Об утверждении Правил осуществления журналирования цифровых событий

Приказ и.о. Министра искусственного интеллекта и цифрового развития Республики Казахстан от 17 июля 2026 года № 420/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 31 июля 2026 года № 39453

В соответствии с пунктом 3 статьи 30-2 Закона Республики Казахстан "О кибербезопасности", ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила осуществления журналирования цифровых событий.

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства искусственного интеллекта и цифрового развития Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Исполняющий обязанности министра искусственного интеллекта и цифрового развития Республики Казахстан *М. Олжабеков*

"СОГЛАСОВАН"
Комитет национальной безопасности Республики Казахстан

Утвержден приказом
Исполняющий обязанности
министра искусственного
интеллекта и цифрового
развития

Республики Казахстан
от 17 июля 2026 года
№ 420/НҚ

Правила осуществления журналирования цифровых событий

Глава 1. Общие положения

1. Настоящие Правила осуществления журналирования цифровых событий (далее – Правила) разработаны в соответствии с пунктом 3 статьи 30-2 Закона Республики Казахстан "О кибербезопасности" и определяют порядок осуществления журналирования цифровых событий.

2. В настоящих Правилах используются следующие основные понятия:

1) пользователь с привилегированными правами – лицо, обладающее расширенными правами доступа к цифровым объектам, позволяющими изменять параметры функционирования систем, конфигурационные файлы, базы данных, а также управлять учетными записями и правами доступа других пользователей;

2) единый доверенный источник времени – это источник, обеспечивающий получение и распространение точных и согласованных данных о текущем времени, которые используются цифровыми объектами для синхронизации времени с международным стандартом UTC;

3) государственная техническая служба – государственное юридическое лицо, созданное по решению Правительства Республики Казахстан;

4) цифровое событие – зафиксированное в цифровой форме обстоятельство, возникшее в результате действий субъекта цифровой среды или функционирования цифрового объекта и отражающее параметры их взаимодействия в цифровой среде;

5) централизованная система сбора журналов цифровых событий – аппаратно-программный комплекс, обеспечивающий централизованный сбор журналов событий цифровых объектов, их хранение и дальнейшую передачу в систему управления событиями кибербезопасности;

6) журналирование цифровых событий – процесс систематической записи, сбора и хранения цифровых записей о событиях, происходящих в цифровых объектах, с целью последующего анализа, выявления отклонений и исследования инцидентов кибербезопасности;

7) единая платформа журналирования цифровых событий – цифровая платформа государственной технической службы, предназначенная для обеспечения сбора, мониторинга, анализа и хранения журналов цифровых событий, возникающих в результате действий пользователей с привилегированными правами в цифровых объектах "цифрового правительства".

Глава 2. Порядок осуществления журналирования цифровых событий

3. Собственники и (или) владельцы цифровых объектов государственных органов и цифровых объектов иных лиц, используемых государственными органами для цифровизации своей деятельности, осуществляют сбор цифровых событий в журналах цифровых событий.

4. В журналах цифровых событий осуществляется запись цифровых событий по следующим обязательным параметрам:

дата и время возникновения цифрового события (в формате ISO 8601, "2026-06-18T15:45:30+05:00");

идентификатор источника цифрового события;

тип цифрового события;

субъект цифровой среды, а также его действия, в результате которых наступило цифровое событие.

При наличии технической возможности у цифровых объектов дополнительно фиксируются:

IP-адрес источника;

IP-адрес назначения;

идентификатор сессии;

идентификатор процесса;

идентификатор корреляции транзакции.

5. Собственники и (или) владельцы цифровых объектов при записи цифровых событий используют единый доверенный источник времени для цифровых объектов. Отклонение в синхронизации времени между цифровыми объектами при журналировании цифровых событий не допускается.

6. Собственники и (или) владельцы цифровых объектов осуществляют учет цифровых событий в журналах цифровых событий по формату и типу записей журналов цифровых событий согласно приложению к настоящим Правилам.

7. Собственники и (или) владельцы цифровых объектов осуществляют сбор журналов цифровых событий, указанных в пункте 3 настоящих Правил, в централизованной системе сбора журналов цифровых событий.

8. В случае временного технического сбоя при передаче журналов цифровых событий в централизованную систему сбора журналов цифровых событий собственники и (или) владельцы цифровых объектов обеспечивают их локальное хранение до восстановления сетевого соединения.

9. Собственники и (или) владельцы цифровых объектов обеспечивают хранение журналов цифровых событий и их неизменность, осуществляя защиту журналов цифровых событий в цифровых объектах, указанных в пункте 3 настоящих Правил, от следующих действий:

удаления или редактирования (в том числе пользователями с привилегированными правами);

несанкционированного изменения;

подмены;

несанкционированного доступа.

10. Изменение параметров журналирования цифровых событий подлежит регистрации в журналах цифровых событий.

11. Собственники и (или) владельцы цифровых объектов обеспечивают хранение сведений в журналах цифровых событий не менее трех лет с момента их записи.

12. Для журналов цифровых событий за последние 90 (девяносто) календарных дней осуществляется хранение в оперативном доступе, а при превышении указанного срока – их перемещение в защищенное от несанкционированного доступа хранилище архивных журналов цифровых событий.

13. Собственники и (или) владельцы цифровых объектов осуществляют передачу журналов цифровых событий из своих централизованных систем сбора журналов цифровых событий в единую платформу журналирования цифровых событий.

14. Собственники и (или) владельцы цифровых объектов при передаче журналов цифровых событий из своих централизованных систем сбора журналов цифровых событий в единую платформу журналирования цифровых событий обеспечивают:

защиту передаваемой информации;

контроль целостности данных;

гарантированную доставку;

повторную передачу при возникновении сбоев на сетях связи.

15. Для архивных журналов цифровых событий собственниками и (или) владельцами цифровых объектов осуществляется периодический контроль их целостности.

16. Периодический контроль целостности архивных журналов цифровых событий осуществляется собственниками и (или) владельцами цифровых объектов с использованием криптографической защиты информации.

Приложение
к Правилам осуществления
журналирования цифровых
событий

Форматы и типы записей журналов цифровых событий

1. Форматы и типы записей журналов цифровых событий операционной системы

1. Типы цифровых событий операционной системы (далее – ОС), подлежащие журналированию:

1) запуск/остановка ОС;

2) работа с объектами ОС (открытие, сохранение, переименование, удаление, создание, копирование);

3) установка и удаление программного обеспечения (далее – ПО);

4) авторизация (вход и выход) пользователей в ОС, успешные и неуспешные попытки авторизации;

5) изменение системной конфигурации;

6) создание, удаление, модификация учетных записей;

7) активация/дезактивация систем защиты, таких как антивирусные системы и системы обнаружения вторжения, и средств ведения журнала цифровых событий;

8) изменение или попытки изменения настроек и средств управления защитой системы;

9) использование учетных записей пользователей с привилегированными правами;

10) подключение/отключение устройства ввода/вывода;

11) неудавшиеся или отвергнутые действия пользователя;

12) неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;

13) запуск, остановка процессов в ОС.

2. Журнал цифровых событий ОС содержит следующие поля:

1) дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

2) наименование хоста;

3) описание цифровых события.

3. Для серверных ОС семейства Unix-подобных систем (Unix, Linux, AIX, HPUX и др.) дополнительно к цифровых событиям, указанных в пункте 1 настоящего Приложения к Правилам журналирования цифровых событий (далее – Приложение), фиксируются следующие цифровых события:

1) подключение идентичной учетной записи с разных IP-адресов на один и тот же сервер;

2) открытие новых портов в ОС;

3) всех цифровых событий в ключевых логах: /var/log/secure, /var/log/messages, /var/log/audit.

4. Для серверных ОС семейства Windows, дополнительно к цифровым событиям, указанным в пункте 1 настоящего Приложения, фиксируются следующие цифровые события:

1) присвоение специальных привилегированных прав новому сеансу (logon) – Windows EID 4672;

2) сетевой вход (Network logon) – Windows EID 4624;

3) доступ к сетевой папке администратора (administrative share access) и доступ к SMB каналам (pipes) – Windows EID 5140/5145;

4) доступ к объекту "Файл" с правами "Запись данных" или "Добавление файла–Windows" EID 4663;

5) запуск потенциально опасных процессов (WmiPrvSE.exe, WinrsHost.exe, wsmprovhost.exe, mmc.exe, psexe*.exe, paexe*.exe) – Sysmon EID 1;

6) установка и запуск службы (сервиса) – Windows EID 7045/7036/4697;

7) создание или изменение параметров заданий в планировщике задач (scheduled tasks) – Windows EID 4698/4702;

8) достигнут таймаут службы– Windows EID 7009;

9) ошибка при запуске службы – Windows EID 7000;

10) изменено значение реестра – Windows EID 4657;

11) запись в пространство имен WMI – Windows EID 4662.

5. Записи в журналах цифровых событий хранятся в текстовом формате.

6. Значения полей журналов цифровых событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

7. Для журналов цифровых событий используется кодировка UTF-8.

8. В один файл журнала цифровых событий не допускается включение записи цифровых событий, имеющих разные форматы данных.

2. Форматы и типы записей журналов цифровых событий системы управления базами данных

9. Типы цифровых событий системы управления базами данных, подлежащие журналированию:

1) контроль сессий (успешная/неуспешная авторизация, регистрация использования незарегистрированных учетных записей);

2) все действия пользователей системы управления базы данных (далее – СУБД) имеющих привилегированные права (включая команды select, create, alter, drop, truncate , rename, insert, update, delete, call (execute), lock);

3) все действия пользователей с привилегированными правами в СУБД (grant, revoke, deny).

10. Журнал цифровых событий СУБД содержит следующие поля:

1) дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

2) имя учетной записи/ID пользователя;

3) IP-адрес хоста или наименование хоста;

4) описание цифрового события;

5) наименование объекта (таблицы, процедуры, функции, при возможности реализации).

11. Записи в журналах цифровых событий хранятся в текстовом формате.

12. Значения полей журналов цифровых событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

13. Для журналов цифровых событий используется кодировка UTF-8.

14. В один файл журнала цифровых событий не допускается запись цифровых событий, имеющих разные форматы данных.

3. Форматы и типы записей журналов цифровых событий телекоммуникационного оборудования

15. Типы цифровых событий телекоммуникационного оборудования (далее – ТКО), подлежащие журналированию:

1) запуск/остановка ТКО;

2) изменение системной конфигурации;

3) создание, удаление, модификация локальных учетных записей;

4) использование учетных записей пользователей с привилегированными правами;

5) подключение/отключение устройства ввода/вывода;

6) неудавшиеся или отвергнутые действия пользователя;

7) запуск, падение, остановка сетевых линков (коннектов).

16. С межсетевых экранов (при наличии технической возможности) ведется запись логов всего трафика (входящего и исходящего), а также запись всех цифровых событий на ТКО.

17. Журнал цифровых событий ТКО содержит следующие поля:

1) дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

2) наименование ТКО;

3) имя учетной записи/ID пользователя;

4) IP-адрес хоста;

5) IP-адрес источника;

6) IP-адрес назначения;

7) описание цифрового события.

18. Записи в журналах цифровых событий хранятся в текстовом формате.

19. Значения полей журналов цифровых событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

20. Для журналов цифровых событий используется кодировка UTF-8.

21. В один файл журнала цифровых событий не допускается запись цифровых событий, имеющих разные форматы данных.

4. Форматы и типы записей журналов цифровых событий прикладного программного обеспечения

22. Типы цифровых событий прикладного программного обеспечения (далее – ППО), подлежащие журналированию:

1) авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;

2) создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;

3) неудавшиеся или отвергнутые действия пользователя;

4) получение пользователем доступа к объектам доступа;

5) действия пользователей ППО (доступ к объекту (данным), изменения объекта (данных), удаления объекта (данных)).

23. Журнал цифровых событий ППО содержит следующие поля:

1) дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

2) наименование источника цифрового события (сервис/служба);

3) имя учетной записи/ID пользователя;

4) IP-адрес пользователя;

5) время начала операции;

6) время окончания операции;

7) описание цифрового события.

24. Записи в журналах цифровых событий хранятся в текстовом формате.

25. Значения полей журналов цифровых событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

26. Для журналов цифровых событий используется кодировка UTF-8.

27. В один файл журнала цифровых событий не допускается запись цифровых событий, имеющих разные форматы данных.

5. Форматы и типы записей журналов цифровых событий, выявляемые средствами защиты информации

28. Типы цифровых событий, выявляемые средствами защиты информации (далее – СЗИ), подлежащие журналированию:

1) создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;

2) запуск/остановка СЗИ;

3) изменение системной конфигурации;

4) создание, удаление, модификация локальных учетных записей.

29. Журнал цифровых событий СЗИ содержит следующие поля:

1) дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

2) наименование источника цифрового события (компонент, сервис, служба);

3) имя учетной записи/ID пользователя;

4) IP-адрес клиента;

5) время начала операции;

6) время окончания операции;

7) описание цифрового события.

30. Записи в журналах цифровых событий хранятся в текстовом формате.

31. Значения полей журналов цифровых событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

32. Для журналов цифровых событий используется кодировка UTF-8.

33. В один файл журнала цифровых событий не допускается запись цифровых событий, имеющих разные форматы данных.

6. Форматы и типы записей журналов цифровых событий систем управления привилегированным доступом

34. Типы цифровых событий систем управления привилегированным доступом (далее – СУПД), подлежащие журналированию:

1) авторизация (вход и выход) пользователей в интерфейсе управления СУПД, успешные и неуспешные попытки авторизации, использование факторов усиленной аутентификации;

2) операции с паролями, сертификатами и ключами доступа в защищенном хранилище, включая их просмотр, копирование, выдачу и возврат;

3) автоматическая и принудительная смена (ротация) паролей или ключей на целевых цифровых объектах;

4) создание, удаление, модификация учетных записей, групп и политик доступа внутри СУПД;

5) начало, приостановка, возобновление и завершение сессий пользователей с привилегированными правами;

6) установление и завершение сессий доступа к целевым цифровым объектам (ОС, СУБД, ТКО) через СУПД;

7) фиксация соответствия реальной учетной записи пользователя и используемой им учетной записи пользователя с привилегированными правами на целевом цифровом объекте;

8) запись действий пользователя в видеоформате или в виде последовательности снимков экрана (скриншотов);

9) ввод команд, запуск процессов, скриптов и программных интерфейсов в рамках установленных сессий;

10) операции по передаче файлов через шлюз доступа (загрузка, выгрузка) с фиксацией наименований цифровых объектов;

11) создание запросов на предоставление временного или экстренного доступа, факты их одобрения или отклонения;

12) обнаружение нарушений установленных политик безопасности и автоматические действия по блокировке сессий или пользователей;

13) изменение системной конфигурации СУПД и параметров ведения журналов цифровых событий.

35. Журнал цифровых событий СУПД содержит следующие поля:

1) дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

2) имя персональной учетной записи пользователя (субъекта);

3) имя целевой учетной записи пользователя с привилегированными правами;

4) IP-адрес хоста источника;

5) IP-адрес или наименование целевого цифрового объекта;

6) тип используемого протокола или службы доступа;

7) описание цифрового события (содержание команды, заголовок окна, наименование файла или результат выполнения операции);

8) уникальный идентификатор сессии для сопоставления цифрового события с записью экрана (видеоархивом).

36. Записи в журналах цифровых событий хранятся в текстовом формате.

37. Значения полей журналов цифровых событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

38. Для журналов цифровых событий используется кодировка UTF-8.

39. В один файл журнала цифровых событий не допускается запись цифровых событий, имеющих разные форматы данных.

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан»
Министерства юстиции Республики Казахстан