**Шаблон для выполнения задания №2**

|  |  |
| --- | --- |
| **1.тема** | **Применение систем искусственного интеллекта для автоматизации анализа побочных каналов утечки информации с использованием машинного обучения** |
| **2.направление/аспект применения ИИ** | * Автоматизация предобработки и фильтрации получаемых сигналов по побочным каналам (например, энергопотребление и электромагнитное излучение при выполнении исследуемого алгоритма). * Классификация и идентификация криптографических операций на формируемых наборах трасс (измерений) * Прогнозирование и выявление зависимости (корреляции) от данных (секретного ключа) |
| **3.аргументация выбора** | **Автоматизация** - снижается необходимость в «ручном» анализе экспертом-криптоаналитиком.  **Устойчивость метода к шуму** - модели на основе ИИ способны работать с зашумленными данными, где классические подходы не выявляют зависимости от данных.  **Повышение эффективности при малом количестве данных атаки** (числе трасс), вплоть до профилирования целевого устройства с возможностью атак по одной трассе.  **Выявление сложных зависимостей** - нахождение нелинейных зависимостей, не выявляемых с помощью традиционных статистических методов (корреляционный анализ). |
| **4.ожидаемый результат** | Применение методов атак по побочным каналам на основе ИИ на ранее устойчивые реализации. Взлом устройств, считавшихся защищенными от классического анализа методами DPA/CPA.  Возможность более точного прогнозирования уязвимостей на этапе проектирования чипов.  Автоматизированное сканирование семейств устройств на наличие схожих уязвимостей по побочным каналам.  Меняется ландшафт угроз для аппаратных криптографических средств защиты, требуется разрабатывать новые методы противодействия атакам по побочным каналам, в том числе тоже основанные на применении ИИ. |