|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.15** | **Поддержка функционирования средств антивирусной защиты** |   **1.1. Описание услуги** | | | | | | |  |
|  | В рамках предоставления услуги обеспечивается комплекс работ по поддержке функционирования средств антивирусной защиты, входящих в подсистему антивирусной защиты 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 |  | **Поддержка функционирования подсистемы антивирусной защиты**  Обеспечение работоспособности серверных компонентов подсистемы антивирусной защиты.  Обеспечение работоспособности агентов антивирусного ПО на рабочих местах пользователей и серверах Заказчика.  Обеспечение актуальности баз данных антивирусной защиты.  Установка и настройка клиента антивирусного ПО в рамках поддержания функционирования подсистемы антивирусной защиты (по заявке).  Установка лицензии, распространение антивирусных баз на рабочие места пользователей и сервера в установленном диапазоне.  Управление настройками групповых политик антивирусной защиты.  Удаление вирусов.  **Регламентные работы:**  Ежедневный контроль функционирования средств антивирусной защиты.  Выполнение периодического сканирования рабочего места пользователя и серверов на наличие вирусов.  Направление отчета о состоянии антивирусной защиты 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** | | | | | | |  |
|  | Изменение настроек групповых политик антивирусной защиты осуществляется на основании рекомендаций производителя антивирусного ПО и технических специалистов, поддерживающих ИТ-инфраструктуру.  В перечень доступных отчётов для запроса входит базовый набор (отчёт о вирусах, отчёт о состоянии защиты).  Удаление вирусов с рабочих мест пользователей и серверов осуществляется в соответствии с инструкцией (руководством) администратора.  Перед началом предоставления услуги Заказчик согласует:  ▪ Диапазоны IP-адресов подсетей АСЗИ, в рамках которых будет функционировать подсистема антивирусной защиты.  ▪ Время запуска и параметры проверок на наличие вирусов для рабочих мест пользователей и Серверов.  ▪ Предоставление Исполнителю административных привилегий в подсистеме антивирусной защиты. При этом смежные права по администрированию подсистемы антивирусной защиты 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 антивирусной защиты;  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 антивирусного ПО Заказчик приобретает самостоятельно.  ▪ Работы по развёртыванию инфраструктуры для работы средств антивирусной защиты, обновлению версии/переводе на другое решение являются предметом отдельного договора;  В случае отсутствия у Исполнителя возможности удалённого управления антивирусной защитой 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 подсистемы антивирусной защиты:  0,000664062 ПРМ (Единица измерения – АРМ/Рабочее место пользователя)  0,001242897 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 | | | | |  |
|  | | | | | | | | |