|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  |  |  |  |
|  | |  |  |  | | --- | --- | --- | |  | **ISS.11** | **Обеспечение безопасности объектов критической информационной инфраструктуры** |   **1.1. Описание услуги** | | | | | | |  |
|  | В рамках предоставления услуги проводится сбор сведений об объекте критической информационной инфраструктуры (далее – КИИ), категорирование объекта КИИ, установление требований к обеспечению безопасности значимого объекта КИИ, проектные работы по созданию системы обеспечения безопасности значимого объекта КИИ, внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие | | | | | | |  |
|  | **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 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 на деятельность по технической защите конфиденциальной информации, выполняет следующие работы:  **1. Сбор сведений об объекте КИИ, в т.ч. выездной**  1.1 Сбор сведений об объекте КИИ (назначение, архитектура, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами и т.д.)  **2. Категорирование объекта КИИ**  2.1 Определение процессов в рамках выполнения функций или осуществления видов деятельности субъекта КИИ;  2.2 Разработка Перечня объектов КИИ с обоснованием и соответствующими видами деятельности;  2.3 Разработка/доработка модели угроз безопасности объекта КИИ;  2.4 Анализ возможных действий нарушителей в отношении объекта КИИ и угроз безопасности информации на основе имеющейся Модели угроз Заказчика;  2.5 Оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий;  2.6 Определение объектов защиты, организационных и технических мер, применяемых для обеспечения безопасности;  2.7 Предоставление проектов документов Акта категорирования объекта КИИ и Сведения об объекте КИИ;  **3. Установление требований к обеспечению безопасности значимого объекта**  3.1 Выдача рекомендаций по корректировке утвержденного технического задания (далее - ТЗ) на создание (модернизацию) значимого объекта КИИ в части требований по обеспечению безопасности или частного ТЗ на создание подсистемы безопасности значимого объекта КИИ;  3.2 Разработка частного ТЗ на создание подсистемы безопасности значимого объекта КИИ;  3.3 Доработка ТЗ на создание (модернизацию) значимого объекта КИИ в части требований по обеспечению безопасности или частного ТЗ на создание подсистемы безопасности значимого объекта КИИ.  **4. Проектные работы по созданию системы обеспечения безопасности значимого объекта КИИ**  4.1 Разработка пояснительной записки к технорабочему проекту подсистемы безопасности значимого объекта КИИ;  4.2 Разработка программ и методик для проведения предварительных испытаний подсистемы безопасности;  4.3 Разработка программ и методик для проведения опытной эксплуатации подсистемы безопаcности;  4.4 Разработка программ и методик для проведения приемочных испытаний подсистемы безопасности.  **5. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие**  5.1 Разработка комплекта организационно-распорядительных документов (политик);  5.2 Участие в проведение предварительных и приемочных испытаниях, опытной эксплуатации. | | | | |  |
|  | Поддержка интеграционных процессов |  | Для данной услуги не осуществляется. | | | | |  |
|  | ИТ-инфраструктура |  | Для данной услуги не осуществляется. | | | | |  |
|  | Модификация ИТ-системы |  | Для данной услуги не осуществляется. | | | | |  |
|  | **1.7. Наименование и место хранения пользовательской документации:** | | | | | | |  |
|  | * ИТ-система |  | Для данной услуги не предусмотрено. | | | | |  |
|  | * Портал Госкорпорации «Росатом» |  | Для данной услуги не предусмотрено. | | | | |  |
|  | * Иное место |  | Для данной услуги не предусмотрено. | | | | |  |
|  |  |  |
|  |  |  |
|  | **1.8. Ограничения по оказанию услуги** | | | | | | |  |
|  | 1.8.1. Соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные ФСТЭК России в области обеспечения безопасности КИИ Российской Федерации;  1.8.2. Приобретение и установку средств защиты информации организует Заказчик;  1.8.3. По отношению к объектам, обрабатывающим информацию, составляющую государственную тайну, услуга не оказывается;  1.8.4. Заказчик перед началом оказания услуги предоставляет Исполнителю:  • сведения:   * должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта; * структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии);   • 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;  • копии введенных в действие организационно-распорядительных документов на объект КИИ;  • доступ к необходимым для оказания услуги сегментам объекта КИИ, программному и аппаратному обеспечению объекта информатизации.  1.8.5. В случае, если требуется доработка документов Заказчик предоставляет:  • действующую модель угроз безопасности информации на объекте КИИ;  • утвержденное ТЗ на создание (модернизацию) объекта КИИ в части требований по обеспечению безопасности или частное ТЗ на создание подсистемы безопасности объекта КИИ;  • проект ТЗ на создание (модернизацию) объекта КИИ или частное ТЗ на создание подсистемы безопасности объекта КИИ.  1.8.6. Для проведения категорирования решением Заказчика 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 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;  1.8.7. В связи с материальным ущербом при инцидентах информационной безопасности, влияющим на выплаты (отчисления) в бюджеты Российской Федерации, необходим справочный материал о них за планируемый трехлетний период;  1.8.8. Декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт безопасности объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта безопасности предусмотрена законодательством Российской Федерации);  1.8.9. При подаче сведений о значимом объекте КИИ во ФСТЭК России возможны ответные письма с корректировками со стороны регулятора.  1.8.10. Состав услуги уточняется индивидуально для потребностей конкретного Заказчика;  1.8.11. Состав и формы организационно-распорядительных документов по безопасности значимых объектов определяются субъектом КИИ с учетом особенностей его деятельности. | | | | | | |  |
|  | **1.9. Норматив на поддержку** | | | | | | |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) | | | | |  |
|  | Функциональная поддержка |  | **1. Сбор сведений об объекте КИИ, в т.ч. выездной (назначение, архитектура, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами и т.д.)**  1.1) Проведение сбора сведений об объекте КИИ – 0,000648148 (ед. измерения – узел\*)  1.2) Создание отчета о проведении сбора сведений об объекте КИИ – 0,157142857 (ед. измерения – отчет)  **2. Категорирование объекта КИИ**  2.1.1) Анализ процессов субъекта КИИ – 0,005555555 (ед. измерения – вид деятельности\*\*)  2.1.2) Формирование списка критических процессов субъекта КИИ на основе проведенного анализа процессов субъекта КИИ – 0,157142857 (ед. измерения – документ)  2.2.1) Анализ ИТ инфраструктуры на наличие объектов КИИ – 0,000185185 (ед. измерения – узел)  2.2.2) Формирование Перечня объектов КИИ на основе проведенного анализа ИТ инфраструктуры – 0,157142857 (ед. измерения – документ)  2.3.1) Анализ угроз безопасности информации объекта КИИ – 0,000277777 (ед. измерения – узел)  2.3.2) Разработка/доработка модели угроз безопасности объекта  КИИ на основе проведенного анализа угроз безопасности информации объекта КИИ – 0,571428571 (ед. измерения – документ)  2.4.1) Анализ возможных действий нарушителей и угроз на основе имеющейся Модели угроз – 0,000277777 (ед. измерения – узел)  2.4.2) Разработка Сведений об угрозах безопасности информации и нарушителях на основе проведенного анализа действий нарушителей и угроз – 0,204761905 (ед. измерения – документ)  2.5.1) Оценка значимости масштаба возможных последствий на основе имеющейся Модели угроз – 0,000277777 (ед. измерения – узел)  2.5.2) Разработка Сведений о возможных последствиях на основе проведенной оценки значимости масштаба возможных последствий– 0,157142857 (ед. измерения – документ)  2.6.1) Анализ объектов защиты, программных и программно-аппаратных средств – 0,000555555 (ед. измерения – узел)  2.6.2) Разработка раздела Организационные и технические меры защиты на основе проведенного анализа объектов защиты, программных и программно-аппаратных средств – 0,238095238 (ед. измерения – документ)  2.7) Предоставление проектов документов Акта категорирования и Сведения об объекте КИИ – 0,157142857 (ед. измерения – документ)  **3. Установление требований к обеспечению безопасности значимого объекта**  3.1) Выдача рекомендаций по корректировке утвержденного технического задания (далее – ТЗ) или частного ТЗ – 0,571428571 (ед. измерения – документ)  3.2)Разработка частного ТЗ на создание подсистемы безопасности значимого объекта КИИ – 0,666666667 (ед. измерения – документ)  3.3) Доработка проекта ТЗ или проекта частного ТЗ – 0,476190476 (ед. измерения – документ)  **4. Проектные работы по созданию системы обеспечения безопасности значимого объекта КИИ**  4.1) Разработка пояснительной записки к технорабочему проекту подсистемы безопасности – 0,666666667 (ед. измерения – документ)  4.2.1) Разработка алгоритмов проверки работоспособности подсистемы безопасности и отдельных средств защиты информации (далее - СЗИ) – 0,00037037 (ед. измерения – узел)  4.2.2) Составление программ и методик для проведения предварительных испытаний на основе разработанных алгоритмов проверки работоспособности подсистемы безопасности и отдельных СЗИ – 0,19047619 (ед. измерения – документ)  4.3.1) Разработка алгоритмов проверки функционирования подсистемы безопасности – 0,00037037 (ед. измерения – узел)  4.3.2) Составление программ и методик для проведения опытной эксплуатации на основе разработанных алгоритмов проверки функционирования подсистемы безопасности – 0,19047619 (ед. измерения – документ)  4.4.1) Разработка алгоритмов проверки соответствия подсистемы безопасности требованиям ТЗ и требованиям по информационной безопасности – 0,00037037 (ед. измерения – узел)  4.4.2) Составление программ и методик для проведения приемочных испытаний на основе разработанных алгоритмов проверки соответствия подсистемы безопасности требованиям ТЗ и требованиям по информационной безопасности – 0,19047619 (ед. измерения – документ)  **5. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ и ввод его в действие**  5.1) Разработка комплекта организационно-распорядительных документов (политик) – 0,00952381 (ед. измерения – документ)  5.2) Участие в проведение испытаний, опытной эксплуатации – 0,19047619 (ед. измерения – протокол)  \*Узел – автоматизированное рабочее место, телекоммуникационное оборудование, сервер и т.д.  \*\*Вид деятельности – вид экономической деятельности по Общероссийскому классификатору видов экономической деятельности, указанный в **актуальной** Выписке из ЕГРЮЛ | | | | |  |
|  | 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 |  | Не предусмотрено | | | | |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | Не предусмотрено | | | | |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | Не предусмотрено | | | | |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | Не предусмотрено | | | | |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости  ИТ-ресурса |  | Не предусмотрено | | | | |  |
|  | | | | | | | | |