vitextra

СТАТЬЯ БАЗЫ ЗНАНИЙ

Password Vault, менеджеры паролей в браузерах и корпоративные менеджеры паролей: что выбрать

2026 © Vitextra SIA. Все права защищены.

Отказ от ответственности

Для целей настоящего Заявления об отказе от ответственности:

- **Компания** (именуемая в данном Отказе от ответственности "Компания", "Мы", "Нас" или "Наш") относится к Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Документ** ссылается на статью Базы знаний.
- **Вы** означает физическое лицо, получающее доступ к Документу, или компанию, или другое юридическое лицо, от имени которого такое физическое лицо получает доступ к Документу или использует его, в зависимости от обстоятельств.
- **Веб-сайт** относится к Vitextra, доступному с https://vitextra.com

Отказ от ответственности

Информация, содержащаяся в Документе, предназначена только для общих информационных целей.

Компания не несет ответственности за ошибки или упущения в содержании Документа.

Ни в коем случае Компания не несет ответственности за какие-либо особые, прямые, косвенные, логически вытекающие или случайные убытки или любой ущерб вообще, будь то в результате действия договора, халатности или других правонарушений, возникающих в результате или в связи с использованием содержания Документа. Компания оставляет за собой право вносить дополнения, удаления или модификации в содержание Документа в любое время без предварительного уведомления.

Отказ от ответственности за ошибки и упущения

Информация, представленная в Документе, предназначена только для общего руководства по вопросам, представляющим интерес. Таким образом, ошибки могут возникать, даже если Компания принимает все меры предосторожности для обеспечения актуальности и точности содержания Документа. Кроме того, учитывая меняющийся характер законов, правил и подзаконных актов, могут возникнуть задержки, упущения или неточности в информации, содержащейся в Документе.

Компания не несет ответственности за какие-либо ошибки или упущения, а также за результаты, полученные в результате использования этой информации.

Отказ от добросовестного использования

Компания может использовать защищенные авторским правом материалы, которые владелец авторских прав явно не разрешил. Компания делает такие материалы доступными для критики, комментариев, новостных репортажей, преподавания, стипендий или исследований.

Компания считает, что это представляет собой "добросовестное использование" любого такого защищенного авторским правом материала, как это предусмотрено в разделе 107 закона США об авторском праве.

Если Вы хотите использовать защищенные авторским правом материалы из Документа в своих собственных целях, выходящих за рамки добросовестного использования, Вы должны получить разрешение от владельца авторских прав.

Отказ от ответственности "Используйте на Свой Страх и Риск"

Вся информация в Документе предоставляется "как есть", без каких-либо гарантий полноты, точности, своевременности или результатов, полученных в результате использования этой информации, и без каких-либо гарантий, явных или подразумеваемых, включая, но не ограничиваясь гарантиями производительности, товарной пригодности и пригодности для конкретного цель.

Компания не несет ответственности перед Вами или кем-либо еще за любое принятое решение или действие, основанное на информации, предоставленной Сервисом, или за любые косвенные, особые или аналогичные убытки, даже если она предупреждена о возможности таких убытков.

Свяжитесь с Нами

Если у вас есть какие-либо вопросы по поводу этого заявления об отказе от ответственности, Вы можете связаться с нами по электронной почте: support@vitextra.com .

Оглавление

Обзор 4

Password Vault вкратце 4

Краткое сравнение 5

Когда подходит Password Vault 6

Когда подходит менеджер паролей браузера 6

Когда подходит корпоративный менеджер паролей 7

Совместное использование инструментов 7

Вопросы, которые стоит задать перед решением 8

Обзор

Организации, которые хотят, чтобы сотрудники перестали хранить пароли в таблицах и заметках, обычно рассматривают три вида инструментов:

- **Менеджеры паролей в браузерах** — встроенное в браузер хранилище паролей, которое сохраняет учётные данные, когда пользователь входит на сайты.
- **Корпоративные менеджеры паролей** — специализированные продукты, обычно со своим сервисом, клиентскими приложениями и расширениями для браузеров, предназначенные для управления учётными данными в масштабах всей организации.
- **Password Vault** — веб-часть SharePoint Framework от Vitextra, которая даёт каждому сотруднику лёгкое личное хранилище внутри Microsoft 365 (SharePoint Online и Microsoft Teams).

Эти инструменты решают разные задачи. В статье описаны общие характеристики каждой категории, чтобы вы могли решить, какая из них подходит для конкретной потребности. Отдельные продукты внутри категории различаются, поэтому сверяйте особенности любого рассматриваемого продукта со своими требованиями.

Password Vault вкратце

Password Vault хранит записи каждого пользователя в зашифрованном виде в файле в OneDrive этого пользователя и показывает их в веб-части на странице SharePoint или в Teams. Доступ внутри веб-части защищён 4-значным PIN-кодом, из которого вычисляется ключ шифрования; пока хранилище заблокировано, записи не показываются, а через 5 минут бездействия оно блокируется автоматически. Поскольку PIN-код состоит всего из 4 цифр, первой линией защиты файла остаётся контроль доступа к OneDrive. В продукт входят генератор паролей, индикатор надёжности, папки, теги, избранное и поиск. Подробнее см. в статье KB10437. Password Vault. Обзор решения.

Не менее важно то, чего он **не** делает:

- нет автоматического заполнения форм входа и расширения для браузера — учётные данные копируются кнопкой **Скопировать в буфер обмена**;
- нет совместного доступа к записям и командных хранилищ;
- нет консоли администрирования и восстановления забытого PIN-кода — после 5 неверных PIN-кодов единственный вариант — сбросить хранилище, что удаляет все записи;
- нет экспорта и импорта.

Краткое сравнение

Столбец Password Vault описывает продукт; два других столбца описывают то, что типично для категории.

Аспект	**Password Vault**	**Менеджеры паролей в браузерах (типично)**	**Корпоративные менеджеры паролей (типично)**
Назначение	Личные учётные данные сотрудника внутри Microsoft 365	Личное удобство при работе в браузере	Управление учётными данными в масштабах организации
Где хранятся данные	Зашифрованный файл в OneDrive самого пользователя	В профиле браузера, часто с синхронизацией через учётную запись поставщика браузера	В собственном сервисе продукта или в инфраструктуре, которую обслуживает организация
Доступ	Страница SharePoint или Microsoft Teams, с рабочей учётной записью и 4-значным PIN-кодом	Браузер, в котором выполнен вход в профиль	Клиентские приложения, расширения для браузеров и веб-доступ продукта
Автозаполнение форм входа	Нет	Да	Обычно да
Совместный доступ с коллегами	Нет	Ограничен или отсутствует в рабочем контексте	Обычно да, с общими папками или хранилищами
Администрирование, политики, аудит	Нет; только развёртывание и разрешение Graph	Зависит от возможностей управления	Обычно обширные

Аспект	**Password Vault**	**Менеджеры паролей в браузерах (типично)**	**Корпоративные менеджеры паролей (типично)**
		браузером	
Восстановление утраченного доступа	Нет; сброс удаляет хранилище	Зависит от учётной записи браузера	Обычно есть варианты восстановления для администраторов или пользователей
Развёртывание	Один пакет SPFx и одно разрешение Graph; без дополнительного клиентского ПО	Уже есть в браузере	Отдельный продукт, который нужно внедрить, настроить и лицензировать на каждого пользователя
Типичная модель стоимости	Лицензия на клиент	Входит в браузер	Обычно подписка на пользователя

Когда подходит Password Vault

- Сотрудникам нужно место для **собственных** рабочих учётных данных — порталов поставщиков, экстранетов партнёров, тестовых систем, консолей устройств, — и организация хочет, чтобы это место было внутри Microsoft 365, а не в личных инструментах или файлах.
- Организация предпочитает, чтобы данные оставались **в её собственном клиенте** (в OneDrive каждого пользователя), а не у дополнительного стороннего сервиса.
- Простой инструмент, который работает на странице SharePoint и в Teams без установки расширений или клиентского ПО, важнее автозаполнения.
- Учётные данные не используются совместно, и их потеря при забытом PIN-коде допустима, потому что их можно восстановить в исходной системе (например, через процедуру «забыли пароль» самого сервиса).

Когда подходит менеджер паролей браузера

- Главная потребность — удобство: сохранение и автоматическое заполнение паролей для сайтов при работе в браузере.
- Пользователи работают в основном в одном браузере, и политика организации разрешает хранить в нём рабочие учётные данные.

Учтите, что менеджер паролей браузера хранит учётные данные в профиле браузера, поэтому то, что доступно, зависит от браузера и учётной записи, под которой вошёл пользователь, а также от того, как организация управляет браузерами.

Когда подходит корпоративный менеджер паролей

- Учётными данными нужно **совместно пользоваться** в командах, например служебными учётными записями или общими почтовыми ящиками.
- Организации нужны централизованные **политики, журналы аудита, проверки доступа и процедуры восстановления**.
- Нужно управлять учётными записями администраторов с **высокими привилегиями** — часто в сочетании с управлением привилегированным доступом.
- Требуется автозаполнение в разных браузерах, настольных и мобильных приложениях.

Эти возможности требуют отдельного продукта, который нужно развернуть, настроить, обучить им пользователей и лицензировать — обычно на каждого пользователя.

Предупреждение

Password Vault предназначен для личных учётных данных. Он не заменяет решение для управления общими учётными записями или учётными записями с высокими привилегиями. Для таких учётных записей следуйте политике безопасности вашей организации.

Совместное использование инструментов

Категории не исключают друг друга. Организация может использовать корпоративный менеджер паролей для ИТ и общих учётных записей и предлагать Password Vault всем сотрудникам как простое личное место для остальных рабочих учётных данных — или разрешить хранение в браузере для сайтов с низким риском. Главное — чёткая политика, в которой сказано, какие учётные данные где хранить.

Примечание

В Password Vault нет импорта и экспорта, поэтому перенос записей в него или из него означает добавление их по одной. Определитесь с выбором до того, как сотрудники начнут наполнять свои хранилища.

Вопросы, которые стоит задать перед решением

1 Нужно ли совместно пользоваться учётными данными или они строго личные?
2 Требуется ли автоматическое заполнение форм входа?
3 Где можно хранить зашифрованные данные — в вашем клиенте Microsoft 365, в учётной записи поставщика браузера или в стороннем сервисе?
4 Нужны ли вам административное восстановление, политики и аудит?
5 Что вы можете развернуть: веб-часть SPFx или клиентское ПО и расширения на каждом устройстве?
6 Что будет с учётными данными, если пользователь потеряет доступ, — можно ли восстановить их в исходной системе?

Подсказка

Как Password Vault защищает данные и кто может получить к ним доступ, описано в статьях KB10452. Как Password Vault защищает ваши данные: шифрование, PIN-код и хранение и KB10456. Кто может видеть ваши пароли в Password Vault. Чтобы попробовать продукт, см. статью KB10438. Как добавить веб-часть Password Vault на страницу и создать хранилище.