**ПРЕДВАРИТЕЛЬНЫЙ ОПРОСНЫЙ ЛИСТ   
К ОСУЩЕСТВЛЕНИЮ РАБОТ ПО ЗАЩИТЕ  
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

|  |  |
| --- | --- |
|  | |
| Наименование организации |  |
|  | |
| Контактное лицо |  |
|  | |
| Телефон |  |
|  | |
| Email |  |
|  | |
| Дата заполнения |  |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Цель проведения | | | обязательно |
|  | | | |
| Оценка действующей системы информационной безопасности  Подготовка к проверке регулятора  Выполнение требований партнеров/контрагентов | | | |
| Другое |  | | |
|  | *Указать* | | |
| *- выбрано;*  *- не выбрано* | | | |
|  | | | |
|  | | | |
| 1. Основные виды деятельности предприятия | | | обязательно |
|  | | | |
|  | | | |
| *Указать* | | | |
|  | | | |
| 1. Основные процессы, в рамках которых возможно функционирование/функционируют КИИ | | | обязательно |
|  | | | |
|  | | | |
| *Указать* | | | |
|  | | | |
| 1. Количество объектов КИИ | | | обязательно |
|  | | | |
|  | | | |
| *Указать* | | | |
|  | | | |
| *В случае, если оценка потенциального количества объектов КИИ не проводилась, указать общее количество*  *ИС, ИТС, АСУ ТП* | | | |
|  | | | |
|  | | | |
| 1. Имеются ли Модель угроз и нарушителей безопасности? | | | обязательно |
|  | | | |
| Да | | Нет | |
|  | | | |
|  | | | |
| 1. Если имеется, то по какой методике сделана? | | | |
|  | | | |
| Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждённая ФСТЭК России от 19 ноября 2007 г.  Методика оценки угроз безопасности информации, утверждённая ФСТЭК России от 05 февраля 2021г.  Затрудняюсь ответить | | | |
|  | | | |
|  | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Подробные сведения о значимых объектах КИИ | | | | | | | обязательно |
|  | | | | | | | |
| **#** | **Наименование потенциального объекта** | **Процессы** | **Тип**  **(ИС/ ИТС/ АСУ ТП)** | **Категория значимости (1,2,3)** | **Прикладное ПО** | **Применяемые**  **СЗИ** | |
|  | | | | | | | |
| 1 |  |  |  |  |  |  | |
|  | | | | | | | |
| 2 |  |  |  |  |  |  | |
|  | | | | | | | |
| 3 |  |  |  |  |  |  | |
|  | | | | | | | |
| 4 |  |  |  |  |  |  | |
|  | | | | | | | |
| 5 |  |  |  |  |  |  | |
|  | | | | | | | |
| 6 |  |  |  |  |  |  | |
|  | | | | | | | |
| 7 |  |  |  |  |  |  | |
|  | | | | | | | |
| 8 |  |  |  |  |  |  | |
|  | | | | | | | |
| 9 |  |  |  |  |  |  | |
|  | | | | | | | |
| 10 |  |  |  |  |  |  | |
|  | | | | | | | |
| 11 |  |  |  |  |  |  | |
|  | | | | | | | |
| 12 |  |  |  |  |  |  | |
|  | | | | | | | |
| 13 |  |  |  |  |  |  | |
|  | | | | | | | |
| 14 |  |  |  |  |  |  | |
|  | | | | | | | |
| 15 |  |  |  |  |  |  | |
|  | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Имеется ли в наличии проектная документация на объекты КИИ? | | | обязательно |
|  | | | |
| Да | | Нет | |
|  | | | |
|  | | | |
| 1. Если да, то укажите имеющуюся документацию | | | обязательно |
|  | | | |
| Положение по обеспечению безопасности объектов КИИ  Общие требования по безопасности  Процедуры и разграничения доступа  Правила защиты машинных носителей информации  Правила антивирусной защиты  Процедуры обеспечения целостности и доступности  Правила защиты технических средств  Правила защиты системы в целом и ее компонентов  Принципы планирования мероприятий по безопасности  План ОНиВД  Правила информирования и обучения персонала правилам работы с объектами КИИ  Регламент реагирования на компьютерные инциденты | | | |
| Другое |  | | |
|  | *Указать* | | |
|  | | | |
| 1. Укажите структурное подразделение и должностное лицо, ответственные за защиту информации на предприятии (контакты) | | | обязательно |
|  | | | |
|  | | | |
| *Указать* | | | |
|  | | | |
| 1. Требования к оформлению отчетной документации по проекту | | | обязательно |
|  | | | |
| Соответствие внутренним стандартам/требованиям/шаблонам предприятия  Соответствие ГОСТ 34 и РД 50  Нет требований (принимается формат Исполнителя) | | | |
|  | | | |
|  | | | |
| 1. Желаемый перечень работ | | | |
|  | | | |
| Моделирование угроз безопасности информации для значимых объектов критической информационной инфраструктуры (КИИ)  Разработка ТЗ к системе обеспечения информационной безопасности КИИ (СОИБ КИИ)  Разработка Технического проекта СОИБ КИИ  Разработка организационно-распорядительной документации (ОРД) для субъекта и объектов КИИ  Разработка Модели угроз и нарушителей безопасности ЗОКИИ  Взаимодействие (подключение) с ГосСОПКа  Внедрение СОИБ КИИ | | | |
|  | | | |
|  | | | |
| 1. Желаемый перечень сопутствующих и иных работ | | | |
|  | | | |
| Проведение тестирования на проникновение и анализа защищенности  Аудит организации в направлении обработки/защиты персональных данных | | | |
|  | | | |
|  | | | |

|  |  |
| --- | --- |
| 1. Поставка технических решений (ПО, ПАК, оборудование) ИБ/ИТ | |
|  | |
| Планируется ли поставка решений ИБ/ИТ?  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ? | |
|  | |
| Какие решения по ИБ/ИТ вами рассматриваются? |  |
|  | *Указать* |
|  | |
|  | |

Благодарим за уделенное время!