

?????? ?????

??????

- [Хранение паролей в хэшированном и зашифрованном виде](#)

????????? ??????? ?
????????????????? ?
????????????????????? ???? ?

Зона ответственности: Printum

“ **Коротко:** Printum не хранит пользовательские пароли в открытом виде. Для пользовательских учетных записей применяется хэширование с использованием алгоритма PBKDF2. Пароли и секреты, необходимые для интеграции с внешними системами, хранятся в зашифрованном виде с использованием AES.

????????????

Система должна обеспечивать защиту учетных данных пользователей и технических секретов от компрометации при хранении.

Пароли не должны храниться в открытом виде. В случае получения злоумышленником доступа к базе данных или конфигурационным файлам система должна минимизировать риск раскрытия учетных данных пользователей и параметров подключения к внешним системам.

??? ??? ?????????????? ? Printum

В Printum используются различные механизмы защиты в зависимости от типа учетных данных.

????????????????????? ???????

Пароли пользователей, используемые для входа в систему Printum, не хранятся в открытом виде.

Для хранения пользовательских паролей применяется алгоритм хэширования PBKDF2.

При формировании хэша используются:

- уникальная соль для каждого пароля;
- многократные итерации вычисления хэша.

В процессе аутентификации пароль пользователя сравнивается с сохраненным хэшированным значением.

???????????? ? ? ? ? ? ? ? ?

Для хранения конфиденциальных данных, необходимых для работы системы, используется шифрование.

К таким данным относятся:

- пароли доступа к МФУ;
- учетные данные для подключения к службам каталогов;
- другие параметры интеграции с внешними системами.

Для шифрования используется алгоритм AES в режиме CBC с длиной ключа 128 бит и схемой дополнения PKCS7.

???????????? ? ? ? ? ? ? ? ?

Для пользователей, аутентифицируемых через LDAP или Active Directory, управление паролями осуществляется соответствующей службой каталогов. В этом случае Printum не хранит пароли доменных пользователей.

В системе используются различные механизмы защиты для разных типов учетных данных:

- пользовательские пароли хэшируются;
- технические секреты и параметры интеграции шифруются.

Механизмы хранения и обработки учетных данных определяются архитектурой системы и не требуют дополнительной настройки со стороны администратора.