**ОПРОСНЫЙ ЛИСТ   
ПО ОЦЕНКЕ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИИ**

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

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Цель проведения | | | |
|  | | | |
| Оценка действующей системы информационной безопасности  Реагирование на инцидент  Требования партнеров | | | |
| Другое | | |  |
|  | | | *Указать* |
| *- выбрано;*  *- не выбрано* | | | |
|  | | | |
|  | | | |
| 1. Объем анализируемой инфраструктуры | | | |
|  | | | |
| В Организации работает не более 10 компьютеров  В Организации работает от 10 до 100 компьютеров  В Организации работает от 100 до 1000 компьютеров | | | |
| Другое | | |  |
|  | | | *Указать* |
| *- выбрано;*  *- не выбрано* | | | |
|  | | | |
| 1. Какая информация защищается в организации | | | |
|  | | | |
| Персональные данные работников, клиентов  Информация о платежах клиентов  Бухгалтерская информация  Информация о сделках | | | |
| Другое | | |  |
|  | | | *Указать* |
|  | | | |
| 1. Имеется ли физическая охрана в организации | | | |
|  | | | |
| Подключены к пульту централизованной охраны/тревожная кнопка  Есть пост физической охраны  Установлена СКУД  Установлено видеонаблюдение  Нет | | | |
| Другое | | |  |
|  | | | *Указать* |
|  | | | |
| 1. Работает ли в организации сотрудник ИТ/ИБ | | | |
|  | | | |
| Да, сотрудник ИБ в штате  Да, сотрудник ИБ на аутсорсе  Да, сотрудник ИТ в штате  Да, сотрудник ИТ на аутсорсе  Нет | | | |
| Другое | | |  |
|  | | | *Указать* |
|  | | | |
| 1. Действует ли в Организации организационно-распорядительная документация в направлении защиты информации? | | | |
|  | | | |
| Да | | Нет | |
|  | | | |
| Если да, то какая? | | | |
|  | | | |
|  | | | |
|  | | | |
| 1. Имеются ли филиалы у организации? | | | |
|  | | | |
| Да | | | Нет |
|  | | | |
|  | | | |
| 1. Желаемый перечень работ по оценке защищенности организации | | | |
|  | | | |
| Оценка защищенности  Тестирование на проникновение и анализ уязвимостей  Разработка необходимой организационно-распорядительной документации для повышения уровня безопасности  Обучение сотрудников правилам информационной безопасности  Аттестация сотрудников на знание правил информационной безопасности | | | |
|  | | | |
|  | | | |
| 1. Желаемый перечень иных и сопутствующих работ | | | |
|  | | | |
| Аудит организации в направлении обработки/защиты персональных данных  Аудит степени выполнения 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»  Аудит на соответствие требований 98-ФЗ «О коммерческой тайне» | | | |
|  | | | |
|  | | | |
| 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!