ЕСЕПКЕ ҚОСЫМШАЛАР

ПРИЛОЖЕНИЯ К ОТЧЕТУ

График выполнения работ
по услуге по ведению и сопровождению
Государственного кадастра источников выбросов и поглощений парниковых газов

№ п/п	Мероприятие	Срок исполнения	Форма завершения
2. Администрирование, техническое обслуживание Государственного кадастра и обеспечение информационной безопасности			
2.1	Администрирование и техническое обслуживание оборудования и программного обеспечения Государственного кадастра	Январь-декабрь	Услуги по администрированию и техническому обслуживанию Системы осуществляются в рамках Договора АО «НИТ» от 18 февраля 2021 г. № 16
2.2	Корректировка, модификация программного обеспечения Государственного кадастра	Январь-декабрь	Не требовалось
2.3	Резервное копирование баз данных кадастровых объектов, исходных кодов Государственного кадастра	Январь-декабрь	Резервные копии представлены на DVD дисках
2.4	Создание резервных копий системных файлов ОС и СУБД, конфигурации аппаратно-программных комплексов, конфигураций телекоммуникационного оборудования	Январь-декабрь	Резервные копии представлены на DVD дисках
2.5	Проверка сервера Государственного кадастра на вирусы и опасное ПО	Январь-декабрь	Система основана на программном обеспечении Linux, при

			которой не требуется антивирусная программа
2.6	Принятие мер по исключению инцидентов ИБ, а также устранение их последствий	Январь-декабрь	Инцидентов за отчетный период не было
2.7	Обеспечение конфиденциальности, целостности и доступности Государственного кадастра	Январь-декабрь	Копия Журнала постоянного учета времени доступности/ конфиденциальности, целостности, мониторинга и восстановления работоспособности Системы (в Приложении к Отчету)
2.8	Разработка и утверждение организационно-распорядительных документов (регламенты, правила, инструкции)	Январь-декабрь	Документы представлены в Приложении в Отчету
2.9	Мониторинг работоспособности Государственного кадастра	Январь-декабрь	Копия Журнала постоянного учета времени доступности/ конфиденциальности, целостности, мониторинга и восстановления работоспособности Системы (в Приложении к Отчету)
2.10	Восстановление работоспособности Государственного кадастра	Январь-декабрь	Копия Журнала постоянного учета времени доступности/простоя,

	(при необходимости)		мониторинга и восстановления работоспособности Системы (в Приложении к Отчету)
2.11	Анализ журналов системных событий и действий	Январь-декабрь	Копия Журнала системных событий и действий (в Приложении к Отчету)
2.12	Проведение регламентных и профилактических работ	Январь-декабрь	Проведение регламентных и профилактических работ Системы осуществляются в рамках Договора АО «НИТ» от 18 февраля 2021 г. № 16
2.13	Своевременное проведение анализа и оценки рисков. Поддержание в актуальном состоянии каталога угроз (рисков) ИБ, проведение мероприятий, предусмотренных планом обработки угроз (рисков) ИБ	Январь-декабрь	Информационный отчет с предоставлением копий каталога угроз (рисков) ИБ, плана обработки угроз (рисков) ИБ
2.14	Заведение и контроль актуальности учетных записей, ведение справочников	Январь-декабрь	Копии Системы авторизации пользователей (в Приложении к Отчету)
2.15	Мониторинг работоспособности аппаратно-программных комплексов	Январь-декабрь	Копия Журнала постоянного учета времени доступности/простоя, мониторинга и восстановления

			работоспособности (в Приложении к Отчету)
2.16	Проведение аудита Государственного кадастра на соответствие требованиям ИБ	Февраль	Проводиться
2.17	Подписание обязательства о неразглашении защищаемой информации Государственного кадастра от лиц, задействованных в сопровождении Государственного кадастра	Февраль	Копии подписанных обязательств
2.18	Анализ защищенности и контроль конфигурации сетевого оборудования и операционных систем	Январь-декабрь	Анализ защищенности и контроль конфигурации сетевого оборудования и операционных систем Системы осуществляется в рамках Договора АО «НИТ» от 18 февраля 2021 г. № 16

Журнал

Учета резервных копий

Систем Реестра и Кадастра

5

Журнал учета резервных копии

(резервного копирования, восстановления)

№	Название резервируемого компонента	Краткое описание выполнения – Дата выполнения	Периодичность выполнения	Откуда сохраняется информация	Куда сохраняется	Срок хранения резервной копии	Подпись
49	nord_db_01_01_2021	1.01.2021	2 недели.	сервер. elektro. gov.kz	носитель НОО	2 года	Калибаев
50	nord_db_14.01.2021	14.01.2021	2 недели	сервер elektro.gov.kz	-/-/-/-/-/-	-/-/-/-/-	
51	nord_db_30.01.2021	30.01.2021	2 недели	-/-/-/-/-/-/-	-/-/-/-/-	-/-/-/-	
52	nord_db_08.02.2021	08.02.2021	2 недели	-/-/-/-/-/-	-/-/-/-/-	-/-/-/-	
53	nord_db_14.02.2021	14.02.2021	2 недели.	-/-/-/-/-/-	-/-/-/-/-	-/-/-/	
54	nord_db_24.02.2021	24.02.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
55	nord_db_12.03.2021	12.03.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
56	nord_db_26.03.2021	26.03.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
57	nord_08.04.2021	08.04.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
58	nord_22.04.2021	22.04.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
59	nord_05.05.2021	05.05.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
60	nord_18.05.2021	18.05.2021	2 недели	-/-/-/-/-/-/-	-/-/-/-	-/-/-/-	
61	nord_31.05.2021	31.05.2021	2 недели	-/-/-/-/-	-/-/-/-	-/-/-/-	
62	nord_12.06.2021	12.06.2021	2 недели	-/-/-/-/-	-/-/-/-	-/-/-/-	
63	nord_25.06.2021	25.06.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	
64	nord_08.07.2021	08.07.2021	2 недели	-/-/-/-/-/-	-/-/-/-	-/-/-/-	

Журнал учета резервных копий

(резервного копирования, восстановления)

№	Название резервируемого компонента	Краткое описание выполнения – Дата выполнения	Периодичность выполнения	Откуда сохраняется информация	Куда сохраняется	Срок хранения резервной копии	Подпись
65	Kod_22.07.2021	22.07.2021	2 недели	ecocarbon.energo.gov.kz	носитель НКЗ	годдо	Кондыбаев
66	Kod_04.08.2021	04.08.2021	2 недели	– – – – – –	– – – –	– – – –	Кондыбаев
67	Kod_13.08.2021	13.08.2021	2 недели	– – – – – –	– – – –	– – – –	Кондыбаев
68	Kod_01.09.2021	01.09.2021	2 недели	– – – – –	– – – –	– – – –	Кондыбаев
69	Kod_15.09.2021	15.09.2021	2 недели	– – – – –	– – – –	– – – –	Кондыбаев
70	Kod_28.09.2021	28.09.2021	2 недели	– – – – –	– – – –	– – – –	Кондыбаев
71	Kod_12.10.2021	12.10.2021	2 недели	– – – – –	– – –	– – –	Кондыбаев
72	Kod_26.10.2021	26.10.2021	2 недели	– – – –	– – –	– – –	Кондыбаев
73	Kod_9.11.2021	9.11.2021	2 недели	– – – –	– – –	– – –	Кондыбаев
74	Kod_23.11.2021	23.11.2021	2 недели	– – – – – –	– – –	– – –	Кондыбаев
75	Kod_5.12.2021_new	5.12.2021	2 недели	ecocarbon.gov.kz	– – –	– – –	Кондыбаев
76			2 недели	– – – –	– – –	– – –	
77			2 недели	– – – – –	– – –	– – –	
78			2 недели	– – – –	– – –	– – –	
79			2 недели	– – – – –	– – –	– – –	
80			2 недели	– – – –	– – –	– – –	

Приложение : 2.14

Журнал

Ведение и контроль актуальности учетных записей пользователей

Не защищено | ecocarbon.gov.kz/admin/audit

Министерство экологии, геологии и природных ресурсов Республики Казахстан

+7 (7172) 57-41-40 Обратная связь Сакен Выход

Общая информация | Помощь | Кадастр | Реестр | Геоинформационный модуль | Администрирование

Журнал посещаемости

Пользователь:

С: 07.11.2021 12:03

По: 07.12.2021 12:03

Поиск

#	Пользователь	Дата/время	Действие	IP адрес	Д
1	870107350058	07.12.2021 12:03:16	Успешная аутентификация	127.0.0.1	
2	870107350058	07.12.2021 12:02:59	Успешная аутентификация	127.0.0.1	
3	870107350058	07.12.2021 11:54:24	Успешная аутентификация	127.0.0.1	
4	870107350058	07.12.2021 10:55:13	Успешная аутентификация	127.0.0.1	
5	870107350058	07.12.2021 10:06:09	Успешная аутентификация	127.0.0.1	
6	870107350058	07.12.2021 10:01:20	Успешная аутентификация	127.0.0.1	
7	870107350058	07.12.2021 09:58:48	Успешная аутентификация	127.0.0.1	
8	870107350058	07.12.2021 09:57:27	Успешная аутентификация	127.0.0.1	
9	870107350058	07.12.2021 09:57:09	Выход из системы	127.0.0.1	
10	870107350058	07.12.2021 09:56:49	Успешная аутентификация	127.0.0.1	
11	870107350058	07.12.2021 09:56:40	Выход из системы	127.0.0.1	
12	870107350058	07.12.2021 09:55:02	Успешная аутентификация	127.0.0.1	
13	870107350058	07.12.2021 09:53:40	Выход из системы	127.0.0.1	
14	870107350058	07.12.2021 09:52:49	Успешная аутентификация	127.0.0.1	
15	850317451249	07.12.2021 08:43:09	Успешная аутентификация	127.0.0.1	

1 2 3 4

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

ENG 12:04 07.12.2021

Не защищено | ecocarbon.gov.kz/admin/audit

Министерство экологии, геологии и природных ресурсов Республики Казахстан

+7 (7172) 57-41-40 Обратная связь Сакен Выход

Общая информация | Помощь | Кадастр | Реестр | Геоинформационный модуль | Администрирование

Журнал посещаемости

Пользователь:

С: 07.11.2021 12:13

По: 07.12.2021 12:13

Поиск

#	Пользователь	Дата/время	Действие	IP адрес	Д
16	870107350058	07.12.2021 09:57:27	Успешная аутентификация	127.0.0.1	
17	870107350058	07.12.2021 09:57:09	Выход из системы	127.0.0.1	
18	870107350058	07.12.2021 09:56:49	Успешная аутентификация	127.0.0.1	
19	870107350058	07.12.2021 09:56:40	Выход из системы	127.0.0.1	
20	870107350058	07.12.2021 09:55:02	Успешная аутентификация	127.0.0.1	
21	870107350058	07.12.2021 09:53:40	Выход из системы	127.0.0.1	
22	870107350058	07.12.2021 09:52:49	Успешная аутентификация	127.0.0.1	
23	850317451249	07.12.2021 08:43:09	Успешная аутентификация	127.0.0.1	
24	870107350058	06.12.2021 18:17:23	Успешная аутентификация	127.0.0.1	
25	870107350058	06.12.2021 18:17:11	Выход из системы	127.0.0.1	
26	850317451249	06.12.2021 17:17:04	Успешная аутентификация	127.0.0.1	
27	870107350058	06.12.2021 16:23:51	Успешная аутентификация	127.0.0.1	
28	870107350058	06.12.2021 10:51:37	Успешная аутентификация	127.0.0.1	
29	870107350058	06.12.2021 10:49:22	Успешная аутентификация	127.0.0.1	
30	870107350058	03.12.2021 15:32:14	Успешная аутентификация	127.0.0.1	

1 2 3 4 5

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

ENG 12:13 07.12.2021

Не защищено | ecocarbon.gov.kz/admin/audit

Министерство экологии, геологии и природных ресурсов Республики Казахстан

+7 (7172) 57-41-40 Обратная связь Сакен Выход

Общая информация | Помощь | Кадастр | Реестр | Геоинформационный модуль | Администрирование

Журнал посещаемости

Пользователь:

С: 07.11.2021 12:13

По: 07.12.2021 12:13

Поиск

#	Пользователь	Дата/время	Действие	IP адрес	Д
31	870107350058	03.12.2021 15:23:24	Неуспешная аутентификация	127.0.0.1	
32	870107350058	02.12.2021 17:31:49	Успешная аутентификация	127.0.0.1	
33	870107350058	02.12.2021 17:28:13	Успешная аутентификация	127.0.0.1	
34	870107350058	02.12.2021 17:26:13	Успешная аутентификация	127.0.0.1	
35	870107350058	02.12.2021 17:25:36	Выход из системы	127.0.0.1	
36	870107350058	02.12.2021 17:17:33	Успешная аутентификация	127.0.0.1	
37	850317451249	02.12.2021 16:59:10	Успешная аутентификация	127.0.0.1	
38	870107350058	02.12.2021 15:23:45	Неуспешная аутентификация	127.0.0.1	
39	870107350058	02.12.2021 14:56:22	Выход из системы	127.0.0.1	
40	870107350058	02.12.2021 14:53:19	Успешная аутентификация	127.0.0.1	
41	870107350058	02.12.2021 14:45:32	Успешная аутентификация	127.0.0.1	
42	870107350058	02.12.2021 14:42:11	Успешная аутентификация	127.0.0.1	
43	870107350058	02.12.2021 14:40:44	Успешная аутентификация	127.0.0.1	
44	870107350058	02.12.2021 14:39:29	Выход из системы	127.0.0.1	
45	870107350058	02.12.2021 14:39:28	Успешная аутентификация	127.0.0.1	

1 2 3 4 5

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

ENG 12:13 07.12.2021

Не защищено | ecocarbon.gov.kz/admin/audit

Министерство экологии, геологии и природных ресурсов Республики Казахстан

+7 (7172) 57-41-40 Обратная связь Сакен Выход

Общая информация | Помощь | Кадастр | Реестр | Геоинформационный модуль | Администрирование

Журнал посещаемости

Пользователь:

С: 07.11.2021 12:13

По: 07.12.2021 12:13

Поиск

#	Пользователь	Дата/время	Действие	IP адрес	Д
46	870107350058	02.12.2021 14:37:15	Успешная аутентификация	127.0.0.1	
47	870107350058	02.12.2021 14:33:10	Успешная аутентификация	127.0.0.1	
48	870107350058	02.12.2021 14:21:13	Успешная аутентификация	127.0.0.1	
49	870107350058	02.12.2021 13:58:36	Успешная аутентификация	127.0.0.1	
50	870107350058	02.12.2021 13:33:30	Успешная аутентификация	127.0.0.1	
51	870107350058	02.12.2021 13:29:20	Успешная аутентификация	127.0.0.1	
52	870107350058	02.12.2021 13:27:05	Успешная аутентификация	127.0.0.1	
53	870107350058	02.12.2021 13:24:32	Успешная аутентификация	127.0.0.1	
54	870107350058	02.12.2021 12:35:27	Успешная аутентификация	127.0.0.1	
55	870107350058	02.12.2021 12:32:58	Успешная аутентификация	127.0.0.1	
56	870107350058	02.12.2021 12:25:05	Успешная аутентификация	127.0.0.1	
57	870107350058	02.12.2021 12:11:42	Успешная аутентификация	127.0.0.1	
58	870107350058	02.12.2021 12:10:26	Успешная аутентификация	127.0.0.1	
59	870107350058	02.12.2021 12:10:05	Выход из системы	127.0.0.1	
60	870107350058	02.12.2021 11:45:34	Успешная аутентификация	127.0.0.1	

1 2 3 4 5

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

ENG 12:13 07.12.2021

Приложение : 2.11

Журнал

Анализ журнала системных событий и действий на сервере.

C:\Users\user\AppData\Local\Temp\scp26682\var\log\auth.log - Notepad++

Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск Плагины Вкладки ?

hosts | reachable.nsf | setting.ini | новый 1 | cabon.energo.gov.kz.conf | новый 2 | server.log.2021-12-06 | auth.log

```
346  Dec  7 02:17:01 ubuntu CRON[12948]: pam_unix(cron:session): session opened for user root by (uid=0)
347  Dec  7 02:17:01 ubuntu CRON[12948]: pam_unix(cron:session): session closed for user root
348  Dec  7 02:27:56 ubuntu sshd[12486]: pam_unix(sshd:session): session closed for user administrator
349  Dec  7 02:27:56 ubuntu systemd-logind[1096]: Removed session 5380.
350  Dec  7 03:15:59 ubuntu sshd[13119]: Accepted password for administrator from 192.168.85.194 port 58811 ssh2
351  Dec  7 03:15:59 ubuntu sshd[13119]: pam_unix(sshd:session): session opened for user administrator by (uid=0)
352  Dec  7 03:15:59 ubuntu systemd-logind[1096]: New session 5384 of user administrator.
353  Dec  7 03:17:01 ubuntu CRON[13200]: pam_unix(cron:session): session opened for user root by (uid=0)
354  Dec  7 03:17:01 ubuntu CRON[13200]: pam_unix(cron:session): session closed for user root
355
```

Результаты поиска - (совпадений: 55)

```
Поиск "192.168.85.194" (найдено 55 совпадений в 1 файлах из 1)
  C:\Users\user\AppData\Local\Temp\scp26682\var\log\auth.log (совпадений: 55)
    Строка 6: Dec  5 07:20:19 ubuntu sshd[31272]: Accepted password for administrator from 192.168.85.194 port 50623 ssh2
    Строка 15: Dec  5 08:20:30 ubuntu sshd[31526]: Accepted password for administrator from 192.168.85.194 port 50873 ssh2
    Строка 22: Dec  5 09:20:41 ubuntu sshd[31776]: Accepted password for administrator from 192.168.85.194 port 51095 ssh2
    Строка 29: Dec  5 10:20:52 ubuntu sshd[32030]: Accepted password for administrator from 192.168.85.194 port 51313 ssh2
    Строка 36: Dec  5 11:21:03 ubuntu sshd[32282]: Accepted password for administrator from 192.168.85.194 port 51544 ssh2
    Строка 41: Dec  5 12:21:14 ubuntu sshd[32523]: Accepted password for administrator from 192.168.85.194 port 56177 ssh2
    Строка 50: Dec  5 13:21:25 ubuntu sshd[310]: Accepted password for administrator from 192.168.85.194 port 56417 ssh2
    Строка 57: Dec  5 14:21:36 ubuntu sshd[579]: Accepted password for administrator from 192.168.85.194 port 56643 ssh2
    Строка 66: Dec  5 15:21:47 ubuntu sshd[827]: Accepted password for administrator from 192.168.85.194 port 56932 ssh2
    Строка 73: Dec  5 16:21:58 ubuntu sshd[1084]: Accepted password for administrator from 192.168.85.194 port 57151 ssh2
    Строка 78: Dec  5 17:22:09 ubuntu sshd[1427]: Accepted password for administrator from 192.168.85.194 port 57402 ssh2
    Строка 87: Dec  5 18:22:19 ubuntu sshd[1674]: Accepted password for administrator from 192.168.85.194 port 53614 ssh2
    Строка 94: Dec  5 19:22:30 ubuntu sshd[1920]: Accepted password for administrator from 192.168.85.194 port 53829 ssh2
    Строка 101: Dec  5 20:22:41 ubuntu sshd[2217]: Accepted password for administrator from 192.168.85.194 port 54056 ssh2
    Строка 108: Dec  5 21:22:52 ubuntu sshd[2472]: Accepted password for administrator from 192.168.85.194 port 54278 ssh2
    Строка 113: Dec  5 22:23:03 ubuntu sshd[2713]: Accepted password for administrator from 192.168.85.194 port 54539 ssh2
    Строка 122: Dec  5 23:23:14 ubuntu sshd[3046]: Accepted password for administrator from 192.168.85.194 port 55053 ssh2
    Строка 129: Dec  6 00:23:25 ubuntu sshd[3376]: Accepted password for administrator from 192.168.85.194 port 49558 ssh2
    Строка 136: Dec  6 01:23:36 ubuntu sshd[3630]: Accepted password for administrator from 192.168.85.194 port 49822 ssh2
    Строка 143: Dec  6 02:23:47 ubuntu sshd[3876]: Accepted password for administrator from 192.168.85.194 port 50090 ssh2
    Строка 148: Dec  6 03:23:58 ubuntu sshd[4125]: Accepted password for administrator from 192.168.85.194 port 50349 ssh2
    Строка 157: Dec  6 04:24:09 ubuntu sshd[4381]: Accepted password for administrator from 192.168.85.194 port 50704 ssh2
    Строка 160: Dec  6 04:59:34 ubuntu sshd[4552]: Invalid user \32administrator from 192.168.85.194
    Строка 163: Dec  6 04:59:47 ubuntu sshd[4552]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.85.194
    Строка 164: Dec  6 04:59:49 ubuntu sshd[4552]: Failed password for invalid user \32administrator from 192.168.85.194 port 50984 ssh2
    Строка 165: Dec  6 04:59:51 ubuntu sshd[4552]: Connection closed by 192.168.85.194 port 50984 [preauth]
    Строка 166: Dec  6 05:00:43 ubuntu sshd[4558]: Accepted password for administrator from 192.168.85.194 port 50989 ssh2
    Строка 178: Dec  6 05:33:10 ubuntu sshd[5214]: Accepted password for administrator from 192.168.85.194 port 51374 ssh2
    Строка 189: Dec  6 07:24:32 ubuntu sshd[6271]: Accepted password for administrator from 192.168.85.194 port 60418 ssh2
    Строка 192: Dec  6 08:00:33 ubuntu sshd[6444]: Accepted password for administrator from 192.168.85.194 port 60963 ssh2
    Строка 201: Dec  6 08:24:43 ubuntu sshd[6592]: Accepted password for administrator from 192.168.85.194 port 60792 ssh2
    Строка 211: Dec  6 09:24:54 ubuntu sshd[7048]: Accepted password for administrator from 192.168.85.194 port 56108 ssh2
    Строка 216: Dec  6 10:25:05 ubuntu sshd[7304]: Accepted password for administrator from 192.168.85.194 port 56127 ssh2
    Строка 228: Dec  6 11:25:16 ubuntu sshd[7555]: Accepted password for administrator from 192.168.85.194 port 61870 ssh2
    Строка 235: Dec  6 12:25:27 ubuntu sshd[7798]: Accepted password for administrator from 192.168.85.194 port 64800 ssh2
    Строка 242: Dec  6 13:25:38 ubuntu sshd[8047]: Accepted password for administrator from 192.168.85.194 port 59430 ssh2
    Строка 249: Dec  6 14:25:49 ubuntu sshd[8293]: Accepted password for administrator from 192.168.85.194 port 60414 ssh2
    Строка 256: Dec  6 15:26:00 ubuntu sshd[8549]: Accepted password for administrator from 192.168.85.194 port 49296 ssh2
    Строка 265: Dec  6 16:26:11 ubuntu sshd[8801]: Accepted password for administrator from 192.168.85.194 port 55521 ssh2
```

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

Normal text file | length : 33 323 lines : 355 | Ln : 350 Col : 103 Sel : 26 | 1 | Unix (LF) | UTF-8 | INS

РУС 14:31 07.12.2021

log - administrator@192.168.139.34 - WinSCP

Локально Выбор Файлы Команды Соединение Параметры Сервер Справка

Синхронизировать | Очередь | Настройки передачи По умолчанию

administrator@192.168.139.34 × Новое соединение

Найти файлы | Получить | Править | Свойства | Новый

Отправить

F:\pem key\123\

Имя
..
cba03aee63ebb4bb8b7944458
79aac493b2548d0f36cf20beb9
79aac493b2548d0f36cf20beb9
ecocarbon.gov.kz.key
ecocarbon.gov.kz.pem
kad-1.0.0.0.ear
kad-ui-bundle.war
RSA256_824716a5fae49dbfb8e

/var/log/

Имя	Размер	Изменено	Права	Владел...
nginx		06.12.2021 6:25:01	rwxr-xr-x	root
lxd		03.02.2017 11:30:04	rwxr-xr-x	root
installer		26.02.2020 5:00:12	rwxr-xr-x	root
fsck		26.02.2020 4:55:45	rwxr-xr-x	root
dist-upgrade		05.01.2017 13:10:16	rwxr-xr-x	root
apt		30.11.2021 6:25:02	rwxr-xr-x	root
wtmp.1	7 KB	30.11.2021 9:55:14	rw-rw-r--	root
wtmp	10 KB	07.12.2021 1:45:37	rw-rw-r--	root
vmware-vmsvc.log	7 KB	06.11.2021 19:00:45	rw-r--r--	root
syslog.7.gz	7 KB	30.11.2021 6:25:01	rw-r-----	syslog
syslog.6.gz	3 KB	01.12.2021 6:25:01	rw-r-----	syslog
syslog.5.gz	669 KB	02.12.2021 6:25:01	rw-r-----	syslog
syslog.4.gz	133 KB	03.12.2021 6:25:01	rw-r-----	syslog
syslog.3.gz	8 KB	04.12.2021 6:25:01	rw-r-----	syslog
syslog.2.gz	3 KB	05.12.2021 6:25:01	rw-r-----	syslog
syslog.1	2 671 KB	06.12.2021 6:25:01	rw-r-----	syslog
syslog	2 232 KB	07.12.2021 3:17:39	rw-r-----	syslog
lastlog	286 KB	06.12.2021 21:45:38	rw-rw-r--	root
kern.log.4.gz	1 KB	19.01.2021 0:53:22	rw-r-----	syslog
kern.log.3.gz	1 KB	02.06.2021 3:50:30	rw-r-----	syslog
kern.log.2.gz	23 KB	07.06.2021 9:12:14	rw-r-----	syslog
kern.log.1	1 KB	10.06.2021 5:09:50	rw-r-----	syslog
kern.log	1 KB	06.12.2021 22:57:59	rw-r-----	syslog
faillog	32 KB	02.06.2021 4:10:00	rw-r--r--	root
dpkg.log.4.gz	28 KB	26.02.2020 4:59:05	rw-r--r--	root
dpkg.log.3.gz	1 KB	17.02.2021 4:08:53	rw-r--r--	root
dpkg.log.2.gz	1 KB	02.06.2021 4:10:01	rw-r--r--	root
dpkg.log.1	2 KB	30.11.2021 5:49:48	rw-r--r--	root
dpkg.log	0 KB	30.11.2021 6:25:02	rw-r--r--	root
dmesg	1 KB	15.02.2017 15:20:27	rw-r-----	root
btmp.1	7 KB	30.11.2021 5:52:33	rw-rw----	root
btmp	9 KB	07.12.2021 1:15:23	rw-rw----	root
bootstrap.log	57 KB	15.02.2017 15:21:10	rw-r--r--	root
auth.log.4.gz	3 KB	15.11.2021 6:25:01	rw-r-----	syslog
auth.log.3.gz	5 KB	21.11.2021 6:25:01	rw-r-----	syslog
auth.log.2.gz	5 KB	29.11.2021 6:25:01	rw-r-----	syslog
auth.log.1	117 KB	05.12.2021 6:25:01	rw-r-----	syslog
auth.log	33 KB	07.12.2021 3:17:01	rw-r-----	syslog
alternatives.log.1	21 KB	26.02.2020 4:58:47	rw-r--r--	root
alternatives.log	0 KB	01.03.2020 6:25:01	rw-r--r--	root

Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

0 B из 49,4 MB в 0 из 8 | 32,5 KB из 6,21 MB в 1 из 41

SCP 0:13:12

РУС 14:29 07.12.2021

Приложение : 2.7, 2.9, 2.10, 2.15

Журнал

постоянного учета времени доступности/простоя, мониторинга и восстановления работоспособности информационной системы Кадастр

log - administrator@192.168.139.34 - WinSCP

Локально Выбор Файлы Команды Соединение Параметры Сервер Справка

Синхронизировать | Очередь | Настройки передачи По умолчанию

administrator@192.168.139.34 | Новое соединение

Найти файлы | Получить | Править | Свойства | Новый

Отправить

F:\pem key\123\

Имя
..
cba03aee63ebb4bb8b7944458
79aac493b2548d0f36cf20beb9
79aac493b2548d0f36cf20beb9
ecocarbon.gov.kz.key
ecocarbon.gov.kz.pem
kad-1.0.0.0.ear
kad-ui-bundle.war
RSA256_824716a5fae49dbfb8e

/home/administrator/jboss7/standalone/log/

Имя	Размер	Изменено	Права	Владел...
..		20.11.2019 14:50:24	rwxrwxr-x	admini...
backupgc.log.0	3 074 KB	18.08.2020 15:26:20	rw-rw-r--	admini...
backupgc.log.1	3 075 KB	22.01.2020 6:41:50	rw-rw-r--	admini...
gc.log.0.current	32 KB	21.11.2020 1:02:21	rw-r--r--	root
gc.log.1.current	1 724 KB	20.11.2020 22:58:49	rw-rw-r--	admini...
gc.log.2.current	576 KB	22.01.2020 15:22:24	rw-rw-r--	admini...
server.log	598 KB	07.12.2021 1:22:17	rw-r--r--	admini...
server.log.2021-06-01	2 257 KB	01.06.2021 5:46:46	rw-rw-r--	admini...
server.log.2021-06-02	3 723 KB	02.06.2021 23:59:42	rw-rw-r--	admini...
server.log.2021-06-03	3 429 KB	03.06.2021 23:58:24	rw-r--r--	admini...
server.log.2021-06-04	3 434 KB	04.06.2021 23:59:16	rw-r--r--	admini...
server.log.2021-06-05	3 432 KB	05.06.2021 23:59:57	rw-r--r--	admini...
server.log.2021-06-06	3 432 KB	06.06.2021 23:58:49	rw-r--r--	admini...
server.log.2021-06-07	3 806 KB	07.06.2021 23:58:30	rw-r--r--	admini...
server.log.2021-06-08	3 433 KB	08.06.2021 23:59:22	rw-r--r--	admini...
server.log.2021-06-09	3 428 KB	09.06.2021 23:58:04	rw-r--r--	admini...
server.log.2021-06-10	4 100 KB	10.06.2021 23:59:55	rw-r--r--	admini...
server.log.2021-06-11	3 430 KB	11.06.2021 23:58:37	rw-r--r--	admini...
server.log.2021-06-12	3 435 KB	12.06.2021 23:59:29	rw-r--r--	admini...
server.log.2021-06-13	3 430 KB	13.06.2021 23:58:10	rw-r--r--	admini...
server.log.2021-06-14	3 435 KB	14.06.2021 23:59:02	rw-r--r--	admini...
server.log.2021-06-15	3 435 KB	15.06.2021 23:59:53	rw-r--r--	admini...
server.log.2021-06-16	3 430 KB	16.06.2021 23:58:35	rw-r--r--	admini...
server.log.2021-06-17	3 435 KB	17.06.2021 23:59:27	rw-r--r--	admini...
server.log.2021-06-18	3 430 KB	18.06.2021 23:58:08	rw-r--r--	admini...
server.log.2021-06-19	3 435 KB	19.06.2021 23:59:00	rw-r--r--	admini...
server.log.2021-06-20	3 435 KB	20.06.2021 23:59:51	rw-r--r--	admini...
server.log.2021-06-21	3 430 KB	21.06.2021 23:58:32	rw-r--r--	admini...
server.log.2021-06-22	3 435 KB	22.06.2021 23:59:24	rw-r--r--	admini...
server.log.2021-06-23	3 430 KB	23.06.2021 23:58:05	rw-r--r--	admini...
server.log.2021-06-24	3 435 KB	24.06.2021 23:58:57	rw-r--r--	admini...
server.log.2021-06-25	3 435 KB	25.06.2021 23:59:48	rw-r--r--	admini...
server.log.2021-06-26	3 430 KB	26.06.2021 23:58:36	rw-r--r--	admini...
server.log.2021-06-27	3 435 KB	27.06.2021 23:59:28	rw-r--r--	admini...
server.log.2021-06-28	3 430 KB	28.06.2021 23:58:09	rw-r--r--	admini...
server.log.2021-06-29	3 435 KB	29.06.2021 23:59:01	rw-r--r--	admini...
server.log.2021-06-30	3 435 KB	30.06.2021 23:59:52	rw-r--r--	admini...
server.log.2021-07-01	3 429 KB	01.07.2021 23:58:34	rw-r--r--	admini...
server.log.2021-07-02	3 434 KB	02.07.2021 23:59:25	rw-r--r--	admini...
server.log.2021-07-03	3 429 KB	03.07.2021 23:58:06	rw-r--r--	admini...

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

0 B из 49,4 MB в 0 из 8 | 8,23 MB из 678 MB в 1 из 195 | SCP | 0:09:17

ENG 12:25 07.12.2021

17

log - administrator@192.168.139.34 - WinSCP

Локально Выбор Файлы Команды Соединение Параметры Сервер Справка

Синхронизировать | Очередь | Настройки передачи По умолчанию

administrator@192.168.139.34 | Новое соединение

Найти файлы | Получить | Править | Свойства | Новый

Отправить

F:\pem key\123\

Имя
..
cba03aee63ebb4bb8b7944458
79aac493b2548d0f36cf20beb9
79aac493b2548d0f36cf20beb9
ecocarbon.gov.kz.key
ecocarbon.gov.kz.pem
kad-1.0.0.0.ear
kad-ui-bundle.war
RSA256_824716a5fae49dbfb8e

/home/administrator/jboss7/standalone/log/

Имя	Размер	Изменено	Права	Владел...
server.log.2021-07-03	3 429 KB	03.07.2021 23:58:06	rw-r--r--	admini...
server.log.2021-07-04	3 434 KB	04.07.2021 23:58:58	rw-r--r--	admini...
server.log.2021-07-05	3 434 KB	05.07.2021 23:59:49	rw-r--r--	admini...
server.log.2021-07-06	3 429 KB	06.07.2021 23:58:31	rw-r--r--	admini...
server.log.2021-07-07	3 434 KB	07.07.2021 23:59:22	rw-r--r--	admini...
server.log.2021-07-08	3 429 KB	08.07.2021 23:58:19	rw-r--r--	admini...
server.log.2021-07-09	3 434 KB	09.07.2021 23:59:11	rw-r--r--	admini...
server.log.2021-07-10	3 433 KB	10.07.2021 23:59:52	rw-r--r--	admini...
server.log.2021-07-11	3 433 KB	11.07.2021 23:58:44	rw-r--r--	admini...
server.log.2021-07-12	3 435 KB	12.07.2021 23:59:35	rw-r--r--	admini...
server.log.2021-07-13	3 430 KB	13.07.2021 23:58:16	rw-r--r--	admini...
server.log.2021-07-14	3 435 KB	14.07.2021 23:59:08	rw-r--r--	admini...
server.log.2021-07-15	3 436 KB	15.07.2021 23:59:59	rw-r--r--	admini...
server.log.2021-07-16	3 430 KB	16.07.2021 23:58:41	rw-r--r--	admini...
server.log.2021-07-17	3 436 KB	17.07.2021 23:59:32	rw-r--r--	admini...
server.log.2021-07-18	3 430 KB	18.07.2021 23:58:14	rw-r--r--	admini...
server.log.2021-07-19	3 435 KB	19.07.2021 23:59:05	rw-r--r--	admini...
server.log.2021-07-20	3 435 KB	20.07.2021 23:59:57	rw-r--r--	admini...
server.log.2021-07-21	3 430 KB	21.07.2021 23:58:38	rw-r--r--	admini...
server.log.2021-07-22	3 435 KB	22.07.2021 23:59:30	rw-r--r--	admini...
server.log.2021-07-23	3 430 KB	23.07.2021 23:58:11	rw-r--r--	admini...
server.log.2021-07-24	3 435 KB	24.07.2021 23:59:03	rw-r--r--	admini...
server.log.2021-07-25	3 435 KB	25.07.2021 23:59:54	rw-r--r--	admini...
server.log.2021-07-26	3 430 KB	26.07.2021 23:58:36	rw-r--r--	admini...
server.log.2021-07-27	3 436 KB	27.07.2021 23:59:27	rw-r--r--	admini...
server.log.2021-07-28	3 430 KB	28.07.2021 23:58:09	rw-r--r--	admini...
server.log.2021-07-29	3 435 KB	29.07.2021 23:59:00	rw-r--r--	admini...
server.log.2021-07-30	3 436 KB	30.07.2021 23:59:52	rw-r--r--	admini...
server.log.2021-07-31	3 430 KB	31.07.2021 23:58:33	rw-r--r--	admini...
server.log.2021-08-01	3 434 KB	01.08.2021 23:59:24	rw-r--r--	admini...
server.log.2021-08-02	3 429 KB	02.08.2021 23:58:19	rw-r--r--	admini...
server.log.2021-08-03	3 434 KB	03.08.2021 23:59:11	rw-r--r--	admini...
server.log.2021-08-04	3 432 KB	04.08.2021 23:59:52	rw-r--r--	admini...
server.log.2021-08-05	3 432 KB	05.08.2021 23:58:44	rw-r--r--	admini...
server.log.2021-08-06	3 434 KB	06.08.2021 23:59:35	rw-r--r--	admini...
server.log.2021-08-07	3 429 KB	07.08.2021 23:58:17	rw-r--r--	admini...
server.log.2021-08-08	3 434 KB	08.08.2021 23:59:08	rw-r--r--	admini...
server.log.2021-08-09	3 432 KB	09.08.2021 23:59:50	rw-r--r--	admini...
server.log.2021-08-10	3 433 KB	10.08.2021 23:58:41	rw-r--r--	admini...
server.log.2021-08-11	3 435 KB	11.08.2021 23:59:33	rw-r--r--	admini...

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

0 B из 49,4 MB в 0 из 8 | 3,34 MB из 678 MB в 1 из 195 | SCP | 0:18:46

РУС 12:34 07.12.2021

18

log - administrator@192.168.139.34 - WinSCP

Локально Выбор Файлы Команды Соединение Параметры Сервер Справка

Синхронизировать | Очередь | Настройки передачи По умолчанию

administrator@192.168.139.34 | Новое соединение

Найти файлы | Получить | Править | Свойства | Новый

Отправить

F:\pem key\123\

Имя
..
cba03aee63ebb4bb8b7944458
79aac493b2548d0f36cf20beb9
79aac493b2548d0f36cf20beb9
ecocarbon.gov.kz.key
ecocarbon.gov.kz.pem
kad-1.0.0.0.ear
kad-ui-bundle.war
RSA256_824716a5fae49dbfb8e

/home/administrator/jboss7/standalone/log/

Имя	Размер	Изменено	Права	Владел...
server.log.2021-08-11	3 435 KB	11.08.2021 23:59:33	rw-r--r--	admini...
server.log.2021-08-12	3 430 KB	12.08.2021 23:58:15	rw-r--r--	admini...
server.log.2021-08-13	3 435 KB	13.08.2021 23:59:06	rw-r--r--	admini...
server.log.2021-08-14	3 435 KB	14.08.2021 23:59:58	rw-r--r--	admini...
server.log.2021-08-15	3 430 KB	15.08.2021 23:58:39	rw-r--r--	admini...
server.log.2021-08-16	3 435 KB	16.08.2021 23:59:31	rw-r--r--	admini...
server.log.2021-08-17	3 430 KB	17.08.2021 23:58:12	rw-r--r--	admini...
server.log.2021-08-18	3 435 KB	18.08.2021 23:59:16	rw-r--r--	admini...
server.log.2021-08-19	3 433 KB	19.08.2021 23:59:57	rw-r--r--	admini...
server.log.2021-08-20	3 433 KB	20.08.2021 23:58:49	rw-r--r--	admini...
server.log.2021-08-21	3 435 KB	21.08.2021 23:59:40	rw-r--r--	admini...
server.log.2021-08-22	3 430 KB	22.08.2021 23:58:22	rw-r--r--	admini...
server.log.2021-08-23	3 435 KB	23.08.2021 23:59:13	rw-r--r--	admini...
server.log.2021-08-24	3 433 KB	24.08.2021 23:59:55	rw-r--r--	admini...
server.log.2021-08-25	3 433 KB	25.08.2021 23:58:46	rw-r--r--	admini...
server.log.2021-08-26	3 435 KB	26.08.2021 23:59:38	rw-r--r--	admini...
server.log.2021-08-27	3 430 KB	27.08.2021 23:58:19	rw-r--r--	admini...
server.log.2021-08-28	3 436 KB	28.08.2021 23:59:10	rw-r--r--	admini...
server.log.2021-08-29	3 433 KB	29.08.2021 23:59:52	rw-r--r--	admini...
server.log.2021-08-30	3 433 KB	30.08.2021 23:58:43	rw-r--r--	admini...
server.log.2021-08-31	3 435 KB	31.08.2021 23:59:35	rw-r--r--	admini...
server.log.2021-09-01	3 429 KB	01.09.2021 23:58:16	rw-r--r--	admini...
server.log.2021-09-02	3 434 KB	02.09.2021 23:59:08	rw-r--r--	admini...
server.log.2021-09-03	3 434 KB	03.09.2021 23:59:59	rw-r--r--	admini...
server.log.2021-09-04	3 429 KB	04.09.2021 23:58:41	rw-r--r--	admini...
server.log.2021-09-05	3 434 KB	05.09.2021 23:59:32	rw-r--r--	admini...
server.log.2021-09-06	3 429 KB	06.09.2021 23:58:14	rw-r--r--	admini...
server.log.2021-09-07	3 434 KB	07.09.2021 23:59:05	rw-r--r--	admini...
server.log.2021-09-08	3 434 KB	08.09.2021 23:59:57	rw-r--r--	admini...
server.log.2021-09-09	3 429 KB	09.09.2021 23:58:38	rw-r--r--	admini...
server.log.2021-09-10	3 435 KB	10.09.2021 23:59:30	rw-r--r--	admini...
server.log.2021-09-11	3 430 KB	11.09.2021 23:58:11	rw-r--r--	admini...
server.log.2021-09-12	3 435 KB	12.09.2021 23:59:03	rw-r--r--	admini...
server.log.2021-09-13	3 435 KB	13.09.2021 23:59:54	rw-r--r--	admini...
server.log.2021-09-14	3 430 KB	14.09.2021 23:58:35	rw-r--r--	admini...
server.log.2021-09-15	3 435 KB	15.09.2021 23:59:27	rw-r--r--	admini...
server.log.2021-09-16	3 430 KB	16.09.2021 23:58:08	rw-r--r--	admini...
server.log.2021-09-17	3 435 KB	17.09.2021 23:59:00	rw-r--r--	admini...
server.log.2021-09-18	3 435 KB	18.09.2021 23:59:51	rw-r--r--	admini...
server.log.2021-09-19	3 430 KB	19.09.2021 23:58:33	rw-r--r--	admini...

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

0 B из 49,4 MB в 0 из 8 | 3,35 MB из 678 MB в 1 из 195 | SCP | 0:19:13

РУС 12:35 07.12.2021

log - administrator@192.168.139.34 - WinSCP

Локально Выбор Файлы Команды Соединение Параметры Сервер Справка

Синхронизировать | Очередь | Настройки передачи По умолчанию

administrator@192.168.139.34 × | Новое соединение

Найти файлы | Получить | Править | Свойства | Новый

Отправить

F:\pem key\123\

Имя
..
cba03aee63ebb4bb8b7944458
79aac493b2548d0f36cf20beb9
79aac493b2548d0f36cf20beb9
ecocarbon.gov.kz.key
ecocarbon.gov.kz.pem
kad-1.0.0.0.ear
kad-ui-bundle.war
RSA256_824716a5fae49dbfb8e

/home/administrator/jboss7/standalone/log/

Имя	Размер	Изменено	Права	Владел...
server.log.2021-09-19	3 430 KB	19.09.2021 23:58:33	rw-r--r--	admini...
server.log.2021-09-20	3 435 KB	20.09.2021 23:59:24	rw-r--r--	admini...
server.log.2021-09-21	3 430 KB	21.09.2021 23:58:06	rw-r--r--	admini...
server.log.2021-09-22	3 435 KB	22.09.2021 23:58:57	rw-r--r--	admini...
server.log.2021-09-23	3 435 KB	23.09.2021 23:59:49	rw-r--r--	admini...
server.log.2021-09-24	3 430 KB	24.09.2021 23:58:30	rw-r--r--	admini...
server.log.2021-09-25	3 435 KB	25.09.2021 23:59:21	rw-r--r--	admini...
server.log.2021-09-26	3 430 KB	26.09.2021 23:58:03	rw-r--r--	admini...
server.log.2021-09-27	3 435 KB	27.09.2021 23:58:54	rw-r--r--	admini...
server.log.2021-09-28	3 435 KB	28.09.2021 23:59:46	rw-r--r--	admini...
server.log.2021-09-29	3 430 KB	29.09.2021 23:58:27	rw-r--r--	admini...
server.log.2021-09-30	3 435 KB	30.09.2021 23:59:19	rw-r--r--	admini...
server.log.2021-10-01	3 429 KB	01.10.2021 23:58:00	rw-r--r--	admini...
server.log.2021-10-02	3 434 KB	02.10.2021 23:58:51	rw-r--r--	admini...
server.log.2021-10-03	3 434 KB	03.10.2021 23:59:43	rw-r--r--	admini...
server.log.2021-10-04	3 429 KB	04.10.2021 23:58:24	rw-r--r--	admini...
server.log.2021-10-05	3 434 KB	05.10.2021 23:59:16	rw-r--r--	admini...
server.log.2021-10-06	3 432 KB	06.10.2021 23:59:57	rw-r--r--	admini...
server.log.2021-10-07	3 432 KB	07.10.2021 23:58:49	rw-r--r--	admini...
server.log.2021-10-08	3 434 KB	08.10.2021 23:59:40	rw-r--r--	admini...
server.log.2021-10-09	3 429 KB	09.10.2021 23:58:22	rw-r--r--	admini...
server.log.2021-10-10	3 435 KB	10.10.2021 23:59:13	rw-r--r--	admini...
server.log.2021-10-11	3 430 KB	11.10.2021 23:58:14	rw-r--r--	admini...
server.log.2021-10-12	3 435 KB	12.10.2021 23:59:06	rw-r--r--	admini...
server.log.2021-10-13	3 438 KB	13.10.2021 23:59:57	rw-r--r--	admini...
server.log.2021-10-14	3 430 KB	14.10.2021 23:58:39	rw-r--r--	admini...
server.log.2021-10-15	3 435 KB	15.10.2021 23:59:30	rw-r--r--	admini...
server.log.2021-10-16	3 433 KB	16.10.2021 23:58:12	rw-r--r--	admini...
server.log.2021-10-17	3 443 KB	17.10.2021 23:59:03	rw-r--r--	admini...
server.log.2021-10-18	3 438 KB	18.10.2021 23:59:55	rw-r--r--	admini...
server.log.2021-10-19	3 430 KB	19.10.2021 23:58:36	rw-r--r--	admini...
server.log.2021-10-20	3 438 KB	20.10.2021 23:59:28	rw-r--r--	admini...
server.log.2021-10-21	3 433 KB	21.10.2021 23:58:09	rw-r--r--	admini...
server.log.2021-10-22	3 443 KB	22.10.2021 23:59:01	rw-r--r--	admini...
server.log.2021-10-23	3 441 KB	23.10.2021 23:59:52	rw-r--r--	admini...
server.log.2021-10-24	3 444 KB	24.10.2021 23:58:34	rw-r--r--	admini...
server.log.2021-10-25	3 475 KB	25.10.2021 23:59:26	rw-r--r--	admini...
server.log.2021-10-26	3 430 KB	26.10.2021 23:58:08	rw-r--r--	admini...
server.log.2021-10-27	3 449 KB	27.10.2021 23:59:00	rw-r--r--	admini...
server.log.2021-10-28	3 443 KB	28.10.2021 23:59:51	rw-r--r--	admini...

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

0 B из 49,4 MB в 0 из 8 | 3,34 MB из 678 MB в 1 из 195 | SCP | 0:19:39

РУС 12:35 07.12.2021

ЕАБ

log - administrator@192.168.139.34 - WinSCP

Локально Выбор Файлы Команды Соединение Параметры Сервер Справка

Синхронизировать | Очередь | Настройки передачи По умолчанию

administrator@192.168.139.34 | Новое соединение

Найти файлы | Получить | Править | Свойства | Новый

Отправить

F:\pem key\123\

Имя
..
cba03aee63ebb4bb8b7944458
79aac493b2548d0f36cf20beb9
79aac493b2548d0f36cf20beb9
ecocarbon.gov.kz.key
ecocarbon.gov.kz.pem
kad-1.0.0.0.ear
kad-ui-bundle.war
RSA256_824716a5fae49dbfb8e

/home/administrator/jboss7/standalone/log/

Имя	Размер	Изменено	Права	Владел...
server.log.2021-10-28	3 443 KB	28.10.2021 23:59:51	rw-r--r--	admini...
server.log.2021-10-29	3 435 KB	29.10.2021 23:58:33	rw-r--r--	admini...
server.log.2021-10-30	3 438 KB	30.10.2021 23:59:27	rw-r--r--	admini...
server.log.2021-10-31	3 430 KB	31.10.2021 23:58:09	rw-r--r--	admini...
server.log.2021-11-01	3 444 KB	01.11.2021 23:59:01	rw-r--r--	admini...
server.log.2021-11-02	3 437 KB	02.11.2021 23:59:52	rw-r--r--	admini...
server.log.2021-11-03	3 432 KB	03.11.2021 23:58:34	rw-r--r--	admini...
server.log.2021-11-04	3 437 KB	04.11.2021 23:59:26	rw-r--r--	admini...
server.log.2021-11-05	3 429 KB	05.11.2021 23:58:07	rw-r--r--	admini...
server.log.2021-11-06	3 434 KB	06.11.2021 23:59:04	rw-r--r--	admini...
server.log.2021-11-07	3 578 KB	07.11.2021 23:58:26	rw-r--r--	admini...
server.log.2021-11-08	3 437 KB	08.11.2021 23:59:17	rw-r--r--	admini...
server.log.2021-11-09	3 434 KB	09.11.2021 23:59:59	rw-r--r--	admini...
server.log.2021-11-10	3 435 KB	10.11.2021 23:58:51	rw-r--r--	admini...
server.log.2021-11-11	3 435 KB	11.11.2021 23:59:43	rw-r--r--	admini...
server.log.2021-11-12	3 430 KB	12.11.2021 23:58:25	rw-r--r--	admini...
server.log.2021-11-13	3 443 KB	13.11.2021 23:59:16	rw-r--r--	admini...
server.log.2021-11-14	3 435 KB	14.11.2021 23:59:58	rw-r--r--	admini...
server.log.2021-11-15	3 433 KB	15.11.2021 23:58:50	rw-r--r--	admini...
server.log.2021-11-16	3 435 KB	16.11.2021 23:59:42	rw-r--r--	admini...
server.log.2021-11-17	3 446 KB	17.11.2021 23:58:23	rw-r--r--	admini...
server.log.2021-11-18	3 435 KB	18.11.2021 23:59:15	rw-r--r--	admini...
server.log.2021-11-19	3 438 KB	19.11.2021 23:59:57	rw-r--r--	admini...
server.log.2021-11-20	3 435 KB	20.11.2021 23:58:49	rw-r--r--	admini...
server.log.2021-11-21	3 449 KB	21.11.2021 23:59:40	rw-r--r--	admini...
server.log.2021-11-22	3 433 KB	22.11.2021 23:58:22	rw-r--r--	admini...
server.log.2021-11-23	3 441 KB	23.11.2021 23:59:14	rw-r--r--	admini...
server.log.2021-11-24	3 435 KB	24.11.2021 23:59:56	rw-r--r--	admini...
server.log.2021-11-25	3 435 KB	25.11.2021 23:58:48	rw-r--r--	admini...
server.log.2021-11-26	3 441 KB	26.11.2021 23:59:39	rw-r--r--	admini...
server.log.2021-11-27	3 430 KB	27.11.2021 23:58:21	rw-r--r--	admini...
server.log.2021-11-28	3 438 KB	28.11.2021 23:59:13	rw-r--r--	admini...
server.log.2021-11-29	3 433 KB	29.11.2021 23:59:55	rw-r--r--	admini...
server.log.2021-11-30	3 888 KB	30.11.2021 23:58:47	rw-r--r--	admini...
server.log.2021-12-01	3 942 KB	01.12.2021 23:58:57	rw-r--r--	admini...
server.log.2021-12-02	29 122 KB	02.12.2021 23:59:32	rw-r--r--	admini...
server.log.2021-12-03	7 262 KB	03.12.2021 23:59:12	rw-r--r--	admini...
server.log.2021-12-04	3 432 KB	04.12.2021 23:59:54	rw-r--r--	admini...
server.log.2021-12-05	4 143 KB	05.12.2021 23:58:46	rw-r--r--	admini...
server.log.2021-12-06	8 429 KB	06.12.2021 23:59:57	rw-r--r--	admini...

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

0 B из 49,4 MB в 0 из 8 | 3,36 MB из 678 MB в 1 из 195 | SCP | 0:21:43

РУС 12:37 07.12.2021

C:\Users\user\AppData\Local\Temp\scp24186\home\administrator\jboss7\standalone\log\server.log.2021-12-06 - Notepad++

Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск Плагины Вкладки ?

server.log.2021-12-06

```
2021-12-06 00:00:00,003 INFO  [com.samgau.kad.api.impl.RefeshTokenServiceBean] (EJB default - 3) trying to remove is_removed=1 records from S_REFRESH_TOKEN table...
2021-12-06 00:00:00,005 DEBUG [org.jboss.as.jpa] (EJB default - 3) EJB default - 3:transaction scoped EntityManager [kad-1.0.0.0.ear$KadDS]: created entity manager session T
2021-12-06 00:00:00,005 TRACE [org.jboss.as.jpa] (EJB default - 3) createQuery took 0ms
2021-12-06 00:00:00,007 INFO  [stdout] (EJB default - 3) Hibernate: delete from KAD.S_REFRESH_TOKEN where IS_REMOVED=?
2021-12-06 00:00:00,010 INFO  [com.samgau.kad.api.impl.RefeshTokenServiceBean] (EJB default - 3) successfully removed
2021-12-06 00:00:00,012 DEBUG [org.jboss.as.jpa] (EJB default - 3) EJB default - 3:transaction scoped EntityManager [kad-1.0.0.0.ear$KadDS]: closing entity managersession
2021-12-06 00:00:46,707 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) PeriodicRecovery: background thread Status <== SCANNING
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) PeriodicRecovery: background thread scanning
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) Periodic recovery first pass at Mon, 6 Dec 2021 00:00:46
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) processing /StateManager/BasicAction/TwoPhaseCoordinator/AtomicAction transactions
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) AtomicActionRecoveryModule first pass
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) processing /StateManager/BasicAction/TwoPhaseCoordinator/AtomicAction transactions
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.txoj] (Periodic Recovery) TORecoveryModule - first pass
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) XARecoveryModule state change IDLE->FIRST_PASS

2021-12-06 00:00:46,708 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Local XARecoveryModule - first pass
2021-12-06 00:00:46,709 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) xarecovery of RecoveryOnlyEJBXAResource{receiverContext=EJBReceiverContext{clientContext=org.jboss.ejb
2021-12-06 00:00:46,709 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Found 0 xids in doubt
2021-12-06 00:00:46,709 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) xarecovery of XAResourceWrapperImpl@511df20e{xaResource=org.jboss.jca.adapters.jdbc.xa.XAManagedConnec
2021-12-06 00:00:46,710 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Found 0 xids in doubt
2021-12-06 00:00:46,710 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) xarecovery of org.jboss.activemq.artemis.wildfly.integration.WildFlyActiveMQXAResourceWrapper@65a06279
2021-12-06 00:00:46,710 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Found 0 xids in doubt
2021-12-06 00:00:46,710 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) XARecoveryModule state change FIRST_PASS->BETWEEN_PASSES

2021-12-06 00:00:46,710 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:56,710 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) Periodic recovery second pass at Mon, 6 Dec 2021 00:00:56
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) AtomicActionRecoveryModule second pass
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.txoj] (Periodic Recovery) TORecoveryModule - second pass
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) XARecoveryModule state change BETWEEN_PASSES->SECOND_PASS

2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Local XARecoveryModule - second pass
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Local XARecoveryModule.transactionInitiatedRecovery completed
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) xarecovery second pass of RecoveryOnlyEJBXAResource{receiverContext=EJBReceiverContext{clientContext=c
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Have 0 Xids to recover on this pass.
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) xarecovery second pass of org.jboss.activemq.artemis.wildfly.integration.WildFlyActiveMQXAResourceWrap
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Have 0 Xids to recover on this pass.
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) xarecovery second pass of XAResourceWrapperImpl@511df20e{xaResource=org.jboss.jca.adapters.jdbc.xa.XAM
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Have 0 Xids to recover on this pass.
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.jta] (Periodic Recovery) Local XARecoveryModule.resourceInitiatedRecovery completed
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) XARecoveryModule state change SECOND_PASS->IDLE

2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) PeriodicRecovery: background thread Status <== INACTIVE
2021-12-06 00:00:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) PeriodicRecovery: background thread backing off
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) PeriodicRecovery: background thread Status <== SCANNING
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) PeriodicRecovery: background thread scanning
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) Periodic recovery first pass at Mon, 6 Dec 2021 00:02:56
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) processing /StateManager/BasicAction/TwoPhaseCoordinator/AtomicAction transactions
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) AtomicActionRecoveryModule first pass
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery) processing /StateManager/BasicAction/TwoPhaseCoordinator/AtomicAction transactions
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.txoj] (Periodic Recovery) TORecoveryModule - first pass
2021-12-06 00:02:56,711 DEBUG [com.arjuna.ats.arjuna] (Periodic Recovery)
```

Чтобы активировать Windows, перейдите в раздел "Параметры".

Normal text file | length : 8 630 812 lines : 45 966 | Ln : 1 Col : 1 Pos : 1 | Unix (LF) | UTF-8 | INS

РУС 12:38 07.12.2021

22

Утверждаю
Генеральный директор
АО «Жасыл Даму»
Министерства экологии,
геологии и природных ресурсов
Республики Казахстан
Алимбаев А.Б.

Введение

Политика информационной безопасности АО «Жасыл Даму» (далее - Политика) – документ первого уровня, который определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения информационной безопасности АО «Жасыл Даму» (далее - Общество.

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности.

Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

1. Общие положения

1. Политика информационной безопасности Общества на основании Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации» и постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

2. Требования, изложенные в Политике, распространяются на все структурные единицы Общества, обязательны для исполнения всеми сотрудниками и должностными лицами.

3. В Обществе закрепляются ответственные лица по информатизации и обеспечению информационной безопасности.

4. Контроль за исполнением требований настоящей Политики обеспечивает структурное подразделение или ответственное лицо по информационной безопасности Общества.

Организацию технического обслуживания и поддержку работоспособности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества, осуществляет структурное подразделение или ответственное лицо по информатизации.

2. Основные понятия и сокращения

5. В настоящей политике используются следующие основные понятия:

1) информационная система– организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

2) информационная безопасность -состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

3) угроза информационной безопасности –потенциальная причина нежелательного инцидента, который может нанести ущерб владельцу или пользователю информации;

4) событие информационной безопасности – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации;

5) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

6) уязвимость –свойство сетевого или системного компонента, использование которого нарушителем может привести к реализации угрозы информационной безопасности;

7) нарушитель – это лицо, умышленно или неумышленно предпринявшее попытку реализации угрозы информационной безопасности, независимо от предпосылок и используемых методов и средств;

8) актив – материальный или нематериальный объект, который является информацией или содержит информацию, или служит для обработки, хранения, передачи информации и имеющий ценность для организации в интересах достижения целей и непрерывности ее деятельности.

3. Объекты защиты и субъекты информационного взаимодействия

6. Объектами защиты являются следующие элементы:

1) информационные ресурсы с ограниченным доступом или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также открытая (общедоступная) информация, необходимая для работы Общества, независимо от формы и вида ее представления;

2) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) информационных систем, с помощью которых производится обработка информации;

3) автоматизированные системы связи и передачи данных (средства телекоммуникаций);

4) каналы связи, по которым передается информация (в том числе ограниченного распространения).

7. Информация, подлежащая защите может находиться:

1) на бумажных носителях;

2) в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники);

3) передаваться по телефону, факсу, телексу и т.п. в виде электрических сигналов;

4) быть представлена в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров;

5) записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны, фотокамеры и др.).

8. Категории информационных ресурсов:

1) конфиденциальная информация - информация с ограниченным распространением: результаты тестирования сотрудников, финансовые отчеты и реестры, журналы администрирования, системные журналы, данные о пользователях информационных систем и т.д.;

2) служебная информация («для служебного пользования») – утверждается руководителем;

3) персональные данные - сведения о частной жизни сотрудников, пользователей, личные данные;

4) общедоступная информация - информационные брошюры, документация по общему описанию, сведения для публикации в средствах массовой информации.

9. Субъектами информационного взаимодействия являются:

1) Министерство – владелец информационных систем;

2) должностные лица и сотрудники - пользователи и поставщики информации в соответствии с возложенными на них функциями;

3) юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах Общества;

4) другие юридические и физические лица, задействованные в обеспечении выполнения Обществом своих функций (консультанты,

24

разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и другие).

4. Цели, задачи и принципы

10. Основной целью системы информационной безопасности является защита Общества от возможного нанесения им материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня рисков.

11. Основными задачами системы информационной безопасности являются:

1) своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению субъектам информационного взаимодействия, нарушению нормального функционирования электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества;

2) создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

3) защиту от вмешательства в процесс функционирования электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества от посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

4) разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Общества (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

5) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

6) защиту от внедрения несанкционированных программ, включая компьютерные вирусы.

12. Политика базируется на следующих принципах:

1) законность –соблюдение законодательства Республики Казахстан и законных интересов всех участников информационного взаимодействия;

2) системность – подход к вопросам организации информационной безопасности должен быть логическим и последовательным, основанным на оценке рисков информационной безопасности;

25

3) эффективность – реализуемые в разумно достаточном объеме меры и мероприятия по управлению информационной безопасностью должны сводить риски к минимуму;

4) целесообразность – соблюдение соразмерности затрат на обеспечение защиты информации и потенциального ущерба при реализации угроз;

5) конфиденциальность – предоставление доступа к информации только авторизованным пользователям, защита чувствительной информации от несанкционированного доступа;

6) целостность – существование информации в неискаженном виде, неизменном по отношению к ее некоторому фиксированному состоянию, а также возможность ее изменения только теми лицами, которые имеют на это право;

7) доступность – наличие своевременного беспрепятственного доступа к информации авторизованному пользователю;

8) осведомленность и персональная ответственность – пользователи и администраторы электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества должны быть информированы об угрозах информационной безопасности и мерах противодействия им, а также нести персональную ответственность за несоблюдение требований информационной безопасности.

5. Угрозы информационной безопасности

13. По сфере воздействия источники угроз информационной безопасности можно разделить на внутренние и внешние.

14. К внутренним источникам угроз информационной безопасности относятся:

1) внутренние нарушители информационной безопасности;

2) используемые аппаратные средства (рабочие станции, серверы, периферийное оборудование, источники бесперебойного питания и т.д.);

3) программные средства (системное, сетевое и прикладное программное обеспечение);

4) сетевое обеспечение (маршрутизаторы, коммутаторы, модемы, каналы связи и т.д.);

5) системы жизнеобеспечения (системы энергоснабжения, системы кондиционирования и водоснабжения).

15. К внешним источникам угроз информационной безопасности относятся:

1) внешние нарушители информационной безопасности;

2) форс-мажорные обстоятельства.

16. По мотивации воздействия на электронные информационные ресурсы, информационные системы и информационно-коммуникационную

инфраструктуру, источники угроз информационной безопасности можно разделить на преднамеренные и случайные:

1) преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников);

2) случайные (неумышленные) угрозы вызваны ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.

6. Меры обеспечения информационной безопасности

17. Меры обеспечения информационной безопасности подразделяются на:

1) правовые (законодательные);
2) организационные (административные);
3) морально-этические;
4) физические;
5) технические (аппаратурные и программные).

18. К правовым мерам обеспечения информационной безопасности относятся действующие законы, указы и нормативные акты Республики Казахстан, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационного взаимодействия в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

19. Организационные (административные) меры обеспечения информационной безопасности это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

20. Морально-этические меры обеспечения информационной безопасности определяют личное отношение человека к конфиденциальной информации или информации, ограниченного распространения. Чтобы бороться с нарушениями режима информации, включая, например, передачу паролей, неосторожное обращение с носителями, распространение конфиденциальных данных в частных разговорах, необходима личная сознательность сотрудника.

21. Физические меры обеспечения информационной безопасности основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

22. Технические (программно-аппаратные) меры обеспечения информационной безопасности основаны на использовании различных электронных устройств и специальных программ, входящих в состав информационных систем Общества и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

7. Требования к комплексу мер обеспечения информационной безопасности

23. Рабочее пространство должностных лиц и сотрудников Общества должно быть организовано в соответствии с Требованиями к унифицированному рабочему месту или терминальной системе государственных органов и местных исполнительных органов, утвержденные приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 25 ноября 2019 года № 322/НҚ.

24. Приобретение товаров в целях реализации требований обеспечения информационной безопасности для обороны страны и безопасности государства осуществляется из реестра доверенного программного обеспечения и продукции электронной промышленности в соответствии с законодательством Республики Казахстан о государственных закупках.

При этом, в случае отсутствия в реестре доверенного программного обеспечения и продукции электронной промышленности необходимой продукции, допускается приобретение товаров в соответствии с законодательством Республики Казахстан о государственных закупках.

25. Все основные информационные активы Министерства, его ведомств и подведомственных организаций должны быть учтены и закреплены за ответственными лицами (договор или приказ о закреплении материальной ответственности).

Каждый актив должен быть четко идентифицирован и классифицирован с точки зрения безопасности, в соответствии с Правилами идентификации, классификации и маркировки активов, связанных со средствами обработки информации.

26. Сведения об архитектуре Общества передаются третьим лицам исключительно по согласованию с руководителями структурных

28

подразделений по информационной безопасности и информационным технологиям, либо лицами, их заменяющими.

27. Функциональные обязанности по обеспечению информационной безопасности и обязательства по исполнению требований технической документации информационной безопасности служащих и работников Общества вносятся в должностные инструкции и (или) условия трудового договора.

28. В случае привлечения сторонних организаций к обеспечению информационной безопасности электронных информационных ресурсов, информационных систем, информационно-коммуникационной инфраструктуры заключаются соглашения, в которых устанавливаются условия работы, доступа или использования данных объектов, а также ответственность за их нарушение.

29. Кадровая служба Общества организует и ведет учет прохождения служащими и работниками Общества обучения в сфере информатизации и области обеспечения информационной безопасности.

30. При увольнении или внесении изменений в условия трудового договора права доступа сотрудников Общества к информации и средствам обработки информации, включающие физический и логический доступ, идентификаторы доступа, подписки, документацию, которая идентифицирует его как действующего сотрудника Министерства, его ведомств и подведомственных организаций аннулируются после прекращения его трудового договора или изменяются при внесении изменений в условия трудового договора.

31. На случай возникновения аварий, стихийных бедствий и иных внештатных ситуаций, разрабатывается, тестируется и реализуется план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации, а также доводится до сведения сотрудников Общества о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях.

33. Объекты информатизации электронного правительства первого и второго классов в соответствии с классификатором подключаются к системе мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования не позднее одного года после их введения в промышленную эксплуатацию.

34. Разграничение доступа к информационным ресурсам осуществляется в соответствии с Правилами разграничения прав доступа к электронным информационным ресурсам.

35. Резервное копирование данных и приложений проводится в соответствии с Регламентом резервного копирования и восстановления информации.

20

36. Проводится инвентаризация активов, в соответствии с Правилами инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

37. Использование Интернет и электронной почты, а также мобильных устройств и носителей информации осуществляется согласно Правил использования Интернет и электронной почты и Правил использования мобильных устройств и носителей информации.

38. Процедуры аутентификации и антивирусного контроля осуществляются согласно действующих правил.

39. По решению руководства Общества проводится аудит информационной безопасности в соответствии с Правилами проведения внутреннего аудита информационной безопасности.

40. Проводится мониторинг событий, связанных с нарушением информационной безопасности, и анализ результатов мониторинга.

41. Осуществляется мониторинг:

1) действий пользователей и персонала;

2) использования средств обработки информации.

11. Требования к документации

42. Требуемые к разработке обязательные документы второго уровня, детализирующие требования Политики:

1) методика оценки рисков информационной безопасности;

2) правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;

3) правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;

4) правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;

5) правила проведения внутреннего аудита информационной безопасности;

6) правила использования средств криптографической защиты информации;

7) правила разграничения прав доступа к электронным информационным ресурсам;

8) правила использования Интернет и электронной почты;

9) правила организации процедуры аутентификации;

10) правила организации антивирусного контроля;

11) правила использования мобильных устройств и носителей информации;

12) правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов.

43. Документы третьего уровня содержат описание процессов и процедур обеспечения информационной безопасности, в том числе:

1) каталог угроз (рисков) информационной безопасности;

2) план обработки угроз (рисков) информационной безопасности;

3) регламент резервного копирования и восстановления информации;

4) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

5) руководство администратора по сопровождению объекта информатизации;

6) инструкцию о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях.

44. Перечень документов четвертого уровня включает рабочие формы, журналы, заявки, протоколы и другие документы, в том числе электронные, используемые для регистрации и подтверждения выполненных процедур и работ, в том числе:

1) журнал регистрации инцидентов информационной безопасности и учета внештатных ситуаций;

2) журнал посещения серверных помещений;

3) отчет о проведении оценки уязвимости сетевых ресурсов;

4) журнал учета кабельных соединений;

5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий;

6) журнал учета изменений конфигурации оборудования, тестирования и учета изменений системного программного обеспечения и прикладного программного обеспечения, регистрации и устранения уязвимостей программного обеспечения;

7) журнал тестирования дизель-генераторных установок и источников бесперебойного питания для серверного помещения;

8) журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений.

45. Политика и техническая документация по информационной безопасности пересматриваются с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.

12. Разделение полномочий и ответственность

46. Руководство Общества осуществляет координацию деятельности всех подразделений для организации и поддержания соответствующего уровня информационной безопасности.

47. В рамках исполнения настоящей Политики проводится регулярный внутренний аудит информационной безопасности. Независимый аудит

информационной безопасности может быть проведен по решению руководства Общества с привлечением независимой аудиторской компании.

48. Руководители структурных подразделений Общества несут ответственность за ознакомление работников с требованиями информационной безопасности.

49. Администраторы электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь Политики.

50. Задачей каждого пользователя электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Министерства, его ведомств и подведомственных организаций является соблюдение правил, инструкций, рекомендаций по обеспечению безопасной работы электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры, извещение руководства обо всех подозрительных ситуациях при работе с ними.

51. За несоблюдение порядка и правил использования электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Общества к виновным могут быть применены меры, предусмотренные трудовыми договорами, а также действующим законодательством Республики Казахстан и настоящей Политикой.

Приложение
к Политике информационной
безопасности

Правила
организации антивирусного контроля

1. Общие положения

1. Правила организации антивирусного контроля (далее - Правила) являются техническим документом и регламентируют порядок организации и проведения контроля антивирусной защиты информационно-коммуникационной инфраструктуры АО «Жасыл Даму» (далее-Общество) от разрушающего воздействия вредоносного программного обеспечения.

2. Требования настоящих правил распространяются на сотрудников Общества.

3. Антивирусная защита представляет собой действия, обеспечивающие предотвращение проникновения компьютерных вирусов (далее – вирусы) к информационно-коммуникационной инфраструктуре Общества посредством использования антивирусных средств.

4. В Правилах используются следующие термины, сокращения и определения:

1) структурное подразделение или ответственное лицо по информатизации - структурное подразделение, или лицо, отвечающее за обеспечение и организацию информационной безопасности в центральном аппарате Министерства, его ведомстве или подведомственной организации;

2) системный администратор – сотрудник Министерства, его ведомства и подведомственной организации, отвечающий за обслуживание и администрирование серверного оборудования, телекоммуникационного оборудования;

3) вредоносное программное обеспечение – разновидность программного обеспечения (далее - ПО) со способностью к саморепликации, используемая злоумышленником для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютерной техники или использования его ресурсов в неблаговидных целях;

4) пользователь - сотрудники Общества работающие с информационными ресурсами;

5) антивирусная защита – организационные, правовые и технические меры, направленные на предотвращение разрушающего воздействия вредоносного ПО на информационные системы и ресурсы;

6) средство антивирусной защиты информационных ресурсов - специальное аппаратное или программное обеспечение, которое обеспечивает защиту от вредоносного ПО и ведет контроль за сохранностью данных на

компьютере;

7) информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;

8) рабочая группа – совещательный орган по вопросам обеспечения информационной безопасности.

9) антивирусный монитор – это часть антивируса, предназначенная для непрерывного контроля ситуаций, при которых может произойти заражение вредоносной программой;

10) ИБ – информационная безопасность.

2. Установка и обновление антивирусных средств

5. К использованию в Обществе допускаются только лицензионные антивирусные средства, входящие в состав утвержденного структурным подразделением либо ответственным за обеспечение ИБ перечня базового лицензионного программного обеспечения, обязательного для установки на рабочих станциях пользователей и серверах.

6. Антивирусные программы устанавливаются системными администраторами на все персональные компьютеры пользователей корпоративной вычислительной сети и сервера.

7. На почтовом сервере и (или) специально выделенном сервере устанавливается почтовый антивирусный шлюз, который осуществляет антивирусную обработку почтовых сообщений, проходящих по SMTP протоколу.

8. Настройка антивирусных средств рекомендует обеспечивать:

1) регулярное обновление антивирусных баз в определенное время дня – не реже 1 раза в день;

2) автоматический запуск антивирусного монитора при каждой перезагрузке компьютера или перезапуске серверов;

3) полную антивирусную проверку (сканирование) локальных дисков, установленных на компьютере и серверах в определенное время и по заданным параметрам;

4) лечение зараженных вирусов файлов или удаление при невозможности лечения;

5) автоматическое сканирование съемных носителей при подключении;

6) оповещение пользователя о подозрительных и зараженных объектах;

7) проверку web-страниц на наличие вредоносного кода.

9. Установка и обновление антивирусных средств на рабочих станциях и серверном оборудовании осуществляются в сроки и периодичностью, установленные в утвержденных структурным подразделением либо ответственным за обеспечение ИБ План-графиках.

34

3. Порядок проведения антивирусного контроля

10. Установка (изменение) системного и прикладного обеспечения компьютеров и локальной вычислительной сети рекомендуется осуществлять специалистами технической поддержки.

11. Устанавливаемое (изменяемое) на компьютер/сервер программное обеспечение необходимо проверять на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка.

12. Обязательному антивирусному контролю подлежит любая информация (тестовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съемных носителей (флэш-накопители, магнитные диски, ленты, CD-ROM, и т.п.), получаемых от сторонних лиц и организаций, в том числе информация на запускаемых веб-страницах.

13. Настройка антивирусных средств на рабочих станциях рекомендуется обеспечивать автоматический антивирусный контроль в реальном режиме времени (антивирусный монитор).

14. Контроль информации на съемных носителях рекомендуется производить непосредственно перед ее использованием.

15. Дополнительный антивирусный контроль электронных архивов, находящихся на серверах, должен проводиться системным администратором.

4. Права и обязанности пользователей и специалистов технической поддержки

16. Пользователю на своем персональном компьютере не допускается:

1) изменять настройки и конфигурацию антивирусных приложений;

2) удалять или добавлять какие-либо антивирусные программы;

3) работать со съемными носителями без предварительной их проверки, установленной на персональном компьютере антивирусной программы;

4) запускать неизвестные приложения, пришедшие по электронной почте или файлы сомнительного происхождения, скаченные из общедоступных сетей или со съемных носителей.

17. Пользователю рекомендуется:

1) ежедневно в начале работы при загрузке компьютера убедиться в наличии справа на панели задач значка (пиктограммы) программы антивирусной защиты, в случае его отсутствия уведомить об этом специалиста технической поддержки;

2) самостоятельно запускать внеплановую антивирусную проверку локальных дисков своего персонального компьютера при получении уведомления от службы технической поддержки о наличии вируса в

корпоративной вычислительной сети, а также при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

3) осуществлять проверку всех файлов и приложений на носителях информации сомнительного или неавторизованного происхождения, или файлов, полученных из общедоступных сетей, на наличие вирусов;

4) в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, незамедлительно сообщить об этом специалистам технической поддержки и остановить эксплуатацию средств вычислительной техники.

18. Специалистам технической поддержки рекомендуется:

1) устанавливать антивирусные программы на персональных компьютерах/серверах и инструктировать пользователей по произведенным настройкам;

2) при установке программных продуктов предварительно производить их проверку на наличие вирусов;

3) непосредственно после установки программных продуктов выполнять внеплановую антивирусную проверку компьютера;

4) контролировать состояние серверов и корпоративной сети от проникновения вредоносных кодов и атак;

5) при проникновении в корпоративную сеть вирусов рассылать всем пользователям предупреждение и указания по проведению мер антивирусной защиты;

6) не реже одного раза в день производить мониторинг обновлений антивирусных баз на сайтах поставщиков систем антивирусной защиты;

7) обеспечить своевременное размещение обновлений баз средств антивирусной защиты информационных ресурсов на локальных серверах;

8) установить на антивирусном шлюзе блокировку на входящую почту пользователей для получения исполняемых файлов (файлов с расширением exe, com, bat);

9) рекомендуется проводить не реже двух раз в день анализ работы антивирусного шлюза;

10) составлять расписания и порядок работы модулей антивирусной программы.

5. Мероприятия по управлению информационной безопасностью для борьбы с вредоносным программным обеспечением

19. Мероприятия по защите данных рекомендуется предусматривать процедуры по организации резервирования важных информационных ресурсов, как основные компоненты обеспечения информационной безопасности.

36

20. Рекомендуется разработать и утвердить План непрерывности бизнеса, содержащий описание операционных процедур по полному восстановлению систем и восстановлению данных в случае вирусной атаки.

21. В случае возникновения ситуаций, свидетельствующих о возможной вирусной атаке и поражении вследствие ее возникновения информационных ресурсов и компонентов систем, системному администратору рекомендуется обеспечить:

1) изоляцию зараженного компонента от подключения к вычислительной сети, тем самым закрыв доступ пользователям к зараженным ресурсам и уменьшив риск распространения вируса в вычислительной сети;

2) анализ масштаба заражения и удаление вируса посредством лицензионных программных средств либо форматирование диска в случае невозможности удаления;

3) восстановление информации/компонентов программного обеспечения с помощью резервных и эталонных копий в соответствии с Регламентом резервного копирования.

4) полную проверку систем на наличие вирусов после восстановления.

22. Служебная информация, хранящаяся на рабочих станциях пользователей и подвергшаяся заражению, после удаления вирусов восстанавливается из резервных копий файлов с выделенного файл-сервера.

23. По факту возникновения инцидента специалистом п технической поддержки совместно с сотрудником подразделения либо ответственным за обеспечение ИБ составляется акт о внештатной ситуации и вносится запись в Журнал по внештатным ситуациям.

24. Каждый случай заражения вредоносным кодом рекомендуется тщательно анализировать. По результатам анализа сотрудник подразделения либо ответственный за обеспечение ИБ вносит предложения по оптимизации защитных мер на обсуждение рабочей группы. Согласованные изменения должны быть включены в соответствующую документацию и реализованы под контролем сотрудника подразделения либо ответственного за обеспечение ИБ.

25. В результате выявления вирусной атаки или после устранения вирусного заражения, в случае если данные были удалены или зашифрованы вирусом, системному администратору необходимо провести необходимые мероприятия по восстановлению данных. В виду большого разнообразия вирусов и последствий от них, проводимые мероприятия определяются индивидуально в каждом отдельном случае. Рекомендуется руководствоваться рекомендациям производителя антивирусного ПО.

6. Защита от мобильного кода

26. Для защиты от мобильного кода, выполняющего несанкционированные действия, рассматриваются следующие меры: