|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.30** | **Администратор информационной безопасности критической информационной инфраструктуры** |   **1.1. Описание услуги** | | | | | | |  |
|  | Заказчику предоставляется услуга Администратора информационной безопасности объектов критической информационной инфраструктуры (далее – КИИ) для выполнения требований по информационной безопасности, составления и актуализации отчетной и организационной распорядительной документации критической информационной инфраструктуры 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 \_для данной услуги не применяется | | | | | | |  |
|  | **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** | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  | **1.5. Интеграция с внешними ИТ-системами** | | | | | | |  |
|  | **ИТ-система** |  | **Группа процессов** | | | | |  |
|  |  |  | Для данной услуги не применяется | | | | |  |
|  | **1.6. Состав услуги** | | | | | | |  |
|  | Центр поддержки пользователей |  | Для данной услуги не применяется | | | | |  |
|  | Функциональная поддержка |  | В рамках предоставления услуги Исполнитель на основании лицензии ФСТЭК России выполняет следующие работы:   1. Составление новых сведений о категорировании в случае планового и внепланового изменения объекта КИИ (модернизация) и согласование со ФСТЭК России; 2. Проведение категорирования объекта КИИ и согласование сведений о проведении категорирования со ФСТЭК России; 3. Составление сведений о значимом объекте КИИ и согласование его подключения с сетями связи общего пользования; 4. Актуализация модели угроз безопасности информации объекта КИИ в ходе модернизации объекта КИИ; 5. Составление для Заказчика ежемесячного отчета о текущем состоянии объектов критической информационной инфраструктуры; 6. Повторное категорирование объектов КИИ и согласование сведений о проведении категорирования со ФСТЭК России; 7. Разработка политики по обеспечению безопасности, на объекты КИИ; 8. Разработка положения по организации и проведению работ по обеспечению безопасности объектов КИИ; 9. Разработка регламентов, описывающих правила и процедуры по обеспечению безопасности объекта КИИ 10. Изменение перечня объектов КИИ после создания или вывода из эксплуатации объекта критической информационной инфраструктуры; 11. Изменение перечня критических процессов в случае изменения видов деятельности организации; 12. Формирование плана мероприятий по обеспечению безопасности объектов КИИ Заказчика (по запросу субъекта, но не реже одного раза в календарный год); 13. Изменение и составление плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимые объекты критической информационной инфраструктуры; согласование с ФСБ России и ФСТЭК России; 14. Составление приказа по обеспечению безопасности объектов КИИ и внесение изменений 15. Оценка критических процессов и подготовка отчета о влиянии компьютерных инцидентов при возникновении ущербов в информационной инфраструктуре; 16. Анализ актуальности и достоверности сведений о проведении категорирования объектов критической информационной инфраструктуры и присвоении ему соответствующей категории значимости, делящийся на этапы: 17. отправка запроса для оценки актуальности и достоверности сведений о проведении категорирования объектов КИИ; 18. проверка сведений о проведении категорирования объектов КИИ и присвоении им соответствующей категории значимости; 19. подготовка отчета о правильности, актуальности и достоверности проведения категорирования и составления сведений о проведении категорирования объектов КИИ. | | | | |  |
|  | 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 |  | В субъекте критической информационной инфраструктуры, где расположены объекты обследования | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | 1.8.1. Для информационной инфраструктуры Заказчика действуют ограничения, предусмотренные требованиями информационной безопасности для КИИ.  Объекты КИИ должны принадлежать по праву собственности Заказчику. Требования и порядок оказания услуги должен соответствовать единым отраслевым методическим указаниям по проведению категорирования, законодательным и нормативным правовым актам Российской Федерации.  1.8.2. Заказчик перед началом оказания услуги предоставляет исполнителю:   * документ, описывающий сведения об объекте КИИ (наименование объекта; адреса размещения объекта; сфера (область) деятельности, в которой функционирует объект; назначение и тип объекта); * документ, описывающий сведения о субъекте КИИ (наименование, адрес местонахождения субъекта, должность, фамилия, имя, отчество (при наличии) руководителя субъекта, а также должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, ИНН субъекта и КПП его обособленных подразделений); * документ, описывающий сведения о взаимодействии объекта КИИ и сетей связи (категория сети электросвязи, наименование оператора связи, цель взаимодействия с сетью электросвязи, способ взаимодействия с сетью электросвязи); * документ, описывающий сведения о лице, эксплуатирующем объект КИИ (наименование, адрес, элемент (компонент) объекта, который эксплуатируется лицом, ИНН лица, эксплуатирующего объект); * документ, описывающий сведения о программных, программно-аппаратных средствах и средствах защиты информации, используемых на объекте КИИ; * документ, описывающий сведения об угрозах безопасности информации, категориях нарушителей и типах компьютерных инцидентах в отношении объекта КИИ; * копии схемы организации сети связи и протоколов испытаний (для средств, прошедших оценку соответствия в форме приемки); * утвержденную и введенную в действие организационно-распорядительную документацию на объект КИИ; * сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; * сведения о должностных лицах ответственных за обеспечение безопасности объектов КИИ; * копию Устава организации, актуальную выписку из Единого государственного реестра юридических лиц; * материалы, выработанные постоянно действующей комиссией по категорированию; * копии сертификатов соответствия требованиям безопасности информации, формуляров, технических условий эксплуатации на компоненты системы защиты информации; * копии действующих эксплуатационных документов на используемые средства защиты информации на объекте КИИ, содержащих актуальную информацию на момент начала оказания услуг; * консолидированную бухгалтерскую отчетность для расчетов масштабов ущербов по экономическим показателям.   1.8.3. Заказчик может давать запросы на аналитическое обоснование подготовки документов согласно работам по услуге с пояснениями принятия того или иного решения.  1.8.4. Консультирование Заказчика по вопросам обеспечения безопасности КИИ, осуществляется администратором на площадке Заказчика в процессе оказания услуги или удаленно.  1.8.5. Состав услуги уточняется индивидуально для потребностей конкретного Заказчика.  1.8.6. Заказчик предоставляет беспрепятственный доступ к объектам КИИ для проведения оценки, анализа, технического осмотра.  1.8.7. Заказчиком должна быть создана постоянно действующая комиссия по категорированию в соответствии с пунктом 11 «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации», утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127. | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  | Составление новых сведений о категорировании в случае планового и внепланового изменения объекта КИИ (модернизация) и согласование со ФСТЭК России (ед. измерения – объект КИИ, трудозатраты на ед. измерения - 0,1250) | | | | |  |
| Проведение категорирования объекта КИИ и согласование сведений о проведении категорирования со ФСТЭК России, (ед. измерения - ОКИИ, трудозатраты на ед. измерения - 0,8000) | | | | |
| Составление сведений о значимом объекте КИИ и согласование его подключения с сетями связи общего пользования (ед. изменения - ОКИИ, трудозатраты на ед. измерения - 0,3888) | | | | |
| Актуализация модели угроз безопасности информации объекта КИИ в ходе модернизации объекта КИИ (ед. измерения –документ, трудозатраты на ед. измерения - 0,2500) | | | | |
| Составление для Заказчика ежемесячного отчета о текущем состоянии объектов критической информационной инфраструктуры (ед. измерения – документ, трудозатраты на ед. измерения - 0,1500) | | | | |
| Повторное категорирование объектов КИИ и согласование сведений о проведении категорирования со ФСТЭК России в случае внесения изменений (ед. измерения –документ, трудозатраты на ед. измерения - 0,2500) | | | | |
| Разработка Положения о порядке и организации работ по обеспечению безопасности объектов КИИ, содержащего:  - цели и задачи обеспечения безопасности ОКИИ;  - основные угрозы безопасности информации ОКИИ;  - основные организационные и технические мероприятия по обеспечению безопасности объектов КИИ;  - состав и структура системы безопасности ОКИИ.  (ед. измерения – документ, трудозатраты на ед. измерения - 0,3402) | | | | |
| Разработка политики обеспечения безопасности объектов КИИ, содержащей правила и процедуры групп мер по информационной безопасности, (ед. измерения – документ, трудозатраты на ед. измерения - 1,4580) | | | | |
| Разработка положения по организации и проведению работ по обеспечению безопасности объектов КИИ (ед. измерения – документ – 0,2500) | | | | |
| Разработка регламента, описывающего правила и процедуры на объект КИИ (ед. измерения – отчетный документ, трудозатраты на ед. измерения - 0,0972) | | | | |
| Изменение перечня объектов критической информационной инфраструктуры после создания или вывода из эксплуатации объекта КИИ, (ед. измерения – документ, трудозатраты на ед. измерения - 0,0250) | | | | |
| Изменение перечня критических процессов в случае изменения видов деятельности организации, (ед. изменения –документ, трудозатраты на ед. измерения - 0,0125) | | | | |
| Изменение и составление плана мероприятий по обеспечению безопасности значимых объектов КИИ субъекта критической информационной инфраструктуры (по запросу субъекта, но не реже одного раза в календарный год), (ед. измерения –документ, трудозатраты на ед. измерения - 0,2500) | | | | |
| Изменение и составление плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимые объекты КИИ, согласование с ФСБ России и ФСТЭК России, (ед. измерения –документ, трудозатраты на ед. измерения - 0,5000) | | | | |
| Составление приказа по обеспечению безопасности объектов КИИ и внесение изменений, (ед. измерения –документ, трудозатраты на ед. измерения - 0,05000) | | | | |
| Оценка критических процессов и подготовка отчета о влиянии компьютерных инцидентов на возникновение ущербов в информационной инфраструктуре (ед. измерения –документ, трудозатраты на ед. измерения - 0,1250) | | | | |
| Анализ актуальности и достоверности сведений о проведении категорирования объектов критической информационной инфраструктуры и присвоении ему соответствующей категории значимости, (ед. измерения – объект КИИ, трудозатраты на ед. измерения - 0,2500) | | | | |
|  | Поддержка интеграционных процессов |  | Не поддерживается | | | | |  |
|  | ИТ-инфраструктура |  | Не поддерживается | | | | |  |
|  | **1.10. Дополнительные параметры оказания услуги** | | | | | | |  |
|  | 1.10.1. Допустимый простой ИТ-ресурса в течении года, часов |  | Для данной услуги не применяется | | | | |  |
|  | 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 | | | | |  |
|  | | | | | | | | |