**Практика 10**

**Цель работы**: получение навыков формирования мер и требований к информационной безопасности в области защиты персональных данных

Задание выполняется **в группах,** объекты – те же организации, что и на практике №1 на основе результатов предыдущей работы (практики). При выполнении задания опираться на подзаконные НПА в области защиты персональных данных.

1. Определить перечень требований НПА в области ПДн в отношении каждой ИСПДн рассматриваемой организации с учетом категории значимости. Составить таблицу с колонками:
   1. Источник (НПА)
   2. Формулировка требования
   3. Состояние выполнения требования в организации (выполняется или нет)

Не относящиеся к организации требования исключить из перечня согласно методике.

1. Разработать план выполнения требований НПА в области безопасности ИСПДн (для не выполняющихся полностью из п.1) в отношении каждой ИСПДн рассматриваемой организации. Составить таблицу для каждой ИСПДн вида:
   1. Требование (из таблицы 1)
   2. Планируемый способ выполнения (организационные или технические меры)
   3. Источники требований к средствам / мерам выполнения (сертификация/оценка соответствия, соответствие типовым примерам, соответствие ГОСТ с номером стандарта и т.д.)

**Оформить результат в виде:**

1. Презентации для рассказа (при необходимости)
2. Файла в формате doc/docx/odt - по одному отдельному файлу на каждый ОКИИ.

|  |  |  |  |
| --- | --- | --- | --- |
| Источник (НПА) | Формулировка требования | Выполняется или нет | Категория |
| ФЗ-152 (ст. 19) | Обеспечение конфиденциальности ПДн | Да  (Шифрование в 1С и CRM) | Все |
| ФЗ-152 (ст. 18.1) | Назначение ответственного за обработку ПДн | Да  (отдел ИБ + специалистом по безопасности данных) | К2-К4 |
| Приказ ФСТЭК №21 | Использование СКЗИ при передаче ПДн | нет  (требуется защищенный VPN для 1С и CRM) | К3-К4 |
| ГОСТ Р 57580.1-2017 | Ведение журналов учета обращений к ПДн | да | К2-К4 |
| Приказ ФСБ №378 | Сертифицированные криптосредства для военных данных | Нет (требуется КриптоПро 4.0) | К4 (военные) |
| Постановление №1119 | Оценка вреда при утечке ПДн клиентов | Да  (пункт политики) | К3-К4 |
| ФЗ-152 (ст. 22) | Уведомление Роскомнадзора | нет | К1-К4 |

|  |  |  |
| --- | --- | --- |
| **Требование (из таблицы 1)** | **Планируемый способ выполнения (организационные или технические меры)** | **Источники требований к средствам / мерам выполнения** |
| Использование СКЗИ при передаче ПДн (Приказ ФСТЭК №21) | Внедрение защищенного VPN-туннеля с использованием сертифицированных СКЗИ | Приказ ФСТЭК №21, ФЗ-152, ГОСТ Р 56939-2016 |
| Сертифицированные криптосредства для военных данных (Приказ ФСБ №378) | Внедрение КриптоПро CSP 4.0 или более новой версии, аттестованной ФСБ | Приказ ФСБ №378, список сертифицированных ФСБ криптосредств |
| Уведомление Роскомнадзора (ФЗ-152, ст. 22) | Организационная мера: подготовка и подача уведомления о наличии ИСПДн в Роскомнадзор | ФЗ-152 (ст.22), Методические рекомендации Роскомнадзора |