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

- Использование СКЗИ и ГОСТ-криптографии
- Управление сертификатами
- Шифрование каналов связи

?????????????? ???? ? ????-???????????

Зона ответственности: Заказчик / Интегратор

> **Коротко:** Printum не использует встроенные средства криптографической защиты информации на базе ГОСТ-алгоритмов. При необходимости применения сертифицированных СКЗИ они должны быть реализованы средствами инфраструктуры заказчика.

??????????

В ряде организаций существуют требования по использованию сертифицированных средств криптографической защиты информации и криптографических алгоритмов, соответствующих требованиям регуляторов.

Такие требования могут распространяться на защиту сетевого взаимодействия между пользователями, серверами и компонентами системы.

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

В стандартной поставке Printum не использует встроенные СКЗИ и не реализует криптографические механизмы на базе алгоритмов:

- ГОСТ Р 34.12-2015;
- ГОСТ Р 34.10-2012;
- ГОСТ Р 34.11-2012.

Для защиты сетевого взаимодействия используются стандартные механизмы TLS 1.2 и TLS 1.3.

В зависимости от конфигурации платформы могут использоваться стандартные криптографические алгоритмы:

- AES-GCM;
- ECDHE;

- SHA-256.

Подробная информация о защите сетевых соединений приведена в статье «Шифрование каналов связи».

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

Если в организации требуется применение сертифицированных ФСБ России средств криптографической защиты информации, такие средства должны внедряться на уровне инфраструктуры.

Для защиты сетевого взаимодействия могут использоваться специализированные VPN-шлюзы и иные средства криптографической защиты, развернутые перед компонентами Printum.

Выбор, внедрение и сопровождение СКЗИ выполняются заказчиком или интегратором.

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

Использование СКЗИ не входит в стандартную поставку Printum.

Соответствие требованиям по применению ГОСТ-криптографии определяется используемыми средствами защиты инфраструктуры заказчика.

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

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Printum поддерживает использование сертификатов для защиты сетевых соединений и может работать с сертификатами, выпущенными корпоративным удостоверяющим центром.

??????????

Система должна обеспечивать возможность использования сертификатов для подтверждения подлинности узлов и защиты сетевых соединений.

Использование инфраструктуры открытых ключей позволяет централизованно управлять доверием между компонентами системы.

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

Printum использует сертификаты при организации защищенных соединений по протоколу HTTPS.

В системе могут использоваться:

- самоподписанные сертификаты;
- сертификаты, выпущенные корпоративным удостоверяющим центром;
- сертификаты, выпущенные публичными центрами сертификации.

Администратор может заменить сертификаты, используемые системой, на сертификаты, соответствующие требованиям организации.

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

При использовании корпоративной PKI выпуск, продление, отзыв и контроль сертификатов выполняются средствами удостоверяющего центра организации.

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

Жизненный цикл сертификатов определяется средствами инфраструктуры открытых ключей и не управляется средствами Printum.

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает передачу данных по защищённым каналам связи с использованием HTTPS, TLS и IPPS. Конкретный уровень защиты определяется используемыми сертификатами и настройками инфраструктуры.

??????????

Передаваемые данные должны быть защищены от перехвата, изменения и подмены в процессе передачи по сети.

Использование защищённых каналов связи обеспечивает конфиденциальность и целостность данных при взаимодействии пользователей, компонентов системы и внешних сервисов.

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

Для защиты данных при передаче Printum поддерживает использование защищённых сетевых соединений.

В зависимости от сценария эксплуатации могут использоваться:

- HTTPS для взаимодействия пользователей с веб-интерфейсами системы;
- TLS для взаимодействия с внешними сервисами и интеграциями;
- IPPS для защищённой печати по сети.

При использовании защищённых соединений обеспечиваются:

- шифрование передаваемых данных;
- контроль целостности данных;
- проверка подлинности удалённого узла на основе сертификатов.

Пользовательские интерфейсы системы работают через веб-сервер Nginx и поддерживают использование HTTPS.

Поддерживается HTTP/2.

Для повышения безопасности веб-сессий используются защищённые cookie-файлы и механизмы защиты веб-приложений, включая ограничения SameSite для cookie и защиту от встраивания страниц в сторонние сайты.

Printum поддерживает работу за обратными прокси-серверами и балансировщиками нагрузки, передающими информацию о защищённом соединении через стандартные HTTP-заголовки.

Printum поддерживает использование сертификатов, выпущенных корпоративным удостоверяющим центром, доверенным центром сертификации или созданных самостоятельно в соответствии с требованиями организации.

Подробная информация о сертификатах приведена в статье «Управление сертификатами (PKI / CA)».

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

Настройка сертификатов, параметров TLS и политик сетевой безопасности выполняется администраторами инфраструктуры заказчика.

При использовании корпоративной инфраструктуры открытых ключей выпуск, продление и отзыв сертификатов выполняются средствами удостоверяющего центра организации.