|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.26** | **Сопровождение информационной системы на соответствие требованиям информационной безопасности** |   **1.1. Описание услуги** | | | | | | |  |
|  | Заказчику предоставляется услуга по сопровождению информационной системы (далее - ИС) Заказчика, оценка влияния изменений, вносимых в ИС, на подсистему информационной безопасности ИС, а также контролю соответствия ИС Заказчика требованиям безопасности 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 применимо | | | | | | |  |
|  | **1.3. Группа корпоративных бизнес-процессов / сценариев, поддерживаемых в рамках услуги** | | | | | | |  |
|  | Для настоящей услуги не применимо | | | | | | |  |
|  | **1.4. Интеграция с корпоративными ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для настоящей услуги не применимо | | | | |  |
|  | **1.5. Интеграция с внешними ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для настоящей услуги не применимо | | | | |  |
|  | **1.6. Состав услуги** | | | | | | |  |
|  | Центр поддержки пользователей |  | Для настоящей услуги не применимо | | | | |  |
|  | Функциональная поддержка |  | В рамках предоставления услуги Исполнитель на основании лицензии ФСТЭК России выполняет следующие работы:   1. Предоставление информации по ИС, для которых проводилась оценка соответствия требованиям о защите информации; 2. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС: 3. Формирование плана работ по защите информации в ИС в соответствии с Едиными отраслевыми методическими указаниями по информационной безопасности в Госкорпорации «Росатом» и её организациях, а также нормативно-методической документацией ФСТЭК России; 4. Анализ угроз безопасности информации в ИС:    * 1. Анализ уязвимостей в общесистемном и прикладном программном обеспечении, на базе которых построена архитектура ИС;      2. Проведение контроля корректности функционирования докер-контейнеров, используемых в ИС;      3. Проведение анализа результата выявленных уязвимостей;      4. Разработка рекомендаций по устранению выявленных уязвимостей; 5. Управление конфигурацией информационной системы и системы защиты: 6. Анализ и оценка потенциального воздействия планируемых изменений, вносимых в ИС в части изменения уровня конфиденциальности сведений, обрабатываемых в ИС, архитектуры ИС или описания технологического процесса обработки информации в ИС; 7. Подготовка предложений по совершенствованию организационных и технических мер защиты информации, реализованных в ИС, в том числе по использованию импортонезависимых средств защиты информации; 8. Актуализация организационно-распорядительных и эксплуатационных документов на систему защиты информации ИС, необходимость изменения которых обусловлена жизненным циклом ИС; 9. Анализ сетевых взаимодействий, планируемых к внесению в ИС, необходимых для реализации планируемых изменений; 10. Контроль выполнения работ по установке, обновлению и модернизации средств защиты информации в ИС 11. Проведение дополнительных испытаний ИС на соответствие требованиям о защите информации по результатам внесенных изменений; 12. Оценка результатов испытаний ИС и подготовка отчётной документации:     1. Подготовка протокола по результатам ежегодного контроля ИС;     2. подготовка протокола контроля защиты информации раз в 2 года. 13. Направление протокола контроля защиты информации в ФСТЭК России раз в 2 года. | | | | |  |
|  | Поддержка интеграционных процессов |  | Для настоящей услуги не применимо | | | | |  |
|  | ИТ-инфраструктура |  | Для настоящей услуги не применимо | | | | |  |
|  | Модификация ИТ-системы |  | Для настоящей услуги не применимо | | | | |  |
|  | **1.7. Наименование и место хранения пользовательской документации:** | | | | | | |  |
|  | * ИТ-система |  | Для настоящей услуги не применимо | | | | |  |
|  | * Портал Госкорпорации «Росатом» |  | Для настоящей услуги не применимо | | | | |  |
|  | * Иное место |  | Для настоящей услуги не применимо | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | 1. Услуга предоставляется Исполнителем в отношении ИС Заказчика, аттестация/оценка соответствия требованиям о защите информации которых проводились АО «Гринатом». 2. В случае развития (модернизации) ИС, приводящего к повышению класса защищенности (уровня защищенности, категории значимости) ИС и (или) к изменению архитектуры системы защиты информации ИС в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры системы защиты информации, состава и мест расположения ИС и его компонентов, проводится повторная аттестация ИС. 3. Услуга предоставляется Исполнителем на основании лицензии, выданной Федеральной службой по техническому и экспортному контролю (Лицензия ФСТЭК России от 10.02.2011 рег. № 1354). 4. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС на основании Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» должно осуществляться в соответствии с эксплуатационной документацией и ОРД по защите информации. 5. Меры по управлению конфигурацией информационной системы и системы защиты входят в состав мер по обеспечению безопасности информации, реализуемых в рамках системы защиты информации с учетом актуальных угроз безопасности информации и применяемых информационных технологий в соответствии с Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» 6. Заказчик перед началом оказания услуги предоставляет Исполнителю:  * акт передачи ИС в поддержку, осуществляемую АО «Гринатом»; * анализ степени конфиденциальности информации, обрабатываемой/планируемой к обработке в ИС; * утвержденное техническое решение/проект на ИС; * организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам ИС (Матрицу доступа субъектов доступа к объектам доступа); * копии сертификатов соответствия требованиям безопасности информации, формуляров, технических условий эксплуатации на средства защиты информации, используемые в ИС; * утвержденное техническое задание на создание (развитие, модернизацию) ИС.  1. В случае развития (модернизации) ИС, в ходе которого изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичные средства или заменены на аналогичные средства проводятся дополнительные аттестационные испытания. Сведения об изменениях аттестованного объекта информатизации и проведенных при этом аттестационных испытаниях включаются в технический паспорт ИС. Действие аттестата соответствия не прекращается. 2. Услуга предоставляется, учитывая порядок организации и проведения работ по аттестации ИС на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденный Приказом ФСТЭК России от «29» апреля 2021 г. № 77. 3. В соответствии с п.31 Порядка организации и проведения работ по аттестации ИС на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну утвержден Приказом ФСТЭК России от «29» апреля 2021 г. № 77 Протокол контроля защиты информации на аттестованном объекте информатизации не реже одного раза в два года представляется владельцем объекта информатизации в ФСТЭК России. 4. В случае использования в ИС прикладного программного обеспечения, реализующего механизмы обеспечения информационной безопасности, разработанного на базе OpenSource технологий, дополнительно Заказчиком должна быть приобретена Услуга по сопровождению разработки безопасного программного обеспечения для проведения анализа исходного кода ПО, анализа заимствованных компонентов ПО, анализа контейнеризированных компонентов ПО, динамического анализа ПО, фаззинг-тестирования ПО. | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  | Сопровождение информационной системы на соответствие требованиям информационной безопасности (ед. изменения - ИС, трудозатраты на ед. измерения - 1,50000000), в состав работ входит: | | | | |  |
| * Предоставление информации по ИС, для которых проводилась оценка соответствия требованиям о защите информации, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,050000000). | | | | |
| * Формирование плана работ по защите информации в ИС, анализ и оценка потенциального воздействия планируемых изменений, вносимых в ИС, подготовка предложений по совершенствованию организационных и технических мер защиты информации, реализованных в ИС , (ед. изменения - ИС, трудозатраты на ед. измерения - 0,05000000). | | | | |
| * Анализ уязвимостей в общесистемном и прикладном программном обеспечении, на базе которых построена архитектура ИС, (ед. изменения – ИС, трудозатраты на ед. измерения - 0,15000000). | | | | |
| * Разработка рекомендаций по устранению выявленных уязвимостей, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,15000000). | | | | |
| * Актуализация организационно-распорядительных и эксплуатационных документов на систему защиты информации ИС, необходимость изменения которых обусловлена жизненным циклом ИС (Анализ степени конфиденциальности информации, обрабатываемой в ИС; Модель угроз и нарушителя ИС; Перечень защищаемых ресурсов ИС, Ролевая модель доступа ИС; Технический паспорт на ИС), (ед. изменения - ИС, трудозатраты на ед. измерения - 0,600000000). | | | | |
| * Анализ сетевых взаимодействий, планируемых к внесению в ИС, необходимых для реализации планируемых изменений, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,150000000). | | | | |
| * Согласование и контроль выполнения работ по установке, обновлению и модернизации средств защиты информации в ИС, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,050000000). | | | | |
| * Проведение дополнительных испытаний ИС на соответствие требованиям о защите информации по результатам внесенных изменений, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,05000000). | | | | |
| * Оценка результатов испытаний ИС и подготовка отчётной документации, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,20000000). | | | | |
|  |  | * Направление протокола контроля защиты информации в ФСТЭК России, (ед. изменения - ИС, трудозатраты на ед. измерения - 0,05000000). | | | | |  |
|  | 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 |  | Для настоящей услуги не применимо | | | | |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | Для настоящей услуги не применимо | | | | |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | Для настоящей услуги не применимо | | | | |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | Для настоящей услуги не применимо | | | | |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости  ИТ-ресурса |  | Для настоящей услуги не применимо | | | | |  |
|  | | | | | | | | |