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

|  |  |  |
| --- | --- | --- |
|  | **OPR.18** | **Обеспечение функционирования, администрирования и контроль соответствия системы защиты информации АСЗИ АО «ТВЭЛ» требованиям по безопасности информации** |

**1.1. Описание услуги** |  |
|  | В рамках предоставления услуги обеспечивается:1. Поддержание в актуальном состоянии конфигурации аттестованной АСЗИ АО «ТВЭЛ» и её системы защиты информации.2. Поддержание в актуальном состоянии организационно-распорядительной и эксплуатационной документации АСЗИ Заказчика.3. Администрирование системы защиты информации АСЗИ Заказчика.4. Поддержка функционирования систем информационной безопасности АСЗИ АО «ТВЭЛ». Проведение периодического контроля соответствия системы защиты информации АСЗИ АО «ТВЭЛ» требованиям безопасности информации. В случае необходимости, проведение аттестационных испытаний ОИ.Услуга направлена на обеспечение функционирования, администрирования и контроль соответствия системы защиты информации АСЗИ АО «ТВЭЛ» требованиям по безопасности информации, предъявляемым к автоматизированным системам класса защищённости от несанкционированного доступа к информации «1Г» и информационным системам персональных данных, в которых необходимо обеспечить 4 уровень защищённости персональных данных. |   |
|  | **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** |   |
|  |   |  | Для настоящей услуги не применяется |   |
|  | **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 |  | **1. Поддержание в актуальном состоянии конфигурации аттестованной АСЗИ АО «ТВЭЛ» и ее системы защиты информации.**Оказание услуги обеспечивает поддержание в актуальном состоянии базовой конфигурации АСЗИ и её системы защиты информации и их соответствие эксплуатационной и организационно-распорядительной документации в рамках жизненного цикла АСЗИ Заказчика.Базовая конфигурация АСЗИ и её системы защиты информации включает:• структуру системы защиты информации АСЗИ;• состав средств защиты информации;• места установки средств защиты информации;• параметры настройки средств защиты информации;• состав программного обеспечения;• места установки программного обеспечения;• состав технических средств;• места установки технических средств;В рамках оказания услуги Исполнителем осуществляется:1.1. Определение совместно с Заказчиком и согласование с органом по аттестации типов возможных изменений базовой конфигурации АСЗИ и ее системы защиты информации;1.2. Учет изменений базовой конфигурации АСЗИ и ее системы защиты информации, в т.ч.:• сохранение информации (данных) об изменениях базовой конфигурации АСЗИ и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию АСЗИ и ее систему защиты информации;• документирование изменений в базовую конфигурацию АСЗИ и ее систему защиты информации;• организация санкционирования органом по аттестации внесения изменений в базовую конфигурацию АСЗИ и ее систему защиты информации;•внесение информации (данных) о санкционированных изменениях в базовой конфигурации АСЗИ и ее системы защиты информации в эксплуатационную и организационно-распорядительную документацию на АСЗИ;Периодичность оказания услуги по учету изменений базовой конфигурации АСЗИ и её системы защиты информации – ежеквартально.**2. Поддержание в актуальном состоянии организационно-распорядительной и эксплуатационной документации АСЗИ.** В рамках оказания услуги Исполнителем осуществляется разработка (адаптация) и актуализация организационно-распорядительных, нормативно-методических и эксплуатационных документов на систему защиты информации АСЗИ, необходимость изменения которых обусловлена жизненным циклом АСЗИ Заказчика.**3. Администрирование системы защиты информации АСЗИ Заказчика.**В рамках оказания услуги Исполнителем осуществляется:- Обеспечение технической поддержки пользователей АСЗИ в части функционирования Средств ЗИ на АРМ;- Обеспечение первой линии поддержки компонентов СЗИ АСЗИ Заказчика. Эскалация обращений и взаимодействие с поставщиком технической поддержки по вопросам реализации приобретенной Заказчиком технической поддержки СЗИ;- Первоначальная установка и настройка СЗИ Заказчика в соответствии с проектной и эксплуатационной документацией на систему защиты информации АСЗИ АО «ТВЭЛ» (не более 10% в год от принятого на обслуживание состава АСЗИ);- Поддержание в актуальном состоянии программного обеспечения СЗИ АСЗИ (при наличии у Заказчика актуальных лицензий и технической поддержки на СЗИ АСЗИ);- Ведение перечня и контроль актуальности переданных Заказчиком лицензий и сертификатов соответствия требованиям безопасности информации на СЗИ АСЗИ;- Исполнитель осуществляет взаимодействие с производителями СЗИ в части получения копий продленных или новых сертификатов соответствия требованиям безопасности информации на СЗИ, а также выяснения планов по продлению сертификатов СЗИ.- Исполнитель заблаговременно, но не менее чем за 6 месяцев до окончания их строка действия, информирует Заказчика об окончании действия лицензий на СЗИ и сертификатов соответствия по требованиям информационной безопасности на СЗИ, продление которых не планируется.- Ведение перечня и контроль актуальности сертификатов технической поддержки и лицензионных ключей на СЗИ АСЗИ;- Исполнитель заблаговременно информирует Заказчика об окончании срока действия сертификатов технической поддержки и лицензионных ключей на СЗИ АСЗИ, но не менее чем за 6 месяцев до окончания их срока действия.- Приобретение (продление) лицензий и сертификатов технической поддержки и лицензионных ключей на СЗИ АСЗИ выполняется Заказчиком самостоятельно, вне рамок оказания услуги.- Устранение совместно со специалистами Заказчика недостатков в функционировании подсистем защиты информации АСЗИ, выявляемых по результатам периодических контролей защищённости объекта информатизации.**4. Поддержка функционирования систем информационной безопасности АСЗИ АО «ТВЭЛ».** Поддержка функционирования системы защиты информации АСЗИ Заказчика в ходе её эксплуатации в составе следующих подсистем:4.1. Подсистема анализа защищённости.Подсистема анализа защищенности реализуется на оборудовании Заказчика:- сопровождение процесса анализа объекта информатизации на возможность организации атаки на проникновение (PenTest); - сопровождение процесса анализа объекта информатизации на соответствие государственным стандартам и рекомендациям российских производителей в рамках стандартных функций подсистемы анализа (Compliance);- поддержание актуальности баз знаний на сервере подсистемы;- создание учетной записи пользователя в подсистеме;- настройка прав субъектов доступа в подсистеме;- создание задачи по проведению периодического анализа или проверки.- добавление нового узла в задачу по анализу;- выпуск и предоставление отчёта на основании ранее проведенных анализов или проверок (на основании ранее созданных задач по выпуску отчётов);- изменение параметров периодической проверки или анализа;- по запросу предоставление ответственному лицу Заказчика отчета об обнаруженных уязвимостях в анализируемых компонентов сети (активного сетевого оборудования, серверов и персональных компьютеров);- выполнение комплекса мероприятий по настройке элементов подсистемы информационной безопасности;- обеспечение технической поддержки пользователей подсистемы в части используемых элементов системы анализа защищенности.4.2. Подсистема антивирусной защиты.- подключение нового узла к серверу управления;- установка клиентского ПО на узлы системы;- поддержание актуальности антивирусных баз и срока действия лицензионного ключа (своевременная замена истекшего ключа на новый, в случае предоставления такого Заказчиком);- создание отчета о состоянии антивирусной защиты на узле;- изменение политики антивирусной защиты (с учетом подчиненности серверов антивирусной защиты);- мониторинг узлов системы на сервере управления, контроль и устранение ошибок конфигурации политики защиты, контроль установки средств защиты на всех узлах АСЗИ, в т.ч. на вновь добавляемых, в рамках договора; - выполнение периодического сканирования узлов на наличие вирусов;- участие в разборе конфликтных ситуаций взаимодействия СрЗИ с прикладным ПО; -участие в разборе инцидентов информационной безопасности в части предоставления имеющейся информации из подсистемы антивирусной защиты. 4.3. Подсистема защиты информации от несанкционированного доступа.- сопровождение компоненты управления аутентификации пользователей;- сопровождение компоненты контроля доступа к съемным носителям информации на АРМ пользователя;- сопровождение компоненты обеспечения контроля целостности;- сопровождение компоненты контроля вывода документов на печать;- сопровождение компоненты регистрации событий входа пользователей в АСЗИ и действий пользователей в АСЗИ;- администрирование ядра СЗИ от НСД;- участие в разборе конфликтных ситуаций а так же взаимодействия СЗИ с прикладным ПО.  4.4. Подсистема обнаружения и предотвращения утечек конфиденциальной информации.- контроль подключения подсистемы обнаружения и предотвращения утечек конфиденциальной информации к источникам событий АСЗИ Заказчика;- обеспечение мониторинга информационных потоков согласно функционала DLP-системы, имеющейся в распоряжении Заказчика;- предоставление доступа к консоли мониторинга событий ответственным лицам Заказчика;- добавление новых источников событий;- добавление правил фильтрации анализируемой информации, в т.ч. на основании образцов защищаемых документов, предоставляемых Заказчиком;- устранение ошибок, возникающих в ходе работы DLP-системы;- мониторинг нагрузки и состояния DLP-системы;- консультации Заказчика по совершенствованию подсистемы обнаружения и предотвращения утечек конфиденциальной информации.**5. Проведение контроля соответствия системы защиты информации АСЗИ АО «ТВЭЛ» требованиям безопасности информации.**В рамках оказания услуги Исполнителем осуществляется:- Проведение аттестации объекта информатизации Заказчика. Аттестация объекта информатизации Заказчика выполняется в случаях:а) окончания срока действия Аттестата соответствия в течение периода исполнения договора;б) если окончание срока действия Аттестата приходиться на период, не превышающий 6 месяцев от даты окончания договора.- Проведение контроля соответствия системы защиты информации объекта информатизации Заказчика в порядке, установленном программой и методиками аттестационных испытаний объекта информатизации;- Периодичность проведения контроля эффективности системы защиты информации объекта автоматизации – ежегодно.- замечания, выявленные при проведении контрольных мероприятий, устраняются Исполнителем в рамках оказания услуг по администрированию системы защиты информации в части касающейся, в остальных случаях передаются Заказчику для устранения с последующим проведением повторных контрольных мероприятий после устранения Заказчиком замечаний. |   |
|  | Поддержка интеграционных процессов |  | Для настоящей услуги не осуществляется |   |
|  | ИТ-инфраструктура |  | Для настоящей услуги не осуществляется |   |
|  | Модификация ИТ-системы |  | Для настоящей 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** |  |
|  | Поддержка технического функционирования подсистемы сетевой безопасности (МЭ, КШ, СОВ) осуществляется в рамках услуги OPR.2Поддержка функционирования подсистемы удаленного доступа с клиент-серверной архитектурой осуществляется в рамках отдельной услуги (Доверенная мобильная платформа).Установка клиентского ПО (СКЗИ) и криптографических ключей на АРМ пользователей, а также учет СКЗИ и изготовление ключей электронной подписи осуществляется в рамках Договора присоединения (услуги: GEN.23; CLB.11; CLB.18).Для автоматизированных/информационных систем в защищённом исполнении действуют ограничения, предусмотренные для объектов информатизации, аттестованных по требованиям безопасности информации.Стоимость и/или состав услуги могут быть изменены Исполнителем по согласованию с Заказчиком при увеличении объемных показателей.Заказчик перед началом оказания услуги обязательно должен предоставить Исполнителю:• Доступ, в том числе удаленный, к необходимым для оказания ИТ/ИБ-услуги сегментам технологической сети, программному и аппаратному обеспечению;• Необходимые права для оказания ИТ/ИБ-услуги;• Актуальные лицензии на программное обеспечение/техническую поддержку средств защиты информации.• Все подсистемы защиты информации на момент начала оказания услуги должны быть реализованы на мощностях Заказчика и предоставлены Исполнителю для поддержки в настроенном, готовом к эксплуатации виде.Для обеспечения мониторинга информационных потоков применяются сенсоры, развернутые в DLP-системе Заказчика.Дополнительно может быть запрошено:• Техническое решение/проект на систему защиты информации; • Документ, описывающий роли, полномочия и привилегии субъектов доступа к объектам доступа;• Копии сертификатов, технических условий эксплуатации на компоненты системы информационной безопасности;• Действующую проектную документацию на используемые компоненты системы защиты информации;• Действующую эксплуатационную документацию на используемые СЗИ, МЭ, антивирусное ПО, содержащую актуальную информацию на момент передачи;• Действующую на предприятии организационно распорядительную документацию в части информационной безопасности (акты, журналы, инструкции, памятки, регламенты и т.д.).Условия обновления:• Обновление текущей версии программ является предметом отдельного соглашения.• Установка (обновление) ПО локальных СЗИ, не обслуживаемых Исполнителем по договору выполняется в рамках разовых работ. |   |
|  | **1.9. Норматив на поддержку** |  |
|  | **Подразделение** |  | **Предельное значение трудозатрат на поддержку 1 единицы объемного показателя по услуге** (чел.мес.) |  |
|  | Функциональная поддержка |  | Поддержание в актуальном состоянии конфигурации аттестованной АСЗИ и ее системы защиты информации (ед. измерения - АСЗИ, трудозатраты на ед. изменения - 0,29234802)Поддержание в актуальном состоянии организационно-распорядительной и эксплуатационной документации АСЗИ (ед. измерения - АСЗИ, трудозатраты на ед. изменения - 0,28842344)Администрирование системы защиты информации АСЗИ (ед. измерения - АСЗИ, трудозатраты на ед. изменения - 0,24650941)Проведение контроля соответствия системы защиты информации АСЗИ требованиям безопасности информации (ед. измерения - АСЗИ, трудозатраты на ед. изменения - 0,37668635)Поддержка функционирования подсистемы антивирусной защиты (ед. измерения - АРМ, трудозатраты на ед. изменения- 0,00071023)Поддержка функционирования подсистемы защиты информации от несанкционированного доступа (ед. измерения - АРМ, трудозатраты на ед. изменения- 0,00203666)Поддержка функционирования подсистемы анализа защищенности (ед. измерения - АРМ, трудозатраты на ед. изменения- 0,0005071)Поддержка функционирования подсистемы обнаружения и предотвращения утечек конфиденциальной информации (ед. измерения - АРМ, трудозатраты на ед. изменения- 0,00044623)Актуализация технического паспорта АСЗИ (ед. измерения - АРМ, трудозатраты на ед. изменения - 0,001000000)Консультационная поддержка пользователей по вопросам обеспечения ИБ (в части организационных и технических мер защиты) (ед. изменения - Пользователь, трудозатраты на ед. измерения - 0,001000000) |  |
|  | Поддержка интеграционных процессов |  |  Для данной услуги не предусмотрено |  |
|  | ИТ-инфраструктура |  |  Для данной услуги не предусмотрено |  |
|  | **1.10. Дополнительные параметры оказания услуги** |  |
|  | 1.10.1. Допустимый простой ИТ-ресурса в течении года, часов |  | По согласованию с Заказчиком, на основании утвержденных планов, графиков |  |
|  | 1.10.2. Срок хранения данных резервного копирования (в календарных днях) |  | Для данной услуги не предусмотрено |  |
|  | 1.10.3. Целевая точка восстановления ИТ-ресурса (RPO) (в рабочих часах) |  | Для данной услуги не предусмотрено |  |
|  | 1.10.4. Целевое время восстановления ИТ-ресурса (RTO) (в рабочих часах) |  | Для данной услуги не предусмотрено |  |
|  | 1.10.5. Обеспечение катастрофоустойчивости ИТ-ресурса |  | Для данной услуги не предусмотрено |  |
|  |