**СРСП 9.** XSL атаки.

**Форма и содержание отчета**

Отчет должен содержать:

1. Титульный лист установленного образца.
2. Описание комплексного поиск возможных методов доступа.
3. Сравнительный анализ рассмотренных терминалов защищенной информационной системы.
4. Перечень использованных информационных источников.

Отчет выполняется на листах формата А4 рукописным или печатным способом. При рукописном оформлении отчета текст следует излагать четким почерком чернилами черного цвета.

**XSL-атака** ([англ.](http://dic.academic.ru/dic.nsf/ruwiki/6161) *eXtended Sparse Linearization*, алгебраическая атака) — это метод [криптографического анализа](http://dic.academic.ru/dic.nsf/ruwiki/80517), основанный на алгебраических свойствах [шифра](http://dic.academic.ru/dic.nsf/ruwiki/7192). Метод предполагает решение особой системы уравнений.

Данный метод был предложен в 2001 году Николя Куртуа (Nicolas T. Courtois).

XSL-атаки ранее считались невозможными, однако 26 мая 2006 года Куртуа продемонстрировал возможность XSL-атаки против модели одного шифра, сходного по своей структуре с шифром [AES](http://dic.academic.ru/dic.nsf/ruwiki/213882)[[1]](http://dic.academic.ru/dic.nsf/ruwiki/1715685#cite_note-1).

Как говорил один из создателей шифра [Rijndael](http://dic.academic.ru/dic.nsf/ruwiki/745803) в частной переписке: «XSL — это не атака, это всего лишь мечта». «Это мечта, способная стать вашим кошмаром», — отвечал Николя Куртуа.

Эффективность данной атаки до сих пор не доказана, но и не опровергнута.

**Алгоритм реализации XSL метода**

1. Обработка имеющейся системы уравнений путем выбора конкретного набора одночленов и уравнений, которые будут использоваться в дальнейших этапах алгоритма
2. Выбор значения параметра Р и умножение выбранных на предыдущем этапе уравнений на результаты произведений (Р-1) выбранных одночленов
3. При недостаточном числе уравнений применение Т’ метода, в котором некоторые выбранные уравнения умножаются на одиночные переменные. Цель данного метода – создание новых уравнений без получения каких-либо новых одночленов.
4. Применение линеаризации, путем представления каждого одночлена в виде новой переменной и выполнения Гауссовского исключения.