|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.10** | **Мониторинг информационной**  **безопасности средств и систем информатизации** |   **1.1. Описание услуги** | | | | | | |  |
|  | Лицензируемый ФСТЭК России вид деятельности. В рамках предоставления услуги обеспечивается комплекс работ по поддержке функционирования системы мониторинга событий информационной безопасности (ИБ) Заказчика (Система), сбор и анализ событий ИБ с ИТ-инфраструктуры Заказчика, выявление инцидентов ИБ, реагирование на инциденты ИБ, оказание методической помощи и консультирование уполномоченных специалистов Заказчика по части устранения последствий инцидентов ИБ, а также, предотвращения аналогичных инцидентов ИБ в будущем. | | | | | | |  |
|  | **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:   * портал самообслуживания <https://support.rosatom.ru/sm/index.do> или по телефону контактного центра АО «Гринатом» +7(499)949-29-99 * п/я soc@greenatom.ru (если информация не содержит пометку ограниченного доступа) * п/я soc@rosatom.ru по ЗКПС (если информация содержит пометку ограниченного доступа) | | | | | | |  |
|  | **1.3. Группа корпоративных бизнес-процессов / сценариев, поддерживаемых в рамках услуги** | | | | | | |  |
|  | Для данной услуги не применяется | | | | | | |  |
|  | **1.4. Интеграция с корпоративными ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  | Система мониторинга |  | Интеграция с системой мониторинга доступности системы | | | | |  |
|  | **1.5. Интеграция с внешними ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  |  | | | | |  |
|  | **1.6. Перечень работ, оказываемых в рамках услуги** | | | | | | |  |
|  | Центр поддержки пользователей |  | Прием, обработка, регистрация и маршрутизация поступающих обращений от пользователей | | | | |  |
|  | Функциональная поддержка |  | * + 1. **Обследование внутреннего периметра ИТ-инфраструктуры Заказчика:** * сбор данных по активам Заказчика и предоставление рекомендаций по составу и типу подключаемых источников событий ИБ.   + 1. **Обеспечение функционирования Системы:** * конфигурирование / добавление / удаление компонентов Системы; * установка / замена доверенных сертификатов; * активация лицензий 1 раз в год; * управление пользователями и ролями доступа; * настройка профилей и задач сбора событий ИБ; * настройка системы хранения данных; * мониторинг состояния Системы; * настройка резервного копирования компонентов Системы; * резервное копирование компонентов Системы; * внеплановое резервное копирование Системы; * восстановление работоспособности компонентов Системы; * обновление базы правил, предоставленных разработчиком или интегратором Системы; * подключение Системы к отраслевому Корпоративному центру ГосСОПКА Госкорпорации «Росатом».   + 1. **Обновление Системы по ТР Заказчика:** * **обновление системы без сохранения данных**: обновление Системы с текущей версии на следующую версию согласно нумерации производителя без сохранения данных. * **обновление системы с сохранением данных[[1]](#footnote-1):** обновление Системы с текущей версии на следующую версию согласно нумерации производителя с сохранением данных.   + 1. **Сбор, анализ событий ИБ и выявление инцидентов ИБ в Системе:** * подключение стандартных источников событий ИБ[[2]](#footnote-2); * проверка правил корреляции событий ИБ на соответствие отраслевым требованиями по ИБ; * проверка правил нормализации для источников событий ИБ; * выявление ложных срабатываний и нерелевантных инцидентов ИБ; * создание исключений для фильтрации ложных срабатываний и нерелевантных инцидентов ИБ; * подтверждение классификации события ИБ как инцидент ИБ; * регистрация инцидента ИБ в Системе; * присвоение уровня критичности инцидента ИБ.   + 1. **Реагирование на инциденты ИБ, выявленные в Системе:** * оповещение Заказчика о возникновении инцидента ИБ; * предоставление информации, связанной с инцидентом ИБ и зафиксированной в Системе; * предоставление рекомендаций по локализации и ликвидации инцидентов ИБ; * получение информации от Заказчика о принятых мерах по локализации и ликвидации выявленного инцидента ИБ, о масштабах распространения и последствиях выявленного инцидента ИБ; * предоставление сведений об инциденте ИБ в отраслевой Корпоративный центр ГосСОПКА Госкорпорации «Росатом».   + 1. **Подключение нестандартных источников событий ИБ[[3]](#footnote-3) в Систему.**     2. **Предоставление отчётности по выявленным инцидентам ИБ:** * еженедельный отчёт по форме отраслевого Корпоративного центра ГосСОПКА Госкорпорации «Росатом» (по запросу не чаще 1-го раза в неделю); * ежемесячный отчёт по форме отраслевого Корпоративного центра ГосСОПКА Госкорпорации «Росатом» (по запросу не чаще 1-го раза в месяц); * ежеквартальный отчет по форме отраслевого Корпоративного центра ГосСОПКА Госкорпорации «Росатом» (по запросу не чаще 1-го раза в квартал). | | | | |  |
|  | Поддержка интеграционных процессов |  | Для данной услуги не применяется | | | | |  |
|  | ИТ-инфраструктура |  | Для данной услуги не применяется | | | | |  |
|  | Модификация ИТ-системы |  | Для данной услуги не применяется | | | | |  |
|  | **1.7. Наименование и место хранения пользовательской документации:** | | | | | | |  |
|  | * ИТ-система |  | Для данной услуги не применяется | | | | |  |
|  | * Портал Госкорпорации «Росатом» |  | Для данной услуги не применяется | | | | |  |
|  | * Иное место |  | Для данной услуги не применяется | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | Перед началом оказания услуги необходимо провести обследование внутреннего[[4]](#footnote-4) периметра ИТ-инфраструктуры Заказчика[[5]](#footnote-5). Полный список технологических ограничений (лимитов) определяется до заключения договора согласно предоставленной Заказчиком опросной карточки подключения услуги[[6]](#footnote-6).  В услугу не входит: проведение обследования внешнего периметра Заказчика, устранение обнаруженных уязвимостей, расследование инцидентов ИБ, ликвидация последствий инцидентов ИБ, восстановление инфраструктуры Заказчика.  Исполнитель не гарантирует соблюдение параметров качества оказания услуги, указанных в пункте 1.6, в случае: 1. Отсутствия действующей технической поддержки и лицензий на программное обеспечение, используемое в Системе; 2. Отсутствия сопроводительной документации (пояснительная записка, техническое решение и т.п.) на Систему; 3. В случае недоступности Системы.  Оказание услуги невозможно при одновременном наличии административных привилегий в Системе у Заказчика и у Исполнителя. После передачи Системы на обслуживание Исполнителю исключаются все административные права, которые были у Заказчика. Данные права полностью передаются Исполнителю.  Минимальный срок хранения данных об инцидентах ИБ устанавливаются нормативными актами Российской Федерации, ФСБ России и ФСТЭК России и в соответствие с имеющимися мощностями у Заказчика.  Для предприятий и организаций, ранее обсуживающихся по услуге OPR.3 «Поддержка функционирования систем информационной безопасности», норматив в части мониторинга событий информационной безопасности (SIEM) осуществляется по услуге ISS.10. Предельное значение трудозатрат рассчитывается менеджером услуги индивидуально. Для оказания услуги в случае отсутствия Системы на мощностях Заказчика разворачивается лог-коллектор силами Исполнителя. | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  | **Обследование внутреннего периметра ИТ-инфраструктуры:**  0,003047600  Единица измерения: узел – АРМ, сервер, телекоммуникационное оборудование.  **Обеспечение функционирования Системы:**  - постоянные работы: 0,031506016   |  |  |  | | --- | --- | --- | | **Наименование работ** | **Трудозатраты на ед. измерения** | **Единица измерения** | | мониторинг состояния Системы | 0,017361111 | Система | | резервное копирование компонентов Системы | 0,002240143 | Система | | обновление базы правил, предоставленных разработчиком или интегратором Системы | 0,011904762 | Система |   -разовые работы:   |  |  |  | | --- | --- | --- | | **Наименование работ** | **Трудозатраты на ед. измерения** | **Единица измерения** | | конфигурирование / добавление / удаление компонентов Системы | 0,047619048 | Компонент | | установка / замена доверенных сертификатов | 0,011904762 | Сертификат | | активация лицензий 1 раз в год | 0,011363636 | Лицензия | | управление пользователями и ролями доступа | 0,001488095 | Пользователь | | настройка профилей и задач сбора событий ИБ | 0,005952381 | Профиль + Задача | | настройка системы хранения данных | 0,017857143 | Система | | настройка резервного копирования компонентов Системы | 0,017857143 | Система | | внеплановое резервное копирование Системы | 0,005952381 | Система | | восстановление работоспособности компонентов Системы | 0,023809524 | Компонент | | подключение Системы к отраслевому Корпоративному центру ГосСОПКА Госкорпорации «Росатом» | 0,238095238 | Подключение |   **Обновление Системы по ТР Заказчика:**   |  |  |  | | --- | --- | --- | | **Наименование работ** | **Трудозатраты на ед. измерения** | **Единица измерения** | | **- обновление системы без сохранения данных** | | | | Конфигурация «All-in-One» | 1,71000000 | Система | | Низконагруженная система | 2,00000000 | Система | | Средненагруженная система | 2,36000000 | Система | | Высоконагруженная Система | 2,620000000 | Система | | Агент | 0,180000000 | Агент | | **- обновление системы с сохранением данных** | | | | Конфигурация «All-in-One» | 2,052000000 | Система | | Низконагруженная система | 2,400000000 | Система | | Средненагруженная система | 2,832000000 | Система | | Высоконагруженная Система | 3,144000000 | Система | | Агент | 0,180000000 | Агент |   **Сбор, анализ событий ИБ и выявление инцидентов ИБ в Системе:**   |  |  | | --- | --- | | до 250 событий в секунду | 0,000029760 | | до 500 событий в секунду | 0,000028270 | | до 1000 событий в секунду | 0,000026790 | | до 2500 событий в секунду | 0,000023810 | | свыше 2500 событий в секунду | 0,000019350 |   Единица измерения: 10 000 событий ИБ.  **Реагирование на инциденты ИБ, выявленные в Системе:**  0,003472000  Единица измерения: Инцидент ИБ.  **Подключение нестандартных источников событий ИБ в Систему:**  0,285710000  Единица измерения: Источник.  **Предоставление отчётности по выявленным инцидентам ИБ:**   |  |  | | --- | --- | | Еженедельный отчёт | 0,011905000 | | Ежемесячный отчёт | 0,047620000 | | Ежеквартальный отчет | 0,095240000 |   Единица измерения: Отчёт. | | | | |  |
|  | 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 |  | 96 | | | | |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | Для данной услуги не применяется | | | | |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости  ИТ-ресурса |  | Для данной услуги не применяется | | | | |  |
|  | | | | | | | | |

1. При условии предоставления серверных мощностей для миграции. [↑](#footnote-ref-1)
2. Стандартный источник событий ИБ – источник ИБ, подключение которого документально описано разработчиком Системы, а также, для которого написано правило нормализации и корреляции и протестировано разработчиком Системы. Правила нормализации и корреляции применяются как есть, без внесения изменений. При необходимости изменений правил нормализации и корреляции работы выполняются в рамках работ по подключению нестандартных источников событий ИБ. Состав работ: настройка профиля в Системе, добавление учётных записей в Системе, создание и запуск задач в Системе. [↑](#footnote-ref-2)
3. Состав работ: настройка профиля в Системе, добавление учётных записей в Системе, создание и запуск задач в Системе, разработка и тестирование правил нормализации и корреляции. [↑](#footnote-ref-3)
4. Рекомендуется дополнительно проводить обследование внешнего периметра ИТ-инфраструктуры Заказчика. [↑](#footnote-ref-4)
5. При необходимости выездного обследования командировочные расходы оплачиваются отдельно. [↑](#footnote-ref-5)
6. Заполненная опросная карточка подключения услуги направляется в рабочем порядке менеджеру услуги. [↑](#footnote-ref-6)