vitextra

СТАТЬЯ БАЗЫ ЗНАНИЙ

Как Password Vault защищает ваши данные: шифрование, PIN-код и хранение

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

Кратко 4

Уровень 1: вход в Microsoft 365 и управление доступом OneDrive 5

Уровень 2: шифрование записей в браузере 5

- **Что шифруется и что нет** 6
- **Существующие хранилища обновляются автоматически** 7

Уровень 3: PIN-код и заблокированное хранилище 8

Автоматическая блокировка 9

Ограничение неудачных попыток 9

Никаких данных у Vitextra 10

Для чего предназначен Password Vault 10

Рекомендации 10

Обзор

Password Vault — это личный менеджер паролей для страниц SharePoint Online и Microsoft Teams. Каждый пользователь хранит свои учётные данные в одном зашифрованном файле в собственном OneDrive. В этой статье по уровням объясняется, как защищены данные, что PIN-код делает и чего не делает, какие части хранилища шифруются и для каких учётных данных предназначен Password Vault. Статья адресована как конечным пользователям, которые хотят разобраться в продукте, так и администраторам и специалистам по безопасности, которые его проверяют.

Кратко

Вопрос	Ответ
Где хранится хранилище?	В одном файле, *vitextra-password-vault.json*, в папке приложения в собственном OneDrive пользователя
Кто может открыть файл?	Тот, у кого есть доступ к OneDrive пользователя в соответствии с разрешениями Microsoft 365, — по умолчанию только сам пользователь
Какое удостоверение используется?	Вошедший пользователь Microsoft 365 — через Microsoft Graph с делегированным разрешением *Files.ReadWrite.AppFolder*
Что шифруется?	Текстовые поля каждой записи: название, имя пользователя, пароль, URL-адрес, заметки, папка и теги (AES, в браузере, ключом, производным от PIN-кода)
Что делает PIN-код?	Ключ шифрования формируется из 4-значного PIN-кода; пока PIN-код не введён, веб-часть вообще не показывает записи
Когда PIN-код запрашивается снова?	После 5 минут без действий в веб-части и после перезагрузки страницы

Вопрос	Ответ
Что происходит после неверных PIN-кодов?	После 5 неверных PIN-кодов подряд хранилище блокируется, и его можно только сбросить, что удаляет все записи
Что отправляется в Vitextra?	Никакие данные хранилища; только технические идентификаторы проверки лицензии и телеметрии использования

Уровень 1: вход в Microsoft 365 и управление доступом OneDrive

У Password Vault нет собственных учётных записей, серверов или баз данных. Веб-часть работает в браузере вошедшего пользователя и читает и записывает хранилище через Microsoft Graph от имени этого пользователя. Файл хранится в собственном OneDrive пользователя, поэтому он защищён теми же механизмами, что и любой другой файл в нём: входом в Microsoft 365 (включая многофакторную проверку подлинности и условный доступ, если они используются в вашей организации), разрешениями OneDrive и политиками Microsoft 365 вашей организации.

Веб-часть использует одно делегированное разрешение, *Files.ReadWrite.AppFolder*, которое позволяет ей работать только в папке приложения в OneDrive вошедшего пользователя. Она не может открывать другие файлы пользователя и не может открыть OneDrive другого пользователя. Подробнее см. KB10454. Разрешение Microsoft Graph Files.ReadWrite.AppFolder: зачем оно нужно Password Vault и как его утвердить.

Поскольку хранилище находится в OneDrive пользователя, а не на странице, каждый пользователь, который открывает страницу или вкладку Teams с веб-частью, видит только своё хранилище. Размещение веб-части на общей странице не открывает доступ ни к каким паролям.

Уровень 2: шифрование записей в браузере

Перед сохранением хранилища Password Vault шифрует текстовые поля каждой записи алгоритмом AES. Шифрование и расшифровка выполняются в браузере пользователя; файл передаётся только между браузером и OneDrive пользователя через Microsoft Graph. Поэтому значения никогда не хранятся и не передаются в

виде открытого текста: человек, открывший файл, видит зашифрованные строки вместо названий, имён пользователей и паролей.

Ключ шифрования формируется из PIN-кода в браузере с помощью PBKDF2-SHA256 (Web Crypto) со случайной 16-байтовой солью и 600 000 итераций; новая соль создаётся при каждом задании или смене PIN-кода. Ключ нигде не хранится — ни в файле хранилища, ни в хранилище браузера, ни у Vitextra. Он существует только в памяти открытой страницы, пока хранилище разблокировано. Чтобы проверить PIN-код, веб-часть формирует из него ключ и расшифровывает контрольное значение — известный текст, зашифрованный этим ключом, — которое хранится в файле вместе с солью и числом итераций. Ни PIN-код, ни хеш PIN-кода не хранятся. Поэтому одного файла хранилища недостаточно, чтобы прочитать записи: нужен PIN-код.

Предупреждение

PIN-код состоит всего из 4 цифр, то есть возможны 10 000 комбинаций. PBKDF2 намеренно замедляет каждую попытку подбора, но тот, кто получит копию вашего файла хранилища, всё же может перебрать все PIN-коды в автономном режиме, вне веб-части: ограничение в пять попыток действует только внутри веб-части. Поэтому первым рубежом защиты остаётся управление доступом к вашему OneDrive. Обеспечивайте безопасность своей учётной записи Microsoft 365 и не передавайте никому файл хранилища или папку, в которой он находится.

Что шифруется и что нет

Данные в файле хранилища	Шифруются
Название записи	Да
Имя пользователя	Да
Пароль	Да
URL-адрес	Да
Заметки	Да
Папка	Да
Теги	Да

Данные в файле хранилища	Шифруются
Признак избранного (звёздочка)	Нет
Идентификаторы записей, даты создания и изменения	Нет
Соль, число итераций и контрольное значение (используются для проверки PIN-кода)	Соль и число итераций: нет; контрольное значение — это известный текст, зашифрованный ключом. PIN-код, его хеш и ключ не хранятся
Идентификатор объекта пользователя в Microsoft Entra ID	Нет
Счётчик неудачных попыток ввода PIN-кода	Нет

Ничего не записывается в списки SharePoint, в свойства веб-части или в хранилище браузера. Ключ и расшифрованные значения существуют только в памяти открытой страницы, пока хранилище разблокировано.

Существующие хранилища обновляются автоматически

Хранилища, созданные в более ранних версиях Password Vault, используют прежний формат файла, в котором ключ формировался из хранящегося в файле хеша SHA-256 от PIN-кода и идентификатора объекта пользователя в Microsoft Entra ID. Когда вы впервые вводите правильный PIN-код в новой версии, веб-часть заново шифрует все записи новым ключом, сформированным с помощью PBKDF2, и сохраняет хранилище в новом формате. Записи и даты их изменения сохраняются, а счётчик неудачных попыток сбрасывается. Вам ничего не нужно делать. После обновления файл больше не содержит хеш PIN-кода.

Примечание

Обновление затрагивает только текущий файл хранилища. Более ранние версии файла, которые OneDrive хранит в журнале версий или в корзине, а также копии в системах резервного копирования остаются в прежнем формате, в котором записи можно было расшифровать из самого файла, без PIN-кода. Кто может их открыть, определяется управлением доступом OneDrive и параметрами хранения и резервного копирования вашей организации.

Уровень 3: PIN-код и заблокированное хранилище

PIN-код — это 4-значный код, который пользователь задаёт при создании хранилища (см. KB10442. Как настроить PIN-код в Password Vault). Он нужен один раз, чтобы открыть хранилище: веб-часть проверяет его сразу после ввода четвёртой цифры. До этого хранилище заблокировано, и веб-часть вообще не показывает записи — даже их названия. Вместо списка отображается запрос **Введите PIN-код** с текстом «Введите свой PIN-код, чтобы продолжить» и четырьмя полями для цифр, а на панели инструментов доступна только кнопка **Обновить**.

Действие	**Доступно, пока хранилище заблокировано**
Просмотр списка с названием, именем пользователя, URL-адресом, папкой, тегами и заметками записей	Нет — список скрыт
Показать пароль (кнопка с глазом) или **Скопировать в буфер обмена** для пароля или имени пользователя	Нет
Создать элемент, **Изменить**, **Удалить**	Нет
Сменить PIN-код (шестерёнка **Настройка**)	Нет
Добавить в избранное / **Удалить из избранного**	Нет
Поиск и фильтр	Нет
Обновить	Да

После ввода правильного PIN-кода хранилище разблокируется, и все эти действия выполняются напрямую, без повторного запроса PIN-кода, пока хранилище снова не заблокируется.

Предупреждение

Пока хранилище разблокировано, всё его содержимое, включая пароли, может показать и скопировать любой, кто пользуется вашим компьютером, — до тех пор, пока хранилище снова не заблокируется. Блокируйте компьютер каждый раз, когда отходите от него.

В запросе **Введите PIN-код** цифры при вводе скрываются. На экранах **Настройка PIN-кода** и **Сменить PIN-код** они видны, поэтому задавайте или меняйте PIN-код там, где никто не может видеть ваш экран.

Автоматическая блокировка

После загрузки страницы хранилище заблокировано: записи не показываются, отображается только запрос **Введите PIN-код**. После ввода правильного PIN-кода хранилище открывается и остаётся разблокированным, пока вы работаете. Если в течение **5 минут** внутри веб-части не было ни щелчка, ни нажатия клавиши (действия на экране **Сменить PIN-код** тоже учитываются), хранилище снова блокируется: список исчезает, показанные пароли скрываются, ключ удаляется из памяти, а все открытые диалоговые окна (**Создать элемент**, **Изменить свойства**, подтверждение удаления) закрываются без сохранения. Перезагрузка страницы также блокирует хранилище, потому что разблокированное состояние существует только в открытой странице. См. KB10451. Автоматическая блокировка: когда Password Vault снова запрашивает PIN-код.

Ограничение неудачных попыток

При каждом неверном PIN-коде отображается сообщение «Неверный PIN-код» и число в поле **Осталось попыток**. Счётчик хранится в файле хранилища и всегда увеличивается на основе последней версии файла, поэтому попытки, сделанные на разных устройствах и страницах, надёжно суммируются. Строка **Осталось попыток** отображается в запросе **Введите PIN-код** всякий раз, когда уже были неверные попытки, в том числе после перезагрузки страницы или на другом устройстве. Со временем счётчик не сбрасывается — сбросить его может только правильный PIN-код. После **5** неверных PIN-кодов подряд хранилище блокируется: веб-часть показывает только экран **Сброс**, а сброс удаляет все записи и PIN-код. См. KB10455. Неверный PIN-код в Password Vault: что происходит после пяти неудачных попыток.

Предупреждение

Забытый PIN-код не можете восстановить или сбросить ни вы, ни ваш администратор, ни Vitextra. Запишите PIN-код и храните запись в надёжном месте, а важные учётные данные храните также в другом месте, одобренном вашей организацией. См. KB10460. Забыли PIN-код Password Vault? Что можно сделать.

Никаких данных у Vitextra

Vitextra не получает, не хранит и не создаёт резервных копий данных хранилища. Единственные запросы веб-части к службам Vitextra — это проверка лицензии и телеметрия использования с техническими идентификаторами. Полный список см. в статье KB10363. Где продукты Vitextra хранят ваши данные: конфиденциальность, расположение данных и GDPR.

Для чего предназначен Password Vault

Password Vault задуман как удобное личное место для повседневных учётных данных — входа на веб-порталы, в системы партнёров, тестовых учётных записей и похожих записей, которые пользователь иначе хранил бы в блокноте или текстовом файле. Его защита сочетает управление доступом Microsoft 365 с шифрованием хранимых значений ключом, производным от 4-значного PIN-кода.

Это не система управления привилегированным доступом: в нём нет совместного использования между пользователями, восстановления администратором, собственного журнала аудита и главного пароля высокой стойкости. Для учётных записей администраторов, служебных учётных записей, общих учётных данных команды и других секретов с высокими привилегиями следуйте политике вашей организации и используйте предписанные ею средства. Сравнение с другими подходами см. в статье KB10440. Password Vault, менеджеры паролей в браузерах и корпоративные менеджеры паролей: что выбрать.

Рекомендации

- Защитите свою учётную запись Microsoft 365: хранилище защищено ровно настолько, насколько защищена учётная запись, которой принадлежит OneDrive.
- Выберите PIN-код, который нелегко угадать (избегайте *0000*, *1234* или года своего рождения), и храните его в надёжном месте.
- Не передавайте и не копируйте файл хранилища: тот, у кого есть копия, может перебрать все 10 000 PIN-кодов в автономном режиме.

- Блокируйте компьютер, когда отходите от него, даже ненадолго.
- Скопированный пароль остаётся в буфере обмена, пока вы не скопируете что-то другое; на общих компьютерах очищайте буфер обмена после использования.
- Если вы работаете с хранилищем на нескольких устройствах или вкладках, изменения объединяются автоматически; нажмите **Обновить**, чтобы увидеть изменения, внесённые в другом месте (см. KB10453. Где Password Vault хранит ваши пароли: папка приложения в OneDrive).
- Храните только те учётные данные, которые ваша организация разрешает хранить в личном менеджере паролей.

Подсказка

Чтобы точно узнать, кто может и кто не может видеть ваши записи, см. KB10456. Кто может видеть ваши пароли в Password Vault.