РусКрипто

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Технологии повышения конфиденциальности – набор математических и технических методов, инструментов и практик, направленных на защиту личных данных и информации пользователей

РусКрипто

Например:

- Гомоморфное шифрование
- Криптографические способы защиты информации
- Конфиденциальные вычисления
- Федеративное обучение
- Дифференциальная приватность

Что хотим

- Ускоренное внедрение технологий повышения конфиденциальности в процессы обработки чувствительных данных

- Рост защищенности персональных данных граждан

- Повышение доступности аналитических данных для обучения моделей искусственного интеллекта

РусКрипто

Вопросы

- Какие есть возможности ускорения процедуры сертификации?
- Как простимулировать использование методов повышения конфиденциальности?
- Как оценить эффективность того или иного метода повышения конфиденциальности применительно к различным типам данных?

РусКрипто

Что мешает

РусКрипто

Отсутствие регуляторных стимулов

Например, учета применения технологий повышения конфиденциальности и минимизации угроз при оценке мер по обеспечению безопасности персональных данных

Ограничения на обработку

Например, дополнения законных оснований обработкой данных с применением технологий повышения конфиденциальности

Сложность процедур сертификации

Например, отсутствие лицензий на сертификацию для компаний, имеющих соответствующие компетенции, юридической и значимости такой сертификации

Обработка данных с применением PET

РусКрипто

Разработка сервиса (продукта) с применением технологии повышения конфиденциальности

Сертификация сервиса (продукта) на соответствие нормативным требованиям и требованиям ПНСТ

Предоставление сервиса (продукта) операторам персональных данных с целью обработки данных

Обработка данных на законном основании в соответствии с сертификатом (область применения и условия эксплуатации)

Роль технической стандартизации

РусКрипто

- Описание технологий повышения конфиденциальности, включая описание конкретных методов и протоколов
- Описание типовых сценариев применения каждой из технологий повышения конфиденциальности, а также типовой модели угроз (модель нарушителя)
- Закрепление модели оценки рисков повторной идентификации для каждого типа технологий повышения конфиденциальности

ПНСТ №1
Общая модель рисков

ПНСТ №2
Технологии обезличивания и анонимизации

ПНСТ №3
Модель оценки контекстных рисков (организационно-технические меры)

ПНСТ №4
Технологии конфиденциальных вычислений

ПНСТ №5
Дифференциальная приватность

Порядок сертификации РЕТ

РусКрипто

1. ПОДГОТОВКА ДОКУМЕНТАЦИИ → **2. ЭКСПЕРТИЗА** → **3. ИСПЫТАНИЯ/ ТЕСТИРОВАНИЕ** → **4. ВЫДАЧА СЕРТИФИКАТА**

- Описание функциональных возможностей
- Описание архитектуры, используемых алгоритмов/протоколов
- Категории защищаемых данных
- Реализуемые сценарии обработки данных
- Оценка рисков и описание мер по их минимизации

- Анализ документации
- Проверка соответствия требованиям, включая проверку соответствия ПНСТ
- Оценка безопасности, включая анализ механизмов защиты данных
- Анализ рисков, включая оценку рисков повторной идентификации в соответствии с ПНСТ

- Проверка функций на соответствие заявленным характеристикам
- Тестирование на устойчивость к атакам, включая атаки на конфиденциальные данные*
- Тестирование на соответствие требованиям безопасности, включая требования ПНСТ

- Наименование и описание
- **Область применения**
- **Условия эксплуатации и ограничения**
- Сведения о разработчике или поставщике

*в рамках ЭПР

РусКрипто

СПАСИБО
ЗА ВНИМАНИЕ