СТАТЬЯ БАЗЫ ЗНАНИЙ

Кто может видеть ваши пароли в Password Vault

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

Могут ли коллеги, открывшие ту же страницу, видеть мои пароли? 4

Могут ли участники канала Teams видеть мои пароли? 5

Могут ли владельцы страниц или администраторы сайтов видеть мои пароли? 5

Могут ли администраторы Microsoft 365 или OneDrive видеть мои пароли? 5

Могут ли другие приложения в моей организации получить доступ к файлу хранилища? 6

Может ли Vitextra видеть мои пароли? 6

Что может увидеть человек за моим незаблокированным компьютером? 6

Можно ли намеренно поделиться записью с коллегой? 7

Связанные статьи 7

Обзор

Password Vault хранит записи каждого пользователя в одном зашифрованном файле, *vitextra-password-vault.json*, в папке приложения в собственном OneDrive этого пользователя. Поэтому то, кто может видеть ваши записи, зависит от того, у кого есть доступ к вашему OneDrive и кто может пользоваться вашим компьютером с выполненным входом, — а не от того, кто может открыть страницу. Ниже разобраны типичные случаи.

Кто	Может видеть ваши записи?
Коллеги, открывающие ту же страницу	Нет — они видят свои собственные хранилища
Участники канала Teams с вкладкой Password Vault	Нет — каждый участник видит своё собственное хранилище
Владельцы страниц и администраторы сайтов	Нет — на странице и на сайте ничего не хранится
Администраторы Microsoft 365 / OneDrive	Они могут получить доступ к файлу, как к любому другому файлу в вашем OneDrive, но не могут прочитать записи без PIN-кода; имея копию файла, они могли бы перебрать все 10 000 PIN-кодов в автономном режиме
Vitextra	Нет — Vitextra не получает данных хранилища
Человек за вашим незаблокированным компьютером	Без PIN-кода — ничего, даже названий записей; пока хранилище разблокировано — всё

Могут ли коллеги, открывшие ту же страницу, видеть мои пароли?

Нет. Веб-часть всегда открывает хранилище того, кто выполнил вход. Если десять коллег откроют одну и ту же страницу SharePoint, каждый из них увидит только свои записи, прочитанные из своего OneDrive. Размещение Password Vault на общей странице не открывает доступ ни к каким паролям.

Могут ли участники канала Teams видеть мои пароли?

Нет. Вкладка Password Vault в канале Teams работает так же, как веб-часть на странице: каждый участник канала, открывший вкладку, видит своё собственное хранилище. Это то же хранилище, которое участник видит на страницах SharePoint и в личном приложении. См. KB10457. Как добавить Password Vault в Microsoft Teams.

Могут ли владельцы страниц или администраторы сайтов видеть мои пароли?

Нет. Password Vault ничего не хранит в списках и библиотеках SharePoint или в свойствах веб-части; на странице находятся только сама веб-часть и её заголовок. Владение страницей или сайтом, а также роль администратора семейства сайтов не дают доступа к файлам хранилищ людей, которые пользуются веб-частью.

Могут ли администраторы Microsoft 365 или OneDrive видеть мои пароли?

У Password Vault нет консоли администрирования: администраторы не могут просматривать хранилища, управлять ими, разблокировать или восстанавливать их средствами продукта.

Сам файл хранилища — это обычный файл в вашем OneDrive, защищённый управлением доступом Microsoft 365 и OneDrive. Как и к любому другому файлу в вашем OneDrive, к нему могут получить доступ администраторы, у которых есть доступ к вашему OneDrive или которые предоставляют его себе в соответствии с политиками вашей организации, — например, при расследовании, с помощью средств соответствия требованиям или при передаче OneDrive уволившегося сотрудника. Поля записей в нём зашифрованы ключом, который формируется из вашего PIN-кода и не хранится в файле, поэтому один только доступ к файлу не позволяет администратору прочитать ваши записи. Однако PIN-код состоит всего из 4 цифр: тот, у кого есть доступ к файлу, может скопировать его и перебрать все 10 000 PIN-кодов в автономном режиме. PBKDF2 замедляет каждую попытку подбора, а ограничение в пять попыток действует только внутри веб-части.

Предупреждение

Против того, кто перебирает все PIN-коды на копии файла, 4-значный PIN-код обеспечивает лишь ограниченную защиту, поэтому первым рубежом защиты остаётся управление доступом OneDrive. Password Vault предназначен для личных повседневных учётных данных. Для учётных записей администраторов, служебных учётных записей и других учётных данных с высокими привилегиями или общих учётных данных следуйте политике вашей организации. См. KB10452. Как Password Vault защищает ваши данные: шифрование, PIN-код и хранение.

Могут ли другие приложения в моей организации получить доступ к файлу хранилища?

Хранилище сохраняется с помощью разрешения Microsoft Graph *Files.ReadWrite.AppFolder*. В SharePoint Online это разрешение предоставляется одному приложению, общему для всех решений SharePoint Framework в клиенте, поэтому другие решения SPFx, развёрнутые в вашей организации и использующие то же разрешение, работают с той же папкой приложения от имени вошедшего пользователя. Такое решение может прочитать или изменить файл хранилища; записи в нём зашифрованы ключом, производным от вашего PIN-кода, с ограничением, описанным в предыдущем разделе. Администраторам следует развёртывать только те решения SPFx, которым они доверяют. См. KB10454. Разрешение Microsoft Graph Files.ReadWrite.AppFolder: зачем оно нужно Password Vault и как его утвердить.

Может ли Vitextra видеть мои пароли?

Нет. Шифрование и расшифровка выполняются в вашем браузере, а файл хранилища передаётся только между вашим браузером и вашим OneDrive. Vitextra не получает, не хранит и не создаёт резервных копий данных хранилища, вашего PIN-кода или производного от него ключа. Веб-часть отправляет в Vitextra только технические идентификаторы проверки лицензии и телеметрии использования; см. KB10363. Где продукты Vitextra хранят ваши данные: конфиденциальность, расположение данных и GDPR.

Что может увидеть человек за моим незаблокированным компьютером?

Любой, кто может пользоваться вашим браузером, пока вы вошли в Microsoft 365,

может открыть страницу с Password Vault. **Без PIN-кода** этот человек вообще не видит записей — даже их названий:

- вместо списка веб-часть показывает только запрос **Введите PIN-код**, а на панели инструментов доступна только кнопка **Обновить**;
- пароли, имена пользователей, URL-адреса, папки, теги и заметки не отображаются, а **Создать элемент**, **Сменить PIN-код**, **Поиск**, фильтр и избранное недоступны;
- этот человек может вводить PIN-коды, и каждый неверный PIN-код учитывается в ограничении в пять попыток (см. ниже).

После ввода правильного PIN-кода все действия — показ и копирование паролей, **Создать элемент**, **Изменить**, **Удалить** и **Сменить PIN-код** — выполняются без повторного запроса PIN-кода.

После того как вы ввели PIN-код, хранилище остаётся разблокированным, пока страница открыта и используется: любой человек за компьютером может показывать и копировать пароли и изменять записи, пока не сработает автоматическая блокировка после **5 минут** без действий (см. KB10451. Автоматическая блокировка: когда Password Vault снова запрашивает PIN-код). Скопированный вами пароль также остаётся в буфере обмена, пока не будет скопировано что-то другое.

Человек, который не знает PIN-код, может также вводить неверные PIN-коды. Пять неверных PIN-кодов подряд блокируют хранилище, и единственный выход — сброс, который удаляет все записи (см. KB10455. Неверный PIN-код в Password Vault: что происходит после пяти неудачных попыток).

Подсказка

Блокируйте компьютер каждый раз, когда отходите от него, и задавайте или меняйте PIN-код там, где никто не видит экран: на экранах **Настройка PIN-кода** и **Сменить PIN-код** цифры видны во время ввода (в запросе **Введите PIN-код** они скрыты).

Можно ли намеренно поделиться записью с коллегой?

Нет. Password Vault — это личное хранилище: в нём нет общих записей, общих папок или командных хранилищ. Для учётных данных, которые должны совместно использоваться в команде, следуйте политике вашей организации.

Связанные статьи

- KB10453. Где Password Vault хранит ваши пароли: папка приложения в OneDrive
- KB10452. Как Password Vault защищает ваши данные: шифрование, PIN-код и хранение
- KB10439. Password Vault: часто задаваемые вопросы