# ОТЗЫВ

официального оппонента доктора технических наук, профессора Цимбала Владимира Анатольевича на диссертацию Монаховой Марии Михайловны на тему «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

Проблема обеспечения безопасного функционирования корпоративных телекоммуникационных сетей (КТС) продолжает оставаться одной из центральных как в отечественной науке и промышленности, так и за рубежом. Политики обеспечения информационной безопасности (ИБ) и создаваемые на их основе системы защиты (СЗ) не могут полностью гарантировать защиту КТС. 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, вызванные просчетами сетевого администрирования и информационными атаками на систему защиты. Состояния КТС, связанные с нарушениями политики ИБ и отказами СЗ в выполнении своих функций, в диссертации определяют понятие инцидента ИБ. В настоящее время процессы контроля инцидентов ИБ автоматизированы лишь частично, отсутствуют эффективные модели и алгоритмы их обнаружения и идентификации в составе единой системы, что часто является основной причиной продолжительного снижения производительности телекоммуникационной сети.

Именно поэтому проведенные Монаховой М.М. исследования, связанные с разработкой и практической реализацией моделей, алгоритмов и программных средств контроля инцидентов, актуальны и имеют практическое значение в решении проблемы обеспечения качества функционирования сетей телекоммуникаций предприятий и организаций различного профиля.

Исследовательскими задачами, решаемыми в диссертационной работе, являются:

- анализ процессов, методов и средств обеспечения контроля инцидентов ИБ в КТС, классификация инцидентов по характеру нарушения технической политики ИБ;
- разработка методики формирования множества существенных факторов возникновения инцидентов ИБ, определяющих параметры контроля;
- разработка моделей и алгоритмов формирования пакетов контролируемых параметров, процедур обнаружения инцидентов ИБ в КТС;
- синтез структурной схемы системы контроля инцидентов ИБ в КТС;
- реализация функциональных модулей системы контроля и их практическое внедрение в КТС предприятий и организаций.

В ходе проведения исследований по теме диссертационной работы автором получен ряд результатов, обладающих научной новизной, практической значимостью и выдвигаемых на защиту.

- предложена формальная модель инцидента ИБ, как специфичного состояния КТС, идентифицируемого по отклонениям параметров ее функционирования от шаблонов, задаваемых технической политикой ИБ;

- предложена классификация инцидентов ИБ по признаку «нарушение технической политики ИБ». Выделены характерные особенности инцидентов: «Неустранённая уязвимость», «Не обнаружена реализация угрозы», «Нет защиты от реализованной угрозы», «Реализация неизвестной угрозы», «Не устраняется воздействие реализации угрозы»;

- разработана методика определения множества существенных факторов возникновения инцидентов ИБ. В основе методики использован способ «усечения» полного множества факторов нарушения технической политики ИБ. Выявляется взаимосвязь инцидентов разного типа с факторами нарушения конкретной технической политики, далее выполняется групповой экспертный анализ факторов, в основе которого использован способ группового ранжирования при обеспечении согласованности экспертов;

- разработан алгоритм формирования пакета контроля инцидентов ИБ, основанный на анализе статистических характеристик обнаружения событий ИБ по значениям контролируемых параметров, выделении комбинаций, обеспечивающих допустимые вероятностные характеристики обнаружения и разработана процедура расстановки параметров оптимального пакета контроля по узлам КТС, что позволяет повысить производительность системы контроля;

- предложен алгоритм обнаружения инцидента, основанный на переборе всех возможных комбинаций событий ИБ, имеющих вид бинарных сигналов. Преимуществом предлагаемого подхода является использование минимального количества анализируемых комбинаций событий, обеспечивающих обнаружение инцидента с вероятностью, не хуже заданной;

- предложена структурная схема системы контроля инцидентов ИБ. Разработан алгоритм ее функционирования, что позволяет сформировать требования к практической реализации систем данного вида.

Основные результаты диссертации являются достоверными, что обусловлено корректностью постановки задач исследования, введением адекватных допущений и ограничений. Кроме того, результаты диссертации подтверждены в ходе экспериментальных исследований фрагмента КТС, воспроизводящего условия возникновения инцидентов в сети, а также в ходе практического использования разработанных средств защиты информации в телекоммуникационных системах и сетях различного

назначения.

Полученные в диссертации результаты в целом развивают методологию обеспечения информационной безопасности и защиты информации в системах и сетях телекоммуникаций.

Практическая значимость диссертационного исследования обусловлена следующим: разработанные методики, информационное и программное обеспечение системы контроля инцидентов ИБ, включающее программные комплексы для расчета значимости элементов КТС, документированного обеспечения, администрирования корпоративной сети, регистрации инцидентов ИБ, мониторинга состояния элементов КТС, АРМ диспетчера позволяют снижать общее количество анализируемых параметров для выявления инцидентов в 1.5 – 2,5 раза; уменьшать среднее время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку - на 33%, среднее время выполнения функции устранения инцидента - на 25%. Кроме того, в корпоративной сети уменьшается общее количество инцидентов. Результаты диссертационной работы использованы в учебном процессе Владимирского государственного университета и на предприятиях промышленности, о чем имеются соответствующие акты.

Замечания и недостатки:

1. Непонятно, почему такие важные критерии (факторы) нарушения Политики безопасности «Не весь входящий и исходящий трафик анализируется на наличие вредоносных программ и сигнатур известных атак» и «Реестр ПО содержит сведения о ПО с «просроченной» лицензией» (Таблица 2.8) в работе не отнесены к существенным?
2. В перечень мер защиты, приведенных в разделе 2.1 (с.31), не включены механизмы контроля целостности информационных ресурсов.
3. В алгоритме формирования пакета контроля инцидента пропущен шаг 4 (с. 55). Однако, следует отметить, что на рис. 3.1 и в автореферате данный шаг присутствует.
4. В алгоритме работы системы контроля инцидентов (с. 65) вводится понятие «программа решения инцидента», которое далее по тексту не используется и не поясняется.

В целом, однако, отмеченные недостатки не носят принципиального характера и не наносят существенного ущерба значимости результатам диссертационной работы, выполненной на высоком научном уровне. Отличительными особенностями работы являются логическая последовательность поставленных задач и направленность на решение важной практической технической задачи – повышения уровня безопасности телекоммуникационных сетей предприятий и организаций различного профиля.

Диссертация написана хорошим литературным языком и аккуратно оформлена. Основные выводы и положения диссертации достаточно широко опубликованы в научных изданиях и докладывались на представительных научно-технических конфе-

ренциях, где получили одобрение научной общественности, признающей авторитет автора в разработке вопросов, положенных в основу диссертационной работы. Требование ВАК о наличии публикаций в изданиях из Перечня ВАК выполнено.

Исследования по тематике представленной диссертации целесообразно продолжить в направлении создания средств автоматизации обнаружения источников возникновения инцидентов и оперативного их парирования.

Содержание автореферата соответствует основным положениям диссертации и позволяет сформировать обоснованное представление по всей работе в целом, а содержание диссертации соответствует паспорту специальности 05.12.13 – Системы, сети и устройства телекоммуникаций

ВЫВОДЫ

1. Представленная диссертация является законченной научно-квалификационной работой, содержащей постановку и решение научной задачи, а также оригинальные теоретические исследования и новые научные и практические результаты.
2. По актуальности тематики, глубине проводимых исследований и значимости полученных результатов диссертация полностью удовлетворяет требованиям пп. 9, 10, 11, 13 «Положения о присуждении ученых степеней», а её автор, Монахова Мария Михайловна, заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Официальный оппонент

Цимбал Владимир Анатольевич, заслуженный деятель науки РФ, д.т.н., проф., профессор кафедры «Автоматизированные системы управления» Военной академии РВСН имени Петра Великого, г.Серпухов

142210, Московская обл., г. Серпухов, ул. Бригадная, д.17,

телефон 8-985-141-79-09, e-mail: tsimbalva@mail.ru

4.06.16. В.А.Цимбал

Подпись заверяю.

Ученый секретарь диссертационного совета ДС 215.030.01 при Военной академии РВСН имени Петра Великого, г.Серпухов заслуженный работник Высшей школы РФ, кандидат военных наук, доцент

В.П. Ефремов