|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.17** | **Поддержка функционирования средств защиты информации от несанкционированного доступа** |   **1.1. Описание услуги** | | | | | | |  |
|  | В рамках предоставления услуги обеспечивается комплекс работ по поддержке функционирования средств защиты информации от несанкционированного доступа (СЗИ от НСД), входящих в подсистему защиты информации от несанкционированного доступа Заказчика; | | | | | | |  |
|  | **1.2. Способ подключения к ИТ-системе (если необходимо и в зависимости от технической возможности организации)** | | | | | | |  |
|  | * Ярлык на Портале терминальных приложений * Прямая ссылка на Web-ресурс из КСПД * Прямая ссылка на Web-ресурс из интернет (требуется СКЗИ на АРМ / не требуется) * «Толстый клиент» на АРМ пользователя (требуется СКЗИ на АРМ / не требуется) * Другой способ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | |  |
|  | **1.3. Группа корпоративных бизнес-процессов / сценариев, поддерживаемых в рамках услуги** | | | | | | |  |
|  | Для настоящей услуги не применяется | | | | | | |  |
|  | **1.4. Интеграция с корпоративными ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  | Система мониторинга информационной безопасности средств и систем информатизации |  | Мониторинг информационной безопасности | | | | |  |
|  | **1.5. Интеграция с внешними ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для настоящей услуги не применяется | | | | |  |
|  | **1.6. Состав услуги** | | | | | | |  |
|  | Центр поддержки пользователей |  | Прием, обработка, регистрация и маршрутизация поступающих обращений от пользователей; | | | | |  |
|  | Функциональная поддержка |  | **В подсистеме защиты информации от несанкционированного доступа:**  Обеспечение работоспособности серверных компонентов подсистемы защиты информации от несанкционированного доступа.  Обеспечение работоспособности клиентов СЗИ от НСД на рабочих местах пользователей и серверах Заказчика.  Установка и настройка клиента ПО СЗИ от НСД в рамках поддержания функционирования подсистемы защиты информации от несанкционированного доступа (по заявке).  Сопровождение компоненты управления аутентификацией пользователей (для режима усиленной аутентификации по паролю или ключевому носителю).  Управление локальными устройствами рабочего места пользователя/Сервера (блокирование/разблокирование).  Сопровождение компоненты обеспечения контроля целостности.  Разграничение доступа к защищаемым ресурсам сети.  Разбор и квитирование событий несанкционированного доступа (НСД).  **Регламентные работы:**  Ежедневный контроль функционирования средств защиты информации от НСД.  Направление отчета по работе СЗИ от НСД по запросу Заказчика. | | | | |  |
|  | Поддержка интеграционных процессов |  | Система мониторинга информационной безопасности средств и систем информатизации | | | | |  |
|  | ИТ-инфраструктура |  | Для настоящей услуги не применяется | | | | |  |
|  | Модификация ИТ-системы |  | Для настоящей услуги не применяется | | | | |  |
|  | **1.7. Наименование и место хранения пользовательской документации:** | | | | | | |  |
|  | * ИТ-система |  |  | | | | |  |
|  | * Портал Госкорпорации «Росатом» |  |  | | | | |  |
|  | * Иное место |  |  | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | Возможность изменения состава обслуживаемых компонентов защиты СЗИ от НСД, в том числе отдельно лицензируемых, обсуждается до начала оказания услуги путём направления запроса от Заказчика в адрес cybersecurity@greenatom.ru (если информация не содержит пометку ограниченного доступа).  В базовый отчёт входит общая информация о работе подсистемы СЗИ от НСД и информация об установленных клиентах СЗИ от НСД за отчётный период.  Перед началом предоставления услуги Заказчик согласует:   * + - Диапазоны IP-адресов подсетей АСЗИ, в рамках которых будет функционировать СЗИ от НСД.     - Предоставление Исполнителю административных привилегий и RDP-доступа к серверным компонентам подсистемы защиты информации от НСД (ко всем серверам безопасности) и к программе управления. При этом смежные права по администрированию подсистемы защиты информации от НСД у работников Заказчика исключаются. Управление параметрами защиты выполняется на основании обращений в адрес Исполнителя.   Перед началом предоставления услуги Заказчик предоставляет Исполнителю:   * + - Пояснительную записку, техническое решение, руководство администратора и руководство пользователя на подсистему защиты информации от несанкционированного доступа;   Полный список технологических ограничений (лимитов) определяется до заключения договора согласно предоставленной Заказчиком опросной карточки подключения услуги. Заполненная опросная карточка направляется на адрес cybersecurity@greenatom.ru (если информация не содержит пометку ограниченного доступа);   * + - Услуга предоставляется Исполнителем на основании лицензии, выданной Федеральной службой по техническому и экспортному контролю на проведение работ, связанных с созданием средств защиты информации.     - Удаленный доступ к необходимым для оказания услуги сегментам технологической сети, программному и аппаратному обеспечению объекта информатизации Заказчика, предоставляется по запросу Исполнителя.     - Лицензию и техническую поддержку для ПО СЗИ от НСД Заказчик приобретает самостоятельно.     - Работы по развёртыванию инфраструктуры для работы подсистемы защиты информации от несанкционированного доступа, обновлению версии ПО СЗИ от НСД/переводу на иное решение являются предметом отдельного договора;   В случае отсутствия у Исполнителя возможности удалённого управления защитой от НСД Заказчика, в рамках выполнении работ по поддержке функционирования средств защиты от НСД, SLA (время исполнения обращения) не гарантируется; | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  | Поддержка функционирования средств защиты информации от несанкционированного доступа:  0,001904277 ПРМ (Единица измерения – АРМ/Рабочее место пользователя)  0,003564155 ПРМ (Единица измерения – Сервер / виртуальная машина) | | | | |  |
|  | Поддержка интеграционных процессов |  | Для настоящей услуги не применяется | | | | |  |
|  | ИТ-инфраструктура |  | Для настоящей услуги не применяется | | | | |  |
|  | **1.10. Дополнительные параметры оказания услуги** | | | | | | |  |
|  | 1.10.1. Допустимый простой ИТ-ресурса в течении года, часов |  | 22 | | | | |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | 30 | | | | |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | 4 | | | | |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | 8 | | | | |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости  ИТ-ресурса |  | нет | | | | |  |
|  | | | | | | | | |