Аршинский Л.В., Шурховецкий Г.Н. **«Оценка защищённости данных методом рассечения-разнесения»**

Аннотация: В докладе рассматривается эффективность защиты информации, размещаемой во внешних хранилищах данных с использованием некриптографического метода рассечения-разнесения. Рассматриваются два подхода:

1. Рассечение «монолитное», когда информация делится на равные или нет части с разнесением в различные, в том числе географически удалённые хранилища так, что каждая часть представляет собой слитный – единый и непрерывный фрагмент исходной информации.

2. Рассечение «диффузное», когда отдельная часть (поток) содержит фрагменты различных участков исходного материала так, что при завладении одним или даже частью потоков смысл исходного сообщения оказывается трудноустановим.

Показано, что второй вариант обеспечивает лучшую защищённость. При этом целесообразно выполнять побитовое рассечение с условием, чтобы хранимые потоки формировались из битов случайным образом. Даются оценки защищённости, показывающие, что при таком подходе определяющим является длина ключа разнесения. Число потоков - вторично