БЕКІТЕМІН
«Жұмабек Ахметұлы Ташенев атындағы университет» АҚ
ректоры
_____Қ.С. Байболов
_____ 2026

АҚПАРАТТЫҚ ҚАУІПСІЗДІК РЕГЛАМЕНТІ

(Сақтық көшірме жасау, кіруді басқару және оқиғаларға жауап беру)

1. Жалпы ережелер

1.1. Осы Ереже «Жұмабек Ахметұлы Ташенев атындағы университет» АҚ (бұдан әрі – Университет) ақпараттық жүйелерінде деректер қауіпсіздігін, қолжетімділік құқықтарын және ақпараттық қауіпсіздік оқиғаларына жауап беру рәсімдерін қамтамасыз ету бойынша міндетті талаптарды белгілейді.
1.2. Бұл талаптар Университеттің IT инфрақұрылымына қолжетімділігі бар барлық штаттық қызметкерлерге, тағылымдамадан өтушілерге және мердігерлерге қолданылады.

2. Сақтық көшірме жасау және қалпына келтіру ережелері

2.1. Сақтық көшірме жасауға арналған нысандар: Дерекқорлар, маңызды корпоративтік қызметтер, сервер конфигурация файлдары, файл сақтау орны және жеке дерекқорлар міндетті түрде сақтық көшірме жасауға жатады.
2.2. "3-2-1" ережесі:
• Деректердің кемінде 3 көшірмесін сақтау;
• Кемінде 2 түрлі медианы пайдалану;
• Кемінде 1 көшірмені қашықтағы сайтта (немесе жазудан қорғау / өзгермейтін сақтық көшірмесі бар оқшауланған бұлттық сақтау орнында) сақтау.
2.3. Сақтау жиілігі және тереңдігі:
• Күнделікті (қосымша): 14–30 күн сақтау;
• Апта сайын (толық): 3 ай сақтау;
• Ай сайын (мұрағат): 1 жыл сақтау (немесе Қазақстан Республикасындағы бухгалтерлік/салық құжаттамасын сақтау мерзімдеріне сәйкес).
2.4. Сақтық көшірме қауіпсіздігі: Барлық сақтық көшірмелер шифрлануы керек (AES-256-дан төмен емес алгоритммен). Сақтық көшірме қоймасына кіру бөлек тіркелгілерді пайдаланатын арнайы ақпараттық қауіпсіздік/АТ әкімшілерімен шектеледі.
2.5. Қалпына келтіру сынағы: Тұтастығын тексеру және резервтік көшірмелерден сынақты орналастыру кемінде тоқсан сайын жүргізіледі, нәтижелері сынақ журналына жазылады.
3. Кіруді бақылау ережелері

3.1. Негізгі қағидаттар:

• Ең аз артықшылық қағидаты: Пайдаланушыларға тек ағымдағы жұмыс міндеттерін орындау үшін қажетті құқықтар беріледі.
• Міндеттерді бөлу (SOD) қағидаты: Маңызды операцияларды бір адам басқармауы керек.
3.2. Тіркелгі өмірлік циклі:
• Кіру тек бөлім басшысы мен HR бөлімінің мақұлдауымен беріледі.
• Құқықтардың өзгеруі: Қызметкер басқа лауазымға ауыстырылған кезде, бұрынғы құқықтар 24 сағат ішінде жойылады.

• Қолжетімділікті қайтарып алу: Қызметкер жұмыстан шығарылған кезде, барлық тіркелгілер (пошта, CRM, VPN, жергілікті компьютерлер) дереу бұғатталады (келісімшарт бұзылған кезде немесе оған дейін).
3.3. Құпия сөз саясаты және аутентификация:
• Құпия сөздің ең аз ұзындығы 12 таңба (бас және кіші әріптерді, сандарды және арнайы таңбаларды пайдалану).
• Артықшылықты (әкімшілік) тіркелгілердің құпия сөздері кемінде 90 күнде бір рет өзгертіледі.
• Қашықтан кіру (VPN), корпоративтік электрондық поштаны, бұлттық қызметтерді және әкімшілік панельдерді пайдалану үшін көп факторлы аутентификацияны (MFA) міндетті түрде пайдалану.
3.4. Құқықтарды қарау: Бөлім басшылары IT қызметімен бірлесіп, барлық пайдаланушылардың қол жеткізу құқықтарын кемінде алты айда бір рет қарайды.

4. Ақпараттық қауіпсіздік оқиғаларына жауап беру ережелері

4.1. Оқиға белгілері: Күдікті электрондық пошталар (фишинг), файлдарды шифрлау немесе жою, рұқсатсыз кіру, сервер жұмысының кенеттен төмендеуі, құпия ақпараттың ағып кетуі.

4.2. Оқиғаны анықтаған кезде қызметкердің міндеттері:
• Ақпараттық қауіпсіздік/IT қолдауына жауапты тұлғаға [+7 707 338 5895] телефоны немесе [info@tashenev.edu.kz] электрондық поштасы арқылы дереу хабарлаңыз.
• Компьютерді (деректерді жедел жадта сақтау үшін) ажыратпаңыз, бірақ ransomware күдігі болса, желілік кабельді немесе Wi-Fi желісін физикалық түрде ажыратыңыз.
• Зиянды бағдарламаны жоюға немесе қатені жасыруға тырыспаңыз.

4.3. Жауап беру кезеңдері (IT/Ақпараттық қауіпсіздік тобы үшін):
1. Анықтау және тіркеу: Оқиғаның уақытын, көзін және ауқымын жазып алыңыз. 2. Локализациялау (қоршау): Жұқтырған желі сегменттерін оқшаулау, бұзылған тіркелгілерді бұғаттау, токендерді жою.

3. Қалпына келтіру: Зиянды кодты жою, осалдықтарды түзету, құпия сөздерді өзгерту.
4. Қалпына келтіру: Расталған сақтық көшірмелерден жүйелерді қалыпты жұмысқа қайтару, тұрақтылықты бақылау.
5. Талдау және есеп беру (өлімнен кейінгі): Оқиға себептері туралы есеп жасау және қауіпсіздік шараларын 3 жұмыс күні ішінде жаңарту.
4.4. Реттеушілерге хабарлау: Қазақстан Республикасы азаматтарының жеке деректерінің жария болуы жағдайында, Компания уәкілетті органға (ҚР Ақпараттық қауіпсіздік және сыбайлас жемқорлыққа қарсы іс-қимыл министрлігі) заңмен белгіленген мерзімде (анықталғаннан кейін 1 жұмыс күні ішінде) хабарлауға міндетті.

5. Жауапкершілік

5.1. Осы Ереженің талаптарын бұзған қызметкерлер тәртіптік, қаржылық, ал Қазақстан Республикасының заңнамасында көзделген жағдайларда әкімшілік немесе қылмыстық жауапкершілікке тартылады.

Таныстыру парағы (қызметкерлердің қолдары қажет болса, қоса беріледі):

№	Қызметкердің толық аты-жөні	Лауазымы	Танысу күні	Қолы
1	Шпенглер С.А.	Цифр. даму орт. басш.	12.01.2026	[signature]
2	Тасболатов Б.	бас әкімші	12.01.2026	[signature]
3	Ағайдаров Е.	жетекші маман	13.01.2026	[signature]
4				

ХАТТАМА № ___
ақпараттық қауіпсіздік тетіктерін жоспарлы түрде тестілеу

Күні: "14" 01 2026
Уақыты: 10⁰⁰ бастап: 18⁰⁰ дейін
Орналасқан жері: Сервер бөлмесі

Комитет мүшелері:
1. Комитет төрағасы: С.А. Шпенглер, Цифрлық даму орталығының басшысы,
2. Комитет мүшесі (орындаушы): Б.А. Тасболатов, Platonus AIS бас әкімшісі
3. Комитет мүшесі: Е. Агайдаров, Platonus AIS жетекші маманы

1. Тест мақсаты

Ақпараттық қауіпсіздік ережелерінің талаптарына сәйкестігін тексеру:
• Сақтық көшірмелердің тұтастығы және қалпына келтіру уақытының мақсаттарына (RTO/RPO) сәйкестік;
• Қолжетімділік құқықтарын шектеудің және тіркелгіні уақтылы бұғаттаудың дұрыстығы;
• Ақпараттық қауіпсіздік оқиғаларына жауап беруге персонал мен техникалық ресурстардың дайындығы.

2. Тесттердің барысы және нәтижелері

№ п/п	Тест нысаны және сценарий	Күтілетін нәтиже (Сәттілік критерийі)	Нақты нәтиже және көрсеткіштер	Статус
Блок А. Сақтық көшірме жасау және қалпына келтіру				
1	[12/30/2025] бастап күнделікті қосымша сақтық көшірмеден [Tashenev] дерекқорын оқшауланған ортаға сынақтан өткізу.	Дерекқор қатесіз орнәластырылды, деректердің тұтастығы расталды және қалпына келтіру уақыты (RTO) 2 сағаттан аспады.	Дерекқор SRV-TEST-01 сынақ қондырғысына сәтті орналастырылды. Бақылау қосындылары сәйкес келеді. Нақты уақыт: 42 минут.	**Аяқталған**
2	Қашықтағы сақтық көшірме сақтау орнына шифрлау және кіру құқықтары тексерілуде.	Файлдар шифрланған (AES-256), стандартты пайдаланушы ретінде кіру бұғатталған.	Шифрлау белсенді. user_test тіркелгісінің кіру әрекеті қабылданбады (Access Denied).	**Аяқталған**
Блок Б. Управление доступом				
3	Соңғы тоқсандағы жұмыстан босатылған қызметкерлердің есеп шоттарының аудиті (HR тізімдері мен DB-Platonus салыстырып тексеру).	Жұмыстан шығарылған қызметкерлердің есепшоттарының 100%-ы жұмыстан шығарылған күні бұғатталады.	12 жазба тексерілді. 11 жазба уақытында бұғатталды, 1 CRM тіркелгісі 2 күн бойы белсенді болып қалды (тексеру кезінде кіру мүмкіндігі бұғатталған).	**Аяқталған**
4	AIS-ке қосылған кезде көп факторлы аутентификацияның (КФА) жұмысын тексеру.	Екінші факторды растамай кіру мүмкін емес.	Тек пайдаланушы аты мен құпия сөзді пайдаланып кіру әрекеті сервер тарапынан қабылданбады.	**Аяқталған**

Блок B. Ақпараттық қауіпсіздік оқиғаларына жауап				
5	Фишингтік электрондық поштаны модельдеу және жұмыс станциясында сынақ қауіпсіз файлды (EICAR сынағы) іске қосу әрекеттері.	Антивирус файлды бұғаттады; қызметкер бұл оқиға туралы IT/IS бөліміне 15 минут ішінде хабарлады.	Антивирус файлды бірден бұғаттады. Қызметкер алты минут ішінде қолдау қызметіне қоңырау шалды.	**Аяқталған**

3. Анықталған кемшіліктер және түзету шаралары

1. Кемшілік: Қызметкер жұмыстан шығарылған кезде CRM жүйесіндегі құқықтарды қайтарып алудағы кідіріс анықталды (3-тармақ).

Түзету шаралары: Кэш жадын кеңейтуді [20 наурыз, 2026 жылға дейін] конфигурациялау. Жауапты тұлға: Platonus AIS бас әкімшісі – Б. Тасболатов.

4. Комиссия қорытындысы

Университеттің резервтік көшірме жасау, кіруді басқару және оқиғаларға жауап беру жүйелері жалпы алғанда ақпараттық қауіпсіздік ережелерінің талаптарына сәйкес келеді және қалыпты жұмыс істеуге дайын деп саналады (3-тармақ бойынша мәселені көрсетілген мерзім ішінде түзетуге байланысты).

Хаттамаға қосымшалар:

1. Дерекқорды сәтті қалпына келтіру журналдарының скриншоттары (1 бет).
2. Бақылау жүйесінің оқиғалар журналын жүктеу (1 бет).

Комиссия мүшелерінің қолдары:
Комиссия төрағасы: _____ / Шпенглер С. /
Комиссия мүшесі: _____ / Тасболатов Б. /
Комиссия мүшесі: _____ / Агайдаров Е. /

1-ші тексеру тізімі. Platonus автоматтандырылған ақпараттық жүйесінің сақтық көшірмесін жасау және қалпына келтіру

Тексеру жиілігі: тоқсан сайын (әсіресе емтихан сессиясына дейін және кейін).

№	Объект / Этап проверки	Техническое действие (Что проверяем)	Критерий успешного прохождения	Статус (Да/Нет)
1	**Дамп базы данных (БД)**	Проверка выполнения автоматических заданий (`cron` / Планировщик задач) на создание резервной копии основной БД (PostgreSQL `pg_dump` / MySQL `mysqldump`).	Дампы создаются ежедневно без ошибок в логах; размер файла соответствует динамике роста БД (не 0 КБ).	Да
2	**Файловое хранилище (Скан-копии и УМК)**	Проверка бэкапа директорий с загруженными документами студентов, силлабусами, транскриптами и дипломными работами.	Все загруженные за последние сутки файлы присутствуют в инкрементальном бэкапе.	Да
3	**Конфигурация и ЭЦП**	Проверка наличия актуальных копий настроек веб-сервера (`server.xml`, `nginx.conf`), лицензионных ключей Platonus и корневых сертификатов НУЦ РК (NCALayer/Kalkan).	Конфигурационные файлы сохранены; при переносе на резервный сервер система распознает лицензию.	Да
4	**Шифрование и изоляция**	Проверка шифрования архивов БД (содержат ИИН, оценки, финансовые данные) и прав доступа к хранилищу бэкапов.	Архивы зашифрованы; доступ по SMB/NFS/S3 закрыт для всех учетных записей, кроме сервисной учетной записи бэкапирования.	[Да
5	**Тестовое разворачивание (Sandbox)**	Разворачивание БД и приложения Platonus на изолированном тестовом стенде из последнего бэкапа.	Веб-интерфейс открывается; корректно отображаются расписание, ведомости текущего семестра и история оценок.	Да

2-ші тексеру тізімі. Platonus AIS жүйесіндегі кіруді басқару

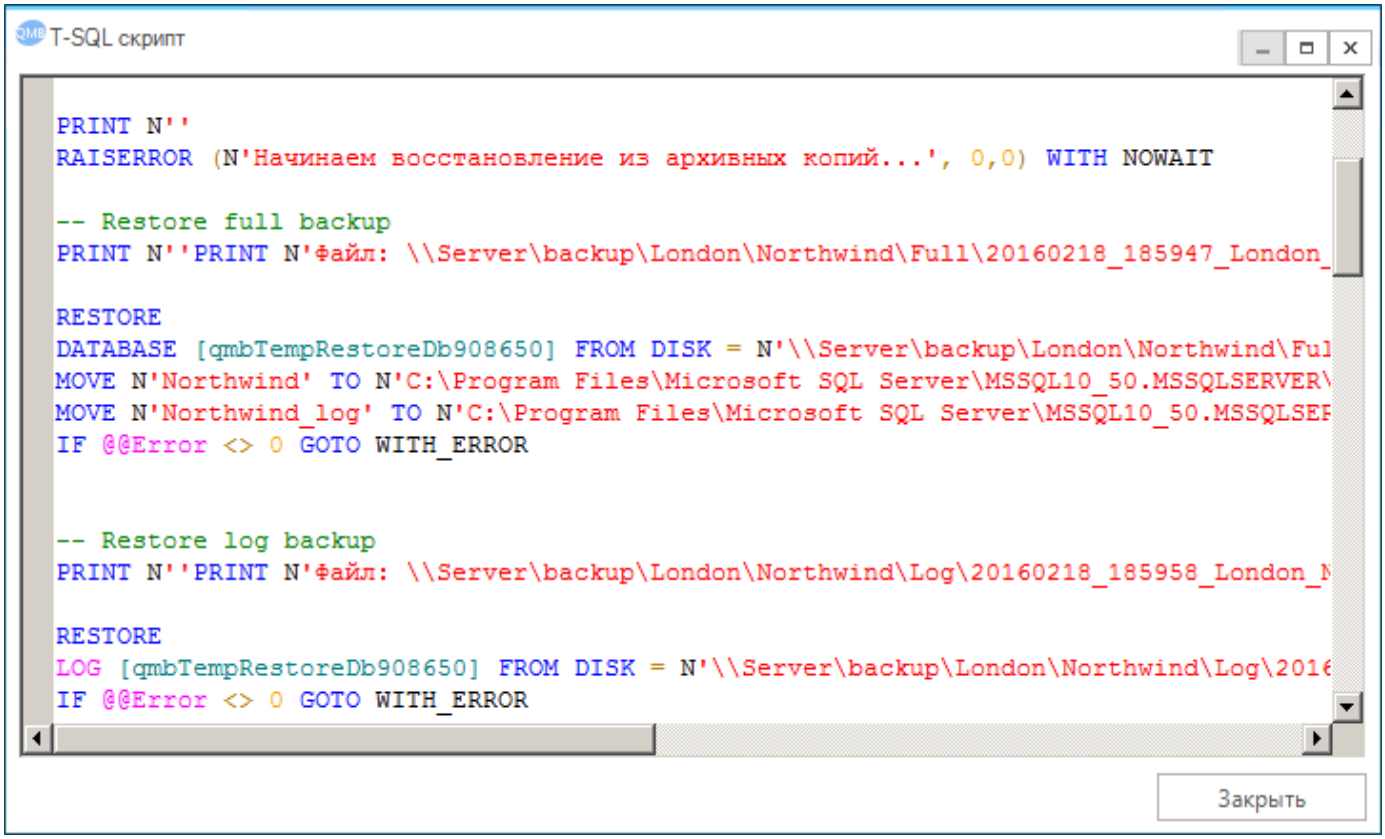
Тексеру жиілігі: Ай сайын және әрбір жаппай тіркеуден/шығарудан немесе бөлім қызметкерлерінің ауысуынан кейін.

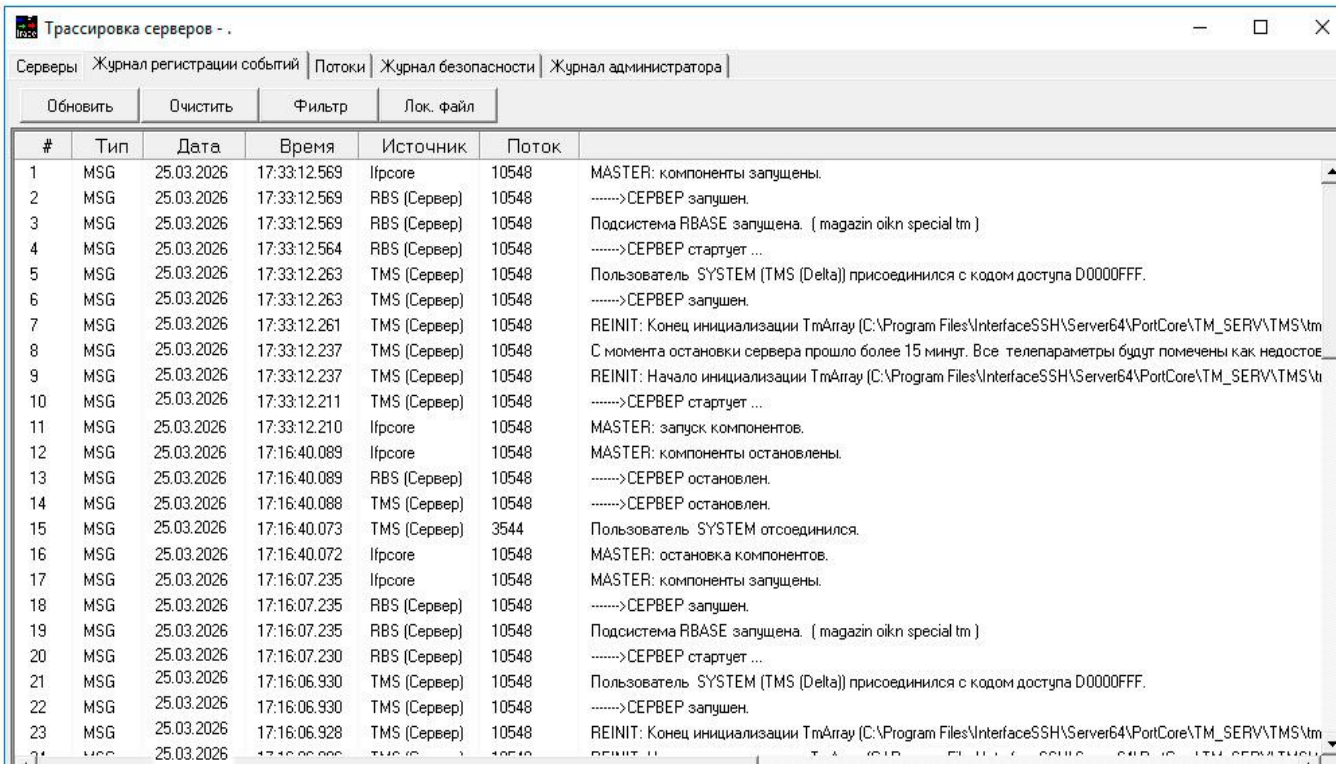
№	Объект / Этап проверки	Техническое действие (Что проверяем)	Критерий успешного прохождения	Статус (Да/Нет)
1	**Ролевая модель (RBAC)**	Выборочный аудит прав учетных записей преподавателей, эдвайзеров, офис-регистратора и бухгалтерии.	Преподаватели имеют доступ к выставлению оценок только по своим дисциплинам; права администратора есть только у штатных ИТ-специалистов.	Да
2	**Блокировка отчисленных и уволенных**	Сверка выгрузки отчисленных/выпустившихся студентов и уволенных сотрудников с активными учетными записями в Platonus.	Учетные записи уволенных ППС заблокированы; выпускники переведены в статус «Выпускник» (доступ только на чтение без права редактирования).	Да
3	**Доступ к журналам оценок (Антифрод)**	Проверка настройки временных окон для выставления и корректировки оценок (РК1, РК2, экзамен) и прав на изменение закрытых ведомостей.	После закрытия ведомости редактирование оценок заблокировано для ППС; изменение возможно только через процедуру апелляции с логированием.	Да
4	**Защита административных интерфейсов и БД**	Проверка сетевой доступности порта управления сервером БД (5432/3306), SSH/RDP и панели управления Tomcat.	Порты БД и управления закрыты на внешнем файрволе; доступ разрешен только из внутренней административной подсети или через VPN с MFA.	Да
5	**Парольная политика и сессии**	Проверка настроек сложности паролей в системе, защиты от перебора (brute-force) и таймаута неактивной сессии.	Включена блокировка учетной записи после 5 неудачных попыток входа; неактивная сессия разрывается автоматически через 15–30 минут.	Да

3-ші тексеру тізімі. Platonus автоматтандырылған ақпараттық жүйесіндегі оқиғаларды бақылау және оларға жауап беру

Тексерулер жиілігі: ай сайын және емтихан сессиялары/қабылдау комиссиясының отырыстары кезінде нақты уақыт режимінде.

№	Объект / Этап проверки	Техническое действие (Что проверяем)	Критерий успешного прохождения	Статус (Да/Нет)
1	**Журналирование действий пользователей (Audit Log)**	Проверка записи критических событий в системный журнал Platonus: вход в систему, изменение оценок, удаление приказов, скачивание баз данных.	В логах фиксируются: точное время, логин/ИИН пользователя, IP-адрес и суть изменения; обычные администраторы не могут удалить логи.	Да
2	**Контроль подписи документов (ЭЦП)**	Проверка корректности работы модуля подписания ведомостей и приказов через ЭЦП (Kalkan/NCALayer) и валидации сертификатов (OCSP/CRL).	Система отклоняет просроченные или отозванные ЭЦП; подписанный документ защищен от последующего редактирования в БД.	Да
3	**Защита от DDoS и перегрузок (WAF / Rate Limiting)**	Проверка правил фильтрации трафика на уровне веб-сервера (Nginx/WAF) на случай массовых одновременных запросов во время выбора элективов или сессии.	Настроено ограничение количества запросов с одного IP (`limit_req`); при имитации всплеска нагрузки сервер не падает с ошибкой `502/504`.	Да
4	**Синхронизация с внешними системами**	Проверка журналов обмена данными с государственными системами (ЕПВО / НОБД) и банковскими шлюзами (Kaspi/Halyk — если подключена оплата).	Ошибки интеграции (HTTP 4xx/5xx) отслеживаются системой мониторинга (Zabbix/Prometheus); уведомление приходит администратору в течение 5 минут.	Да
5	**План действий при компрометации ведомости**	Проверка готовности к сценарию несанкционированного изменения оценок (взлом аккаунта преподавателя).	Администратор может за 10 минут выявить по логам список измененных записей, заблокировать скомпрометированный аккаунт и восстановить исходные баллы из бэкапа.	Да


T-SQL скрипт
PRINT N''
RAISERROR (N'Начинаем восстановление из архивных копий...', 0,0) WITH NOWAIT
-- Restore full backup
PRINT N''PRINT N'Файл: \\Server\backup\London\Northwind\Full\20160218_185947_London_
RESTORE
DATABASE [qmbTempRestoreDb908650] FROM DISK = N'\\Server\backup\London\Northwind\Ful
MOVE N'Northwind' TO N'C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\
MOVE N'Northwind_log' TO N'C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSEF
IF @@Error <> 0 GOTO WITH_ERROR
-- Restore log backup
PRINT N''PRINT N'Файл: \\Server\backup\London\Northwind\Log\20160218_185958_London_N
RESTORE
LOG [qmbTempRestoreDb908650] FROM DISK = N'\\Server\backup\London\Northwind\Log\2016
IF @@Error <> 0 GOTO WITH_ERROR
Закрыть


Трассировка серверов - .
Серверы
Журнал регистрации событий
Потоки
Журнал безопасности
Журнал администратора
Обновить
Очистить
Фильтр
Лок. файл
Тип Дата Время Источник Поток
1 MSG 25.03.2026 17:33:12.569 lfpcore 10548 MASTER: компоненты запущены.
2 MSG 25.03.2026 17:33:12.569 RBS (Сервер) 10548 ------->СЕРВЕР запущен.
3 MSG 25.03.2026 17:33:12.569 RBS (Сервер) 10548 Подсистема RBASE запущена. (magazin oikn special tm)
4 MSG 25.03.2026 17:33:12.564 RBS (Сервер) 10548 ------->СЕРВЕР стартует ...
5 MSG 25.03.2026 17:33:12.263 TMS (Сервер) 10548 Пользователь SYSTEM (TMS (Delta)) присоединился с кодом доступа D0000FFF.
6 MSG 25.03.2026 17:33:12.263 TMS (Сервер) 10548 ------->СЕРВЕР запущен.
7 MSG 25.03.2026 17:33:12.261 TMS (Сервер) 10548 REINIT: Конец инициализации TmArray (C:\Program Files\InterfaceSSH\Server64\PortCore\TM_SERV\TMS\tm
8 MSG 25.03.2026 17:33:12.237 TMS (Сервер) 10548 С момента остановки сервера прошло более 15 минут. Все телепараметры будут помечены как недостов
9 MSG 25.03.2026 17:33:12.237 TMS (Сервер) 10548 REINIT: Начало инициализации TmArray (C:\Program Files\InterfaceSSH\Server64\PortCore\TM_SERV\TMS\t
10 MSG 25.03.2026 17:33:12.211 TMS (Сервер) 10548 ------->СЕРВЕР стартует ...
11 MSG 25.03.2026 17:33:12.210 lfpcore 10548 MASTER: запуск компонентов.
12 MSG 25.03.2026 17:16:40.089 lfpcore 10548 MASTER: компоненты остановлены.
13 MSG 25.03.2026 17:16:40.089 RBS (Сервер) 10548 ------->СЕРВЕР остановлен.
14 MSG 25.03.2026 17:16:40.088 TMS (Сервер) 10548 ------->СЕРВЕР остановлен.
15 MSG 25.03.2026 17:16:40.073 TMS (Сервер) 3544 Пользователь SYSTEM отсоединился.
16 MSG 25.03.2026 17:16:40.072 lfpcore 10548 MASTER: остановка компонентов.
17 MSG 25.03.2026 17:16:07.235 lfpcore 10548 MASTER: компоненты запущены.
18 MSG 25.03.2026 17:16:07.235 RBS (Сервер) 10548 ------->СЕРВЕР запущен.
19 MSG 25.03.2026 17:16:07.235 RBS (Сервер) 10548 Подсистема RBASE запущена. (magazin oikn special tm)
20 MSG 25.03.2026 17:16:07.230 RBS (Сервер) 10548 ------->СЕРВЕР стартует ...
21 MSG 25.03.2026 17:16:06.930 TMS (Сервер) 10548 Пользователь SYSTEM (TMS (Delta)) присоединился с кодом доступа D0000FFF.
22 MSG 25.03.2026 17:16:06.930 TMS (Сервер) 10548 ------->СЕРВЕР запущен.
23 MSG 25.03.2026 17:16:06.928 TMS (Сервер) 10548 REINIT: Конец инициализации TmArray (C:\Program Files\InterfaceSSH\Server64\PortCore\TM_SERV\TMS\tm