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

- 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)

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

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.

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

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».

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

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.

???????? ??????? ? 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.