ТИПОВЫЕ НАРУШЕНИЯ, ВЫЯВЛЯЕМЫЕ В ХОДЕ ПРОВЕРОК РЕГУЛЯТОРАМИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Типовые нарушения, выявляемые Роскомнадзором:

- В части Уведомления об обработке ПДн*:
  – Несоответствие сведений, содержащихся в уведомлении, реальной обстановке дел в организации, либо указана не полная информация;
  – Указание не полных сведений по СКЗИ*;
- Согласие субъекта на обработку ПДн:
  – Указание не всех категорий ПДн;
  – Несоответствие требованиям ст.9 ФЗ «О персональных данных» о согласии субъекта ПДн на обработку его ПДн;
  – Указание не всех субъектов ПДн, которым поручается обработка или передаются ПДн;
- Обработка ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- Обработка и хранение ПДн в неавтоматизированном виде с нарушением законодательства (Постановление Правительства РФ от 15 сентября 2008 г. № 687);
- Не выполнение требований по обучению и ознакомлению сотрудников с порядком обработки, хранения ПДн и ответственностью за нарушение требований законодательства при обработке ПДн;
- Отсутствие условий соблюдения конфиденциальности ПДн в договорах с третьими лицами, а также требований к защите обрабатываемых ПДн;
- Отсутствие разграничения на автоматизированную и неавтоматизированную обработку в приказе об утверждении списка лиц, допущенных к ПДн;
- Отсутствие разделения Актов об уничтожении на бумажный и электронный вид носителя;
- Отсутствие регламентации процедуры уничтожения электронных и бумажных носителей в Положении по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн*;
- Приказ «Об утверждении перечня ПДн» не разделен на автоматизированную и неавтоматизированную обработку;
- Журнал регистрации однократного пропуска не регламентирован и не введен Приказом/Распоряжением «Об утверждении перечня мер, направленных на выполнение требований законодательства РФ при ведении журнала, содержащего ПДн, необходимые для однократного пропуска субъекта ПДн на территорию»;
- Модели угроз безопасности ПДн/информации не полные, неконкретные;
- Схема, отражающая рабочие места, где ведется обработка ПДн, с указанием внутренних и внешних потоков составлена не точно;
- Отсутствие у оператора места (мест) хранения ПДн (материальных носителей), перечня лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ;

**ПДн – персональные данные*
**ИСПДН – информационная система персональных данных*
**СКЗИ – средство криптографической защиты информации*

Типовые нарушения, выявляемые ФСТЭК России:

- использование несертифицированных СЗИ*, либо с истекшим сроком действия сертификата;
- утрата документации и эталонного дистрибутива СЗИ;
- несоответствие настроек СЗИ требованиям руководящих документов и внутренним документам оператора;
- наличие следов использования неучтенных съемных носителей информации в системном реестре;
- низкий уровень знаний сотрудников (в том числе администраторов безопасности) в сфере защиты и обеспечения безопасности информации;
- использование сертифицированных ФСБ России СЗИ для выполнения требований ФСТЭК России;
- неполные, некорректные внутренние документы (в том числе Модель угроз безопасности ПДн/информации);
- отсутствие аттестата соответствия на ГИС;
- недостаточная физическая защита технических средств (компьютеров, серверов).

** СЗИ – средство защиты информации*

Типовые нарушения, выявляемые ФСБ России:

- некорректно построенная Модель угроз безопасности ПДн/информации, в том числе Модель нарушителя;
- использование СКЗИ* более низкого класса, чем необходимо;
- отсутствие необходимых журналов, либо журналы есть, но не ведутся;
- отсутствие учета СКЗИ;
- использование СКЗИ без лицензии ФСБ России;
- отсутствие защиты среды функционирования криптосредств;
- недостаточные меры по физической защите носителей ключевой информации;
- утеря эталонных дистрибутивов криптосредств, документации, формуляров.

**СКЗИ – средство криптографической защиты информации*