

OBSKURA

НЕВИДИМАЯ БЕЗОПАСНОСТЬ ДЛЯ ВАШИХ ДАННЫХ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВЕРСИЯ **0.3.0** · MACOS · WINDOWS · LINUX · ОКТЯБРЬ 2026

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

СОДЕРЖАНИЕ

01	**Добро пожаловать в Obskura**	Что умеет программа, базы данных и сейфы	03
02	**Установка и первый запуск**	macOS, Windows, Linux · ключ доступа · интерфейс	04
03	**Пароли и ключевые файлы**	Учётные данные, Argon2id, выбор шифра	05
04	**Базы паролей**	Создание, разблокировка, порядок в записях	07
05	**Работа с записями**	Генератор, поля, вложения, история	08
06	**Инструменты базы данных**	Поиск, безопасное копирование, меню базы	09
07	**Сейфы файлов**	Создание сейфа и шифрование файлов	10
08	**Работа с файлами**	Открытие, изменение, экспорт	11
09	**Удалённые серверы**	SFTP, WebDAV, SMB, FTP/FTPS	12
10	**Несколько устройств в реальном времени**	Синхронизация в реальном времени, уведомления	14
11	**Ключ доступа и устройства**	Сопутствующие файлы, идентификаторы и пути устройств	15
12	**Автоматическое резервное копирование**	Второе место, датированные копии, по устройствам	17
13	**Импорт и экспорт**	Онлайн-менеджеры, CSV из KeePass и других	18
14	**Языки**	Автоматический язык, XML-файлы, новые переводы	20
15	**Блокировка и настройки**	Автоблокировка, буфер обмена, тема, имя устройства	23
16	**Сочетания клавиш и криптография**	Сочетания клавиш и технические подробности	24
17	**Рекомендации и решение проблем**	Резервные копии, частые вопросы	25

ОБОЗНАЧЕНИЯ

Названия кнопок и меню выделены **полужирным**. Сочетания клавиш записываются так: `Ctrl/⌘` + `L`, где `Ctrl` относится к Windows и Linux, а `⌘` — к macOS. Имена файлов и расширения набраны `моноширинным шрифтом`. На снимках экрана интерфейс показан на языке этого руководства.

ВВЕДЕНИЕ

01 ДОБРО ПОЖАЛОВАТЬ В OBSKURA

Obskura защищает пароли и файлы шифрованием военного уровня. Никаких учётных записей и сторонних сервисов: ваши данные остаются там, где решите вы, — на компьютере или на вашем сервере.

Каждая база данных и каждый сейф — это обычный файл или обычная папка. Их можно хранить на диске компьютера, на USB-накопителе, в синхронизируемой папке вроде Dropbox, OneDrive или iCloud Drive или прямо на своём сервере SFTP, WebDAV, SMB или FTP — и заводить сколько угодно: личную, рабочую, общую для семьи. Несколько компьютеров могут работать с ними одновременно и видят изменения друг друга в реальном времени, даже если обращаются к ним по разным путям.

БАЗА ПАРОЛЕЙ

Один файл `.obk` по образцу KeePass. Содержит записи с именем пользователя, паролем, адресом, заметками, дополнительными полями, вложениями и историей изменений, разложенные по группам.

СЕЙФ ФАЙЛОВ

Папка по образцу Cryptomator. Вы перетаскиваете в неё документы, фотографии и архивы: каждый файл шифруется отдельно, включая имена и структуру папок.

КАК УСТРОЕНА ЗАЩИТА

При создании базы данных или сейфа вы выбираете **главный пароль**, **ключевой файл** или и то и другое. Из этих учётных данных Obskura получает ключ шифрования с помощью Argon2id — алгоритма, специально созданного, чтобы сделать подбор пароля крайне медленным. Затем данные шифруются AES-256 — стандартом, одобренным для информации с грифом **TOP SECRET**.

Учётные данные нигде не сохраняются. Без них содержимое нечитаемо для кого угодно, включая разработчиков.

ВАЖНО

Забытый пароль или потерянный ключевой файл восстановить невозможно. Выберите пароль, который запомните, и храните копию ключевого файла в надёжном отдельном месте.

КРАТКО

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · Каскады шифров · Argon2id до 2 ГиБ · HKDF-SHA256 · AES-SIV для имён файлов · Очистка памяти при закрытии · Без учётной записи · SFTP · WebDAV · SMB · FTPS · Реальное время · Автоматическое резервное копирование · Пути для каждого устройства · 8 языков · macOS · Windows · Linux

НАЧАЛО РАБОТЫ

02 УСТАНОВКА И ПЕРВЫЙ ЗАПУСК

macOS

Откройте файл `.dmg` и перетащите Obskura в **Программы**. Если при первом запуске macOS заблокирует приложение, откройте **Системные настройки → Конфиденциальность и безопасность** и выберите **Всё равно открыть**.

Windows

Запустите установщик `.exe`, который автоматически использует язык Windows, или портативную версию без установки. Если появится предупреждение SmartScreen, нажмите **Подробнее → Выполнить в любом случае**.

Linux

Используйте пакет `.deb` (Debian, Ubuntu), `.rpm` (Fedora, openSUSE) или `.AppImage`, который не требует установки: сделайте его исполняемым и запустите.

ПЕРВЫЙ ЗАПУСК: ЯЗЫК И КЛЮЧ ДОСТУПА

Obskura открывается на языке системы (итальянский, английский, немецкий, испанский, русский, китайский, японский или арабский; для остальных — английский). При первом запуске программа предложит создать **ключ доступа Obskura** или, если вы уже пользуетесь Obskura на другом компьютере, ввести созданный там ключ. Зачем он нужен, объясняется в главе 11.

НАЧАЛЬНЫЙ ЭКРАН

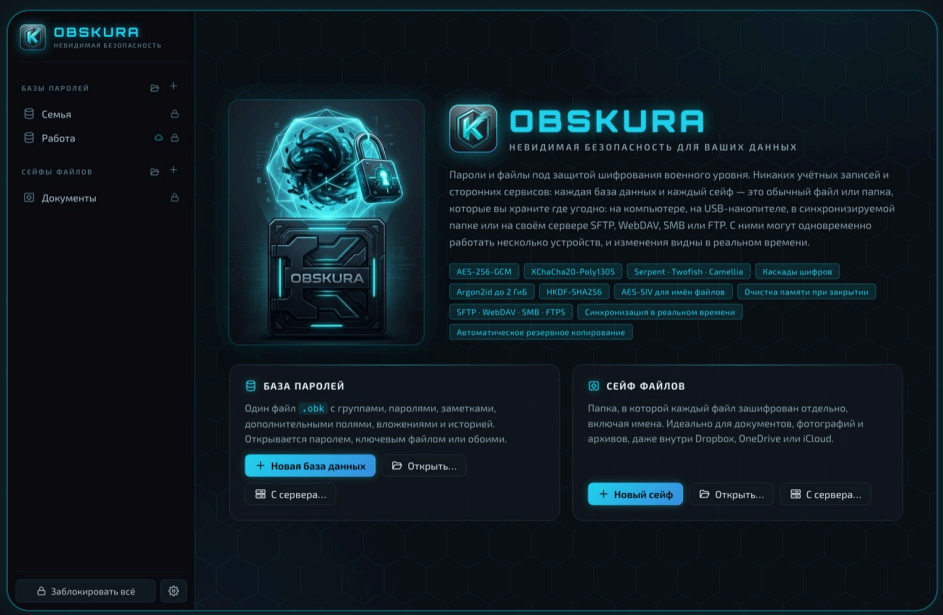


РИС. 1 Экран приветствия с боковой панелью.

На **боковой панели** есть разделы **Базы паролей** и **Сейфы файлов**. Рядом с каждым заголовком две кнопки: папка, чтобы **открыть** существующий элемент, и **+**, чтобы создать новый.

- Каждый недавно открытый элемент остаётся в списке — только с названием: пути никогда не показываются. Замок показывает состояние: **закрыт** — заблокирован, **открыт** — разблокирован.
- При наведении на элемент появляется **×**, чтобы убрать его из недавних (файл не удаляется), или замок, чтобы сразу заблокировать.
- Внизу: **Заблокировать всё** и шестерёнка **Настроек**.

ЗАЩИТА ДАННЫХ

03 ПАРОЛИ И КЛЮЧЕВЫЕ ФАЙЛЫ

Базы данных и сейфы открываются **главным паролем**, **ключевым файлом** или обоими вместе. Сочетание двух — самая сильная защита: нужно то, что вы *знаете*, и то, что у вас *есть*.

ГЛАВНЫЙ ПАРОЛЬ

Длинная фраза надёжнее сложного слова: четыре-пять случайных слов легко запомнить и крайне трудно подобрать. Индикатор под полем оценивает стойкость в битах.

Кнопка с кубиком открывает **генератор**, если вам нужен случайный пароль.

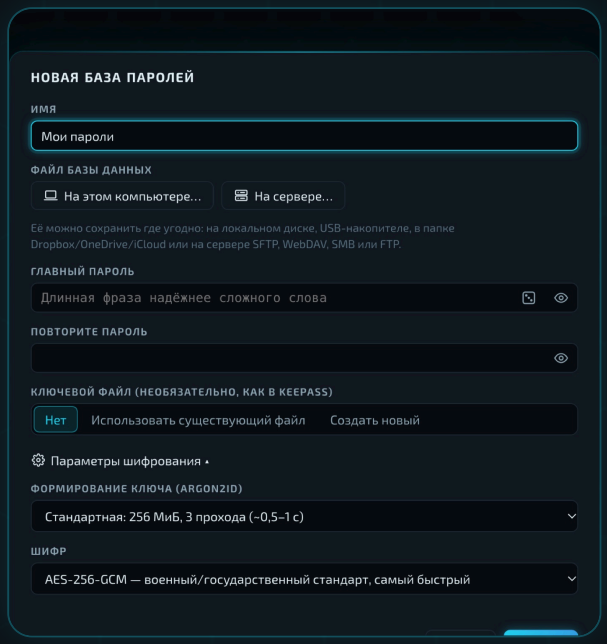


РИС. 2 Создание базы данных с открытыми параметрами шифрования.

КЛЮЧЕВОЙ ФАЙЛ

Как и в KeePass, ключом может служить **любой файл**. Можно выбрать **Использовать существующий файл** или **Создать новый**: Obskura создаст случайный ключевой файл в указанном месте.

Храните его, например, на USB-накопителе отдельно от базы данных. Obskura запоминает, где он лежит на каждом устройстве, и сама ищет его при каждом открытии (глава 11).

ПАРАМЕТРЫ ШИФРОВАНИЯ

В разделе **Параметры шифрования** вы выбираете, насколько затратным будет формирование ключа и какой шифр использовать. Значения по умолчанию — «Стандартная» и AES-256-GCM — безопасны для любых задач; все варианты описаны на следующей странице.

КЛЮЧЕВОЙ ФАЙЛ НЕЛЬЗЯ ИЗМЕНЯТЬ

Если ключом служит произвольный файл (фотография, документ), малейшее изменение делает его непригодным. Файлы, созданные Obskura, имеют распознаваемый текстовый формат и остаются действительными даже при смене переводов строк. В любом случае храните резервную копию.

ЗАЩИТА ДАННЫХ

03 ВЫБОР ШИФРА

ФОРМИРОВАНИЕ КЛЮЧА (ARGON2ID)

Argon2id превращает ваши учётные данные в ключ шифрования: чем больше памяти и проходов, тем дороже злоумышленнику перебирать миллионы паролей.

УРОВЕНЬ	ПАРАМЕТРЫ	ВРЕМЯ ОТКРЫТИЯ
Стандартный	256 МиБ памяти, 3 прохода	около 0,5–1 секунды
Высокий	1 ГиБ, 4 прохода	около 2–4 секунд
Экстремальный	2 ГиБ, 6 проходов	около 5–12 секунд

ЭКСТРЕМАЛЬНЫЙ УРОВЕНЬ

Каждое открытие требует **2 ГиБ свободной памяти**. На компьютере с малым объёмом ОЗУ база данных или сейф могут не открыться: выбирайте этот уровень, только если будете работать на подходящих компьютерах.

ШИФРЫ

Все шифры используют 256-битные ключи и **аутентифицированы**: любое изменение данных обнаруживается.

ШИФР	ОСОБЕННОСТИ
AES-256-GCM	**По умолчанию.** Стандарт США, одобренный для информации TOP SECRET, самый быстрый благодаря аппаратному ускорению.
XChaCha20-Poly1305	Поточный шифр, быстрый на любом процессоре даже без инструкций AES.
Serpent-256-GCM	Финалист конкурса AES с наибольшим запасом стойкости (32 раунда). Медленнее.
Twofish-256-GCM	Финалист конкурса AES, разработан Брюсом Шнайером с коллегами.
Camellia-256-GCM	Международный стандарт ISO/IEC, рекомендован в Европе (NESSIE) и Японии (CRYPTREC).
Каскад AES · Twofish · Serpent	**Самый стойкий вариант.** Три шифрования подряд с независимыми ключами: данные останутся защищены, даже если когда-нибудь будут взломаны два алгоритма из трёх.
Каскад AES · XChaCha20	Сочетает блочный и поточный шифры совершенно разных семейств.

СЕЙФЫ

В сейфах выбранный шифр защищает и ключи, и содержимое каждого файла. Если сменить его через **Изменить пароль / ключевой файл**, уже имеющиеся файлы останутся зашифрованы прежним шифром, а добавленные после — новым. Действующий шифр показан в правом нижнем углу сейфа.

МЕНЕДЖЕР ПАРОЛЕЙ

04 БАЗЫ ПАРОЛЕЙ

СОЗДАНИЕ БАЗЫ ДАННЫХ

1. Нажмите **Новая база данных** на начальном экране или **+** рядом с **Базы паролей**.
2. Введите **название** и выберите, где сохранить файл `.obk`: **На этом компьютере…** или **На сервере…**.
3. Задайте пароль и/или ключевой файл (глава 03).
4. Нажмите **Создать**. База данных откроется уже разблокированной.

ОТКРЫТИЕ И РАЗБЛОКИРОВКА

1. Выберите базу на боковой панели или откройте существующий файл `.obk` значком папки.
2. Введите пароль. Ключевой файл и резервная копия ищутся автоматически; если ключевой файл не найден, выберите его кнопкой **Выбрать…**.
3. Нажмите **Разблокировать** или `Enter`.

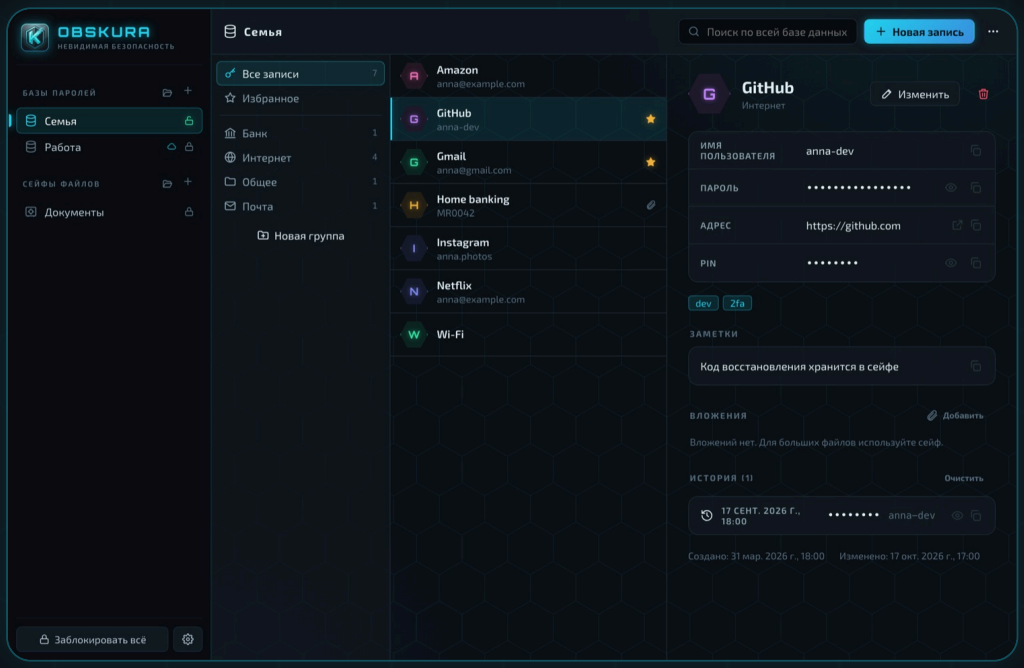


РИС. 3 Разблокированная база данных: группы, список записей и подробности выбранной записи.

ТРИ КОЛОНКИ

- **Группы**: **Все записи**, **Избранное** и ваши папки. При наведении на группу появляются команды для создания подгруппы, изменения или удаления; **Новая группа** — в конце списка.
- **Записи**: название и имя пользователя каждой записи. Звезда отмечает избранное, скрепка — вложения. **Двойной щелчок** сразу копирует пароль.
- **Подробности**: все поля записи с кнопками, чтобы показать, скопировать или открыть адрес в браузере.

БАЗЫ ПАРОЛЕЙ

05 РАБОТА С ЗАПИСЯМИ

Чтобы добавить запись, нажмите **Новая запись** (или `Ctrl/⌘` + `N`); чтобы изменить — выберите её и нажмите **Изменить**. Сохраняйте кнопкой внизу или `Ctrl/⌘` + `S`. Каждое изменение сразу записывается в файл базы данных.

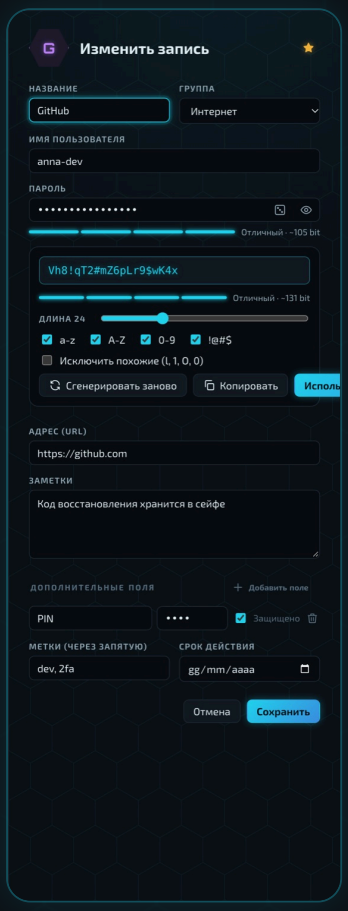


РИС. 4 Редактор записи с открытым генератором.

ПОЛЯ ЗАПИСИ

Название и группа	Название записи и папка, в которой она лежит.
Имя пользователя	Учётная запись, эл. почта или номер клиента.
Пароль	С индикатором стойкости и генератором.
Адрес	Открывается в браузере из подробностей.
Заметки	Произвольный текст, зашифрованный, как и всё остальное.
Метки	Ключевые слова через запятую.
Срок действия	Дата, после которой пароль стоит сменить.

Звезда вверху добавляет запись в **Избранное**.

ГЕНЕРАТОР ПАРОЛЕЙ

Нажмите кубик в поле пароля. Выберите **длину** (от 8 до 64 символов) и наборы символов (`a-z`, `A-Z`, `0-9`, `!@#$`); **Исключить похожие** убирает символы, которые легко спутать, например l, 1, O и 0. Затем **Сгенерировать заново**, **Копировать** или **Использовать этот пароль**. Пароли создаёт криптографический генератор случайных чисел системы.

ДОПОЛНИТЕЛЬНЫЕ ПОЛЯ

Добавляйте сведения вроде PIN-кодов, кодов восстановления или контрольных вопросов. Отметьте **Защищено**, чтобы они отображались скрытыми, как пароль.

ВЛОЖЕНИЯ И ИСТОРИЯ

Прикрепляйте файлы размером до **64 МБ** каждый (для больших файлов используйте сейф). Каждое изменение сохраняет предыдущую версию: **История** хранит последние **20** и позволяет скопировать старый пароль.

БАЗЫ ПАРОЛЕЙ

06 ИНСТРУМЕНТЫ БАЗЫ ДАННЫХ

ПОИСК

Поле **Поиск по всей базе данных** вверху (или `Ctrl/⌘` + `F`) фильтрует записи всех групп по мере ввода. `Esc` очищает поиск.

БЕЗОПАСНОЕ КОПИРОВАНИЕ

Кнопки копирования рядом с именем пользователя, паролем и защищёнными полями помещают значение в буфер обмена, который Obskura **автоматически очищает** через 20 секунд (меняется в настройках). Буфер очищается, только если в нём всё ещё скопированное значение: если вы тем временем скопировали что-то другое, оно останется.

МЕНЮ БАЗЫ ДАННЫХ

Кнопка ⋯ в правом верхнем углу содержит:

ПУНКТ	НАЗНАЧЕНИЕ
Свойства базы данных	Изменить название и описание базы.
Изменить пароль / ключевой файл	Задать новые учётные данные. База перешифровывается новыми ключами.
Сохранить резервную копию…	Записать зашифрованную копию базы в другое место.
Автоматическое резервное копирование…	Настроить второе место для копий (глава 12).
Устройства и пути…	Посмотреть, какие устройства пользуются базой, и их пути (глава 11).
Импорт / экспорт	Из онлайн-менеджера или CSV и в CSV (глава 13).
Заблокировать базу данных	Закрыть базу и стереть её данные из памяти.

СОХРАНЕНИЕ И СИНХРОНИЗАЦИЯ

Каждое изменение сохраняется сразу и **атомарно**: новый файл пишется отдельно и заменяет старый только целиком, поэтому отключение питания не может его испортить. Если тем временем другой компьютер изменил базу, Obskura **объединяет** версии перед сохранением: ничего не теряется (глава 10). Решение требуется только в одном случае — когда на другом устройстве изменили **пароль или ключевой файл**: Obskura предложит заблокировать базу и открыть её с новыми учётными данными.

> **СОВЕТ**
>
> Чтобы пользоваться одной базой на нескольких компьютерах, разместите её на своём сервере (глава 09) или в синхронизируемой папке: она может быть открыта везде одновременно.

ЗАШИФРОВАННЫЕ ФАЙЛЫ

07 СЕЙФЫ ФАЙЛОВ

Сейф — это папка, в которой ваши файлы хранятся в зашифрованном виде. Снаружи это просто набор файлов с нечитаемыми именами: не понять ни что в них, ни как они организованы.

СОЗДАНИЕ СЕЙФА

1. Нажмите **Новый сейф** или **+** рядом с **Сейфы файлов**.
2. Выберите название и папку для сейфа — хоть внутри Dropbox, OneDrive или iCloud Drive, хоть на сервере.
3. Задайте пароль и/или ключевой файл и нажмите **Создать**.

ДОБАВЛЕНИЕ ФАЙЛОВ

- **Перетащите** файлы и папки из Finder / Проводника в окно: они шифруются в открытую сейчас папку.
- Или воспользуйтесь кнопками **Добавить файлы** и **Добавить папку**.
- Оригиналы не затрагиваются: после шифрования их можно удалить самостоятельно.

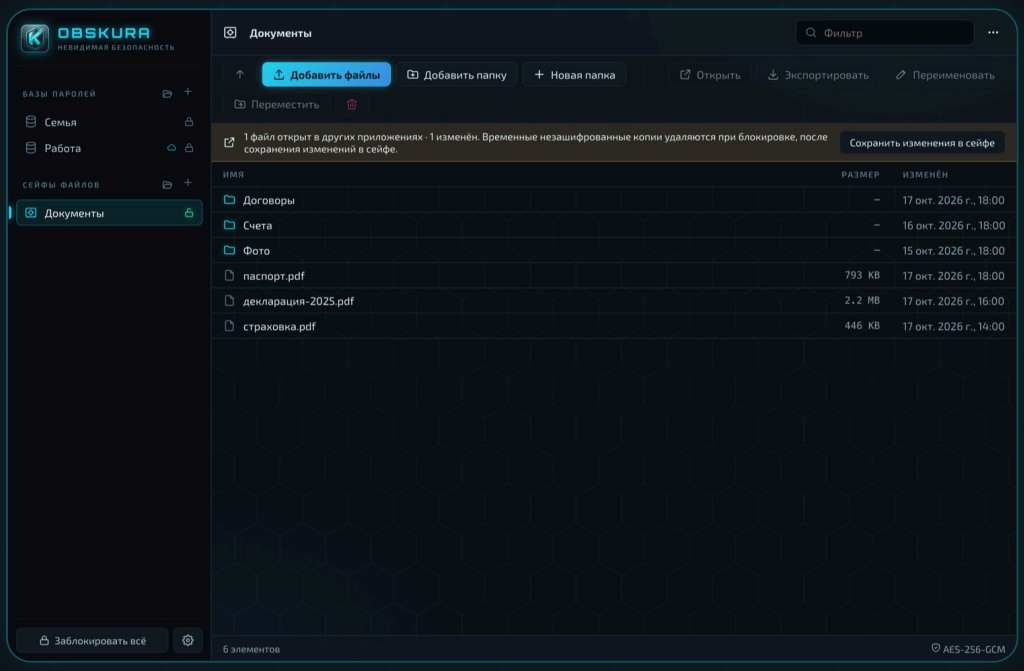


РИС. 5 Разблокированный сейф.

ПАНЕЛЬ КОМАНД

↑ — к родительской папке · **Новая папка** создаёт вложенную папку · **Открыть**, **Экспортировать**, **Переименовать**, **Переместить** и **Удалить** действуют на выбранные элементы. Несколько элементов выбираются `Ctrl/⌘` + щелчок или `Shift` + щелчок. Строка состояния внизу показывает число элементов и ход операций.

СЕЙФЫ ФАЙЛОВ

08 РАБОТА С ФАЙЛАМИ

ОТКРЫТИЕ И ИЗМЕНЕНИЕ ФАЙЛА

Дважды щёлкните файл (или выберите его и нажмите **Открыть**). Obskura расшифрует его в защищённую временную папку и откроет в программе по умолчанию.

1. Измените и сохраните файл как обычно в другой программе.
2. В Obskura появится полоса со списком открытых и изменённых файлов.
3. Нажмите **Сохранить изменения в сейфе**, чтобы зашифровать новую версию.

> **ВРЕМЕННЫЕ НЕЗАШИФРОВАННЫЕ КОПИИ**
>
> Пока файл открыт, его расшифрованная копия существует на диске. При блокировке сейфа Obskura сначала сохраняет оставшиеся изменения, а затем **удаляет временные копии**. Закройте файл в другой программе перед блокировкой.

ЭКСПОРТ

Экспортировать расшифровывает выбранные элементы вместе с папками в выбранную вами папку. Экспортированные файлы **не зашифрованы**: используйте эту функцию, только если они нужны вне сейфа.

УПОРЯДОЧИВАНИЕ

Переименование — **Переименовать** или `F2`; перемещение — **Переместить** с выбором папки назначения. **Удалить** (или `Del`) всегда просит подтверждения. Поле **Фильтр** показывает только элементы, в имени которых есть введённый текст.

СИНХРОНИЗАЦИЯ С ОБЛАКОМ

Каждый файл сейфа зашифрован отдельно: если вы меняете документ, служба синхронизации загружает только этот файл. Поэтому сейфы хорошо работают в Dropbox, OneDrive, Google Drive и iCloud Drive.

КАК СЕЙФ ВЫГЛЯДИТ НА ДИСКЕ

ЭЛЕМЕНТ	СОДЕРЖИМОЕ
`vault.obkv`	Ключи сейфа, зашифрованные вашими учётными данными.
`vault.obkv.bak`	Идентичная страховочная копия на случай повреждения первого файла.
`vault.obkx`	Сопутствующий файл, зашифрованный ключом доступа: ключевой файл, резервная копия и пути каждого устройства (глава 11).
`d/`	Все зашифрованные файлы и папки рядом друг с другом: настоящая структура не видна.

Чтобы открыть существующий сейф, нажмите значок папки рядом с **Сейфы файлов** и выберите его корневую папку. Не изменяйте и не перемещайте файлы внутри вручную.

ГДЕ ХРАНИТЬ

09 УДАЛЁННЫЕ СЕРВЕРЫ

Базам данных и сейфам не обязательно быть на компьютере: Obskura открывает и сохраняет их прямо на вашем сервере, без программ синхронизации. Данные передаются и хранятся на сервере **уже зашифрованными**: администратор сервера или взломщик увидит только нечитаемые файлы.

ПРОТОКОЛ	ГДЕ ИСПОЛЬЗУЕТСЯ	ПРИМЕЧАНИЯ
SFTP	NAS (Synology, QNAP, TrueNAS), серверы Linux, VPS	Рекомендуется. Пароль или ключ SSH.
WebDAV	Nextcloud, ownCloud, Synology, QNAP, Box, Koofr	По HTTPS. Для Nextcloud путь `/remote.php/dav/files/<пользователь>`.
SMB	Общие папки Windows, NAS, Samba	SMB 2 и 3; укажите имя общего ресурса.
FTPS	Хостинги и FTP-серверы с TLS	FTP, зашифрованный через `AUTH TLS`.
FTP	Обычные FTP-серверы	Учётные данные сервера передаются открыто: лучше FTPS или SFTP.

НАСТРОЙКА ПОДКЛЮЧЕНИЯ

1. Откройте **Настройки** → **Подключения к серверам** и нажмите **Новое подключение**.
2. Выберите протокол и введите адрес, порт (если он нестандартный), пользователя и пароль.
3. Нажмите **Проверить подключение**, затем **Сохранить**.

Пароль сервера попадает в **системную связку ключей** (Связка ключей macOS, Диспетчер учётных данных Windows, Secret Service в Linux) и никогда — в файл настроек. Кроме того, он копируется в зашифрованном виде в сопутствующий файл: другие ваши компьютеры восстанавливают подключение сами.

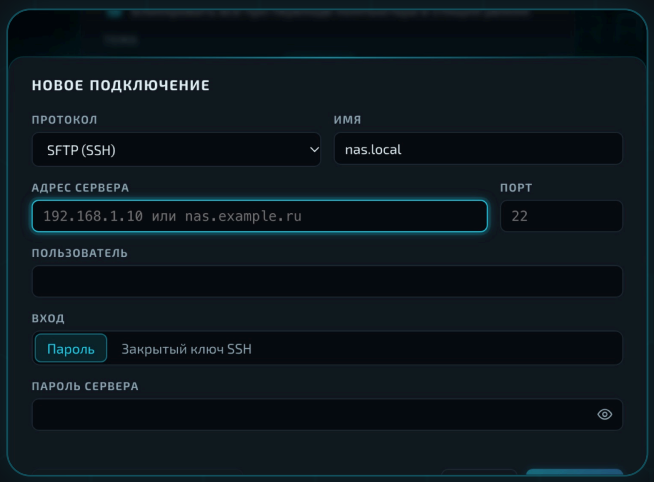


РИС. 6 Новое подключение SFTP.

КЛЮЧ СЕРВЕРА (SFTP)

При первом подключении Obskura показывает **отпечаток** ключа сервера и просит его принять, как это делает `ssh`. Если позже отпечаток изменится, подключение будет отклонено, пока вы снова не подтвердите: возможно, кто-то выдаёт себя за ваш сервер. Если на сервере ничего не менялось, не принимайте.

ОТКРЫТИЕ И СОХРАНЕНИЕ НА СЕРВЕРЕ

- **Открыть:** значок папки рядом с **Базы паролей** или **Сейфы файлов** предлагает **С этого компьютера…** и **С сервера…**. На начальном экране то же — кнопка **С сервера…**.
- **Создать:** в окне **Новая база данных** или **Новый сейф** выберите **На сервере…** вместо **На этом компьютере…**.
- Элементы на сервере отображаются среди недавних со значком **облака**; после открытия на верхней панели появляется метка `СЕРВЕР`.



РИС. 7 Обозреватель сервера: выбор подключения и папки.

В обозревателе выберите подключение в левом верхнем углу и переходите по папкам. Для базы данных нажмите файл `.obk`; для сейфа войдите в его папку (где лежит `vault.obkv`) и нажмите **Открыть этот сейф**. Значок «папка+» создаёт новую папку на сервере.

ПРОИЗВОДИТЕЛЬНОСТЬ

Базы данных небольшие и открываются мгновенно даже удалённо. Сейфы передают по одному файлу — когда вы его открываете или экспортируете: для очень больших файлов важна скорость соединения.

СОВМЕСТНАЯ РАБОТА

10 НЕСКОЛЬКО УСТРОЙСТВ В РЕАЛЬНОМ ВРЕМЕНИ

Одна и та же база данных или сейф могут быть открыты одновременно на нескольких компьютерах: изменения, сделанные на одном, через несколько секунд появляются на остальных.

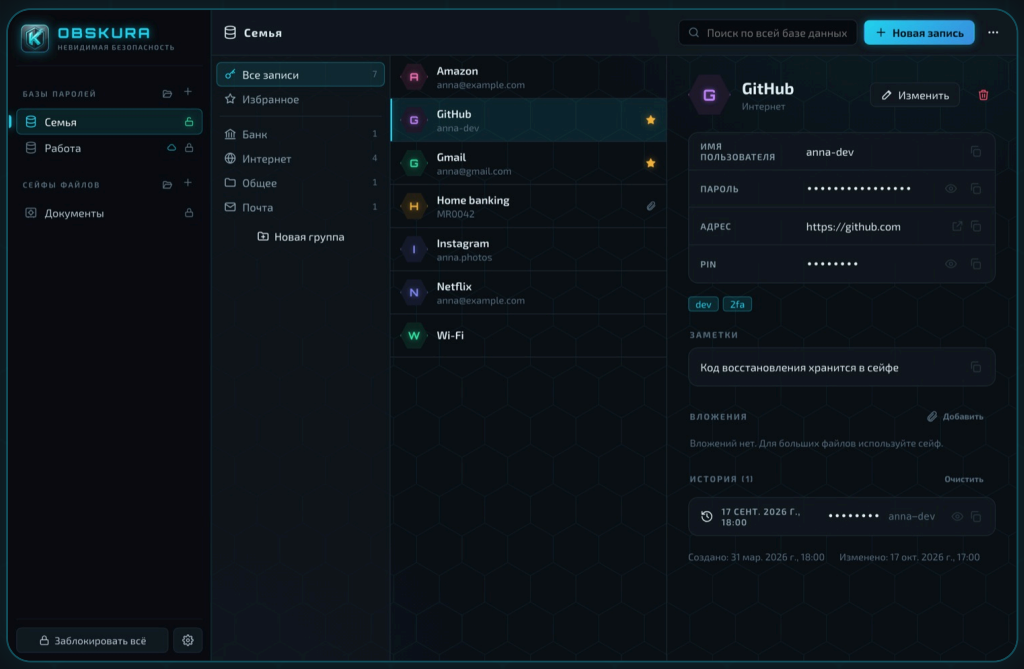


РИС. 8 Уведомление: другое устройство добавило и изменило записи.

КАК ЭТО РАБОТАЕТ

- Obskura проверяет файл каждые **2 секунды** на локальном диске или в синхронизируемой папке и каждые **5 секунд** на сервере. При проверке читаются только первые 88 байт файла.
- Найдя новую версию, программа **объединяет** её с вашей по записям, показывает уведомление о добавленных, изменённых или удалённых записях и сразу обновляет список.
- Если два человека меняют **одну и ту же запись**, побеждает самое новое изменение; другое не теряется — оно попадает в **Историю** записи.
- Удаление доходит до всех, если только кто-то тем временем не изменил эту запись: тогда приоритет у изменения, и запись остаётся.
- В сейфах, когда кто-то добавляет, переименовывает или удаляет файлы в открытой у вас папке, список обновляется сам.

ЧАСЫ КОМПЬЮТЕРОВ

Чтобы понять, какое изменение новее, Obskura использует время компьютеров: держите его синхронизированным (автоматическая установка времени обычно включена во всех системах).

ВСЁ НАЙДЁТСЯ ГДЕ УГОДНО

11 КЛЮЧ ДОСТУПА И УСТРОЙСТВА

Рядом с каждой базой данных и каждым сейфом лежит небольшой зашифрованный файл, который помнит, где находятся ключевой файл, резервные копии и серверы и как к ним обращается каждое ваше устройство. Его защищает ключ доступа Obskura.

КЛЮЧ ДОСТУПА OBSKURA

Это код из 55 символов, создаваемый при первом запуске (или вводимый, если вы создали его на другом компьютере). Он хранится в системной связке ключей; в разделе **Настройки → Ключ доступа Obskura** можно:

- **Показать** — посмотреть и скопировать его, чтобы ввести на другом компьютере.
- **Изменить ключ…** — создать новый. Obskura сразу перешифрует доступные сопутствующие файлы; остальные обновятся при следующем открытии (прежние ключи остаются действительными для их чтения).
- **Ввести ключ…** — использовать текущий ключ, если его сменили на другом компьютере.

СОПУТСТВУЮЩИЕ ФАЙЛЫ

Они зашифрованы AES-256-GCM и нечитаемы без ключа доступа:

ФАЙЛ	СОДЕРЖИТ
`<имя>.obk.obkx`	Рядом с каждой базой данных: расположение ключевого файла, настройки резервного копирования, подключения к серверам и записи устройств.
`vault.obkx`	Внутри каждого сейфа: те же сведения.
`recenti.obkx`	В папке данных приложения: список недавних. На диске не остаётся открытых путей.

ОТКРЫТИЕ С ДРУГОГО КОМПЬЮТЕРА

Когда ключ доступа введён на новом компьютере, достаточно выбрать базу данных: Obskura прочитает сопутствующий файл, восстановит недостающие подключения к серверам, найдёт ключевой файл (по пути, известному для этого устройства, рядом с базой, по путям других устройств или в резервной копии) и предложит резервную копию, если оригинал недоступен.

> **ВАЖНО**
>
> Ключ доступа не заменяет пароль базы данных: без пароля (и ключевого файла) данные остаются нечитаемыми. Тем не менее храните его в надёжном месте: без него ключевой файл и резервные копии придётся выбирать вручную.

УСТРОЙСТВА И ПУТИ

У каждого компьютера с Obskura есть **уникальный идентификатор**, создаваемый при первом запуске, и **имя** (имя компьютера, меняется в разделе **Настройки → Имя этого устройства**). Открывая базу данных или сейф, компьютер записывает в зашифрованный сопутствующий файл собственную запись:

СВЕДЕНИЯ	ПРИМЕР
Идентификатор и имя	`3f2a9c1e-…` · «Домашний MacBook»
Система и версия	macOS · Obskura 0.3.0 · последний доступ
Путь к базе данных	`/Users/anna/Dropbox/scheta.obk` на Mac, `D:\Dropbox\scheta.obk` на ПК
Путь к ключевому файлу	`/Volumes/USB/klyuch.obkey` или `E:\klyuch.obkey`
Собственное резервное копирование	папка этого устройства или общая конфигурация (глава 12)

ОКНО «УСТРОЙСТВА И ПУТИ»

В меню ⋯ базы данных или сейфа выберите **Устройства и пути…**:

- видны все зарегистрированные устройства с системой, версией, последним доступом, использованием ключевого файла и местом резервной копии;
- значок глаза показывает пути каждого устройства; карандаш переименовывает это устройство;
- корзина позволяет **забыть** устройство, которым вы больше не пользуетесь: его пути и резервная копия удаляются из файла (если оно снова откроет базу, то будет зарегистрировано заново).



РИС. 9 Устройства, которые пользуются базой данных.

ЗАЧЕМ ЭТО НУЖНО

У одной и той же базы в Dropbox разные пути на Mac, Windows и Linux, а USB-накопитель с ключевым файлом получает другую букву или имя. Благодаря записям для каждого устройства каждое находит свои пути, не перезаписывая чужие.

СОХРАННОСТЬ ДАННЫХ

12 АВТОМАТИЧЕСКОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ

У каждой базы данных и каждого сейфа может быть **второе место хранения** — на этом компьютере (например, внешний диск) или на любом настроенном сервере. При каждом изменении Obskura копирует туда новую версию в фоне, не замедляя работу.

1. В меню ⋯ базы данных или сейфа выберите **Автоматическое резервное копирование…**
2. Включите **Автоматическое резервное копирование включено** и выберите папку: **На этом компьютере…** или **На сервере…**.
3. Если место назначения — сервер, можно отметить **Использовать эту конфигурацию на всех устройствах**.
4. Для баз данных выберите, сколько **датированных копий** хранить.
5. Нажмите **Сохранить**. **Выполнить сейчас** запускает полную копию.

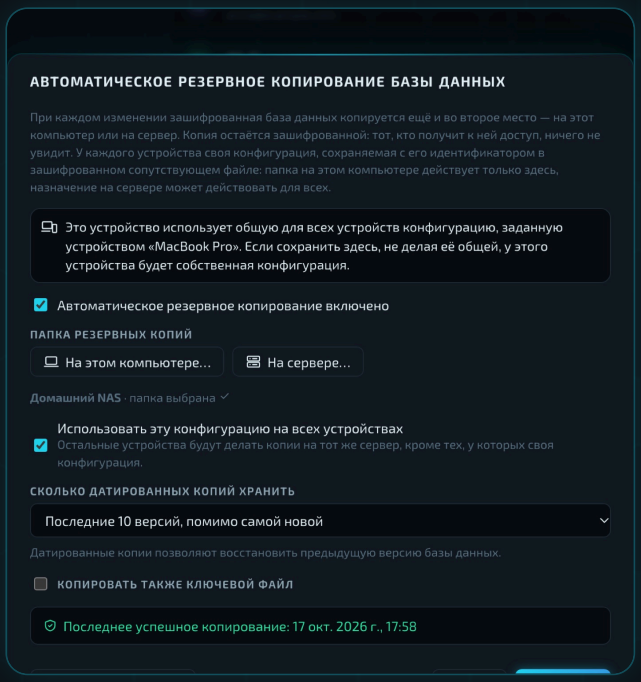


РИС. 10 Резервное копирование на NAS, общее для всех устройств.

ЧТО	КАК КОПИРУЕТСЯ
База данных	Файл `.obk` в папке резервных копий плюс датированные копии `имя.ГГГГММДД-ччммсс.obk`; самые старые сверх лимита удаляются.
Сейф	Копия зашифрованной папки: при каждом изменении копируются заново только затронутые файлы. Копия открывается как обычный сейф.
Ключевой файл	Необязательно: копируется один раз при сохранении настройки в указанную папку.

РЕЗЕРВНАЯ КОПИЯ ДЛЯ КАЖДОГО УСТРОЙСТВА

- У каждого устройства **своя конфигурация**, сохранённая с его идентификатором в сопутствующем файле: локальная папка (например, внешний диск Mac) действует только на этом устройстве.
- Место на сервере может стать **общим**: им пользуются остальные устройства, кроме тех, у которых своя конфигурация. Окно показывает, кто её задал.
- Копии остаются **зашифрованными**: месту хранения копий не нужно доверять.
- Если копирование не удалось, появляется предупреждение; Obskura повторит попытку при следующем изменении.

КЛЮЧЕВОЙ ФАЙЛ И РЕЗЕРВНАЯ КОПИЯ

Не кладите ключевой файл в ту же папку, что и резервную копию: получивший доступ к ней получит и базу данных, и половину учётных данных.

ИЗ ДРУГИХ ПРОГРАММ И В НИХ

13 ИМПОРТ И ЭКСПОРТ

ИМПОРТ ИЗ ОНЛАЙН-МЕНЕДЖЕРА

Obskura сама входит в ваш прежний сервис, загружает зашифрованное хранилище и расшифровывает его на вашем компьютере, без промежуточного файла, экспортированного в открытом виде. Учётные данные используются только для этого входа и не сохраняются.

1. Откройте базу данных назначения и выберите ⋯ → **Импорт из онлайн-менеджера…**
2. Выберите сервис и войдите; при двухэтапной проверке Obskura запросит код.
3. Проверьте предпросмотр: число записей, папки, примеры.
4. Решите, воссоздавать ли папки как группы и пропускать ли уже имеющиеся записи, затем нажмите **Импортировать**.

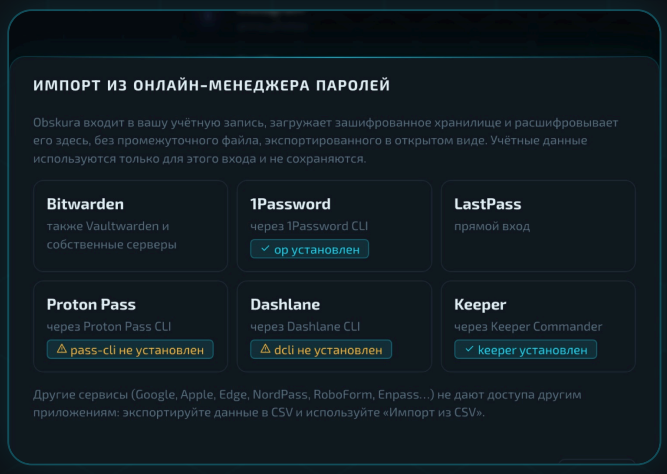


РИС. 11 Выбор сервиса для импорта.

СЕРВИС	ДОСТУП
Bitwarden / Vaultwarden	Напрямую, включая bitwarden.eu и собственные серверы; также с личным ключом API.
LastPass	Напрямую, с двухэтапной проверкой (код или подтверждение на телефоне).
1Password	Через 1Password CLI (`op`), с разрешением в приложении 1Password или по эл. почте, паролю и Secret Key.
Proton Pass	Через Proton Pass CLI (`pass-cli`), со входом через браузер.
Dashlane	Через Dashlane CLI (`dcli`), после первого `dcli sync` в терминале.
Keeper	Через Keeper Commander (`keeper`).

Сохраняются папки, дополнительные поля, коды TOTP, карты и заметки. Другие сервисы (Google, Apple, Edge, NordPass…) не дают доступа другим приложениям: экспортируйте их в CSV.

ИМПОРТ ИЗ CSV (KEEPASS И ДРУГИЕ)

1. Экспортируйте в CSV в исходной программе: KeePass 2 **Файл → Экспорт → KeePass CSV (1.x)**, KeePassXC **База данных → Экспорт → Файл CSV**, Bitwarden, 1Password, Chrome, Edge и Firefox — в их настройках.
2. В Obskura откройте базу данных и выберите ⋯ → **Импорт из CSV (KeePass, …)…**
3. Выберите файл: Obskura распознает формат и столбцы и покажет предпросмотр.
4. Решите, воссоздавать ли группы из файла и пропускать ли уже имеющиеся записи, затем нажмите **Импортировать**.

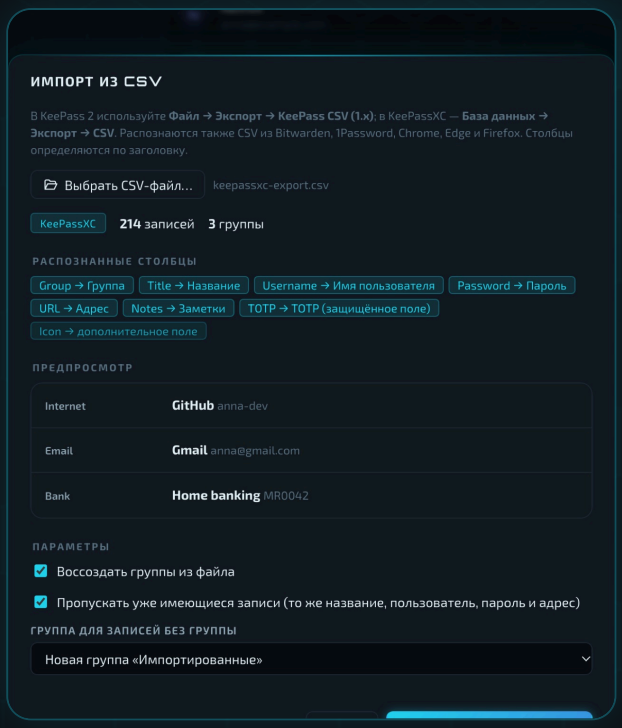


РИС. 12 Предпросмотр экспорта KeePassXC.

Сохраняются группы, метки, коды TOTP (как защищённое поле), даты создания и сроки действия; нераспознанные столбцы становятся дополнительными полями. Повторный импорт того же файла не создаёт дубликатов.

ЭКСПОРТ В CSV

⋯ → **Экспорт в CSV…** создаёт файл со столбцами KeePassXC, а также метками, сроком действия, избранным и дополнительными полями: его можно снова импортировать в Obskura, KeePassXC и большинство менеджеров паролей.

> **CSV НЕ ЗАШИФРОВАН**
>
> Файл содержит все пароли в открытом виде. Используйте его только для переноса данных и затем удалите. После импорта удалите и CSV, экспортированный из старой программы. Для резервных копий используйте автоматическое резервное копирование — копии остаются зашифрованными.

НАСТРОЙКА

14 ЯЗЫКИ

Obskura говорит на восьми языках, и можно добавить другие: все тексты приложения хранятся в XML-файлах, по одному на язык.

ВЫБОР ЯЗЫКА

При запуске Obskura использует язык системы; если его нет среди встроенных — английский. В разделе **Настройки → Язык** можно оставить **Автоматически** или выбрать язык: смена происходит сразу, включая сообщения об ошибках. Арабский читается справа налево, и интерфейс соответственно зеркалится.

Italiano	it
English	en
Deutsch	de
Español	es
Русский	ru
中文（简体）	zh
日本語	ja
العربية	ar

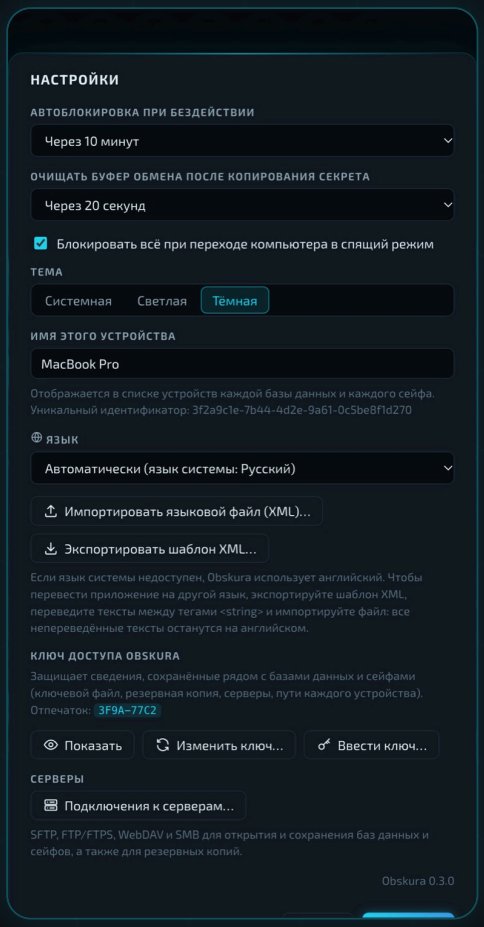


РИС. 13 Раздел «Язык» в настройках.

ДОБАВЛЕНИЕ ЯЗЫКА

1. В разделе **Настройки → Язык** нажмите **Экспортировать шаблон XML...**: вы получите полный файл текущего языка (или скачайте с сайта zip с XML-файлами всех языков).
2. Измените в заголовке `code` (код языка, например `fr` или `pt-BR`), `name` и для языков с письмом справа налево `dir="rtl"`.
3. Переведите текст каждого элемента `<string>` в любом текстовом редакторе и сохраните в UTF-8.
4. Нажмите **Импортировать языковой файл (XML)...**: язык сразу появится в списке и будет автоматически использоваться в системах на этом языке.

ФОРМАТ ФАЙЛА

Языковой файл — это XML с элементом `<language>` и одним `<string>` на каждый текст:

```
<?xml version="1.0" encoding="UTF-8"?>
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.cancel">Annuler</string>
  <string key="db.syncFailed">Échec de la synchronisation : {message}</string>
  <string key="vault.itemsN.one">{count} élément</string>
  <string key="vault.itemsN.other">{count} éléments</string>
</language>
```

- атрибут `key` не переводится и не меняется;
- заполнители в фигурных скобках, например `{count}` или `{name}`, оставляются как есть: приложение подставляет вместо них числа и имена;
- теги `<b>` и `<code>` в тексте нужно сохранить;
- ключи, оканчивающиеся на `.one`, `.two`, `.few`, `.many` и `.other`, — это формы множественного числа: используйте формы своего языка, `.other` обязательна;
- отсутствующий текст показывается на английском, поэтому частичный перевод уже работает.

ИСПРАВЛЕНИЕ ВСТРОЕННОГО ЯЗЫКА

XML-файл с тем же `code`, что у встроенного языка (например, `ru`), не заменяет его, а исправляет только содержащиеся в нём записи. В настройках он отображается с пометкой **исправления** и удаляется кнопкой ×, возвращая исходные тексты.

СОВЕТ

Импортированные файлы остаются в папке данных приложения и действуют только на этом компьютере: импортируйте их и на остальных.

ПЕРЕВОД С ПОМОЩЬЮ ПУСТОГО ШАБЛОНА XML

Для нового языка можно взять пустой шаблон `obskura-translation-template.xml`, который загружается с сайта (`obskura.bytenooks.com`, раздел «Скачать»). В нём по одной строке на каждый текст приложения: перевод пишется между `<string …>` и `</string>`, а атрибут `en` содержит английский текст для справки и может остаться на месте (приложение его игнорирует).

```
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.lock" en="Lock">Verrouiller</string>
  <string key="common.settings" en="Settings">Paramètres</string>
  <string key="common.cancel" en="Cancel">Annuler</string>
</language>
```

1. Загрузите шаблон и сохраните его под кодом своего языка, например `fr.xml`.
2. В первой строке `<language>` заполните `code`, `name`, `english-name` и при необходимости `dir="rtl"`.
3. Пишите перевод в текстовом редакторе с сохранением в UTF-8, соблюдая правила выше.
4. **Удалите строки, которые не переводите**: пустой текст будет показан в приложении пустым, а отсутствующая строка — на английском.
5. Импортируйте файл в **Настройки → Язык** и проверьте тексты в приложении.

ПОДЕЛИТЕСЬ ПЕРЕВОДОМ

Отправьте его разработчику со страницы контактов сайта: выберите тему «Перевод» и приложите файл XML (до 3 МБ; полный языковой файл весит около 100–150 КБ). Присланные переводы могут войти в следующие версии.

БЕЗОПАСНОСТЬ

15 БЛОКИРОВКА И НАСТРОЙКИ

При блокировке базы данных или сейфа Obskura закрывает сеанс и **стирает из памяти** ключи и расшифрованные данные. Чтобы открыть их снова, снова нужны учётные данные.

СПОСОБЫ БЛОКИРОВКИ

- **Заблокировать всё** внизу боковой панели или `Ctrl/⌘` + `L`.
- Замок рядом с разблокированным элементом на боковой панели или пункт **Заблокировать** в меню ⋯.
- **Автоматически** — после периода бездействия или при переходе компьютера в спящий режим.

НАСТРОЙКИ

НАСТРОЙКА	ДЕЙСТВИЕ	ПО УМОЛЧАНИЮ
Автоблокировка при бездействии	Блокирует всё через 1–60 минут без использования мыши и клавиатуры или никогда.	10 минут
Очищать буфер обмена	Очищает буфер через 10–120 секунд после копирования секрета или никогда.	20 секунд
Блокировка в спящем режиме	Блокирует всё при переходе компьютера в спящий режим.	Включено
Тема	Системная, Светлая или Тёмная.	Тёмная
Имя этого устройства	Отображается в списке устройств каждой базы и сейфа; под ним — уникальный идентификатор.	Имя компьютера
Язык	Автоматически или один из доступных языков; импорт и экспорт XML-файлов (глава 14).	Автоматически
Ключ доступа Obskura	Показать, изменить или ввести ключ (глава 11).	—
Серверы	Подключения SFTP, FTP/FTPS, WebDAV и SMB (глава 09).	—

Настройки не содержат секретов: пароли серверов хранятся в системной связке ключей, а список недавних зашифрован ключом доступа.

СПРАВКА

16 СОЧЕТАНИЯ КЛАВИШ И КРИПТОГРАФИЯ

СОЧЕТАНИЯ КЛАВИШ

КЛАВИШИ	ГДЕ	ДЕЙСТВИЕ
`Ctrl/⌘` + `L`	Везде	Заблокировать всё
`Esc`	Диалоговые окна	Закрыть окно
`Ctrl/⌘` + `F`	База данных	Поиск
`Ctrl/⌘` + `N`	База данных	Новая запись
`Ctrl/⌘` + `S`	Редактор записи	Сохранить запись
Двойной щелчок	Список записей	Копировать пароль
`Ctrl/⌘` + `A`	Сейф	Выбрать всё
`Enter`	Сейф	Открыть файл или папку
`F2`	Сейф	Переименовать
`Del` · `⌘` + `⌫`	Сейф	Удалить выбранные элементы
`⌫`	Сейф	К родительской папке

КРИПТОГРАФИЧЕСКИЕ ПОДРОБНОСТИ

КОМПОНЕНТ	АЛГОРИТМ
Формирование ключа	Argon2id: 256 МиБ / 3 прохода, 1 ГиБ / 4 прохода или 2 ГиБ / 6 проходов, случайная соль 256 бит.
Составной ключ	SHA-256 от пароля (нормализованного NFC) и ключевого файла, как в KeePass KDBX4.
Шифрование	AES-256, XChaCha20, Serpent, Twofish, Camellia или каскады, всегда с аутентификацией (GCM или Poly1305); в каскадах у каждого слоя свой ключ, полученный через HKDF.
Подключи	HKDF-SHA256 с новым начальным значением при каждом сохранении.
Целостность	Аутентифицированный заголовок: любое изменение делает открытие невозможным.
Имена в сейфах	AES-SIV с привязкой к содержащей их папке.
Содержимое файлов	Блоки по 64 КиБ, случайный ключ для каждого файла, защита от перестановки и усечения.
Сопутствующие файлы	AES-256-GCM с ключом, полученным через HKDF из ключа доступа Obskura (256 случайных бит).
Память	Ключи и расшифрованные данные остаются в нативном процессе и стираются при закрытии.

ПОДДЕРЖКА

17 РЕКОМЕНДАЦИИ И РЕШЕНИЕ ПРОБЛЕМ

РЕКОМЕНДАЦИИ

- **Включите автоматическое резервное копирование** или регулярно копируйте файлы `.obk` и папки сейфов на внешний диск. Они уже зашифрованы, так что копия безопасна, где бы она ни хранилась.
- **Храните ключевой файл отдельно** от базы данных и держите хотя бы одну запасную копию.
- **Сохраните ключ доступа Obskura** на бумаге или в месте, отличном от компьютера.
- **Используйте разные пароли для каждого сервиса**, созданные генератором: помнить нужно будет только один.
- **Блокируйте, отходя от компьютера**: `Ctrl/⌘` + `L` — самый быстрый способ.
- **Забывайте устройства**, которыми больше не пользуетесь, в окне **Устройства и пути**.

ЧАСТЫЕ ВОПРОСЫ

Я ЗАБЫЛ ГЛАВНЫЙ ПАРОЛЬ. МОЖНО ЛИ ЕГО ВОССТАНОВИТЬ?

Нет. Именно это и делает Obskura надёжной: никто, даже разработчики, не может открыть базу данных или сейф без правильных учётных данных.

«НЕВЕРНЫЙ ПАРОЛЬ ИЛИ КЛЮЧЕВОЙ ФАЙЛ», ХОТЯ Я УВЕРЕН, ЧТО ВСЁ ВЕРНО.

Проверьте, что выбран тот же ключевой файл, что и при создании, и что он не изменялся. Если использовались пароль *и* ключевой файл, нужны оба. Проверьте также Caps Lock.

ОТКРЫТИЕ ЗАНИМАЕТ НЕСКОЛЬКО СЕКУНД. ЭТО НОРМАЛЬНО?

Да: это время работы Argon2id, нарочно замедляющего подбор пароля. На уровне «Высокий» нужны несколько секунд и 1 ГиБ свободной памяти, на «Экстремальном» — до 12 секунд и 2 ГиБ.

НА ДРУГОМ КОМПЬЮТЕРЕ КЛЮЧЕВОЙ ФАЙЛ НЕ НАХОДИТСЯ.

Подключите носитель, на котором он хранится: Obskura ищет его по пути, которым этот компьютер пользовался в прошлый раз, рядом с базой, по путям других устройств и в резервной копии. Если не находит — выберите его кнопкой **Выбрать…**: в следующий раз путь будет запомнен для этого устройства.

ПОЯВИЛОСЬ СООБЩЕНИЕ «ЗАЩИЩЕНЫ ДРУГИМ КЛЮЧОМ ДОСТУПА».

Ключ доступа сменили на другом компьютере. Нажмите **Ввести текущий ключ** и используйте новый; разблокировать можно и так — паролем, выбрав ключевой файл вручную.

ПОЯВИЛОСЬ «УЧЁТНЫЕ ДАННЫЕ ИЗМЕНЕНЫ В ДРУГОМ МЕСТЕ».

Кто-то на другом устройстве сменил пароль или ключевой файл базы. Выберите **Заблокировать** и откройте её с новыми учётными данными; **Перезаписать** отменит изменение, сделанное в другом месте.

НЕ УДАЁТСЯ ПОДКЛЮЧИТЬСЯ К СЕРВЕРУ.

Проверьте адрес, порт и учётные данные кнопкой **Проверить подключение**. Для WebDAV проверьте базовый путь (для Nextcloud `/remote.php/dav/files/<пользователь>`), для SMB — имя общего ресурса. При самоподписанном сертификате включайте **Принимать самоподписанные сертификаты** только в доверенной сети.

ИЗМЕНЕНИЯ В ФАЙЛЕ СЕЙФА НЕ СОХРАНЯЮТСЯ.

Убедитесь, что файл сохранён в другой программе, затем нажмите **Сохранить изменения в сейфе**. Если заблокировать сейф с ещё открытым файлом, Obskura всё равно попытается сохранить его перед удалением временной копии.

ПРИЛОЖЕНИЕ ОТКРЫВАЕТСЯ НЕ НА МОЁМ ЯЗЫКЕ.

Obskura следует языку системы; если вашего нет среди встроенных, используется английский. Выберите язык в разделе **Настройки → Язык** или импортируйте XML-файл (глава 14).

MACOS ИЛИ WINDOWS СООБЩАЮТ, ЧТО ПРИЛОЖЕНИЕ НЕ ПРОВЕРЕНО.

Приложение не подписано коммерческим сертификатом. Чтобы открыть его в первый раз, следуйте инструкциям главы 02.



OBSKURA

НЕВИДИМАЯ БЕЗОПАСНОСТЬ ДЛЯ ВАШИХ ДАННЫХ

Менеджер паролей и зашифрованные сейфы файлов · на вашем компьютере или сервере

macOS · Windows · Linux · Версия **0.3.0**

https://obskura.bytenooks.com