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

База знаний по информационной безопасности Printum. Требования, реализация, ограничения.

- Антивирусная защита
  - Совместимость с антивирусным ПО
- Журналирование
  - Атрибутный состав записи в журнале
  - Аудит действий администраторов
  - Журналы без чувствительных данных
  - Защита журналов от изменения и доступ к журналам
  - Мониторинг и анализ событий безопасности
  - Передача событий в SIEM
  - Перечень регистрируемых событий безопасности
  - Синхронизация времени (NTP)
- Защита среды исполнения
  - Мандатное управление доступом
  - Профили безопасности
- Защита учетных данных
  - Хранение паролей в хэшированном и зашифрованном виде
- Контейнеры
  - Rootless режим контейнера
  - Отсутствие SUID-SGID файлов и утилит повышения привилегий
  - Соответствие рекомендациям CIS Benchmark

    - Фиксированные теги контейнерных образов
    - Хранение секретов в контейнерных образах

- Контроль целостности
    - Контроль целостности ПО и конфигурационных файлов

- Резервное копирование
    - Механизмы резервного копирования и восстановления

- Сетевая безопасность
    - Использование небезопасных сетевых протоколов
    - Сегментация сети и зоны безопасности

- Управление доступом
    - Анонимный доступ запрещён
    - Блокировка и управление учётными записями
    - Доменная аутентификация и единый вход (SSO)
    - Идентификация и аутентификация пользователей
    - Парольная политика
    - Ролевая модель RBAC
    - Тайм-аут сессии и автоматическое завершение сеанса
    - Технические учётные записи

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

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

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

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Printum совместим с корпоративными антивирусными решениями, включая Kaspersky Endpoint Security for Linux и Dr.Web. Для корректной работы системы рекомендуется настроить исключения для каталогов хранения данных, контейнеров и спулеров печати.

??????????

Система должна обеспечивать корректную работу в инфраструктуре, где используются корпоративные средства антивирусной защиты и защиты от вредоносного программного обеспечения.

Антивирусная защита не должна нарушать работу компонентов системы, приводить к потере данных или блокировать штатные процессы обработки заданий печати и мониторинга.

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

Совместимость Printum с антивирусным программным обеспечением подтверждена для следующих решений:

- Kaspersky Endpoint Security for Linux;
- Dr.Web.

Клиент ПМ для Windows совместим с антивирусными решениями, используемыми на рабочих станциях пользователей.

Для обеспечения стабильной работы системы рекомендуется настроить исключения антивирусного сканирования для следующих объектов:

- каталогов хранения контейнеров Docker (/var/lib/docker или /var/lib/containers в зависимости от используемого контейнерного рантайма);
- каталогов хранения заданий ПринтМенеджера;
- каталогов спулера печати CUPS.

Настройка исключений позволяет избежать влияния антивирусного сканирования на производительность системы и обработку заданий печати.

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

Установка, сопровождение и настройка антивирусного программного обеспечения выполняются администраторами инфраструктуры заказчика.

При внедрении антивирусной защиты рекомендуется настроить исключения для каталогов и сервисов, используемых компонентами Printum.

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

На момент подготовки документа продолжается процесс включения компонентов Printum в AllowList Kaspersky.

Актуальный статус включения в AllowList и перечень подтверждённых версий антивирусного программного обеспечения рекомендуется уточнять у службы поддержки Printum.

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

Журналирование

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

Зона ответственности: Printum

> **Коротко:** Каждая запись журнала информационной безопасности Printum содержит сведения о времени события, субъекте, объекте, типе операции, результате выполнения и других атрибутах, необходимых для расследования инцидентов и передачи событий во внешние системы мониторинга.

??????????

Система должна обеспечивать регистрацию событий безопасности с сохранением информации, достаточной для расследования инцидентов, анализа действий пользователей и последующей корреляции событий во внешних системах мониторинга.

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

Для каждого зарегистрированного события безопасности в журнале информационной безопасности сохраняется следующий набор атрибутов:

Атрибут	Содержание
Время события (UTC)	Дата и время регистрации события
Группа события	Категория события безопасности
Тип события	Конкретное зарегистрированное событие
Уникальный идентификатор события	Уникальный код события
Тип операции	Выполненное действие (создание, изменение, удаление, авторизация и др.)
Субъект операции	Пользователь, выполнивший действие
IP-адрес субъекта	Сетевой адрес источника события

Объект операции	Объект, над которым выполнялось действие
Идентификатор объекта	Адрес или идентификатор объекта операции
Компонент системы	Наименование и версия компонента Printum
Результат операции	Успешное или неуспешное выполнение действия
Изменённые параметры	Старые и новые значения изменённых данных
Дополнительная информация	Диагностическая информация и сведения об ошибках
Метод запроса	Используемый HTTP-метод
Уровень важности	Критичность события безопасности

Совокупность указанных атрибутов позволяет определить источник события, объект воздействия, характер выполненной операции, результат её выполнения и изменения, внесённые в систему, что обеспечивает возможность расследования инцидентов и последующей корреляции событий безопасности.

В журнале фиксируются операции создания, изменения, удаления, просмотра, аутентификации, авторизации, установки, удаления, синхронизации и другие действия пользователей и компонентов системы.

Атрибутный состав записи соответствует требованиям ГОСТ Р 59548-2022 к журналированию событий безопасности и используется для поиска событий, расследования инцидентов, формирования отчётов и передачи событий во внешние системы мониторинга и SIEM.

Журналирование

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum обеспечивает регистрацию действий администраторов и других привилегированных пользователей в журнале информационной безопасности. Журнал позволяет определить, кто, когда и какие изменения выполнял в системе.

??????????

Система должна обеспечивать контроль действий пользователей с административными полномочиями.

Регистрация административных действий позволяет расследовать инциденты, контролировать изменения настроек системы и обеспечивать персональную ответственность пользователей с расширенными правами доступа.

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

Действия администраторов и других пользователей, обладающих соответствующими полномочиями, регистрируются в журнале информационной безопасности Printum.

Журналируются операции:

- создания объектов системы;
- изменения настроек;
- удаления объектов;
- изменения параметров безопасности;
- управления пользователями и ролями;
- управления интеграциями;
- архивирования и восстановления журнала информационной безопасности;
- другие административные операции.

Для каждого события сохраняются сведения о пользователе, времени выполнения операции, результате выполнения, источнике подключения и изменённых параметрах.

При регистрации изменений значений параметров фиксируются предыдущие и новые значения изменённых данных. Конфиденциальные значения, такие как пароли и секреты доступа, не отображаются в открытом виде.

Для отдельных объектов системы дополнительно используется механизм контроля изменений, позволяющий сохранять историю изменений объектов.

Доступ к журналу информационной безопасности предоставляется только пользователям, которым назначено соответствующее право доступа.

Подробная информация о составе записи журнала приведена в статье «Атрибутный состав записи в журнале».

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

Для централизованного мониторинга действий администраторов события безопасности могут передаваться во внешнюю SIEM или SOC.

Подробная информация приведена в статье «Передача событий в SIEM».

Журналирование

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

Зона ответственности: Printum

> **Коротко:** Журналы Printum могут содержать сведения о пользователях, необходимые для аудита и расследования инцидентов, однако не содержат паролей, токенов доступа и других секретных данных в открытом виде.

??????????

Система должна обеспечивать регистрацию событий безопасности и действий пользователей без раскрытия конфиденциальной информации, способной привести к компрометации системы или учетных записей.

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

Журналы системы используются для регистрации действий пользователей, административных операций, событий безопасности и работы компонентов системы.

Для обеспечения возможности аудита и расследования инцидентов журналы могут содержать сведения о пользователях и объектах системы, включая:

- имя пользователя;
- логин пользователя;
- другие сведения, необходимые для идентификации источника события.

При этом в журналах не сохраняются в открытом виде:

- пароли пользователей;
- сервисные пароли;
- токены доступа;
- криптографические ключи;

- иные секретные данные, используемые для аутентификации или доступа к внешним системам.

При аутентификации пользователей пароли не записываются в журналы событий.

Для хранения пользовательских паролей используется хэширование, а для хранения технических секретов и параметров интеграции применяется шифрование.

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

Зона ответственности: Printum

> **Коротко:** Доступ к журналу информационной безопасности определяется назначенной пользователю ролью. Записи журнала не могут редактироваться через интерфейс системы. Выгрузка журнала выполняется в защищённый архив, который может быть загружен только в тот же экземпляр Printum, из которого был выгружен.

??????????

Система должна ограничивать доступ к журналам безопасности и предотвращать несанкционированное изменение зарегистрированных событий.

Доступ к журналам должен предоставляться только уполномоченным пользователям, а зарегистрированные события должны сохранять свою целостность.

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

Доступ к журналу информационной безопасности контролируется ролевой моделью Printum.

Доступ к журналу предоставляется только после успешной аутентификации пользователя.

Записи журнала информационной безопасности не могут редактироваться через интерфейс системы.

Журнал информационной безопасности может быть выгружен в архив. Выгруженный архив шифруется и предназначен для загрузки только в тот же экземпляр Printum, из которого был выгружен.

Такой архив нельзя открыть как обычный файл или загрузить в другой экземпляр Printum.

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

При наличии административного доступа к серверам системы доступ к данным журналов может быть получен средствами операционной системы и используемых компонентов инфраструктуры.

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum обеспечивает регистрацию событий безопасности и их передачу во внешние системы мониторинга. Обнаружение, корреляция и анализ инцидентов информационной безопасности выполняются средствами SIEM или SOC заказчика.

?????????

Система должна обеспечивать возможность мониторинга событий безопасности, анализа действий пользователей и расследования инцидентов информационной безопасности.

Для обнаружения инцидентов необходимо получать сведения о событиях безопасности, произошедших в системе, а также обеспечивать возможность их последующего анализа и корреляции.

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

Printum ведёт журнал информационной безопасности и регистрирует события, связанные с аутентификацией пользователей, изменением настроек системы, управлением учётными записями, изменением ролей и другими действиями, влияющими на безопасность системы.

Для каждого события сохраняется набор атрибутов, достаточный для анализа и расследования инцидентов. Состав записи журнала описан в статье «Атрибутный состав записи в журнале».

Printum поддерживает передачу событий безопасности во внешние системы мониторинга и управления событиями безопасности (SIEM). Подробная информация приведена в статье «Передача событий в SIEM».

Средства корреляции событий, автоматического обнаружения инцидентов, управления инцидентами и автоматизированного реагирования в состав Printum не входят.

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

Обнаружение, идентификация и корреляция инцидентов информационной безопасности выполняются средствами SIEM, SOC или других систем мониторинга безопасности, используемых заказчиком.

Для повышения эффективности мониторинга рекомендуется разрабатывать правила корреляции и сценарии реагирования с учётом перечня регистрируемых событий безопасности и требований службы информационной безопасности организации.

Журналирование

???????? ???????? ? SIEM

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Printum поддерживает передачу событий безопасности во внешние SIEM и системы мониторинга по протоколу Syslog, включая TCP, UDP и TCP с TLS. Передача выполняется только в исходящем направлении.

??????????

Система должна обеспечивать возможность передачи событий безопасности во внешние системы мониторинга, корреляции событий и расследования инцидентов.

Передаваемые события должны содержать достаточный объём информации для анализа событий безопасности и интеграции с корпоративным SOC или SIEM.

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

Printum поддерживает передачу событий безопасности во внешние системы мониторинга и управления событиями безопасности (SIEM).

Для передачи событий поддерживаются следующие механизмы:

- Syslog по UDP;
- Syslog по TCP;
- Syslog по TCP с TLS.

Для защищённого соединения может использоваться проверка сертификатов и TLS-шифрование канала связи.

Параметры подключения к внешней системе настраиваются через панель администратора Мониторинга, включая адрес назначения и используемый порт.

Передаваемые события могут фильтроваться по следующим параметрам:

- диапазон дат;
- типы событий;

- группы событий;
- результаты выполнения операций;
- уровень важности событий;
- локации.

Состав передаваемых событий соответствует атрибутному составу журнала информационной безопасности Printum и описан в статье «Атрибутный состав записи в журнале».

Для контроля передачи событий система ведёт учёт успешно и неуспешно переданных сообщений, а также отслеживает прогресс выгрузки событий.

При временной недоступности внешней системы события накапливаются и передаются после восстановления соединения.

Передача событий выполняется только в исходящем направлении. Приём данных через данный механизм не осуществляется.

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

Заказчик обеспечивает доступность и настройку внешней SIEM или иной системы мониторинга безопасности.

Для использования защищённого соединения по TLS должны быть настроены необходимые сертификаты и параметры доверия между системами.

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

Зона ответственности: Printum

> **Коротко:** Printum регистрирует события аутентификации, авторизации, управления пользователями, изменения конфигурации, административных операций и другие события безопасности. В текущих версиях системы журналируется несколько сотен типов событий.

??????????

Система должна обеспечивать регистрацию событий безопасности, достаточных для расследования инцидентов, контроля действий пользователей и администраторов, а также последующего анализа событий безопасности.

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

Printum ведёт журнал информационной безопасности и регистрирует события, связанные с действиями пользователей, администраторов и компонентов системы.

В журнале регистрируются события следующих категорий.

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

- аутентификация по логину и паролю;
- аутентификация через SAML;
- аутентификация через Kerberos;
- авторизация на МФУ;
- авторизация по карте доступа;
- импорт карт доступа;
- создание и завершение пользовательских сессий;
- управление пользовательскими сессиями.

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

- блокировка пользователя после неуспешных попыток входа;
- ручная блокировка и разблокировка пользователей;
- истечение срока действия пароля;
- попытки доступа к административному интерфейсу без авторизации.

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

- создание, изменение и удаление пользователей;
- управление группами пользователей;
- изменение ролей;
- изменение ролевой модели;
- изменение паролей;
- настройка PIN-кодов.

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

- изменение параметров безопасности;
- изменение парольных политик;
- изменение настроек доменной авторизации;
- изменение настроек интеграций;
- изменение параметров мониторинга;
- изменение групп устройств;
- изменение системных настроек и правил обработки данных.

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

- просмотр журнала информационной безопасности;
- архивирование журнала;
- восстановление данных из архива.

??????

- просмотр отчётов;
- сохранение отчётов.

Полный перечень регистрируемых событий определяется версией системы и может расширяться по мере развития функциональности Printum.

Для каждого события сохраняется набор атрибутов, описанный в статье «Атрибутный состав записи в журнале».

Регистрация событий выполняется через встроенные механизмы аудита системы. Создание записей журнала в обход зарегистрированных механизмов аудита архитектурой системы не предусматривается.

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

Количество и состав регистрируемых событий может отличаться в зависимости от версии системы и используемых компонентов Printum.

?????????????? ??????? (NTP)

Зона ответственности: Заказчик / Интегратор

> **Коротко:** Printum использует системное время серверов для формирования временных меток событий. Синхронизация времени хостов с корпоративным NTP-сервером выполняется средствами операционной системы и инфраструктуры заказчика.

??????????

Система должна обеспечивать корректную регистрацию времени событий безопасности.

Единое системное время необходимо для сопоставления событий между компонентами Printum, внешними системами мониторинга, SIEM и другими элементами инфраструктуры.

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

Printum использует системное время сервера для формирования временных меток событий.

Все временные метки хранятся с указанием временной зоны. Для событий информационной безопасности используются временные метки, формируемые на основании текущего времени сервера.

При передаче событий во внешние системы временные метки сериализуются в формате ISO 8601.

Точность хранения временных меток обеспечивается используемой программной платформой и базой данных и составляет до микросекунд.

Все контейнеры Мониторинга и ПринтМенеджера используют системное время хоста, на котором они запущены.

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

Printum не управляет NTP-службой операционной системы и не выполняет синхронизацию времени самостоятельно.

Синхронизация системного времени серверов, на которых работают компоненты Printum, выполняется средствами инфраструктуры заказчика.

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

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает работу в средах, использующих мандатное управление доступом на базе SELinux. Ограничения доступа процессов реализуются средствами операционной системы и профилей безопасности.

??????????

Система должна обеспечивать возможность эксплуатации в средах, использующих мандатное управление доступом.

Мандатное управление доступом позволяет ограничивать действия процессов независимо от полномочий пользователя и предотвращать выполнение несанкционированных операций.

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

Поддержка мандатного управления доступом реализуется за счёт использования SELinux и специализированных профилей безопасности для компонентов Printum.

При использовании SELinux в режиме Enforcing процессы Мониторинга, ПринтМенеджера и Агентов работают в соответствии с установленными политиками безопасности и могут выполнять только разрешённые действия.

Ограничения доступа определяются профилями безопасности и контролируются средствами операционной системы.

Такой подход позволяет реализовать принцип:

> “ запрещено всё, что явно не разрешено политикой безопасности.

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

Для использования мандатного управления доступом необходимо:

- использовать операционную систему с поддержкой SELinux;
- включить SELinux;
- установить профили безопасности Printum;
- использовать режим Enforcing.

Настройка и сопровождение SELinux выполняются администраторами инфраструктуры заказчика.

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

Мандатное управление доступом обеспечивается средствами операционной системы и не функционирует при отключённом SELinux.

Защита среды исполнения

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает использование профилей безопасности SELinux для ограничения доступа компонентов системы к ресурсам операционной системы. Профили поставляются отдельно и предназначены для эксплуатации в инфраструктурах с повышенными требованиями информационной безопасности.

??????????

Система должна обеспечивать возможность ограничения доступа процессов к ресурсам операционной системы и выполнять только разрешённые действия.

Применение профилей безопасности позволяет снизить последствия ошибок конфигурации, эксплуатации уязвимостей и компрометации отдельных компонентов системы.

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

Для эксплуатации в защищённых контурах поставляются профили безопасности на базе SELinux.

Профили реализованы в виде SELinux-модулей и обеспечивают контроль доступа компонентов Printum к ресурсам операционной системы.

В комплект поставки входят следующие SELinux-модули:

- **printum_global** — общие правила безопасности для Мониторинга и ПринтМенеджера;
- **printum_agent** — профиль Агента Мониторинга;
- **printum_m_install** — профиль установки, обновления и восстановления Мониторинга;
- **printum_pm_install** — профиль установки, обновления и восстановления ПринтМенеджера.

Профили устанавливаются до развёртывания системы и применяются средствами SELinux.

Работа профилей предполагает использование режима SELinux Enforcing, при котором разрешены только действия, явно предусмотренные политиками безопасности.

Профили реализуют принцип минимально необходимых привилегий: компонентам Printum предоставляется доступ только к тем ресурсам операционной системы, которые требуются для их работы.

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

Для использования профилей безопасности необходимо:

- использовать операционную систему с поддержкой SELinux;
- включить SELinux;
- использовать режим Enforcing.

Установка и сопровождение профилей выполняются администраторами инфраструктуры заказчика.

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

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

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.

??????????

Rootless ????? ???????????

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Основные контейнеры Printum запускаются от непривилегированных пользователей и не требуют запуска процессов внутри контейнера от root. Поддержка rootless-режима контейнерного рантайма зависит от используемой инфраструктуры.

???????????

Контейнеры не должны запускать прикладные процессы с привилегиями суперпользователя без необходимости.

Использование непривилегированных пользователей снижает риск повышения привилегий и ограничивает последствия компрометации контейнера.

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

Основные контейнерные образы Printum используют непривилегированных пользователей для запуска сервисов.

Базовые образы создают пользователя **printum** с идентификатором пользователя, отличным от root. В Dockerfile компонентов явно задаётся запуск процессов от непривилегированного пользователя:

- Мониторинг — пользователь printum;
- ПринтМенеджер — пользователь printum;
- File Server ПринтМенеджера — пользователь printum;
- Nginx ПринтМенеджера — пользователь nginx;
- PostgreSQL — пользователь postgres.

Для доступа к подсистеме печати пользователь printum в контейнерах ПринтМенеджера дополнительно включается в группу lp.

Базовые инфраструктурные образы Printum используют rootless-варианты образов, включая PostgreSQL, ClickHouse, Redis и Nginx.

Контейнеры Printum не требуют запуска в privileged-режиме. Дополнительные Linux capabilities через cap_add не используются.

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

Использование rootless-режима контейнерного рантайма определяется используемой инфраструктурой и средствами контейнеризации заказчика.

При необходимости эксплуатации в режиме Podman Rootless или аналогичных сценариях настройка контейнерного рантайма выполняется администраторами инфраструктуры заказчика.

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

В текущей версии отдельные служебные компоненты (CUPS и Mailcatcher) используют образы, для которых rootless-варианты ещё не реализованы.

Для основных компонентов Printum запуск процессов от непривилегированных пользователей обеспечивается штатно.

?????????? SUID-SGID ?????? ? ?????? ?????????? ??????????

Зона ответственности: Printum

Коротко: Контейнерные образы Printum не содержат файлов с установленными битами SUID/SGID и не включают утилиты повышения привилегий, позволяющие получить дополнительные права внутри контейнера.

??????????

Контейнерные образы не должны содержать механизмы, позволяющие повысить привилегии процесса или пользователя внутри контейнера.

Удаление SUID/SGID-файлов и утилит повышения привилегий снижает риск несанкционированного получения дополнительных полномочий при компрометации контейнера.

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

При сборке производственных контейнерных образов Printum выполняется удаление файлов с установленными битами SUID и SGID.

Аналогичная обработка применяется для основных компонентов системы:

- Мониторинг;
- ПринтМенеджер;
- File Server ПринтМенеджера;
- CUPS.

Дополнительно из образов удаляются утилиты повышения привилегий, включая su.

Такой подход исключает использование механизмов повышения привилегий через SUID/SGID-бинарники и ограничивает возможности получения дополнительных прав внутри

контейнера.

Удаление выполняется на этапе сборки образов и входит в стандартный процесс подготовки production-версий контейнеров.

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

Printum обеспечивает:

- отсутствие файлов с установленными битами SUID и SGID в производственных образах;
- отсутствие утилит повышения привилегий;
- соответствие принципу минимально необходимых привилегий для контейнерных компонентов.

????????????? ?????????????? CIS Benchmark

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum реализует ряд рекомендаций CIS Benchmark для контейнерных сред, включая использование непривилегированных пользователей, удаление SUID/SGID-файлов, применение профилей безопасности SELinux и отказ от хранения секретов внутри контейнерных образов.

??????????

Контейнерная платформа должна соответствовать рекомендациям по безопасной настройке и эксплуатации контейнерных сред.

Рекомендации CIS Benchmark направлены на снижение рисков компрометации контейнеров, ограничения привилегий процессов и обеспечение безопасного развёртывания приложений.

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

В составе контейнерной платформы Printum реализованы следующие меры безопасности:

- использование непривилегированных пользователей внутри контейнеров;
- отказ от запуска контейнеров в privileged-режиме;
- отсутствие дополнительных Linux capabilities через cap_add;
- удаление SUID/SGID-файлов и утилит повышения привилегий;
- применение профилей безопасности SELinux;
- отсутствие встроенных секретов, паролей и токенов в контейнерных образах;
- использование фиксированных версий контейнерных образов.

Подробная информация приведена в соответствующих статьях раздела «Контейнеры».

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

Часть рекомендаций CIS Benchmark относится к настройке контейнерной платформы и инфраструктуры заказчика.

К таким настройкам относятся:

- параметры контейнерного рантайма;
- ограничения CPU и памяти;
- использование read-only файловых систем контейнеров;
- аудит операционной системы;
- сканирование контейнерных образов;
- настройки оркестратора контейнеров.

Настройка указанных механизмов выполняется администраторами инфраструктуры заказчика.

Контейнеры

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum использует контейнерные образы с фиксированными версиями компонентов. Теги latest для production-образов не используются.

??????????

Контейнерные образы должны использовать фиксированные версии компонентов, обеспечивающие воспроизводимость развёртывания и возможность контроля изменений между версиями.

Использование фиксированных тегов позволяет исключить непредсказуемое изменение состава программного обеспечения при повторном развёртывании системы.

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

Production-образы Printum собираются на основе контейнерных образов с фиксированными версиями.

Для основных компонентов используются версии, явно указанные в Dockerfile и конфигурации сборки.

Контейнерные образы публикуются с версионными тегами, позволяющими однозначно определить используемую версию программного обеспечения.

Фиксация версий обеспечивает воспроизводимость сборок и упрощает контроль изменений при обновлении системы.

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

Размещение контейнерных образов во внутреннем реестре организации, включая Nexus или иные корпоративные registry, определяется требованиями и политиками заказчика.

Организация хранения, репликации и контроля доступа к реестру контейнерных образов выполняется средствами инфраструктуры заказчика.

Контейнеры

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

Зона ответственности: Printum

Коротко: Контейнерные образы Printum не содержат встроенных паролей, токенов, ключей API и других аутентификационных данных. Конфиденциальные параметры передаются в контейнеры во время запуска через переменные окружения.

??????????

Контейнерные образы не должны содержать аутентификационные данные, токены доступа, пароли и иные секреты в открытом виде.

Секреты должны передаваться в приложение отдельно от образа контейнера и не входить в состав публикуемых артефактов.

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

Production-образы Мониторинга и ПринтМенеджера не содержат встроенных паролей, токенов, ключей API и иных аутентификационных данных.

При сборке образов в них не копируются файлы конфигурации, содержащие секреты, включая файлы переменных окружения и ключи доступа.

Конфиденциальные параметры передаются контейнерам во время запуска через переменные окружения, определяемые в файлах конфигурации развертывания.

Для production-развертывания используются файлы .env, подключаемые средствами контейнерной платформы. В образах отсутствуют встроенные значения паролей баз данных, токенов интеграций и иных учётных данных.

Контейнерные образы публикуются отдельно от конфигурации конкретного заказчика и могут использоваться в различных инсталляциях без хранения индивидуальных секретов внутри образа.

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

Управление секретами, защита файлов конфигурации и контроль доступа к переменным окружения выполняются средствами инфраструктуры заказчика.

Конкретный способ хранения и передачи секретов определяется правилами эксплуатации и требованиями информационной безопасности организации.

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

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum выполняет контроль целостности поставляемого программного обеспечения при установке и использует контрольные суммы для проверки критически важных данных. Для проверки дистрибутива применяется алгоритм SHA-512.

??????????

Система должна обеспечивать возможность проверки целостности программного обеспечения и критически важных данных для выявления фактов повреждения или несанкционированного изменения.

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

При установке Printum автоматически выполняется проверка контрольной суммы скачанного дистрибутива.

Для контроля целостности используется алгоритм SHA-512. Контрольная сумма полученного архива сравнивается с эталонным значением. Установка допускается только после успешного завершения проверки целостности.

Контроль целостности архивов журнала информационной безопасности реализован с использованием алгоритма SHA-256. Для каждого архива сохраняется контрольная сумма, которая используется при последующей проверке целостности данных.

Контейнерные компоненты Printum поставляются в виде версионируемых образов с фиксированными версиями компонентов. Контрольные суммы контейнерных образов могут использоваться средствами реестра образов для проверки их неизменности.

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

Контроль целостности контейнерных образов при эксплуатации выполняется средствами используемого реестра образов и процессов сопровождения инфраструктуры заказчика.

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

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum включает встроенные средства резервного копирования и восстановления данных Мониторинга и ПринтМенеджера. Резервное копирование выполняется с использованием штатных скриптов, а процедуры восстановления описаны в эксплуатационной документации.

???????????

Система должна обеспечивать возможность создания резервных копий и восстановления работоспособности после сбоев, ошибок эксплуатации или отказов оборудования.

Резервное копирование позволяет сохранить критически важные данные системы и обеспечить их последующее восстановление.

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

Для Мониторинга и ПринтМенеджера предусмотрены штатные скрипты резервного копирования и восстановления.

В состав поставки входят:

- скрипты резервного копирования Мониторинга;
- скрипты восстановления Мониторинга;
- скрипты резервного копирования ПринтМенеджера;
- скрипты восстановления ПринтМенеджера.

При выполнении резервного копирования могут сохраняться:

- данные PostgreSQL;
- данные ClickHouse (в Мониторинге);

- данные Redis;
- файлы конфигурации системы;
- файлы параметров окружения (.env);
- конфигурация Nginx и HAProxy;
- данные ПринтМенеджера, включая задания печати и архивные данные.

Если параметры окружения хранятся в зашифрованном виде, их резервные копии также сохраняются в зашифрованном виде.

Процедуры восстановления системы документированы и входят в комплект эксплуатационной документации.

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

Периодичность резервного копирования определяется администратором системы и может быть организована средствами операционной системы, например через планировщик задач cron.

Хранение резервных копий на отдельных носителях, репликация резервных копий на резервную площадку, разграничение доступа к резервным копиям и регулярная проверка возможности восстановления выполняются средствами инфраструктуры и организационными процедурами заказчика.

При необходимости резервное копирование Printum может быть дополнено средствами резервного копирования, используемыми в инфраструктуре заказчика, включая снапшоты виртуальных машин, системы резервного копирования и средства аварийного восстановления.

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

Printum предоставляет механизмы создания резервных копий и восстановления данных, но не содержит встроенного централизованного сервера резервного копирования и не управляет политиками хранения резервных копий.

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

Сетевая безопасность

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum использует современные сетевые протоколы и поддерживает защищённые варианты передачи данных. Отдельные небезопасные протоколы могут использоваться при взаимодействии с оборудованием, возможности которого ограничены производителем устройства.

???????????

Система не должна требовать использования небезопасных сетевых протоколов при эксплуатации в защищённой инфраструктуре.

При наличии альтернатив предпочтение должно отдаваться защищённым протоколам передачи данных.

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

Пользовательские интерфейсы Printum работают по HTTPS.

Для отправки уведомлений по электронной почте поддерживается использование SMTP с TLS.

Для интеграции с каталогами пользователей поддерживается использование LDAPS.

Сетевой агент поддерживает работу по протоколам SNMPv1, SNMPv2c и SNMPv3. Конкретная версия протокола определяется настройками устройства и требованиями инфраструктуры заказчика.

При взаимодействии с устройствами печати могут использоваться различные протоколы передачи данных в зависимости от возможностей конкретной модели устройства.

Для отдельных моделей МФУ может использоваться FTP при получении результатов сканирования, если устройство не поддерживает альтернативные способы передачи

данных.

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

Выбор допустимых протоколов и ограничение использования отдельных протоколов выполняются в соответствии с политиками информационной безопасности организации.

При наличии поддержки со стороны оборудования рекомендуется использовать защищённые варианты сетевого взаимодействия.

Сетевая безопасность

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

Зона ответственности: Заказчик / Интегратор

Коротко: Printum поддерживает развёртывание в сегментированных сетях и не требует размещения всех компонентов в одном сетевом сегменте. Разделение компонентов по зонам безопасности определяется архитектурой инфраструктуры заказчика.

?????????

Система должна поддерживать эксплуатацию в инфраструктурах, использующих разделение на зоны безопасности и сетевые сегменты.

Сегментация сети позволяет ограничивать сетевое взаимодействие между компонентами и снижать последствия возможных инцидентов безопасности.

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

Архитектура Printum допускает размещение компонентов системы в различных сетевых сегментах.

Мониторинг и ПринтМенеджер могут размещаться в разных сегментах сети и взаимодействовать через документированные сетевые порты.

Поддерживается филиальная архитектура, при которой несколько экземпляров ПринтМенеджера располагаются в различных филиалах и взаимодействуют с централизованным Мониторингом.

Возможны различные варианты развёртывания системы, включая использование балансировщиков нагрузки, выделенных серверов приложений и распределённой инфраструктуры.

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

Определение зон безопасности, настройка межсетевых экранов, маршрутизации, DMZ и правил сетевого взаимодействия выполняются средствами инфраструктуры заказчика.

При внедрении предоставляется перечень используемых портов и схема сетевого взаимодействия компонентов системы.

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

Управление доступом

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

Зона ответственности: Printum

> **Коротко:** Доступ к функциям и данным Printum предоставляется только после успешной аутентификации пользователя. Анонимный доступ к защищенным ресурсам системы не допускается.

??????????

Система должна исключать возможность доступа неавторизованных пользователей к функциям, данным и административным интерфейсам.

Пользователь должен пройти процедуру аутентификации до получения доступа к защищенным ресурсам системы.

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

Доступ к Личному кабинету, панели администрирования и другим защищенным разделам системы предоставляется только после успешной аутентификации пользователя.

При обращении к защищенным ресурсам система выполняет проверку подлинности пользователя и его полномочий.

После успешной аутентификации права пользователя определяются назначенной ролью и действующей моделью разграничения доступа.

При завершении пользовательской сессии или истечении срока её действия доступ к защищенным функциям прекращается до повторной аутентификации пользователя.

Для интеграционных взаимодействий используются механизмы аутентификации и авторизации, предусмотренные соответствующим интерфейсом взаимодействия.

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

Фактический перечень доступных функций определяется назначенной пользователю ролью.

После завершения пользовательской сессии или истечения времени её действия пользователю необходимо повторно пройти аутентификацию для получения доступа к системе.

При использовании внешних механизмов аутентификации доступ к системе зависит от корректной работы соответствующей службы авторизации.

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

Зона ответственности: Printum

> **Коротко:** Printum поддерживает автоматическую и административную блокировку учетных записей пользователей, ручную разблокировку пользователей, а также централизованное управление учетными записями через панель администрирования.

??????????

Система должна обеспечивать управление жизненным циклом учетных записей пользователей и предотвращать несанкционированный доступ при нарушении требований безопасности.

Блокировка учетных записей позволяет ограничить доступ к системе при попытках подбора пароля, длительном отсутствии активности пользователя или иных событиях, определенных политикой безопасности организации.

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

Управление учетными записями пользователей осуществляется через панель администрирования системы.

Администратор может:

- создавать и изменять учетные записи пользователей;
- изменять параметры пользователей;
- назначать роли;
- назначать парольные политики;
- изменять пароль пользователя;
- принудительно требовать смену пароля при следующем входе пользователя в систему.

В рамках парольной политики поддерживается автоматическая блокировка пользователей после превышения допустимого количества неудачных попыток авторизации.

Для настройки доступны следующие параметры:

- количество попыток авторизации до блокировки;
- период блокировки после неудачной авторизации.

Дополнительно поддерживается автоматическая блокировка пользователей при длительном отсутствии активности в системе. Для этого может быть настроен период отслеживания неактивности пользователя.

Администратор системы может вручную разблокировать пользователя через панель администрирования, не дожидаясь окончания периода блокировки.

Настройки блокировки могут отличаться для различных пользователей и подразделений в зависимости от назначенной парольной политики.

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

При использовании доменной авторизации блокировка учетной записи пользователя в службе каталогов может ограничивать возможность входа в систему независимо от настроек Printum.

После изменения пароля пользователя администратором при следующем входе в систему пользователю может потребоваться установить новый пароль.

Автоматическая блокировка пользователей выполняется в соответствии с параметрами назначенной парольной политики.

???????? ????????????? ? ?????? ???? (SSO)

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает доменную аутентификацию и единый вход через LDAP/Active Directory, SAML 2.0 и Kerberos/GSSAPI. Пользователи, группы и организационная структура могут синхронизироваться из корпоративной службы каталогов.

??????????

Система должна поддерживать централизованную аутентификацию пользователей через корпоративную инфраструктуру управления учётными записями.

Использование доменной аутентификации и единого входа позволяет централизованно управлять пользователями, применять корпоративные политики безопасности и снизить необходимость ведения отдельных локальных учётных записей.

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

Printum поддерживает интеграцию с корпоративными службами каталогов и механизмами единого входа.

Поддерживаются следующие механизмы аутентификации:

- LDAP / Active Directory;
- SAML 2.0;
- Kerberos / GSSAPI.

LDAP / Active Directory

Printum поддерживает синхронизацию пользователей, групп и организационной структуры из службы каталогов.

Поддерживаются:

- Microsoft Active Directory;
- FreeIPA;
- Samba DC;
- РЕД АДМ;
- ALD Pro.

Синхронизация выполняется независимо для каждого подключённого домена. Ошибки синхронизации одного домена не блокируют обработку остальных доменов.

Пользователи, отсутствующие в службе каталогов в течение нескольких циклов синхронизации, автоматически помечаются как удалённые в домене.

SAML 2.0

Printum поддерживает аутентификацию через внешнего поставщика удостоверений (Identity Provider) по протоколу SAML 2.0.

Автоматическое создание неизвестных пользователей при входе через SAML не используется. Пользователь должен быть предварительно создан или синхронизирован в Printum.

Kerberos / GSSAPI

Printum поддерживает доменную аутентификацию через Kerberos/GSSAPI.

При использовании Kerberos возможно применение механизмов сквозной доменной аутентификации в соответствии с настройками инфраструктуры организации.

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

Для SAML и Kerberos настраивается правило сопоставления пользователя внешней системы с учётной записью Printum.

После успешной аутентификации пользователю предоставляется доступ в соответствии с назначенной ролью и действующей моделью разграничения доступа.

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

Настройка и сопровождение LDAP/Active Directory, SAML, Kerberos/GSSAPI и связанных политик безопасности выполняются администраторами инфраструктуры заказчика.

Для использования доменной аутентификации должны быть настроены соответствующие службы каталогов, поставщики удостоверений и необходимые параметры доверия между

системами.

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

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Printum поддерживает локальную и централизованную аутентификацию пользователей, а также различные способы авторизации на устройствах. Конкретные методы аутентификации зависят от используемых компонентов системы и инфраструктуры заказчика.

??????????

Система должна обеспечивать однозначную идентификацию пользователей и подтверждение их подлинности перед предоставлением доступа к функциям и данным.

Аутентификация пользователей позволяет исключить несанкционированный доступ к системе, обеспечить применение политик безопасности и связать действия пользователя с его учетной записью.

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

Перед предоставлением доступа к защищенным функциям системы пользователь проходит процедуру аутентификации.

Printum поддерживает несколько способов аутентификации пользователей:

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

Для пользователей, созданных непосредственно в системе, используется аутентификация по имени пользователя и паролю.

Парольная политика, блокировка пользователей и управление жизненным циклом учетных записей выполняются средствами Printum.

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

Printum поддерживает интеграцию с корпоративными службами каталогов и системами единого входа.

Поддерживаются:

- LDAP;
- Microsoft Active Directory;
- Kerberos / GSSAPI;
- SAML 2.0.

В этом случае аутентификация пользователей выполняется средствами корпоративной инфраструктуры.

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

Для встроенных приложений и сценариев защищенной печати поддерживаются различные способы авторизации пользователей на устройствах.

В зависимости от производителя устройства, модели МФУ и используемого встроенного приложения могут использоваться:

- логин и пароль;
- PIN-код;
- RFID-карта;
- иные поддерживаемые производителем механизмы идентификации пользователя.

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

После успешной аутентификации действия пользователя в системе выполняются от имени его учетной записи и могут использоваться для применения политик безопасности, разграничения доступа и регистрации событий безопасности.

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

При использовании LDAP, Active Directory, Kerberos или SAML настройка и сопровождение соответствующих служб выполняются администраторами инфраструктуры заказчика.

Управление доменными учетными записями, группами пользователей и парольными политиками осуществляется средствами корпоративной инфраструктуры.

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

Доступность конкретных способов аутентификации зависит от используемых компонентов системы и конфигурации инфраструктуры.

Доступность способов авторизации на МФУ зависит от производителя устройства, модели МФУ и возможностей установленного встроенного приложения.

При использовании централизованной аутентификации требования к паролям, срокам их действия и блокировке пользователей определяются соответствующей службой аутентификации.

Управление доступом

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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает настраиваемую парольную политику для локальных пользователей системы. Администратор может управлять требованиями к сложности паролей, сроками их действия, историей использования, блокировкой пользователей и параметрами пользовательских сессий.

??????????

Система должна обеспечивать контроль требований к паролям пользователей, предотвращать использование слабых паролей и обеспечивать защиту учётных записей от несанкционированного доступа.

Парольная политика позволяет реализовать требования организации к сложности паролей, срокам их действия и процедурам управления учётными записями пользователей.

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

Для локальных пользователей Printum поддерживает настраиваемые парольные политики.

Администратор может создавать несколько парольных политик и назначать их отдельным пользователям, группам пользователей или подразделениям.

В рамках парольной политики могут настраиваться:

- минимальная длина пароля;
- минимальное количество букв;
- минимальное количество цифр;
- минимальное количество специальных символов;
- срок действия пароля;
- период обязательной смены пароля;
- период запрета повторной смены пароля;
- максимальное количество неудачных попыток аутентификации;
- период блокировки после неудачных попыток входа;
- период блокировки неактивных пользователей;
- количество ранее использованных паролей, запрещённых к повторному использованию;

- период, в течение которого ранее использованные пароли считаются уникальными;
- требование смены пароля при первом входе в систему;
- запрет последовательностей одинаковых символов;
- запрет цифровых и алфавитных последовательностей;
- запрет использования визуально похожих символов («I», «l», «1»).

Printum поддерживает хранение истории паролей и может запрещать повторное использование ранее применявшихся паролей.

При изменении парольной политики пользователи, чьи пароли перестали соответствовать новым требованиям, могут быть обязаны сменить пароль при следующем входе в систему.

Для защиты учётных записей поддерживается автоматическая блокировка пользователя после заданного количества неуспешных попыток аутентификации.

Также поддерживается автоматическая блокировка пользователей, не использовавших систему в течение установленного периода времени.

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

Пароли пользователей не хранятся в открытом виде.

Для хранения паролей используются стандартные механизмы Django на основе алгоритма PBKDF2 с HMAC-SHA256 и индивидуальной криптографической солью для каждого пароля.

В процессе аутентификации система выполняет проверку хэша пароля без хранения или передачи пароля в открытом виде.

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

При использовании локальной аутентификации параметры парольной политики определяются администраторами Printum.

При использовании доменной аутентификации, LDAP, Active Directory, Kerberos или SAML требования к паролям, срокам их действия и блокировке пользователей определяются соответствующей службой аутентификации организации.

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

Парольная политика применяется только к локальным пользователям Printum.

Для пользователей, аутентифицируемых через внешние службы каталогов или системы единого входа, требования к паролям определяются средствами соответствующей

инфраструктуры.

Управление доступом

??????? ?????? RBAC

Зона ответственности: Printum

> **Коротко:** В Printum реализована гибкая ролевая модель (RBAC), позволяющая разграничивать доступ пользователей к функциям системы, данным, локациям и административным интерфейсам в соответствии с их должностными обязанностями.

??????????

Система должна обеспечивать разграничение прав доступа пользователей и администраторов в соответствии с их полномочиями.

Ролевая модель позволяет реализовать принцип минимальных привилегий, ограничить доступ к функциям системы и данным пользователей, а также разделить административные обязанности между различными категориями сотрудников.

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

В Printum используется ролевая модель управления доступом (RBAC), в рамках которой пользователю назначается роль, определяющая его полномочия в системе.

При настройке роли администратор может управлять доступом по нескольким направлениям:

- набор доступных функций;
- уровень доступа к данным пользователей;
- уровень доступа к локациям;
- права администрирования филиалов;
- доступ к административным панелям системы.

При установке системы создаются базовые роли:

- Пользователь;
- Оператор;
- Инженер;

- Администратор;
- Сотрудник СБ.

В зависимости от назначенной роли пользователю могут предоставляться права на:

- работу с устройствами;
- работу со складом;
- просмотр журналов;
- работу с заданиями печати;
- просмотр журнала информационной безопасности;
- управление пользователями;
- управление принтерами;
- управление правилами печати;
- управление интеграциями;
- управление агентами мониторинга;
- управление системными настройками;
- управление импортом и экспортом данных;
- управление локациями и филиалами.

При импорте пользователей из службы каталогов для них может автоматически назначаться роль по умолчанию, определённая администратором системы.

Администратор может изменить роль по умолчанию или назначить импортированным пользователям другие роли в соответствии с принятой моделью разграничения доступа.

Администратор системы может создавать собственные роли, комбинируя необходимые функции и уровни доступа, а также назначать роль по умолчанию для новых пользователей.

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

Фактический набор доступных функций определяется назначенной пользователю ролью.

При изменении роли пользователя новые полномочия начинают действовать после повторной авторизации пользователя в системе.

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

Зона ответственности: Printum

> **Коротко:** Printum поддерживает ограничение времени жизни пользовательских сессий, автоматическое завершение сеансов при бездействии пользователя и контроль одновременных сессий.

??????????

Система должна обеспечивать автоматическое завершение пользовательских сессий после истечения заданного периода времени или отсутствия активности пользователя.

Данный механизм снижает риск несанкционированного доступа к системе в случаях, когда пользователь оставил рабочее место без завершения работы или не выполнил выход из системы вручную.

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

Управление пользовательскими сессиями осуществляется в рамках парольной политики.

Для каждой парольной политики могут быть настроены следующие параметры:

- общее время пользовательской сессии;
- максимальное время неактивности пользователя;
- максимальное время неактивности пользователя на принтере;
- разрешение или запрет одновременных сессий пользователя.

По истечении установленного времени действия сессии пользователь автоматически теряет авторизацию в системе.

Если пользователь не выполняет действий в течение заданного периода времени, его сессия автоматически завершается. При следующем обращении к панели администрирования или Личному кабинету пользователю потребуется повторно пройти аутентификацию.

Для работы на устройствах также может быть настроен отдельный тайм-аут неактивности пользователя на принтере.

Printum поддерживает контроль одновременных сессий пользователя. Если использование дублирующих сессий запрещено, открытие новой сессии приводит к завершению ранее открытой сессии этого пользователя.

Администратор системы может принудительно завершать активные пользовательские сессии через раздел управления сессиями в панели администрирования.

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

Изменение параметров управления пользовательскими сессиями применяется только к новым сессиям после повторной авторизации пользователя.

При запрете дублирующих сессий открытие новой сессии приводит к завершению предыдущей сессии пользователя. Несохраненные изменения могут быть потеряны.

После завершения сессии пользователю необходимо повторно пройти аутентификацию для продолжения работы с системой.

Управление доступом

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

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Для взаимодействия внутренних компонентов и интеграции с внешними сервисами Printum использует отдельные технические учётные записи. Пароли технических сервисов могут изменяться администраторами системы и не связаны с учётными записями пользователей.

??????????

Система должна обеспечивать использование отдельных технических учётных записей для выполнения служебных операций и взаимодействия компонентов системы.

Использование сервисных учётных записей позволяет разделить действия пользователей и внутренних процессов системы, а также обеспечить независимое управление их полномочиями и учётными данными.

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

Для работы внутренних сервисов и компонентов Printum используются отдельные технические учётные записи и сервисные пароли.

В зависимости от конфигурации системы технические учётные записи могут использоваться для:

- PostgreSQL;
- Redis;
- ClickHouse;
- CUPS;
- FTP;
- служб каталогов;
- других интеграционных сервисов.

Пароли сервисов хранятся отдельно от пользовательских учётных записей и могут быть изменены администратором системы.

Для большинства внутренних сервисов при установке используются автоматически сгенерированные сложные пароли.

Рекомендуется использовать пароли длиной не менее 16 символов с использованием цифр, букв разных регистров и специальных символов.

Администратор может изменять пароли технических сервисов без изменения пользовательских учётных записей.

В отказоустойчивых конфигурациях изменение паролей должно быть синхронизировано между всеми компонентами системы, использующими соответствующий сервис.

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

Для подключения к внешним системам могут использоваться отдельные технические учётные записи.

К таким системам относятся:

- LDAP и Active Directory;
- SMTP-серверы;
- FTP-серверы;
- другие внешние сервисы, используемые в конкретной инфраструктуре.

Создание, сопровождение и управление жизненным циклом таких учётных записей выполняется администраторами инфраструктуры заказчика.

При изменении паролей внешних сервисов соответствующие параметры подключения должны быть обновлены в настройках Printum.

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

Пароли технических сервисов не связаны с пользовательскими учётными записями и не изменяются средствами парольной политики пользователей.

После изменения паролей внутренних сервисов может потребоваться обновление конфигурационных файлов и перезапуск компонентов системы.

В отказоустойчивых конфигурациях изменение паролей должно быть выполнено на всех узлах, использующих соответствующий сервис.

Для хранения конфиденциальных параметров конфигурации может использоваться шифрование конфигурационных файлов средствами системы.

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

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

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.