СЕКРЕТНО

Экз №1

Министерство промышленности и торговли Российской Федерации

**Публичное Акционерное Общество «Северсталь»**

УТВЕРЖДАЮ

Э.Д. Сноуден

№ 2-1-2024 «19» февраля 20\_\_г

**АКТ**

**Разграничения доступа к информации обрабатываемой в информационной (автоматизированной) системе**

АС «Нестор»

Комиссия, назначенная приказом № 01-ИБ-2024 провела классификацию информации, планирующейся к обработке средствами информационной (автоматизированной) системы АС «Нестор»

УСТАНОВИЛА:

1. В рассматриваемой системе выделяются две группы пользователей:  
   а) Системный администратор

б) Администратор безопасности

1. Для системы была избрана дискреционная модель разграничения доступа
2. На основании Акта классификации информации № 1-1-2024 от 19.02.2024 была построена матрица разграничения доступа, представленная в Приложении 1

Приложение 1 на 3 л в 1 экз

|  |  |  |
| --- | --- | --- |
|  | ПОДПИСЬ |  |
| Начальник отдела информационной безопасности |  | Э.Д. Сноуден |
| Начальник отдела информатизации |  | Д.С. Кодеров |
| Системный администратор |  | А.П. Логинов |
| Сетевой администратор |  | В.А. Пакетный |
| Инженер по защите информации |  | М.О. Монастырский |

Приложение № 1

К Акту

Комиссии по введению

В эксплуатацию

АС «Нестор»

От 19.02.24 № 2-1-2024

Таблица 1 «Матрица доступа»

| **№** | **Информационный ресурс** | **Системный администратор** | **Администратор безопасности** |
| --- | --- | --- | --- |
| 1.1 Журналы создаваемые операционными системами | | | |
| 1.1.1 | Журнал событий «Приложения» ОС Windows | Чтение | Полный доступ |
| 1.1.2 | Журнал событий «Система» ОС Windows | Чтение | Полный доступ |
| 1.1.3 | Журнал событий «Безопасность» ОС Windows |  | Полный доступ |
| 1.1.4 | глобальный системный журнал Unix | Чтение | Полный доступ |
| 1.1.5 | информация об авторизации пользователей UNIX |  | Полный доступ |
| 1.1.6 | Журнал драйверов устройств Unix | Чтение | Полный доступ |
| 1.1.7 | Вывод программы update-alternatives, в котором находятся символические ссылки на команды или библиотеки по умолчанию. | Чтение | Полный доступ |
| 1.1.8 | Записи, зарегистрированные во время установки системы | Чтение | Полный доступ |
| 1.1.9 | Записи, созданные службой аудита auditd | Чтение | Полный доступ |
| 1.1.10 | Информация, которая пишется при загрузке операционной системы | Чтение | Полный доступ |
| 1.1.11 | Отчет службы crond об исполняемых командах и сообщения от самих команд. | Чтение | Полный доступ |
| 1.1.12 | связано с печатью и принтерами. | Чтение | Полный доступ |
| 1.1.13 | Неудачные попытки входа в систему. |  | Полный доступ |
| 1.1.14 | Журнал содержит сообщения от ядра и предупреждения | Чтение | Полный доступ |
| 1.1.15 | сообщения USENET. | Чтение | Полный доступ |
| 1.1.16 | Журналы X сервера | Чтение | Полный доступ |
| 1.1.17 | Последняя сессия пользователей |  | Полный доступ |
| 1.1.18 | Список входов пользователей в систему на данный момент. | Чтение | Полный доступ |
| 1.1.19 | Иные системные журналы | Чтение | Полный доступ |
| 1.1.20 | Системные журналы систем составляющих часть инфраструктуры КИИ |  | Полный доступ |
| 1.2 Журналы прикладного ПО | | | |
| 1.2.1 | Для программ установленных с помощью dpkg | Чтение | Полный доступ |
| 1.2.2 | Журналы файлового сервера Samba |  | Полный доступ |
| 1.2.3 | События входа в учетную запись Active Directory |  | Полный доступ |
| 1.2.4 | Управление учетными записями Active Directory |  | Полный доступ |
| 1.2.5 | Доступ к службе каталогов Active Directory |  | Полный доступ |
| 1.2.6 | События входа Active Directory |  | Полный доступ |
| 1.2.7 | Доступ к объектам Active Directory |  | Полный доступ |
| 1.2.8 | Изменение политики Active Directory |  | Полный доступ |
| 1.2.9 | Использование привилегий Active Directory |  | Полный доступ |
| 1.2.10 | Журнал FTP | Чтение | Полный доступ |
| 1.2.11 | Журнал DNS | Чтение | Полный доступ |
| 1.2.12 | Журнал DHCP | Чтение | Полный доступ |
| 1.2.13 | Журнал IP-телефонии | Чтение | Полный доступ |
| 1.2.14 | Журнал SMTP | Чтение | Полный доступ |
| 1.2.15 | Журнал Kerberos | Чтение | Полный доступ |
| 1.2.16 | Журнал Web-серверов | Чтение | Полный доступ |
| 1.2.17 | Журнал СУБД | Чтение | Полный доступ |
| 1.2.18 | Журналы VPN | Чтение | Полный доступ |
| 1.2.19 | Журналы прочих сервисов, программ и служб | Чтение | Полный доступ |
| 1.2.20 | Журналы сервисов, программ и служб АРМ составляющих часть КИИ |  | Полный доступ |
| 1.3 Журналы сетевого взаимодействия | | | |
| 1.3.1 | Перехват сетевого трафика | Чтение | Полный доступ |
| 1.3.2 | Журналы Межсетевых экранов |  | Полный доступ |
| 1.3.3 | Прочие сетевые журналы | Чтение | Полный доступ |
| 1.3.4 | Записи сетевого взаимодействия субъектами которого являются АРМ, составляющие часть КИИ |  | Полный доступ |
| 1.4 Средства безопасности | | | |
| 1.4.1 | Журналы средств АВЗ |  | Полный доступ |
| 1.4.2 | Журналы средств обнаружения/предотвращения вторжений |  | Полный доступ |
| 1.4.3 | Журналы средств предотвращения утечек информации |  | Полный доступ |
| 1.4.4 | Журналы брандмауэров | Чтение | Полный доступ |
| 1.4.5 | Иные средства обеспечения безопасности | Чтение | Полный доступ |
| 1.4.6 | Журналы СКУД |  | Полный доступ |
| 1.4.7 | Журналы средств безопасности в части касающейся записей о КИИ |  | Полный доступ |
| 1.5 Иные категории журналов | | | |
| 1.5.1 | Журналы, создаваемые системами, составляющими часть КИИ |  | Полный доступ |
| 1.5.2 | Прочие журналы | чтение | Полный доступ |

Отп 2 экз.

Экз № 1 – в дело

Экз № 2 – в адрес

Исп и отп Монастырский Максим Олегович

(903) 132 90 78

19.02.2024