

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

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.
