ОТЗЫВ

на автореферат диссертации Мартьянова Евгения Александровича на тему «Исследование и разработка методик оценки защищенности информационных объектов от потенциальных нарушителей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Диссертационная работа Е.А. Мартьянова посвящена разработке моделей и методов выявления инсайдеров среди пользователей корпоративной информационной системы (КИС). Решение задач обнаружения (предотвращения и минимизации ущерба) инсайдерских атак несомненно является актуальным и важным направлением исследований в области информационной безопасности. Специфика проблемы обуславливается тем, что количество нелегальных действий (злоумышленников-инсайдеров) крайне мало по сравнению с общим количеством действий всех пользователей КИС. В этих условиях практически невозможно сформировать представительную выборку и применить методы машинного обучения для поиска аномалий (нехарактерного поведения пользователей).

В ходе выполнения работы автором получены следующие основные результаты:

- построена модель, характеризующая работу типичного (честного) пользователя и позволяющая применить теорию запретов;

- предложен метод выявления потенциальных инсайдеров среди пользователей КИС, проанализирована точность метода;

- разработаны программно-алгоритмические средства, позволяющие выявлять подозрительную активность пользователей по сбору избыточной информации;

- созданное алгоритмическое и программное обеспечение успешно внедрено для решения практических задач.

По автореферату имеются следующие замечания.

1. Неудачным представляется название работы – в нем делается акцент на разработке методики. Вместе с тем описания методики в автореферате не приводится, неясным остается и что такое «исследование методики». При этом в диссертации вполне понятно и корректно сформулирована цель – «разработка статистических методов…..», предложенные автором метод и модель вынесены в научную новизну. Получается «разрыв» между тем, как работа называется и что в ней конкретно делается.

2. Как представляется, в автореферате необходимо было уделить существенно больше внимания изложению решений, предложенных автором. Глава 2, содержащая основные новые подходы, дана описательно и поверхностно. Из обзора «выпали» экспертные методы выявления