РАЙОННЫЙ
СЕМИНАР/ 2022

Модель угроз информационной безопасности как основополагающий документ по защите персональных данных

14 ноября 2022

ЧТО ЭТО ТАКОЕ?

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Под угрозой (в общем) понимается потенциально возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

Модель угроз информационной безопасности — это описание существующих угроз для ИС, насколько они реалистичны, каковы шансы, что они воплотятся в жизнь, и какие последствия может повлечь за собой нарушение безопасности в сфере защиты ПДн.

ГДЕ ЭТО ПРИМЕНЯЕТСЯ?

- выбор организационных и технических мер по обеспечению безопасности ПДн и их реализации в системе защиты ПДн;
- определение требуемого уровня защищенности ПДн;
- анализ защищенности от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию угроз с использованием организационных и технических мер обеспечения безопасности ПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование.

ПОЧЕМУ ЭТО НАДО?

Необходимость разработки модели угроз регламентирована рядом нормативных документов. Вот некоторые из них:

- Часть 2 статьи 19 закона **№ 152-ФЗ «О персональных данных»**
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных **(утверждены приказом ФСТЭК России от 18 февраля 2013г. № 21)**
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах **(утверждены ФСТЭК России от 11 февраля 2013г. № 17)**

ИЗ ЧЕГО ЭТО СОСТОИТ?

Модель угроз

- Описание информационной системы
- Структурно-функциональные характеристики
- Описание угроз безопасности
- Модель нарушителя
- Возможные уязвимости
- Способы реализации угроз
- Последствия от нарушения свойств безопасности информации

+ пара разделов для ФСБ и некоторые пожелания от ФСТЭК

ЧТО ЖЕ ХОЧЕТ ФСБ?

ВИДЕТЬ В СТРУКТУРЕ ДОКУМЕНТА РАЗДЕЛЫ:

- **Обобщенные возможности источников атак**
- **Реализация угроз безопасности информации, определяемых по возможностям источников атак**

КОНЕЧНАЯ ЦЕЛЬ ЭТИХ РАЗДЕЛОВ

Установить **класс средств криптографической защиты информации.**
Чаще всего применимый класс криптосредств – **КС3**
(к примеру «Застава»).

А ГДЕ ЭТО ВЗЯТЬ?

«Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности»

УТВЕРЖДЕНЫ
ФСБ России
31 марта 2015 года

ЧТО С ЭТИМ ДЕЛАТЬ?

Разработать применимо для Вашего ОУ

НЕ РАЗМЕЩАТЬ В ОТКРЫТОМ ДОСТУПЕ (на сайте)