Цифрлық оқиғаларды журналға енгізуді жүзеге асыру қағидаларын бекіту туралы

Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрінің м.а. 2026 жылғы 17 шілдедегі № 420/НҚ бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2026 жылғы 31 шілдеде № 39453 болып тіркелді

Қазақстан Республикасының "Киберқауіпсіздік туралы" Заңының 30-2-бабының 3-тармағына сәйкес, БҰЙЫРАМЫН:

1. Қоса беріліп отырған Цифрлық оқиғаларды журналға енгізуді жүзеге асыру қағидалары бекітілсін.

2. Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы бұйрықты ресми жариялағаннан кейін оны Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің интернет-ресурсында орналастыруды;

3) осы бұйрық мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Заң департаментіне осы тармақтың 1) және 2) тармақшаларында көзделген іс-шаралардың орындалуы туралы мәліметтер ұсынуды қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Жасанды интеллект және цифрлық даму вице-министріне жүктелсін.

4. Осы бұйрық алғаш ресми жарияланғаннан кейін он күнтізбелік күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Жасанды интеллект және цифрлық даму
министрінің міндетін атқарушы *М. Олжабеков*

"КЕЛІСІЛДІ"
Қазақстан Республикасының
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасының
Жасанды интеллект және цифрлық
даму министрінің
міндетін атқарушы
2026 жылғы 17 шілдедегі
№ 420/НҚ

Бұйрығымен бекітілген

Цифрлық оқиғаларды журналға енгізуді жүзеге асыру қағидалары

1-тарау. Жалпы ережелер

1. Осы Цифрлық оқиғаларды журналға енгізуді жүзеге асыру қағидалары (бұдан әрі – Қағидалар) Қазақстан Республикасының "Киберқауіпсіздік туралы" Заңының 30-2-бабының 3-тармағына сәйкес әзірленді және цифрлық оқиғаларды журналдауды жүзеге асыру тәртібін айқындайды.

2. Осы Қағидаларда мынадай негізгі ұғымдар пайдаланылады:

1) артықшылықты құқықтары бар пайдаланушы – цифрлық объектіге қол жеткізу құқықтары жоғары, оның жұмыс істеуінің штаттық пайдалану жағдайларын қамтамасыз ететін пайдаланушы;

2) бірыңғай сенімді уақыт көзі – цифрлық объектілердің уақытты халықаралық UTC стандартымен синхрондауы үшін пайдаланылатын ағымдағы уақыт туралы дәл және келісілген деректерді алуды және таратуды қамтамасыз ететін уақыт көзі;

3) мемлекеттік техникалық қызмет – Қазақстан Республикасы Үкіметінің шешімі бойынша құрылған мемлекеттік заңды тұлға;

4) цифрлық оқиға – цифрлық орта субъектісінің іс-қимылдары немесе цифрлық объектінің жұмыс істеуі нәтижесінде туындаған және олардың цифрлық ортадағы өзара іс-қимыл параметрлерін көрсететін цифрлық нысанда тіркеп-белгіленген мән-жай;

5) цифрлық оқиғалар журналдарын жинаудың орталықтандырылған жүйесі – цифрлық объектілер оқиғалары журналдарын орталықтандырылған жинауды, оларды сақтауды және киберқауіпсіздік оқиғаларын басқару жүйесіне кейіннен беруді қамтамасыз ететін бағдарламалық-аппараттық кешен;

6) цифрлық оқиғаларды журналға енгізу – кейіннен талдау, ауытқуларды анықтау және киберқауіпсіздіктің оқыс оқиғаларын зерттеу мақсатында цифрлық объектілерде болып жатқан оқиғалар туралы цифрлық жазбаларды жүйелі түрде жазу, жинау және сақтау процесі;

7) цифрлық оқиғаларды журналдаудың бірыңғай платформасы – цифрлық объектілерде артықшылықты құқықтары бар пайдаланушылардың әрекеттері нәтижесінде туындайтын цифрлық оқиғалар журналдарын жинауды, мониторингтеуді, талдауды және сақтауды қамтамасыз етуге арналған мемлекеттік техникалық қызметтің цифрлық платформасы.

2-тарау. Цифрлық оқиғаларды журналға енгізуді жүзеге асыру тәртібі

3. Мемлекеттік органдардың цифрлық объектілерінің және мемлекеттік органдар өз қызметін цифрландыру үшін пайдаланатын өзге тұлғалардың цифрлық объектілерінің

меншік иелері және (немесе) иегерлері цифрлық оқиғаларды цифрлық оқиғалар журналдарында жинауды жүзеге асырады.

4. Цифрлық оқиғалар журналында цифрлық оқиғаларды жазу мынадай міндетті параметрлер бойынша жүзеге асырылады:

цифрлық оқиғаның туындаған күні мен уақыты (ISO 8601 форматында, "2026-06-18T15:45:30+05:00");

цифрлық оқиға көзінің сәйкестендіргіші;

цифрлық оқиғаның түрі;

цифрлық оқиғаның субъектісі, сондай-ақ нәтижесінде цифрлық оқиға туындаған оның іс-әрекеттері.

Цифрлық объектілерде техникалық мүмкіндік болған жағдайда қосымша мынадай параметрлер тіркеледі:

көздің IP-мекенжайы;

тағайындалған IP-мекенжай;

сессия сәйкестендіргіші;

процесс сәйкестендіргіші;

транзакция корреляциясының сәйкестендіргіші.

5. Цифрлық объектілердің меншік иелері және (немесе) иегерлері цифрлық оқиғаларды жазу кезінде цифрлық объектілер үшін бірыңғай сенімді уақыт көзін пайдаланады. Цифрлық оқиғаларды журналдау кезінде цифрлық объектілер арасындағы уақыт синхрондауының ауытқуына жол берілмейді.

6. Цифрлық объектілердің меншік иелері және (немесе) иегерлері осы Қағидаларға қосымшаға сәйкес цифрлық оқиғалар журналдары жазбаларының форматы мен түрі бойынша цифрлық оқиғалар журналдарында цифрлық оқиғаларды есепке алуды жүзеге асырады.

7. Цифрлық объектілердің меншік иелері мен (немесе) иегерлері осы Қағидалардың 3-тармағында көрсетілген цифрлық оқиғалар журналдарын, цифрлық оқиғалар журналдарын жинаудың орталықтандырылған жүйесінде жинауды жүзеге асырады.

8. Цифрлық оқиғалар журналдарын цифрлық оқиғалар журналдарын жинаудың орталықтандырылған жүйесіне беру кезінде уақытша техникалық ақаулық болған жағдайда, цифрлық объектілердің меншік иелері және (немесе) иегелері желілік байланыс қалпына келтірілгенге дейін оларды жергілікті сақтауды қамтамасыз етеді.

9. Цифрлық объектілердің меншік иелері және (немесе) иегерлері осы Қағидалардың 3-тармағында көрсетілген цифрлық объектілердегі цифрлық оқиғалар журналдарын мынадай іс-әрекеттерден қорғауды жүзеге асыра отырып, цифрлық оқиғалар журналдарының сақталуын және олардың өзгермейтіндігін қамтамасыз етеді:

жою немесе өңдеу (оның ішінде артықшылықты құқығы бар пайдаланушылардың жоюы немесе өңдеуі);

рұқсат етілмеген өзгерту;

ауыстыру;

рұқсат етілмеген қолжетімділік.

10. Цифрлық оқиғаларды журналдау параметрлерінің өзгеруі цифрлық оқиғалар журналдарында тіркелуге жатады.

11. Цифрлық объектілердің меншік иелері және (немесе) иегерлері цифрлық оқиғалар журналдарындағы мәліметтердің жазылған сәтінен бастап кемінде үш жыл сақталуын қамтамасыз етеді.

12. Соңғы 90 (тоқсан) күнтізбелік күн ішіндегі цифрлық оқиғалар журналдары жедел қолжетімділікте сақталады, ал көрсетілген мерзімнен асқан кезде олар рұқсатсыз қол жеткізуден қорғалған цифрлық оқиғалардың архивтік журналдары қоймасына ауыстырылады.

13. Цифрлық объектілердің меншік иелері және (немесе) иегерлері цифрлық оқиғалар журналдарын өздерінің цифрлық оқиғалар журналдарын жинаудың орталықтандырылған жүйелерінен цифрлық оқиғаларды журналдаудың бірыңғай платформасына беруді жүзеге асырады.

14. Цифрлық объектілердің меншік иелері және (немесе) иелері цифрлық оқиғалар журналдарын өздерінің цифрлық оқиғалар журналдарын жинаудың орталықтандырылған жүйелерінен цифрлық оқиғаларды журналдаудың бірыңғай платформасына беру кезінде мыналарды қамтамасыз етеді:

берілетін ақпаратты қорғауды;

деректер тұтастығын бақылауды;

кепілдендірілген жеткізуді;

байланыс желілерінде ақаулықтар туындаған кезде қайта беруді.

15. Цифрлық оқиғалардың архивтік журналдары үшін олардың тұтастығына цифрлық объектілердің меншік иелері мен (немесе) иегерлері мерзімді бақылау жүзеге асырады.

16. Цифрлық оқиғалардың архивтік журналдарының тұтастығын мерзімдік бақылау цифрлық объектілердің меншік иелері мен (немесе) иегерлері ақпаратты криптографиялық қорғауды пайдалана отырып жүзеге асырады.

Цифрлық оқиғаларды
журналға енгізуді жүзеге
асыру қағидаларына қосымша

Цифрлық оқиғалар журналдары жазбаларының форматтары мен түрлері

1. Операциялық жүйенің цифрлық оқиғалар журналдары жазбаларының форматтары мен түрлері

1. Журналдауға жататын операциялық жүйенің (бұдан әрі – ОЖ) цифрлық оқиғаларының түрлері:

1) Жүйені қосу/тоқтату;

2) ОЖ объектілерімен жұмыс (ашу, сақтау, атын өзгерту, жою, құру, көшіру);

3) бағдарламалық қамтылымды (бұдан әрі – БҚ) орнату және жою;

4) ОЖ-де қолданушылардың авторландыру (енгізу және шығару), сәтті және сәтсіз авторландыру әрекеттері;жүйелік конфигурацияны өзгерту;

5) жүйелік конфигурациясының өзгеруі;

6) есептік жазбаларды құру, жою және түрлендіру;

7) антивирустық жүйелер және басып кіруді табу жүйелері және оқиғаларды тіркеу журналын жүргізу құралы секілді қорғау жүйелерін активициялау/дезактивациялау;

8) баптау және жүйені қорғауды басқару құралдарын өзгерту әрекеті және өзгерту;

9) артықшылықты есептік жазбаларды пайдалану;

10) кіріс/шығыс құрылғысын қосу/ажырату;

11) қолданушының сәтсіз немесе қабылданбаған әрекеттері;

12) деректерді және басқа ресурстарды қозғайтын сәтсіз немесе қабылданбаған әрекеттер;

13) ОЖ-да процестерді іске қосу, тоқтату.

2. ОЖ цифрлық оқиғалар журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) хосттың атауы;

3) оқиғаның сипаттамасы.

3. Unix-ұқсас жүйелердің серверлік ОЖ үшін (Unix, Linux, AIX, HPUX және т.б.) осы Қосымшаның 1-тармағында көрсетілген цифрлық оқиғаларға қосымша мынадай цифрлық оқиғалар тіркеледі:

1) әртүрлі IP-мекенжайлардан бірдей есептік жазбаны бір серверге қосу;

2) жүйеде жаңа порттар ашу;

3) негізгі логтардағы барлық оқиғаларды тіркеу: /var/log/secure, /var/log/messages, /var/log/audit.

4. Windows тобының серверлік операциялық жүйелері үшін осы Қосымшаның 1-тармағында көрсетілген цифрлық оқиғаларға қосымша мынадай цифрлық оқиғалар тіркеледі:

1) жаңа сессияға (logon) арнайы артықшылықтар беру – Windows EID 4672;

2) желілік кіру (Network logon) – Windows EID 4624;

3) әкімшінің желілік папкасына қол жеткізу (administrative share access) және SMB арналарға қол жеткізу (pipes)– Windows EID 5140/5145;

4) "Деректерді жазу" немесе "Файлды қосу" құқықтарымен "Файл" объектісіне қол жеткізу – Windows EID 4663;

5) ықтимал қауіпті процестерді іске қосу (WmiPrvSE.exe, WinrsHost.exe, wsmprovhost.exe, mmc.exe, psexe * .exe, paexe * .exe) – Sysmon EID 1;

6) қызметті (сервисті) орнату және іске қосу – Windows EID 7045/7036/4697;

7) міндеттер жоспарлағышындағы (scheduled tasks) тапсырмалардың параметрлерін жасау немесе өзгерту – Windows EID 4698/4702;

8) қызмет таймаутына қол жеткізілді – Windows EID 7009;

9) қызметті іске асыру кезіндегі қате – Windows EID 7000;

10) тізілімнің мәні өзгерген – Windows EID 4657;

11) WMI аттар кеңістігіндегі жазба – Windows EID 4662.

5. Цифрлық оқиғалар журналдарындағы жазбалар мәтіндік үлгіде сақталады.

6. Цифрлық оқиғалар журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

7. Цифрлық оқиғалар журналдары үшін UTF-8 кодтамасы пайдаланылады.

8. Цифрлық оқиғалар журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

2. Деректер базасын басқару жүйесіндегіцифрлық оқиғалар журналдарының үлгілері мен түрлері

9. Журналдауға жататын деректер базасын басқару жүйесінің оқиғаларының түрлері:

1) сессияларды бақылау (сәтті/сәтсіз авторландыру, тіркелмеген есептік жазбалардың пайдаланылуын тіркеу);

2) әкімшілік артықшылықтар бар деректер базасын (бұдан әрі – ДБ) қолданушылардың барлық іс-қимылдары (оның ішінде: select, create, alter, drop, truncate , rename, insert, update, delete, call (execute), lock);

3) басқа ДБ қолданушыларға жеңілдіктер тағайындау құқығы бар қолданушылардың барлық іс-қимылдары (grant, revoke, deny).

10. ДБ цифрлық оқиғалар журналы мынадай өрістер болады:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) есептік жазбаның/қолданушының ID атауы;

3) хосттың IP-мекенжай немесе хост атауы;

4) оқиғаның сипаттамасы;

5) объектінің атауы (іске асыру мүмкіндігі болған жағдайда кестелер, рәсімдер, функциялар).

11. Цифрлық оқиғалар журналдарындағы жазбалар мәтіндік үлгіде сақталады.

12. Цифрлық оқиғалар журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

13. Цифрлық оқиғалар журналдары үшін UTF-8 кодтамасы пайдаланылады.

14. Цифрлық оқиғалар журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

3. Телекоммуникациялық жабдықтың цифрлық оқиғалар журналдарының үлгілері мен түрлері

15. Телекоммуникациялық жабдықтың (бұдан әрі - ТКЖ) цифрлық оқиғаларының журналдандыруға жататын түрлері:

1) жүйені іске қосу/тоқтату;

2) жүйенің конфигурациясын өзгерту;

3) локалдық есептік жазбалардын құру, жою, түрлендіру;

4) артықшылықты есептік жазбалардын пайдалану;

5) кіріс/шығыс құрылғысын қосу/ажырату;

6) қолданушының сәтсіз немесе қабылданбаған іс-қимылдары.

7) желілік линктердің (қосылыстар) іске қосылуы, төмендеуі, тоқтауы.

16. Желіаралық экрандардан (техникалық мүмкіндік болса) барлық трафиктің (кіріс және шығыс) логтарын жазу, сондай-ақ құрылғыдағы барлық оқиғаларды жазып алу талап етіледі.

17. ТКЖ цифрлық оқиғалар журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) құрылғының атауы;

3) есептік жазбаның/қолданушының ID;

4) хосттың IP-мекенжайы;

5) бастапқы IP-мекенжайы;

6) тағайындалған IP-мекенжайы;

7) оқиғаның сипаттамасы.

18. Цифрлық оқиғалар журналдарындағы жазбалар мәтіндік үлгіде сақталады.

19. Цифрлық оқиғалар журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

20. Цифрлық оқиғалар журналдары үшін UTF-8 кодтауы пайдаланылады.

21. Цифрлық оқиғалар журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

4. Қолданбалы бағдарламалық қаматамасыз етудің цифрлық оқиғалар журналдарының үлгілері мен түрлері

22. Қолданбалы бағдарламалық қаматамасыз ету (бұдан әрі - ҚБҚ) цифрлық оқиғаларының журналдауға жататын түрлері:

1) олданушыларды авторландыру (енгізу және шығару), сәтті және сәтсіз авторландыру іс-қимылдары;

2) локалдық есептік жазбалардын және конфигурациялық файлдарды құру, көшіру, ауыстыру, жою, түрлендіру;

3) қолданушының сәтсіз немесе қабылданбаған әрекеттері;

4) қолданушының қол жеткізу объектілеріне қолжетімділік алуы;

5) қолданбалы БҚ қолданушысының іс-қимылдары (объектіге (деректерге) қолжетімділік, объектінің (деректердің) өзгерістері, объектіні (деректерді) жою).

23. ҚБҚ цифрлық оқиғалар журналы мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) оқиға (сервис/қызмет) көзінің атауы;

3) есептік жазбаның атауы/қолданушының ID;

4) қолданушының IP-мекенжайы;

5) операцияның басталу уақыты;

6) операцияның аяқталу уақыты;

7) оқиғаның сипаттамасы.

24. Цифрлық оқиғалар журналдарындағы жазбалар мәтіндік үлгіде сақталады.

25. Цифрлық оқиғалар журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

26. Цифрлық оқиғалар журналдары үшін UTF-8 кодтауы пайдаланылады.

27. Цифрлық оқиғалар журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

5. Ақпаратты қорғау құралдарымен анықталатын цифрлық оқиғалар журналдары жазбаларының үлгілері мен түрлері

28. Ақпаратты қорғау құралдарымен (бұдан әрі - АҚҚ) анықталатын, журналдауға жататын цифрлық оқиғалардың түрлері:

1) локалдық есептік жазбалар және конфигурациялық файлдар құру, көшіру, ауыстыру, жою, өзгерту;

2) қызметтің іске қосылуы/тоқтауы;

3) жүйе конфигурациясын өзгерту;

4) локалдық есептік жазбалар құру, жою, түрлендіру.

29. АҚҚ цифрлық оқиғалар журналында мынадай өрістерді қамтиды:

1) күні мен уақыты (күн нысаны: КК:АА:ЖЖЖЖ, уақыт нысаны: СС:ММ:СС);

2) оқиға (сервис/қызмет) көзінің атауы;

3) есептік жазбаның атауы/қолданушының ID;

4) клиенттің IP-мекенжайы;

5) операцияның басталу уақыты;

6) операцияның аяқталу уақыты;

7) оқиғаның сипаттамасы.

30. Цифрлық оқиғалар журналдарындағы жазбалар мәтіндік үлгіде сақталады.

31. Цифрлық оқиғалар журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

32. Цифрлық оқиғалар журналдары үшін UTF-8 кодтауы пайдаланылады.

33. Цифрлық оқиғалар журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.

6. Артықшылықты қолжетімділікті басқару жүйелерінің цифрлық оқиғалар журналдары жазбаларының үлгілері мен түрлері

34. Артықшылықты қолжетімділікті басқару жүйелерінің (бұдан әрі - АҚБЖ) журналдауға жататын оқиғалардың түрлері:

1) пайдаланушылардың АҚБЖ басқару интерфейсінде авторизациядан (кіру және шығу) өтуі, авторизацияның сәтті және сәтсіз әрекеттері, күшейтілген аутентификация факторларын пайдалану;

2) қорғалған қоймада парольдермен, сертификаттармен және қолжетімділік кілттерімен жасалатын операциялар, оның ішінде оларды қарау, көшіру, беру және қайтару;

3) нысаналы цифрлық объектілерде құпиясөздерді немесе кілттерді автоматты және мәжбүрлі түрде ауыстыру (ротациялау);

4) АҚБЖ ішінде есептік жазбаларды, топтарды және қолжетімділік саясаттарын құру, жою және өзгерту;

5) артықшылықты құқықтары бар пайдаланушылар сессияларының басталуы, тоқтатылуы, қайта жалғасуы және аяқталуы;

6) АҚБЖ арқылы нысаналыцифрлық объектілерге (ОЖ, ДҚБЖ, ТКЖ) қолжетімділік сессияларын орнату және аяқтау;

7) нысаналы цифрлық объектіде пайдаланушының нақты есептік жазбасы мен артықшылықты құқықтары бар пайдаланушының пайдаланған есептік жазбасының сәйкестігін тіркеу;

8) пайдаланушы әрекеттерін бейнеформатта немесе экран суреттері (скриншоттар) тізбегі түрінде жазу;

9) сессиялар шеңберінде командаларды енгізу, процестерді, скрипттерді және бағдарламалық интерфейстерді іске қосу;

10) шлюз арқылы файлдарды беру операциялары (жүктеу, жүктеп алу), цифрлық объектілер атауларын тіркеумен;

11) уақытша немесе төтенше қолжетімділік беру туралы сұрауларды жасау, оларды мақұлдау немесе қабылдамау фактілері;

12) қауіпсіздік саясаттарының бұзылуын анықтау және сессияларды немесе пайдаланушыларды автоматты түрде бұғаттау бойынша әрекеттер;

13) АҚБЖ жүйелік конфигурациясын және цифрлық оқиғалар журналдарын жүргізу параметрлерін өзгерту.

35. АҚБЖ цифрлық оқиғалар журналы мынадай өрістерді қамтиды:

1) күн мен уақыт (күн форматы: КК:АА:ЖЖЖЖ, уақыт форматы: СС:ММ:СС);

2) пайдаланушының дербес есептік жазбасының атауы (субъектінің);

3) артықшылықты құқықтары бар пайдаланушының нысаналы есептік жазбасының атауы;

4) бастапқы хосттың IP-мекенжайы;

5) нысаналы цифрлық объектінің IP-мекенжайы немесе атауы;

6) қолжетімділік үшін пайдаланылатын хаттама немесе қызмет түрі;

7) цифрлық оқиғаның сипаттамасы (команданың мазмұны, терезе тақырыбы, файл атауы немесе операцияны орындау нәтижесі);

8) цифрлық оқиғаны экран жазбасымен (бейнеархивпен) салғастыруға арналған сессияның бірегей идентификаторы.

36. Цифрлық оқиғалар журналдарындағы жазбалар мәтіндік үлгіде сақталады.

37. Цифрлық оқиғалар журналдары өрістерінің мәндерін ажыратқыш символдармен ажырату, егер өріс ұзын үлгіде болса және өріс мазмұнында ажыратқыш символ бар болса, өрістерді шектеуші символдарды қолданады.

38. Цифрлық оқиғалар журналдары үшін UTF-8 кодтауы пайдаланылады.

39. Цифрлық оқиғалар журналының бір файлына түрлі үлгідегі деректер қамтылған оқиғаларды жазуға жол берілмейді.