|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |

|  |  |  |
| --- | --- | --- |
|  | **ISS.13** | **Поддержка функционирования систем обнаружения вторжений** |

**1.1. Описание услуги** |  |
|  | В рамках предоставления услуги обеспечивается поддержка и администрирование подсистемы обнаружения вторжений network based;Услуга осуществляется в соответствии с федеральными нормативными правовыми актами и локальными нормативными актами Госкорпорации «Росатом» в области защиты информации. |   |
|  | **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 \_\_\_ Для настоящей услуги не применяется

  |  |
|  | **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 (интеграция с системой ГосСОПКА) |   |
|  | **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 |  | Для network based:Работа с правилами обнаружения* Обновление правил обнаружения атак
* Включение и отключение правил и групп правил обнаружения атак
* Добавление и редактирование пользовательских правил обнаружения атак
* Создание резервной копии пользовательских правил обнаружения атак
* Создание пользовательских правил обнаружения атак
* Отладка пользовательских правил

Настройка уведомления об атаках (вторжениях)Настройка сетевых интерфейсовЗапуск системы обнаружения вторжений в режиме предотвращения вторжений (по согласованию с Заказчиком)Запуск и остановка системы обнаружения вторженийПросмотр системных журналовРезервное копирование и восстановление конфигурационных файловНастройка пороговых значений загрузки системных ресурсов (если применимо).Предоставление отчетности (по запросу заказчика)Проверка механизма срабатывания правилПодержание работоспособности системы |   |
|  | Поддержка интеграционных процессов |  | В рамках данной услуги не осуществляется |   |
|  | ИТ-инфраструктура |  | Услуга оказывается на инфраструктуре заказчика, в отдельных случаях оборудование может предоставляться исполнителем |   |
|  | Модификация ИТ-системы |  | В рамках данной услуги не осуществляется |   |
|  | **1.7. Наименование и место хранения пользовательской документации:** |  |
|  | * ИТ-система
 |  |  |   |
|  | * Портал Госкорпорации «Росатом»
 |  |  |   |
|  | * Иное место
 |  | Не предусмотрено |  |
|  |  |  |
|  |  |   |
|  | **1.8. Ограничения по оказанию услуги** |  |
|  | Услуга не подразумевает реагирования на обнаруженные события, если система обнаружения вторжений работает в режиме обнаружения вторжений. Исполнитель не гарантирует соблюдение параметров качества оказания услуги, в случае отсутствия у Заказчика:* активной технической поддержки и лицензий на аппаратно-программное обеспечение, используемое в системе обнаружения вторжений;
* сопроводительной документации (пояснительная записка, техническое решение и т.п.) на систему обнаружения вторжений;

Оказание услуги невозможно при одновременном наличии административных привилегий в системе обнаружения вторжений у Заказчика и у Исполнителя. После передачи подсистемы контроля (анализа) защищенности информации на обслуживание исключаются все административные права, которые были у Заказчика. Данные права полностью передаются исполнителю. |   |
|  | **1.9. Норматив на поддержку** |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) |  |
|  | Функциональная поддержка |  | Поддержка функционирования систем обнаружения вторжений network based – 0,000018258 (Единица измерения – IP адрес в защищаемой сети)Поддержка функционирования систем обнаружения вторжений |  |
|  | Поддержка интеграционных процессов |  |  Не предусмотрена. |  |
|  | ИТ-инфраструктура |  |  Не предусмотрена. |  |
|  | **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 |  | Обсуждается отдельно, при наличии требования Заказчика |  |
|  |