ОТЗЫВ

на автореферат диссертации Монаховой М.М. «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 диссертации является решение научно-технической задачи разработки новых моделей, алгоритмов и процедур контроля инцидентов информационной безопасности (ИБ), направленных на повышение эффективности обеспечения ИБ в системах и сетях телекоммуникаций. Это, безусловно, задача актуальная, которая, кроме теоретического, имеет явную практическую направленность в вопросах обеспечения ИБ современных предприятий и организаций. Это вызвано тем, что политики обеспечения ИБ, и создаваемые на их основе системы защиты информации (СЗИ), не могут полностью гарантировать защиту информационно-телекоммуникационной сети. После внедрения защитных мер и средств всегда остаются уязвимые места в сети, которые могут сделать обеспечение ИБ неэффективным. Кроме того, могут быть сбои и отказы самой СЗИ, выявляться новые угрозы.

Достоинством работы является ее практическая значимость. На основе предложенных методики, моделей и алгоритмов был разработан программный комплекс, наиболее полно охватывающий решение задачи контроля инцидентов ИБ в телекоммуникационной сети, таких как выявление, идентификация, устранение и предотвращение инцидентов. В комплекс вошли модули расчета значимости элементов корпоративной сети, документированного обеспечения, администрирования, регистрации инцидентов ИБ, мониторинга состояния сетевых элементов, АРМ диспетчера. Результаты опытной эксплуатации на ряде предприятий модулей системы контроля инцидентов показали: среднее время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку снижается на треть, среднее время выполнения функции устранения

инцидента снижается на четверть, снизилось время назначения исполнителя на решения инцидента. Кроме того, уменьшается общее количество инцидентов ИБ в корпоративной сети.

Среди основных результатов исследования, имеющие научную новизну, хотелось бы отметить предложенную автором формальную модель инцидента ИБ, как специфичного состояния КТС, идентифицируемого по отклонениям параметров ее функционирования от эталонных значений, задаваемых технической политикой ИБ, классификацию инцидентов ИБ, алгоритм формирования пакета контроля инцидентов ИБ в КТС, основанный на анализе статистических характеристик обнаружения событий ИБ по значениям контролируемых параметров.

Замечания

Из текста автореферата не понятно, почему возможна минимизация логической функции, образованной дизъюнкцией термов в алгоритме формирования пакета контроля инцидента безопасности на шаге 6 и как происходит устранение обнаруженного инцидента.

Вывод

Несмотря на замечания, диссертация, судя по автореферату, представляет собой самостоятельно выполненное, законченное исследование по решению актуальной научной задачи, соответствует требованиям Положения ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.12.13 - «Системы, сети и устройства телекоммуникаций», а ее автор Монахова М.М. достойна присуждения ученой степени кандидата технических наук.

Начальник отдела ЗАО «АЭРОКОН»
д-р технических наук, профессор

Толстов
Евгений Федорович

Адрес: ЗАО «АЭРОКОН»,
ул. Жуковского, 1, Жуковский, Московская обл., 140180
Телефон: 8 (495) 556-43-77

E-mail: E_tolstov@mail.ru

Подпись д.т.н., профессора Е.Ф.Толстова удостоверяю.
Ученый секретарь Совета
ЗАО «АЭРОКОН» Э.Г. Багдасарян

МП