СЕКРЕТНО

Экз №1

Министерство промышленности и торговли Российской Федерации

**Публичное Акционерное Общество «Северсталь»**

УТВЕРЖДАЮ

Э.Д. Сноуден

№ 1-1-2024 «19» февраля 20\_\_г

**АКТ**

**Классификации 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. Перечень информации обрабатываемой информации представлен в таблице 1 Приложения 1
2. В случае, если служба явно не указана в Таблице 1 Приложения 1, службу следует относить к категории «иные» соответствующей категории Таблицы 1 Приложения 1
3. В случае, если система составляет часть КИИ, все ее журналы следует относить к специальным разделам Таблицы 1 Приложения 1

Приложение 1 на 2 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 № 1-1-2024

Таблица 1 «Категории информации»

| **№** | **Информационный ресурс** |
| --- | --- |
| 1.1 Журналы создаваемые операционными системами | |
| 1.1.1 | Журнал событий «Приложения» ОС Windows |
| 1.1.2 | Журнал событий «Система» ОС Windows |
| 1.1.3 | Журнал событий «Безопасность» ОС Windows |
| 1.1.4 | глобальный системный журнал Unix |
| 1.1.5 | информация об авторизации пользователей UNIX |
| 1.1.6 | Журнал драйверов устройств Unix |
| 1.1.7 | Вывод программы update-alternatives, в котором находятся символические ссылки на команды или библиотеки по умолчанию. |
| 1.1.8 | Записи, зарегистрированные во время установки системы |
| 1.1.9 | Записи, созданные службой аудита auditd |
| 1.1.10 | Информация, которая пишется при загрузке операционной системы |
| 1.1.11 | Отчет службы crond об исполняемых командах и сообщения от самих команд. |
| 1.1.12 | связано с печатью и принтерами. |
| 1.1.13 | Неудачные попытки входа в систему. |
| 1.1.14 | Журнал содержит сообщения от ядра и предупреждения |
| 1.1.15 | сообщения USENET. |
| 1.1.16 | Журналы X сервера |
| 1.1.17 | Последняя сессия пользователей |
| 1.1.18 | Список входов пользователей в систему на данный момент. |
| 1.1.19 | Иные системные журналы |
| 1.1.20 | Системные журналы систем составляющих часть инфраструктуры КИИ |
| 1.2 Журналы прикладного ПО | |
| 1.2.1 | Для программ установленных с помощью dpkg |
| 1.2.2 | Журналы файлового сервера Samba |
| 1.2.3 | События входа в учетную запись Active Directory |
| 1.2.4 | Управление учетными записями Active Directory |
| 1.2.5 | Доступ к службе каталогов Active Directory |
| 1.2.6 | События входа Active Directory |
| 1.2.7 | Доступ к объектам Active Directory |
| 1.2.8 | Изменение политики Active Directory |
| 1.2.9 | Использование привилегий Active Directory |
| 1.2.10 | Журнал FTP |
| 1.2.11 | Журнал DNS |
| 1.2.12 | Журнал DHCP |
| 1.2.13 | Журнал IP-телефонии |
| 1.2.14 | Журнал SMTP |
| 1.2.15 | Журнал Kerberos |
| 1.2.16 | Журнал Web-серверов |
| 1.2.17 | Журнал СУБД |
| 1.2.18 | Журналы VPN |
| 1.2.19 | Журналы прочих сервисов, программ и служб |
| 1.2.20 | Журналы сервисов, программ и служб АРМ составляющих часть КИИ |
| 1.3 Журналы сетевого взаимодействия | |
| 1.3.1 | Перехват сетевого трафика |
| 1.3.2 | Журналы Межсетевых экранов |
| 1.3.3 | Прочие сетевые журналы |
| 1.3.4 | Записи сетевого взаимодействия субъектами которого являются АРМ, составляющие часть КИИ |
| 1.4 Средства безопасности | |
| 1.4.1 | Журналы средств АВЗ |
| 1.4.2 | Журналы средств обнаружения/предотвращения вторжений |
| 1.4.3 | Журналы средств предотвращения утечек информации |
| 1.4.4 | Журналы брандмауэров |
| 1.4.5 | Журналы SOC |
| 1.4.6 | Иные средства обеспечения безопасности |
| 1.4.7 | Журналы СКУД |
| 1.4.8 | Журналы средств безопасности в части касающейся записей о КИИ |
| 1.5 Иные категории журналов | |
| 1.5.1 | Журналы, создаваемые системами, составляющими часть КИИ |
| 1.5.2 | Прочие журналы |

Отп 2 экз.

Экз № 1 – в дело

Экз № 2 – в адрес

Исп и отп Монастырский Максим Олегович

(903) 132 90 78

19.02.2024