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

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.

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