**ОПРОСНЫЙ ЛИСТ
ПО АУДИТУ БЕЗОПАСНОСТИ
УДАЛЁННОГО ПОДКЛЮЧЕНИЯ СОТРУДНИКОВ**

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

|  |
| --- |
| 1. Цель проведения
 |
|  |
| [ ]  Оценка действующей системы информационной безопасности[ ]  Подготовка к проверке регулятора[ ]  Требования партнеров |
| [ ]  Другое |  |
|  | *Указать* |
| [x]  *- выбрано;* [ ]  *- не выбрано* |
|  |
|  |
| 1. Какое оборудование использует сотрудник при переходе на удалённую работу?
 |
|  |
| [ ]  Ноутбук[ ]  Флэш/токен с ЭЦП[ ]  Внешний носитель с данными |
| [ ]  Другое |  |
|  | *Указать* |
|  |
| 1. Использует ли сотрудник инструкции, в том числе по настройке и информационной безопасности?
 |
|  |
| [ ]  Да | [ ]  Нет |
|  |
|  |
| 1. Какие учётные данные использует сотрудник?
 |
|  |
| [ ]  VPN[ ]  NTLM (доменная учетная запись)[ ]  Email[ ]  CRM, ЭДО, ERP (в том числе 1С)[ ]  Платежное ПО (ДБО, АБС и т. д.) |
| [ ]  Другое |  |
|  | *Указать* |
|  |
| 1. Укажите, что еще использует сотрудник помимо вышеперечисленного
 |
|  |
|  |
| *Указать* |
|  |
| 1. Имеется ли регламент предоставления удаленного доступа сотрудникам?
 |
|  |
| [ ]  Да | [ ]  Нет |
|  |
|  |
| 1. Какие технологии предоставления доступа применяются?
 |
|  |
| [ ]  VPN[ ]  VDI[ ]  RDP[ ]  Облачные хранилища[ ]  Проброс портов |
| [ ]  Другое |  |
|  | *Указать* |
|  |
| 1. Имеется ли филиалы у организации?
 |
|  |
| [ ]  Да | [ ]  Нет |
|  |
|  |
| 1. Укажите количество удалённых сотрудников
 |
|  |
|  |
| *Указать* |
|  |
| 1. Укажите количество человек в штате отдела информационной безопасности и отдела информационных технологий, включая филиалы
 |
|  |
|  | **ИБ** | **ИТ** |
|  |
| Количество сотрудников ГО |  |  |
|  |
| Количество в филиалах |  |  |
|  |
|  |
| 1. Желаемый перечень работ по аудиту безопасности удалённого доступа
 |
|  |
| [ ]  Аудит безопасности[ ]  Тестирование на проникновение и анализ уязвимостей[ ]  Разработка необходимой организационно-распорядительной документации для повышения уровня безопасности[ ]  Обучение сотрудников правилам информационной безопасности при удаленной работе[ ]  Аттестация сотрудников на знание правил информационной безопасности при удаленной работе |
|  |
|  |
| 1. Желаемый перечень иных и сопутствующих работ
 |
|  |
| [ ]  Разработка модели угроз по новой методике ФСТЭК[ ]  Аудит на соответствие требованиям ГОСТ 57580/Приведение в соответствие требованиям ГОСТ 57580[ ]  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!