфер обмена полный идентификатор профиля


Элемент	Подсказка
кнопка 	Редактировать название и описание группы
кнопка 	Удалить из Избранного группу или профиль доступа
кнопка 	Поместить выбранные профили доступа в Избранное

Нажатие на треугольный маркер  слева в каталоге групп сворачивает и разворачивает содержимое соответствующей группы.

Нажатие на строку с доступом запускает формирование и скачивание файла с параметрами доступа, указанного в строке.



Некоторые профили доступа могут отображаться неактивными, если они на момент входа у пользователя отсутствуют (к примеру, недоступны по временному ограничению деятельности пользователя или если их источник (шлюз) в текущий момент недоступен), но были ранее сохранены в **Избранном**.

Нажатие на кнопку  справа в строке с доступом помещает в буфер обмена полный (несокращенный) идентификатор доступа.

5.1 Добавление группы


Группу можно создавать как и в общем дереве, так и делать вложенной в уже существующей группе.

Для формирования новой группы необходимо выполнить следующие шаги:

Шаг 1. Нажать на кнопку **Редактировать избранное**  Редактировать избранное.

Шаг 2. Для добавления не первой (вложенной) группы необходимо выбрать группу, в которую нужно добавить создаваемую группу. Повторное нажатие на выбранную группу отменит выбор, и новая группа будет создана в корне.

Шаг 3. Нажать на кнопку **Добавить группу**  Добавить группу в левой части окна.


Шаг 4. Ввести название создаваемой группы и ее описание в модальном окне и нажать на кнопку **Принять**  Принять.



1. Для ввода в поля названия и описания группы запрещены угловые скобки $\langle \rangle$.
2. Описание группы вводится опционально.
3. Максимальная длина названия составляет 255 символов.
4. Вложенность групп не ограничена.

Шаг 5. В правой части окна выбрать желаемые доступы для их добавления в группу. Один доступ может быть добавлен в разные группы.

Шаг 6. Нажать на кнопку **Переместить**  по центру экрана.

Шаг 7. Для завершения создания группы доступов нажать на кнопку **Сохранить и выйти**  Сохранить и выйти. Подтвердить сохранение во всплывающем окне.

Для отмены создания группы следует нажать на кнопку **Отменить**. Подтвердить операцию во всплывающем окне.

Созданная группа располагается в дереве в алфавитном порядке.






На последнем уровне вложенности находятся сокращенные наименования доступов в формате [аккаунт]@[наименование целевой системы] |[имя шлюза доступа].





Если доступ был добавлен в группу ранее, но сейчас его нет в актуальном списке доступов, то он отображается неактивным, строка не реагирует на наведение и нажатие.

5.2 Редактирование названия и описания группы

Для редактирования названия или описания выбранной группы необходимо:

- Шаг 1. Нажать на кнопку **Редактировать избранное**  Редактировать избранное.
- Шаг 2. Выбрать группу, название или описание которой следует изменить, нажатием на нее. Повторное нажатие отменяет выбор группы.
- Шаг 3. Нажать на кнопку  напротив интересующей группы.
- Шаг 4. Внести необходимые изменения и сохранить их нажатием на кнопку **Принять**  Принять.
- Шаг 5. Для сохранения внесенных изменений нажать на кнопку **Сохранить и выйти** , затем в диалоговом окне на кнопку **Продолжить**  Продолжить.

5.3 Удаление группы и профиля доступа

Для удаления профиля доступа или всей группы необходимо нажать на кнопку **Редактировать избранное** , выбрать нужный профиль доступа или группу и нажать на кнопку  напротив интересующей группы или профиля доступа. Подтвердить операцию.


При удалении группы удаляется также все ее содержимое. Операция удаления является необратимой.

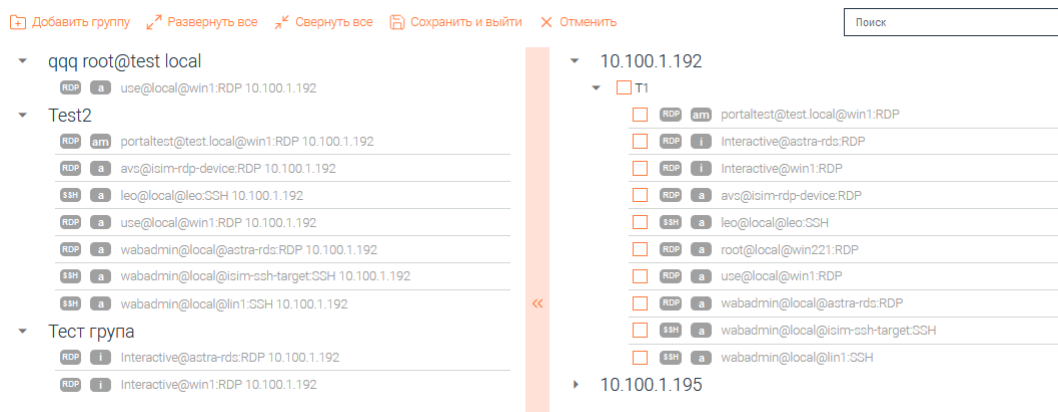


Доступы из общего списка при этом не удаляются и доступны для повторного добавления в группы.

5.4 Добавление профилей доступа в Избранное

Для добавления профиля доступа из списка доступных профилей доступа в группу необходимо:


- Шаг 1. Нажать на кнопку **Редактировать избранное**  Редактировать избранное.
- Шаг 2. Выбрать нужную группу для добавления профилей доступа, нажав на нее.
- Шаг 3. В правой части окна в списке всех шлюзов отметить флагами слева профили доступа, которые необходимо добавить.





Установка (снятие) флага в строке группы авторизации или строке имени шлюза устанавливает (снимает) все флаги внутри группы авторизаций.

Шаг 4. Нажать на кнопку .



Если для помещения выбран хотя бы один профиль доступа, но при этом ни одна группа не выбрана, то при нажатии на кнопку  вызывается мастер добавления группы. После подтверждения операции создания группы она создается на странице вкладки **Избранное**, а выбранные профили доступа помещаются в нее.

Шаг 5. Для сохранения внесенных изменений нажать на кнопку **Сохранить и выйти** , затем в диалоговом окне на кнопку **Продолжить**  **Продолжить**.



При переносе в **Избранное** профиля доступа из состава фермы система сохранит доступ как мастер-шлюз, без возможности балансировки. Использование балансировщика при работе с **Избранным** будет дополнено в следующих версиях Портала доступа. Подробнее про фермы доступа см. [раздел 6](#).

6 ВСЕ ПРОФИЛИ ДОСТУПА

На вкладке **Все профили доступа** отображается полный перечень профилей доступа к целевым системам, разрешенных для учетной записи пользователя, со шлюзов доступа, подключенных к Порталу доступа (см. [рисунок 3](#)):

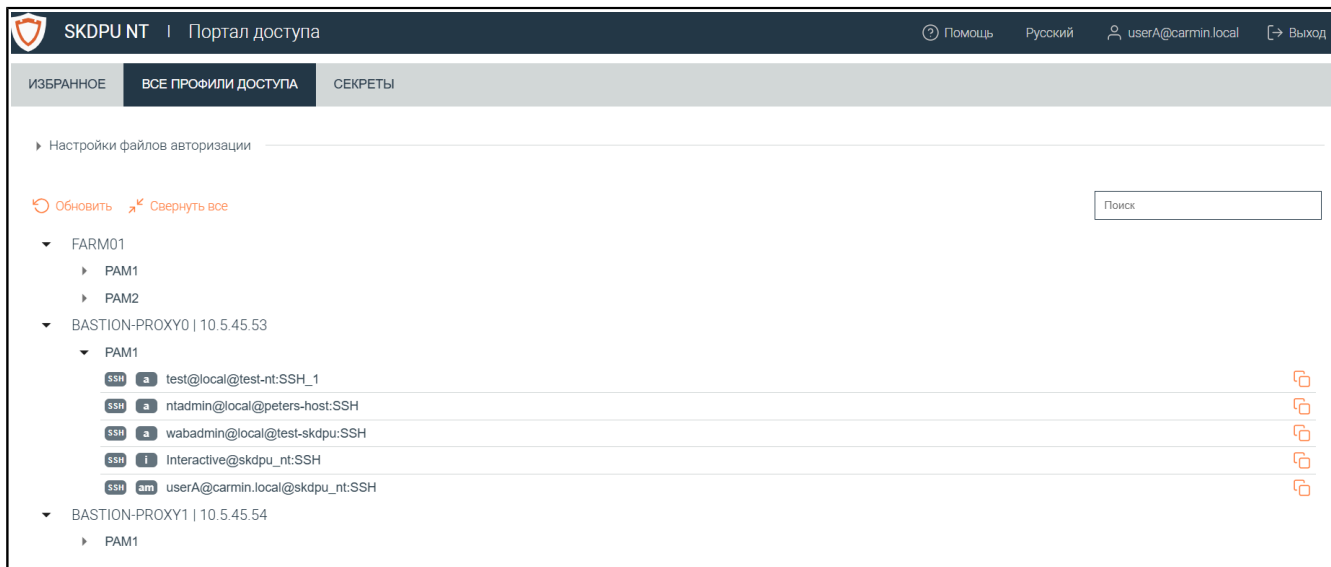


Рисунок 3 – Страница **Все профили доступа**



Наличие профиля доступа в списке не означает однозначной доступности целевого устройства в данный момент времени.

Для распределения нагрузки к Порталу доступа могут быть подключены группы шлюзов доступа с реплицированной политикой ("фермы"). Список профилей доступа со таких шлюзов доступа отображается однократно, без дублирования, а в качестве имени шлюза доступа указано наименование группы репликации.



Репликация – это полное копирование политики (описания прав доступа к целевым устройствам и пр.) с одного шлюза доступа (мастера) на другой шлюз/другие шлюзы доступа (слейв).

У пользователя в дереве доступов на Портале доступа может быть несколько групп шлюзов доступа с репликацией и одновременно автономные шлюзы доступа без репликации, отличие только в том, что у автономных шлюзов доступа указывается IP-адрес/hostname, а у группы с репликацией всегда указывается только имя.

Профили доступа различают по методу аутентификации на целевых системах:

- **a (account)** – тип доступа, при котором осуществляется соединение с подменой учетной записи: система авторизует пользователя на целевом устройстве с учетными данными, отличными от тех, с которыми был осуществлен вход на шлюз доступа;


- **am (account mapping)** – тип доступа, при котором осуществляется прямое соединение: пользователь авторизуется на целевом устройстве с теми же учетными данными (логином и паролем), с которыми он осуществил вход на шлюз доступа;
- **i (interactive login)** – тип доступа, при котором разрешено соединение с вводом учетных данных вручную: пользователь самостоятельно авторизуется на целевой системе, используя логин и пароль именно этого устройства (подразумевается, что пользователь знает эти данные).


Профили доступа различают также по протоколу подключения к целевым ресурсам: SSH, RDP, VNC, TELNET, APP.


Для осуществления подключения к требуемому целевому ресурсу необходимо выбрать из списка соответствующий профиль доступа. При нажатии будет произведено скачивание файла авторизации, содержащего параметры доступа и одноразовый пароль, по которому можно будет осуществить подключение с помощью выбранного профиля доступа .



Время актуальности файла с одноразовым паролем по умолчанию составляет 30 секунд. После истечения этого времени нельзя будет войти с помощью данного файла авторизации. В этом случае необходимо скачать файл еще раз.

Нажатие на треугольный маркер  слева в каталоге групп сворачивает и разворачивает содержимое соответствующей группы.

Нажатие на кнопку  справа в строке с профилем доступа помещает в буфер обмена полный (несокращенный) идентификатор профиля доступа.

Нажатие на кнопку **Обновить**  **Обновить** отправляет на сервер запрос на новое формирование списка профилей доступа. После отправки запроса кнопка блокируется на время, чтобы не увеличивать нагрузку на шлюз доступа.

Нажатие на кнопку **Свернуть все**  **Свернуть все** сворачивает все раскрытые группы доступов.

Поиск при вводе каждого последующего символа отображает в дереве только строки, содержащие данную подстроку, и верхнеуровневые группы, в которых содержатся найденные строки.



На вкладке **Все профили доступа** поиск будет происходить по списку всех профилей доступа.

Пользователю предоставляется возможность сгруппировать профили доступа для обеспечения удобного режима выполнения своих служебных обязанностей (см. [раздел 5](#)).

6.1 Кастомизация содержимого файлов авторизации

Для более удобного входа пользователя на удаленное устройство посредством Портала доступа реализована возможность настройки (изменения) параметров, входящих в файл авторизации: пользователь имеет возможность выбрать программу-агент для доступа, разрешение экрана, глубину цвета для работы с RDP, VNC, APP.

Ниже представлены все возможные варианты значений параметров.

Настройки файлов авторизации			
SSH-клиент:	RDP-клиент:	Разрешение экрана:	Глубина цвета:
Bastion-PuTTY (.puttywab) (по умолчанию)	rdesktop (.sh) (по умолчанию)	Полноэкранный режим (по умолчанию)	8
ssh (.cmd)	rdp (.rdp)	Поддержка мультимонитора	15
remmina (.remmina)	xfreerdp (.sh)	640x480	16
	remmina (.remmina)	800x600	24 (по умолчанию)
		1024x768	32
		1280x720	
		1280x768	
		1280x800	
		1280x1024	
		1366x768	
		1400x900	
		1400x1050	
		1680x1050	
		1920x1080	

Рисунок 4 – Настройки файлов авторизации



Содержимое меню настроек зависит от операционной системы, откуда производится вход. Выбранные значения сохраняются в кэш данного браузера для дальнейшего использования:

- Для операционной ситемы Windows можно выбрать любой из SSH-клиентов, а для RDP-клиента возможно использование только штатного клиента RDP.
- Для операционной системы Linux можно выбрать для SSH-клиента только значения ssh или remmina, а для RDP-клиента любой из четырех вариантов.

7 СЕКРЕТЫ

Закладка **Секреты** позволяет организовать хранение паролей, ключей и других видов секретов с использованием дополнительной защиты паролем, не хранящимся в системе ("пломбой").

Секрет – это контейнер, содержащий аутентификационную информацию (логины, пароли и ключи), а также дополнительные сведения для удобства пользователя при работе с ней (ссылки на ресурсы, описание, журнал изменений). Секреты лежат в отдельной ячейке, называемой сейф. У пользователя может быть несколько сейфов, в каждом из которых может быть несколько секретов (см. [рисунок 5](#)).

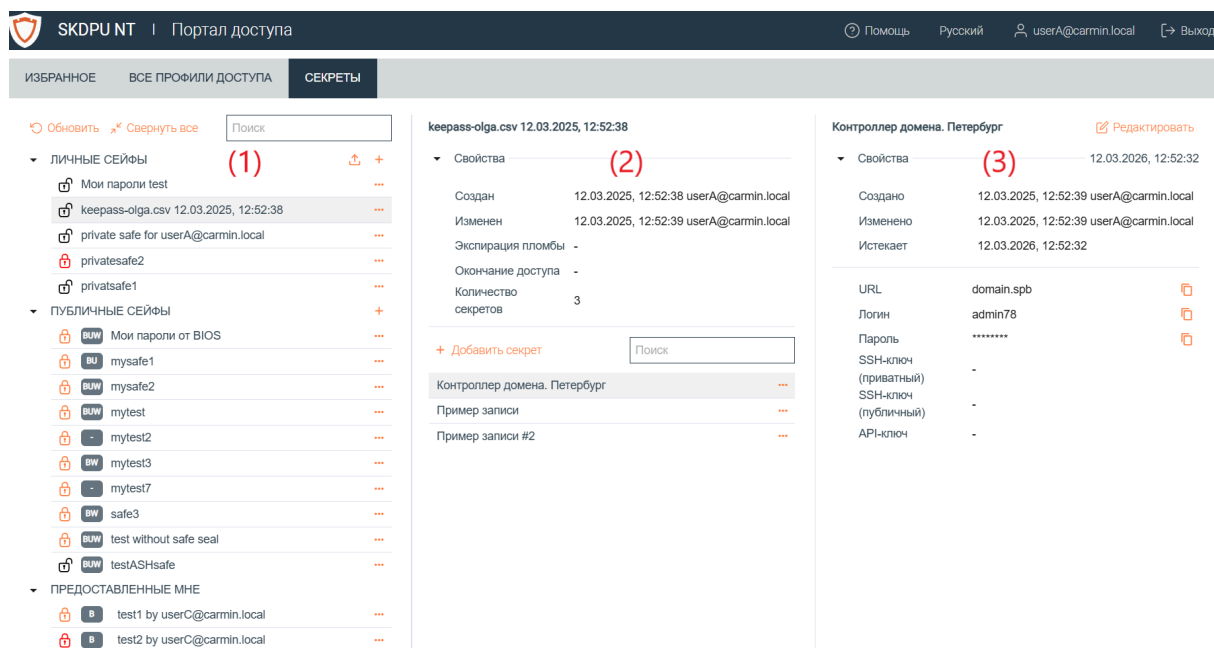


Рисунок 5 – Закладка Секреты

Окно закладки **Секреты** разделено на три вертикальные области:

- (1) – Дерево сейфов (см. [раздел 7.1](#))
- (2) – Карточка сейфа (см. [раздел 7.2](#))
- (3) – Карточка секрета (см. [раздел 7.3](#))



По умолчанию при авторизации пользователя видна только область **Дерево сейфов**. Для того чтобы увидеть карточку сейфа или карточку секрета, необходимо нажать на соответствующий сейф и секрет в нем (см. [раздел 7.2](#) и [раздел 7.3.1](#)).

7.1 Дерево сейфов


Область **Дерево сейфов** представляет собой дерево объектов, корневыми элементами которого являются категории сейфов, содержащие внутри сами сейфы.

Пользователь может видеть следующие категории сейфов:

- **Личные сейфы** – содержит сейфы с личными секретами пользователя, к которым невозможно предоставить общий доступ.
- **Публичные сейфы** – содержит сейфы с секретами пользователя, к которым возможно предоставить общий доступ.
- **Предоставленные мне** – отображает сейфы других пользователей, к которым предоставлен доступ данному пользователю (с указанием пользователя, предоставившего доступ).

Сейфы внутри категорий по умолчанию скрыты. Чтобы развернуть нужную категорию, необходимо нажать на треугольный маркер . Чтобы скрыть все категории, необходимо нажать на кнопку **Свернуть все**  **Свернуть все**.

Поле **Поиск** при вводе каждого последующего символа отображает в дереве только строки, содержащие данную подстроку, и верхнеуровневые группы, в которых содержатся найденные строки.

Нажатие на кнопку **Обновить**  **Обновить** выполняет обновление дерева сейфов через запрос на сервер и получение актуальных данных.

Данные из KeePass версии 2.x могут быть загружены в систему нажатием на кнопку .





Пользователь может дополнительно защитить свой сейф, установив на него специальный пароль – пломбу. Если пломба установлена, содержимое сейфа, кроме имени и полей раздела **Свойства** в карточке сейфа, будет недоступно пользователю до ввода пломбы (см. [раздел 7.1.2](#)).




Закрытие сейфа пломбой закрывает возможность доступа к секретам сейфа со стороны системы хранения. Дополнительный слой безопасности потребует дополнительных операций для доступа к секретам и может выполняться медленнее, чем для сейфов без пломбы.

Каждая строка сейфа имеет отметку о состоянии пломбы (см. [таблица 2](#)):

Таблица 2 – Соответствие иконки пломбы состоянию сейфа


Иконка	Состояние сейфа	Всплывающее сообщение
	сейф не закрыт пломбой	"Пломба отсутствует"
	сейф закрыт пломбой, не вскрыт	"Установлена пломба. Сейф закрыт"
	сейф закрыт пломбой, не вскрыт, срок пломбы истекает	"Срок действия пломбы истекает"
	сейф закрыт пломбой, вскрыт	"Установлена пломба. Сейф вскрыт"

Иконка	Состояние сейфа	Всплывающее сообщение
	сейф закрыт пломбой, вскрыт, срок пломбы истекает	"Срок действия пломбы истекает"

Пользователь также может увидеть отметку о типе доступа, который он предоставил другим пользователям к данному сейфу, на сейфах категории **Публичные сейфы** и посмотреть доступ, который предоставили ему, в категории **Предоставленные мне сейфы**. Наведение курсора мыши на сейф вызывает всплывающие сообщения о типе доступа (см. [таблица 3](#)):

Таблица 3 – Соответствие подсказок элементам сервиса

Иконка	Тип доступа	Всплывающее сообщение
	Доступ к сейфу не открыт ни одному пользователю	-
	Сейф открыт на просмотр списка секретов и информации о секрете (browse)	"просмотр"
	Сейф открыт на просмотр списка секретов с возможностью вскрыть и использовать секрет (browse, usage)	"просмотр, чтение"
	Сейф открыт на просмотр списка секретов с возможностью вскрыть и редактировать секрет (browse, write)	"просмотр, запись"
	Сейф открыт на просмотр, использование или редактирование секрета хотя бы одному пользователю (browse, usage, write)	"просмотр, чтение, запись"

Каждая строка сейфа содержит кнопку , которая вызывает функциональное меню, позволяющее управлять сейфом (см. [рисунок 6](#)):

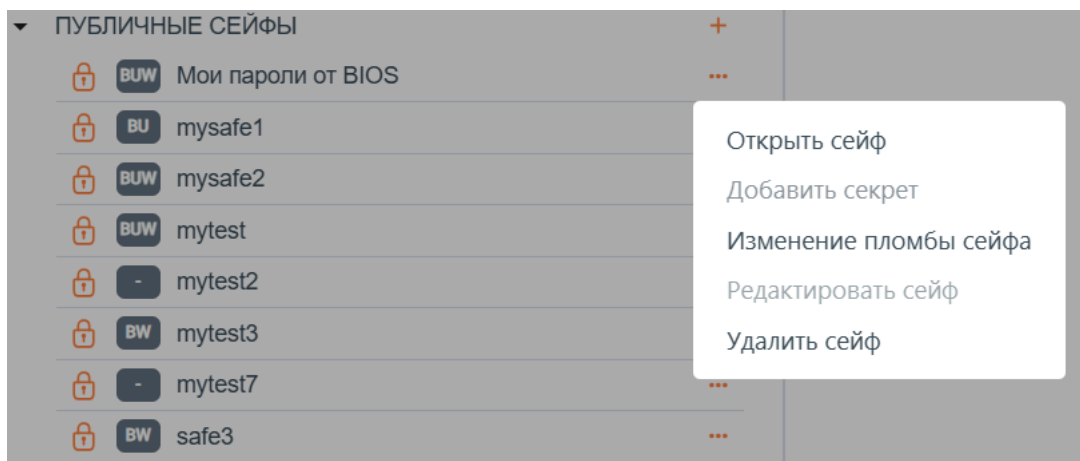


Рисунок 6 – Функциональное меню сейфа

- **Открыть сейф** – вызывает диалоговое окно введения пломбы.
- **Добавить секрет** – вызывает процедуру добавления секрета.
- **Изменение пломбы сейфа/Установить пломбу на сейф** – вызывает окно для изменения или установки пломбы.
- **Редактировать сейф** – открывает карточку сейфа на редактирование.
- **Удалить сейф** – запускает процедуру удаления сейфа.



Если операция недоступна, это означает, что сейф закрыт на пломбу и нужно вначале его вскрыть. Для **Предоставленных мне** сейфов доступна только операция вскрытия сейфа.

7.1.1 Создание нового сейфа

Добавление нового сейфа доступно только для категорий **Личные сейфы** и **Публичные сейфы**.

Для создания нового сейфа необходимо:

Шаг 1. В области **Дерево сейфов** у нужной категории сейфов нажать на кнопку **+**

ДОБАВИТЬ СЕЙФ

Название сейфа

Описание сейфа

Пломба сейфа

Подтверждение пломбы сейфа

Экспирация пломбы

✕ Отменить ✓ Принять

Шаг 2. В появившейся форме заполнить необходимые поля и установить пломбу, если необходимо. При заполнении полей проверяются следующие условия:

- Имя сейфа должно быть заполнено и уникально для данного пользователя в пределах категории сейфов.
- Максимальное количество символов в имени сейфа и описании (если заполнено) равно 256.



В поле имени не должно быть следующих символов: = / \ ; " ~ * { } < > пробел и все специальные символы. Поле описания может содержать любые символы, кроме: { } < >

- Пломба и дата экспирации пломбы должны соответствовать парольной политике. Введенную пломбу можно посмотреть нажатием на иконку
- Поля **Пломба сейфа** и **Подтверждение пломбы сейфа**, если заполнены, должны быть идентичны. Поля для подтверждения пломбы и даты экспирации пломбы становятся доступны только после ввода пломбы в основное поле.





При несоответствии значения поля правилам валидации выдается соответствующее сообщение ниже вводимого поля.

Шаг 3. Сохранить сейф нажатием на кнопку **Принять** ✓ Принять. После сохранения новый сейф отображается в секции дерева по алфавиту.

7.1.2 Вскрытие сейфа

Для вскрытия сейфа, на который была установлена пломба, необходимо:

Шаг 1. В списке сейфов найти нужный закрытый сейф и нажать на него, если обращение к сейфу происходит первый раз в течение данной авторизационной сессии. В противном случае, нажать на кнопку  с правой стороны нужного сейфа и выбрать **Открыть сейф**.

Шаг 2. В открывшемся модальном окне ввести пароль-пломбу. Введенную пломбу можно посмотреть нажатием на кнопку .

Шаг 3. Вскрыть сейф нажатием на кнопку **Принять**  **Принять**.


Если пароль введен неправильно, будет показано соответствующее сообщение под полем с паролем. Если пароль верен, откроется карточка сейфа (см. [раздел 7.2](#)).



Если пользователь вскрыл сейф, но какое-то время (установленный таймаут) не производит с сейфом никаких действий, то доступ к сейфу автоматически закрывается. Чтобы его открыть, нужно будет снова ввести пломбу. Доступ к сейфу также закрывается при прерывании сессии, и в рамках новой сессии пломба вводится заново.

7.1.3 Добавление секрета

Для добавления нового секрета необходимо:

Шаг 1. В списке сейфов найти нужный сейф и нажать на кнопку . Сейф может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Добавить секрет**.

Новый секрет

Название	<input type="text" value="secret"/>
Описание	<input type="text"/>
Истекает	<input type="text" value="18.03.2026"/>
URL	<input type="text"/>
Логин	<input type="text"/>
Пароль	<input type="password"/>
SSH-ключ (приватный)	<input type="text"/>
SSH-ключ (публичный)	<input type="text"/>
API-ключ	<input type="text"/>

[✕ Отменить](#) [✓ Принять](#)

Шаг 3. Ввести необходимые данные в **Карточке секрета** справа. При заполнении полей проверяются следующие условия:

- Имя секрета должно быть заполнено и уникально в пределах сейфа.
- Максимальное количество символов в имени секрета и описании (если заполнено) равно 256.



В поле имени не должно быть следующих символов: = / \ ; " ~ * { } < > пробел и все специальные символы. Поле описания может содержать любые символы, кроме: { } < >

- Пароль должен соответствовать парольной политике. Введенный пароль можно посмотреть нажатием на кнопку .

Кнопка около поля **Пароль** вызывает окно с минимальными требованиями по заполнению пароля и возможностью сгенерировать пароль нажатием на кнопку **Сгенерировать** [✓ Сгенерировать](#). Сгенерированные пароли будут видны в разделе **Результат**.

Внизу поля **Пароль** будет показано качество пароля, например, **quality: 3**. Качество пароля определяется его длиной и сложностью и может быть от 1 до 4.

ГЕНЕРАЦИЯ ПАРОЛЯ


Минимальная длина пароля	8
Минимальное количество строчных символов	1
Минимальное количество заглавных символов	1
Минимальное количество цифровых символов	1
Минимальное количество специальных символов	1
Сгенерировать пароль длиной	<input type="text" value="8"/>

[✓ Сгенерировать](#)

Результат _____

[✕ Закрыть](#)

- Файлы для SSH-ключей должны быть не более 40 KB.

Шаг 4. Для загрузки SSH-ключей в виде файла необходимо нажать на кнопку **Загрузить**  и выбрать необходимый файл. После загрузки поле с ключом становится неактивно. Чтобы изменить содержимое ключа, сначала нужно очистить поле, нажав на соответствующую кнопку **✕**.

Шаг 5. Сохранить секрет нажатием на кнопку **Принять** [✓ Принять](#).

Новый секрет также может быть добавлен из области **Карточка сейфа** (см. [раздел 7.2.2](#))



В связи с нагрузкой системы, особенно для сейфов, закрытых пломбой, рекомендуемое количество секретов в сейфе не более 200. Технически создать больше можно, но это замедлит работу.

7.1.4 Установка пломбы

На сейф, при создании которого пломба не была установлена, можно установить пломбу после его создания отдельным действием.

Для установки на сейф пломбы необходимо:

Шаг 1. В списке сейфов найти нужный сейф без установленной пломбы и нажать на кнопку **...**. Сейф может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Установить пломбу на сейф**.


УСТАНОВИТЬ ПЛОМБУ НА СЕЙФ


Новая пломба

Подтверждение новой пломбы

Экспирация пломбы

✕ Отменить ✓ Принять


Шаг 3. В открывшемся модальном окне ввести пломбу и дату валидности сейфа. Введенную пломбу можно посмотреть нажатием на кнопку .

 Поля должны соответствовать описанному ранее формату (см. [раздел 7.1.1](#)). Поля для подтверждения пломбы и даты экспирации пломбы становятся доступны только после ввода пломбы в основное поле.

Шаг 4. Сохранить пломбу нажатием на кнопку **Принять**  Принять.

7.1.5 Изменение пломбы

Для изменения установленной ранее пломбы необходимо:

Шаг 1. В списке сейфов найти нужный сейф с установленной ранее пломбой и нажать на кнопку . Сейф может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Изменение пломбы сейфа**.

ИЗМЕНЕНИЕ ПЛОМБЫ СЕЙФА


Текущая пломба

Новая пломба

Подтверждение новой пломбы

Экспирация пломбы

✕ Отменить ✓ Принять

Шаг 3. В открывшемся модальном окне ввести текущую и новую пломбы и изменить дату валидности сейфа, если необходимо. Введенную пломбу можно посмотреть нажатием на кнопку .



Поля должны соответствовать описанному ранее формату (см. [раздел 7.1.1](#)). Поля для подтверждения пломбы и даты экспирации пломбы становятся доступны только после ввода пломбы в основное поле.

Шаг 4. Сохранить изменения нажатием на кнопку **Принять** ✓ [Принять](#).

7.1.6 Редактирование сейфа

Для изменения параметров сейфа необходимо:

Шаг 1. В списке сейфов найти нужный сейф и нажать на кнопку **...**. Сейф может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Редактировать сейф**.

РЕДАКТИРОВАТЬ СЕЙФ

Название сейфа

Описание сейфа

[x Отменить](#) [✓ Принять](#)

Шаг 3. Изменить имя сейфа или его описание в открывшемся модальном окне. Поля должны соответствовать описанному ранее формату (см. [раздел 7.1.1](#)).

Шаг 4. Сохранить сейф нажатием на кнопку **Принять** ✓ [Принять](#).



Если название было изменено, сейф перемещается в дереве сейфов согласно алфавиту.

Пользователь также может редактировать доступ к сейфу (см. [раздел 7.2.1](#))

7.1.7 Удаление сейфа

Для удаления сейфа необходимо:

Шаг 1. В списке сейфов найти нужный сейф и нажать на кнопку **...**. Сейф может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Удалить сейф**.

Шаг 3. Подтвердить удаление в диалоге подтверждения операции нажатием на кнопку **Принять** ✓ [Принять](#).



Сейф, закрытый пломбой, можно удалить, не вскрывая его. При этом все хранящиеся в нем секреты будут утеряны. Операция удаления является безотзывной.

7.2 Карточка сейфа

Область **Карточка сейфа** позволяет просмотреть информацию о сейфе, а также создать новые секреты, управлять ими и настраивать доступ к сейфу для других пользователей.

Данная область содержит следующие разделы (см. [рисунок 7](#)):

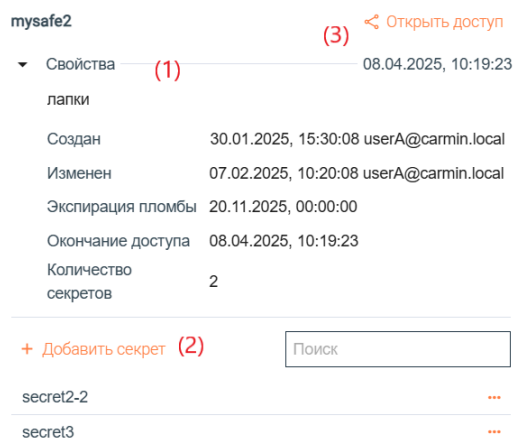


Рисунок 7 – Карточка сейфа

Для просмотра карточки сейфа необходимо в области **Дерево сейфов** найти нужный сейф и нажать на него. Если сейф закрыт пломбой, необходимо вскрыть его, введя соответствующий пароль в модальном окне (см. [раздел 7.1.2](#)). При отмене операции ввода пломбы пользователю будет доступен только раздел **Свойства**. Если сейф не закрыт пломбой или вскрыт, пользователю будет доступен также раздел с секретами, содержащимися в сейфе.

Поле **Поиск** позволяет отфильтровать секреты, содержащиеся в данном сейфе, по названию. При введении символов отображаются только строки, содержащие данную подстроку.



Регулировать доступ к сейфу возможно только для не закрытых пломбой или вскрытых сейфов категорий **Публичные сейфы**. Для **Предоставленных мне** сейфов, к которым пользователю предоставлен доступ другим пользователем, изменить список секретов нельзя.

Каждая строка секрета содержит кнопку **...**, которая вызывает функциональное меню, позволяющее управлять секретом (см. [рисунок 8](#)):

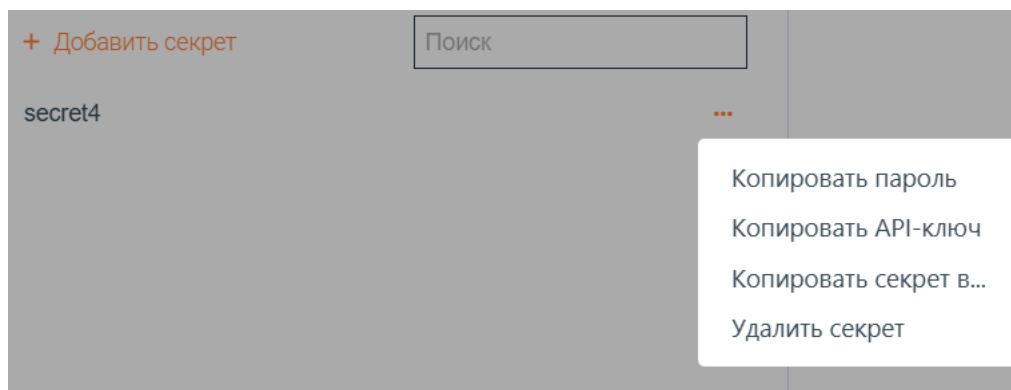


Рисунок 8 – Функциональное меню секрета


- **Копировать пароль** – копирует пароль из карточки секрета в буфер обмена. Виден, если пароль установлен.
- **Копировать API-ключ** – копирует API-ключ из карточки секрета в буфер обмена. Виден, если API-ключ установлен.
- **Копировать секрет в** – запускает процедуру копирования секрета в другой сейф.
- **Удалить секрет** – запускает процедуру удаления секрета.



Операции для **Предоставленных мне** сейфов открыты только с правами доступа на чтение и на чтение и редактирование (см. [раздел 7.1](#)). Для доступа в режиме просмотра функциональное меню отсутствует. Опция удаления секрета недоступна при любых правах доступа.

7.2.1 Доступ к сейфу

Для настройки доступа к публичным сейфам для других пользователей необходимо:

Шаг 1. В карточке нужного сейфа нажать на кнопку **Открыть доступ**  [Открыть доступ](#). Для сейфов, закрытых пломбой, кнопка доступна только после вскрытия сейфа.

ОТКРЫТЬ ДОСТУП

Открыть доступ на просмотр

Открыть доступ на чтение секрета

Открыть доступ на запись секрета

Доступ предоставляется до

+ Создать ссылку

▼ Действующие ссылки (2)

9e7e6a95-a7c9-47...	просмотр	до: 18.03.2025, 16:50:30	<input type="button" value="🗑"/>	<input type="button" value="🗑"/>
abc59fdb-c8c1-4c8...	просмотр, чтение	до: 18.03.2025, 16:50:34	<input type="button" value="🗑"/>	<input type="button" value="🗑"/>

Ссылка действует 60 minutes

▼ Доступ к сейфу (2)

admin	просмотр	до: 11.05.2025, 16:06:08	<input type="button" value="🗑"/>
userC@carmin.local	просмотр, чтение, запись	до: 12.05.2025, 13:33:06	<input type="button" value="🗑"/>

X Закрыть

Шаг 2. В окне управления доступом выбрать вариант доступа к сейфу – только просмотр, просмотр и использование секрета (чтение), просмотр и редактирование секрета (запись). По умолчанию выбран только просмотр. Доступ на просмотр дает возможность только просматривать список секретов, но не дает возможности редактировать секрет или использовать значения, сохраненные в нем.

Шаг 3. Установить дату окончания доступа вручную или с помощью **Календаря**. Дата окончания доступа должна соответствовать парольной политике. По умолчанию устанавливается максимальное значение.



Если дата не соответствует парольной политике, выдается соответствующее сообщение ниже вводимого поля.

Шаг 4. Добавить ссылку нажатием на кнопку **Создать ссылку** + Создать ссылку .

Если сейф ранее уже был открыт на доступ другим пользователям, в блоке **Действующие ссылки** будут видны соответствующие валидные (активные) ссылки со временем окончания действия ссылки. Ссылку можно удалить до истечения срока ее валидности, нажав на кнопку **Удалить** в соответствующей строке. Чтобы удалить все активные ссылки, необходимо нажать на кнопку **Удалить** около поля **Действующие ссылки**.




Если действующая ссылка удаляется, возможность получения по ней доступа к сейфу будет отключена.

Шаг 5. Скопировать ссылку для отправки необходимому пользователю, нажав на кнопку . Время действия ссылки видно ниже поля **Действующие ссылки** и обычно

составляет 60 минут. Это время может быть изменено в соответствующих настройках администратором.



По истечении времени, указанного в поле **Доступ предоставляется до**, доступ к сейфу для стороннего пользователя закрывается.

Шаг 6. После всех внесенных изменений закрыть окно управления доступом к сейфу, нажав на кнопку **Заккрыть**  **Заккрыть**.

Блок **Доступ к сейфу** содержит пользователей, которым был ранее предоставлен доступ к сейфу и которые приняли этот доступ, с указанием соответствующих прав и времени валидности доступа. Если пользователю отправляется вторая ссылка с измененным типом доступа, то, при подтверждении пользователем ссылки (см. [раздел 7.2.1.3](#)), у него остаются оба права доступа до истечения времени действия одного из них. Доступ для пользователя можно удалить принудительно (до истечения срока действия), нажав на кнопку **Удалить** в соответствующей строке. Чтобы удалить все активные доступы, необходимо нажать на кнопку **Удалить** около поля **Доступ к сейфу**.



Если доступ к сейфу удален, то у пользователя, который работает с этим сейфом, возможность работы с ним будет отключена на сервере, изменения не будут сохранены, а при обновлении окна он перестанет видеть этот сейф в списке доступных ему сейфов.

7.2.1.1 Предоставление доступа к сейфу на разных узлах Портала доступа

Пользователи в распределенном контуре могут работать с разными экземплярами Портала доступа, развернутыми на разных узлах контура. Если Пользователь1 работает на узле1 Портала доступа и предоставляет доступ к своему сейфу Пользователю2, работающему на узле2, то у Пользователя2 должен быть доступ к узлу1 Портала доступа. В таком случае при получении ссылки на сейф и пломбы (если установлена), Пользователь2 сможет посмотреть содержимое сейфа и взаимодействовать с ним в рамках предоставляемых ему прав доступа (см. [раздел 7.2.1.3](#)).



Предоставление доступа возможно, если для обоих экземпляров Портала доступа в настройках указано одно и то же хранилище секретов.

Если Пользователь1 меняет содержимое своего сейфа или поля уже созданного секрета, то при обновлении страницы через время, установленное для обновления контура, Пользователь2 увидит эти изменения в поле **Изменено** секрета со временем изменения и логином Пользователя1 (см. [раздел 7.3.1](#)). Верно и обратное: при изменении сейфа Пользователем2 (если предоставлены соответствующие права) Пользователь1 увидит эти изменения в своем сейфе при обновлении страницы.



Содержимое, открытое с доступов на запись, в распределенной системе подвержено задержкам сетевого взаимодействия и прочим неизбежным в сети случайностям.

Если пользователи вносят изменения в сейф одновременно, то актуальной будет та карточка секрета, которую сохранили последней. До обновления страницы пользователи видят в секрете установленное ими значение, а после обновления - новое значение, даже если оно было изменено не им.



Для избегания конфликтов рекомендуется использовать разрешение на запись для корреспондентов только для карточек, предполагающих хранение секрета только в одном поле.

7.2.1.2 Предоставление доступа к сейфу на разных экземплярах Портала доступа на одном узле

Пользователи в распределенном контуре могут работать с разными экземплярами Портала доступа, настроенными на одном узле. Если Пользователь1 работает в экземпляре1 Портала доступа и предоставляет доступ к своему сейфу Пользователю2, работающему в экземпляре2, то у Пользователя2 должен быть доступ к экземпляру1 Портала доступа. В таком случае при получении ссылки на сейф и пломбы (если установлена), Пользователь2 сможет посмотреть содержимое сейфа и взаимодействовать с ним в рамках предоставляемых ему прав доступа (см. [раздел 7.2.1.3](#)).



Предоставление доступа возможно, если для обоих экземпляров Портала доступа в настройках указано одно и то же хранилище секретов.

Если Пользователь1 меняет содержимое своего сейфа или поля уже созданного секрета, то при обновлении страницы через время, установленное для обновления контура, Пользователь2 увидит эти изменения в поле **Изменено** секрета со временем изменения и логином Пользователя1 (см. [раздел 7.3.1](#)). Верно и обратное: при изменении сейфа Пользователем2 (если предоставлены соответствующие права) Пользователь1 увидит эти изменения в своем сейфе при обновлении страницы.



Содержимое, открытое с доступов на запись, в распределенной системе подвержено задержкам сетевого взаимодействия и прочим неизбежным в сети случайностям.

Если пользователи вносят изменения в сейф одновременно, то актуальной будет та карточка секрета, которую сохранили последней. До обновления страницы пользователи видят в секрете установленное ими значение, а после обновления - новое значение, даже если оно было изменено не им.



Для избегания конфликтов рекомендуется использовать разрешение на запись для корреспондентов только для карточек, предполагающих хранение секрета только в одном поле.

7.2.1.3 Получение доступа к чужому сейфу

Пользователь может получить доступ к чужому сейфу и взаимодействовать с ним в рамках выданных ему прав доступа (см. [раздел 7.2.1](#)).

Для взаимодействия с сейфом необходимо:

Шаг 1. Получить ссылку на чужой сейф вне системы по защищенному каналу связи и пломбу к этому сейфу, если она установлена.

Шаг 2. Нажать на ссылку.

Шаг 3. Авторизоваться на портале доступа. Вкладка **Секреты** откроется автоматически.

Шаг 4. Выбрать в поле **Дерево сейфов** нужный сейф в категории **Предоставленные мне** и нажать на него. Если сейф закрыт пломбой, вскрыть его вводом пломбы в модальном окне (см. [раздел 7.1.2](#)).

Шаг 5. Просмотреть содержимое сейфа. Если предоставлены права на чтение или редактирование, возможно взаимодействие с секретами сейфа (см. [раздел 7.2](#)).

Пользователь может отказаться от предоставляемого доступа нажатием на кнопку **Отказаться от доступа** и подтверждением операции в модальном окне. В этом случае доступ на сейф закрывается, сейф удаляется из категории **Предоставленные мне сейфы**.



Если в распределенном контуре развернуто несколько экземпляров Портала доступа на одном или разных узлах, то пользователь для получения доступа к сейфу изначально должен иметь доступ и авторизоваться на том Портале доступа, ссылку на который ему прислали. В дальнейшем он может пользоваться любым доступным ему экземпляром Портала доступа, настроенным на то же самое хранилище секретов.

7.2.2 Добавление нового секрета

Для добавления нового секрета из карточки сейфа необходимо:

Шаг 1. В области **Карточка сейфа** нажать на кнопку **Добавить секрет** + **Добавить секрет** .

Новый секрет

Название	<input type="text" value="secret"/>
Описание	<input type="text"/>
Истекает	<input type="text" value="18.03.2026"/>
URL	<input type="text"/>
Логин	<input type="text"/>
Пароль	<input type="password"/>
SSH-ключ (приватный)	<input type="text"/>
SSH-ключ (публичный)	<input type="text"/>
API-ключ	<input type="text"/>

[✕ Отменить](#) [✓ Принять](#)

Шаг 2. Ввести необходимые данные в **Карточке секрета** справа. Поля должны соответствовать описанному ранее формату (см. [раздел 7.1.3](#)).

Шаг 3. Сохранить новый секрет нажатием на кнопку **Принять** [Принять](#).

Секрет также может быть добавлен через область **Дерево сейфов** (см. [раздел 7.1.3](#)).

7.2.3 Копирование пароля из секрета

Для копирования пароля из секрета, если таковой был установлен, необходимо:

Шаг 1. В области **Карточка сейфа** найти нужный секрет и нажать на кнопку . Секрет может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Копировать пароль**.

Пароль будет скопирован в буфер обмена. Пароль также можно скопировать в **Карточке секрета** (см. [раздел 7.3.1](#)).

7.2.4 Копирование API-ключа из секрета

Для копирования API-ключа из секрета, если таковой был установлен, необходимо:

Шаг 1. В области **Карточка сейфа** найти нужный секрет и нажать на кнопку . Секрет может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Копировать API-ключ**.

API-ключ будет скопирован в буфер обмена. API-ключ также можно скопировать в **Карточке секрета** (см. [раздел 7.3.1](#)).

7.2.5 Копирование секрета в другой сейф

Для копирования секрета в другой сейф необходимо:

Шаг 1. В области **Карточка сейфа** найти нужный секрет и нажать на кнопку **...**. Секрет может быть найден через строку поиска.

Шаг 2. В функциональном меню выбрать **Копировать секрет в**.

КОПИРОВАТЬ СЕКРЕТ В...

Выберите сейф

- ▼ Личные сейфы
 - privatsafe1
 - private safe for userA@carmin.local
 - Мои пароли test
 - keepass-olga.csv 12.03.2025, 12:52:38
- ▼ Публичные сейфы
 - testASHsafe
- ▼ Предоставленные мне

✕ Отменить ✓ Принять

Шаг 3. Выбрать сейф для копирования в модальном окне. Сейф может быть найден через строку **Поиска**.



В списке мест назначения для копирования отображаются только не закрытые пломбой сейфы и вскрытые сейфы, таймаут вскрытия которых еще не истек. При переносе во вскрытый сейф происходит перекодирование секрета пломбой нового сейфа.

Шаг 4. Подтвердить копирование секрета нажатием на кнопку **Принять** ✓ **Принять**.





Имя секрета должно быть уникально в пределах сейфа для копирования. Если сейф уже содержит секрет с таким именем, выдается соответствующая ошибка. Скопированный секрет более не связан с исходным, и все изменения в нем не будут отражаться в исходном секрете. Верно и обратное: все изменения в исходном секрете после копирования не будут отражаться в созданной копии.

7.2.6 Удаление секрета

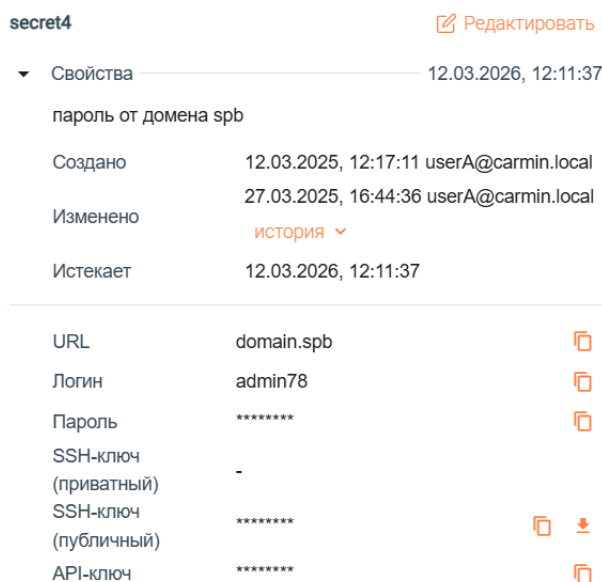
Секрет может быть удален только пользователем, создавшим его.

Для удаления секрета необходимо:

- Шаг 1. В области **Карточка сейфа** найти нужный секрет и нажать на кнопку . Секрет может быть найден через строку поиска.
- Шаг 2. В функциональном меню выбрать **Удалить секрет**.
- Шаг 3. Подтвердить удаление в диалоге подтверждения операции нажатием на кнопку **Принять**  **Принять**.

7.3 Карточка секрета

Область **Карточка секрета** позволяет просмотреть информацию о секрете, историю его изменений, а также редактировать, заполнять и очищать пароль и ключи у существующих секретов (см. [рисунок 9](#)).










secret4		 Редактировать
▼ Свойства		12.03.2026, 12:11:37
пароль от домена spb		
Создано	12.03.2025, 12:17:11 userA@carmin.local	
Изменено	27.03.2025, 16:44:36 userA@carmin.local	
	история ▼	
Истекает	12.03.2026, 12:11:37	
<hr/>		
URL	domain.spb	
Логин	admin78	
Пароль	*****	
SSH-ключ (приватный)	-	
SSH-ключ (публичный)	*****	 
API-ключ	*****	

Рисунок 9 – Карточка секрета



Область **Карточка секрета** доступна на редактирование для **Предоставленных мне** сейфов только с соответствующими правами доступа (см. [раздел 7.1](#))

7.3.1 Просмотр карточки секрета

Для просмотра информации о секрете необходимо:

- Шаг 1. Перейти в карточку сейфа (см. [раздел 7.2](#)).
- Шаг 2. В разделе **Секретов** выбрать нужный или найти необходимый секрет поиском и нажать на него. Откроется поле **Карточка секрета**.

secret4		✎ Редактировать
▼ Свойства	12.03.2026, 12:11:37	
пароль от домена spb		
Создано	12.03.2025, 12:17:11 userA@carmin.local	
Изменено	27.03.2025, 16:44:36 userA@carmin.local	
	история ▼	
Истекает	12.03.2026, 12:11:37	
<hr/>		
URL	domain.spb	📄
Логин	admin78	📄
Пароль	*****	📄
SSH-ключ (приватный)	-	
SSH-ключ (публичный)	*****	📄 ↓
API-ключ	*****	📄

Раздел **Свойства** содержит информацию о времени создания секрета и пользователе, который создал секрет, дату изменения секрета и историю изменений, если секрет был изменен более одного раза, а также дату валидности секрета. На самом верху раздела **Свойства** находится информация о сроке экспирации секрета.

Ниже раздела **Свойства** располагается информация о URL, для которого данный секрет был создан, а также информация о логине-пароле и ключах, содержащихся в секрете.

Информация из заполненных полей может быть скопирована в буфер обмена нажатием на кнопку **Копировать** [📄](#). Также возможно скачать SSH-ключи нажатием на кнопку **Скачать** [↓](#).

7.3.2 Редактирование секрета

Для редактирования информации о секрете необходимо:

Шаг 1. Перейти в карточку секрета.

Шаг 2. Нажать на кнопку **Редактировать** [✎ Редактировать](#). Откроется поле **Карточка секрета** в режиме редактирования.

Редактировать секрет

Название	<input type="text" value="Контроллер домена. Петербург"/>
Описание	<input type="text"/>
Истекает	<input type="text" value="12.03.2026"/>
URL	<input type="text" value="domain.spb"/>
Логин	<input type="text" value="admin78"/>
Пароль	<input type="password" value="....."/> quality: 3
SSH-ключ (приватный)	<input type="text"/>
SSH-ключ (публичный)	<input type="text"/>
API-ключ	<input type="text"/>

[✕ Отменить](#) [✓ Принять](#)

Шаг 3. Изменить необходимые данные. Система проверяет те же валидации, что и при создании секрета (см. [раздел 7.1.3](#) и [раздел 7.2.2](#)).

Кнопка около поля **Пароль** вызывает окно с минимальными требованиями по заполнению пароля и возможностью сгенерировать пароль нажатием на кнопку **Сгенерировать** [✓ Сгенерировать](#). Сгенерированные пароли будут видны в разделе **Результат**. Внизу поля **Пароль** показано качество пароля, например, **quality: 3**. Качество пароля определяется его длиной и сложностью и может быть от 1 до 4.



Если вводится значение пароля, использованное ранее среди последних пяти паролей, выдается соответствующая ошибка. Глубина хранения паролей задается Администратором на этапе настройки работы функционала.

Шаг 4. Сохранить изменения нажатием на кнопку **Принять** [✓ Принять](#).









Изменения в секрете будут доступны пользователям, которым открыт доступ к сейфу, через некоторое время после обработки сервером и обновления страницы.

8 УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

В [таблице 4](#) приведены условные обозначения, которые используются в документе.

Таблица 4 – Условные обозначения

Обозначение	Описание
	Важная информация, с которой необходимо ознакомиться
	Дополнительная информация
	Информация, которая может оказаться полезной
	Шаг сценария выполнен успешно
	Шаг сценария выполнен с ошибкой
	Результат выполнения сценария
(см. Избранное).	Ссылки
/etc/network/file.txt	Путь к файлу, директории или скрипту
<i>dst</i>	Наименование переменной или компонента
sudo -i	Используемая команда
<code>команда1 команда2</code>	Последовательность команд
<code>ntadmin</code>	Данные, которые вводит или выбирает пользователь
<code>ntsuper</code>	Имя учетной записи
Имя пользователя	Элементы пользовательского интерфейса
Установка завершена	Сообщения системы

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

API	Application Programming Interface — описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.
APP	Remote APP — удаленное приложение.
RDP	Remote Desktop Protocol — протокол удаленного рабочего стола
SSH	Secure SHell (безопасная оболочка) — протокол защищенной передачи данных.
TELNET	TErminaL NETwork — сетевой протокол для реализации текстового интерфейса по сети (при помощи транспорта TCP).
VNC	Virtual Network Computing — система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер).

ПЕРЕЧЕНЬ РИСУНКОВ

Рисунок 1 – Главная страница.....	7
Рисунок 2 – Страница Избранное.....	10
Рисунок 3 – Страница Все профили доступа.....	15
Рисунок 4 – Настройки файлов авторизации.....	17
Рисунок 5 – Закладка Секреты.....	18
Рисунок 6 – Функциональное меню сейфа.....	21
Рисунок 7 – Карточка сейфа.....	28
Рисунок 8 – Функциональное меню секрета.....	29
Рисунок 9 – Карточка секрета.....	36

ПЕРЕЧЕНЬ ТАБЛИЦ

Таблица 1 – Соответствие подсказок элементам веб-интерфейса.....	10
Таблица 2 – Соответствие иконки пломбы состоянию сейфа.....	19
Таблица 3 – Соответствие подсказок элементам сервиса.....	20
Таблица 4 – Условные обозначения.....	39

