

## ОТЗЫВ

**на автореферат диссертации Монаховой Марии Михайловны «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети», представленной на соискание ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций**

Целью представленной диссертации является повышение безопасности телекоммуникационных систем путём разработки, исследования и практической реализации новых моделей контроля инцидентов информационной безопасности. Это, безусловно, задача актуальная, которая, кроме теоретического, имеет явную практическую направленность в вопросах обеспечения безопасности телекоммуникационных систем и сетей.

Судя по автореферату, следующие результаты обладают научной новизной:

1. Предложена формальная модель инцидента ИБ, как специфического состояния корпоративной телекоммуникационной сети, идентифицируемого по отклонениям параметров ее функционирования от эталонных значений, задаваемых технической политикой информационной безопасности.

2. Разработана методика определения существенных факторов возникновения инцидентов информационной безопасности, в основе которой использован способ группового ранжирования факторов при обеспечении согласованности экспертов.

3. Разработан алгоритм формирования пакета контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети, основанный на анализе статистических характеристик обнаружения событий информационной безопасности по значениям контролируемых параметров, выделении комбинаций, обеспечивающих допустимые вероятностные характеристики обнаружения.

4. Предложена структурная схема автоматизированной системы контроля инцидентов информационной безопасности, как основа для практической реализации систем данного класса.

Достоинством работы является ее практическая направленность. На основе предложенных моделей разработано информационное и программное обеспечение системы контроля инцидентов, включающее программные комплексы для расчета значимости элементов телекоммуникационной сети,

документированного обеспечения, администрирования корпоративной сети, регистрации инцидентов информационной безопасности, мониторинга состояния элементов телекоммуникационной сети, АРМ диспетчера.

На основе изучения материалов автореферата возникло замечание по существу работы: не понятно, как быстро устраняется обнаруженный инцидент безопасности.

В целом диссертация представляет собой законченную работу, имеющую как теоретическую, так и практическую ценность в вопросах обеспечения безопасности телекоммуникационных систем и сетей. Предложены модели и алгоритмы, отвечающие критерию научной новизны. Результаты диссертации опубликованы в центральной печати, прошли апробацию на научно-технических конференциях, внедрены в ряде предприятий.

Работа в целом удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям. Монахова М.М. заслуживает присвоения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Доцент кафедры «Информационно-математические технологии и информационное право» Юридического института федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет путей сообщения Императора Николая II», кандидат технических наук

30.05.16

Л.М. Груздева



Подпись руки г.п. *Груздева Л.М.*  
Заверяю *Вашин* 30.05.2016  
Начальник УДО *Власова*