



Безопасное управление
паролями сотрудников

Kaspersky Password Manager для бизнеса

kaspersky

60%

всех утекших паролей можно взломать за час¹

>20%

паролей длиной 15 символов можно взломать за минуту¹



Kaspersky Password Manager для бизнеса

Безопасное управление паролями сотрудников

Современные компании используют десятки корпоративных сервисов, приложений и систем. Управление доступами к ним становится сложной задачей, особенно в условиях распределенной инфраструктуры, удаленной работы и роста числа кибератак, ведь сегодня компрометация учетных данных — самая частая точка входа для атакующих.

Kaspersky Password Manager для бизнеса — это решение для безопасного хранения и использования паролей, документов, кодов второго фактора, ключей доступа и других конфиденциальных данных сотрудников.

Решение помогает снизить риски утечек учетных данных и обеспечить пользователям удобную и безопасную работу с корпоративными сервисами.

Преимущества для бизнеса



Повышение уровня защиты конфиденциальных данных

Снижение риска утечек по причине компрометации учетных данных



Упрощение расследования инцидентов безопасности

Хранение всей истории действий пользователей: экспорт паролей, их обновление и т. д.



Соответствие корпоративным требованиям безопасности

Внедрение и контроль в соответствии с корпоративными политиками управления паролями



Безопасная работа сотрудников с корпоративными сервисами

Удобство использования и минимизация «человеческого фактора»

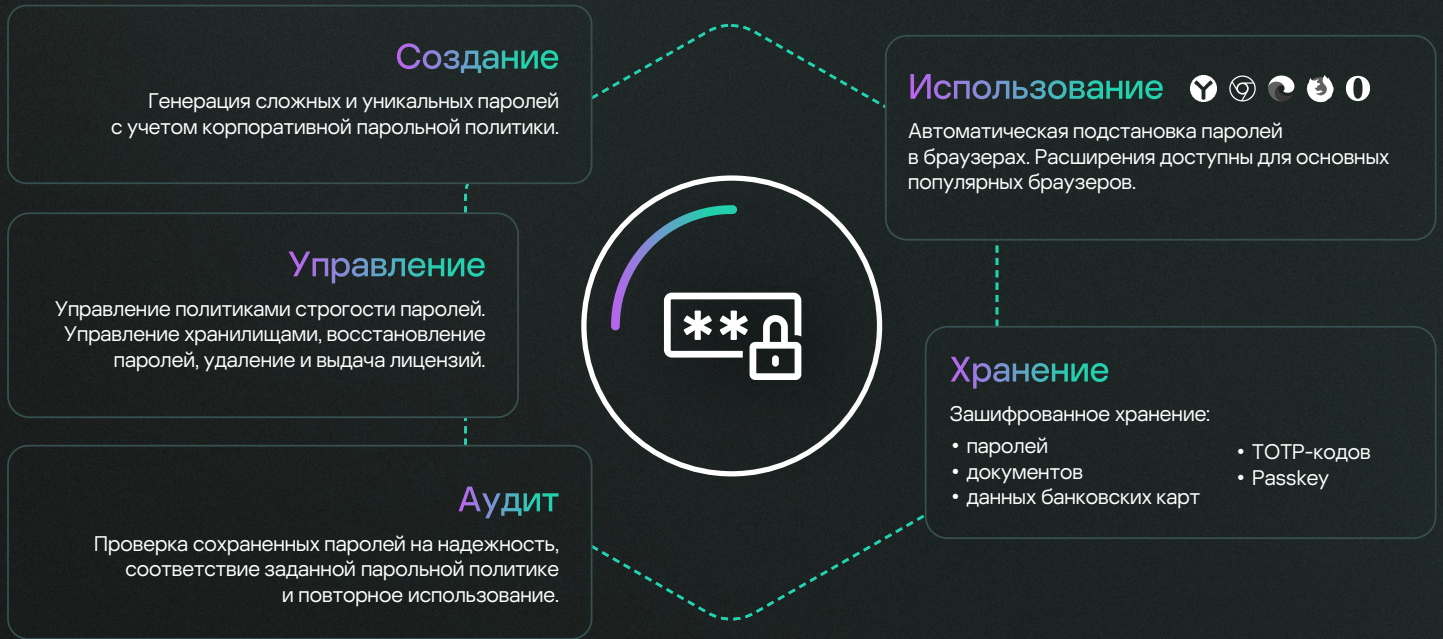


Централизованное управление корпоративными паролями сотрудников

Прозрачность использования доступов, управление правами пользователей и их хранилищами

¹ По данным исследования «Лаборатории Касперского»

Управление жизненным циклом паролей сотрудников



Ключевые преимущества



End-to-end² шифрование по принципу Zero-knowledge³

Данные хранятся в зашифрованном хранилище, доступ к которому имеет только пользователь с мастер-паролем



On-premises⁴ развертывание

Решение развертывается в инфраструктуре организации, таким образом обеспечивая полный контроль над данными



Полнофункциональное клиентское приложение

Локальная обработка и шифрование данных, стабильная работа приложения вне зависимости от браузера, доступ к хранилищу сохраняется даже при потере связи с сервером

2 End-to-end шифрование: метод защиты, при котором информация шифруется прямо на устройстве пользователя до отправки на сервер и расшифровывается только уполномоченным получателем

3 Zero-knowledge: модель хранения данных без доступа провайдера к данным пользователя

4 On-premises развертывание: размещение ПО на собственной инфраструктуре компании



Kaspersky Password Manager для бизнеса

Подробнее

www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

#kaspersky
#активируйбудущее