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

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».

Revision #1
Created 2026-06-08 19:38:48 UTC by DD
Updated 2026-06-08 19:38:48 UTC by DD