«УТВЕРЖДАЮ»

Проректор по научной работе РГРТУ

д.т.н., проф. _____ Таганов А.И.

"30" 05 2016 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию и автореферат диссертации 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

Актуальность темы диссертационной работы

Применение новых информационных и телекоммуникационных технологий на предприятиях и в организациях немыслимо без повышенного внимания к вопросам информационной безопасности. Разрушение информационного ресурса, блокирование средств телекоммуникаций или их несанкционированное использование могут вызвать аномальное функционирование корпоративной информационно-телекоммуникационной среды, и в результате нанести предприятию значительный материальный ущерб, вплоть до остановки производства. Широкомасштабная стандартизация и унификация средств вычислительной техники, телекоммуникаций, программного обеспечения, протоколов информационного взаимодействия и распределенный характер управления в значительной степени расширяют возможности несанкционированного воздействия на ресурсы информационно-телекоммуникационной среды. Подобное положение дел резко обостряет проблему обеспечения информационной безопасности (ИБ) в современных корпоративных телекоммуникационных сетях (КТС).

Обеспечение ИБ реализуется посредством многорубежной системы защиты, функционирование которой регламентировано политиками ИБ. Политика нижнего уровня – техническая, формируется, как правило, зада-

нием значений параметров настройки узлов КТС и средств защиты, работающих в составе единой системы. Из таких значений формируется так называемый «профиль защиты» КТС. Несоответствие профилю является инцидентом ИБ.

Таким образом, диссертационная работа, посвященная разработке и практическому внедрению моделей и алгоритмов контроля инцидентов ИБ в корпоративной телекоммуникационной сети, является чрезвычайно актуальной и важной для обеспечения информационной безопасности в системах и сетях телекоммуникаций.

Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации

Анализ диссертационной работы, автореферата и научных трудов соискателя позволил сделать вывод о том, что научная новизна диссертационной работы обоснована и в ней получены автором лично следующие результаты.

1. Предложена формальная модель инцидента, как специфичного состояния КТС, идентифицируемого по отклонениям параметров ее функционирования от эталонных значений, задаваемых технической политикой ИБ.

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

3. Разработан алгоритм формирования пакета контроля инцидентов ИБ в КТС, основанный на анализе статистических характеристик обнаружения событий ИБ по значениям контролируемых параметров, выделении комбинаций, обеспечивающих допустимые вероятностные характеристики обнаружения.

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

Положения, выносимые на защиту:

- формальная модель инцидента ИБ в КТС, обеспечивающая теоретическое обоснование построения систем контроля инцидентов ИБ;

- методика определения множества существенных факторов возникновения инцидентов ИБ, позволяющая снижать количество контролируемых параметров для выявления инцидентов;

- алгоритм формирования пакетов контролируемых параметров, обеспечивающий повышение производительности системы контроля;

- структурная схема и результаты внедрения программных модулей системы контроля инцидентов, позволяющие разрабатывать системы данного класса.

Обоснованность и достоверность научных положений, основных выводов и результатов диссертации обеспечивается за счет анализа состояний исследования в данной области, согласованности теоретических выводов с результатами экспериментальной проверки моделей. Основные результаты работы, полученные автором, прошли апробацию на международных и российских научных конференциях. Достоверность научных положений, выводов и практических рекомендаций, полученных в диссертационной работе, подтверждается корректным обоснованием постановок задач, точной формулировкой критериев, результатами экспертной оценки, а также их внедрением на практике.

Значимость для науки и практики результатов, полученных автором диссертации

Основным научным достижением автора является разработка новых моделей и алгоритмов контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети. Полученные научные результаты вносят существенный вклад в развитие механизмов обеспечения информационной безопасности систем и сетей телекоммуникаций. Сделанные теоретические выводы подтверждены экспериментальной проверкой с использованием разработанных программных средств в процессе диссертационного исследования. Практическое значение результатов работы определяется тем, что они нашли конкретные эффективные применения в корпоративной телекоммуникационной сети ОАО ВЗ «Электроприбор» г. Владимир, сети передачи данных администрации Владимирской области, использованы в технических мероприятиях по обеспечению ИБ ООО «НПП «ИНПРОКОМ» г. Балакирево Владимирской обл.

Рекомендации по использованию результатов и выводов диссертации

Результаты исследований имеют достаточно общий характер, что позволяет распространить их на широкий круг создаваемых и модернизируемых КТС предприятий и организаций. Результаты и выводы, полученные в диссертационной работе, рекомендуются к применению на предприятиях, использующих информационные и телекоммуникационные технологии для организации управленческой и технологической деятельности. Считаем целесообразным продолжение работ по данному направлению во Владимирском регионе и в частности во Владимирском государственном университете.

Замечания по диссертационной работе

1. Из текста работы не ясно, как средняя нагрузка в экспериментальной телекоммуникационной сети (рис. 4.2 диссертации) влияет на статистические характеристики измерителей параметров инцидентов.
2. В диссертации отсутствуют сведения об использовании стандартных средств сетевого контроля и диагностики, приведенных в разд. 1.2 (стр.19), в разработанной системе контроля инцидентов.
3. Не понятно, как можно измерить «отклонение» текстового файла настройки от эталона (например, для межсетевого экрана), если в настройках ничего не изменилось, просто переставлены строки.
4. Фактор №25 нарушения технической политики безопасности (стр. 33, табл.2.3) носит название «В папках пользователей присутствует информация «неслужебного» характера». Измерение параметра, соответствующего данному фактору, в реальной КТС выглядит проблематичным.

Заключение

Диссертация представляет собой законченную научно - исследовательскую работу на актуальную тему. Выполненные исследования и полученные результаты развивают методику обеспечения информационной безопасности систем и сетей телекоммуникаций, открывают новые возможно-

сти обеспечения условий их эффективного использования. Полученные результаты использованы в промышленности и образовании.

Название диссертации, автореферат и публикации в полной мере отражают содержание работы.

Диссертационная работа «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети» соответствует паспорту научной специальности 05.12.13 – Системы, сети и устройства телекоммуникаций и «Положению о присуждении ученых степеней», утвержденному постановление Правительства Российской Федерации от 24 сентября 2013 г. №842, а ее автор – Монахова Мария Михайловна по уровню профессиональных, специальных и научных знаний заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Отзыв рассмотрен и одобрен на заседании кафедры радиоуправления и связи РГРТУ. Протокол №9 от 24 мая 2016 г.

Действительный член Международной Академии связи,
Заслуженный работник высшей школы РФ,
почетный член РНТО РЭС им. А.С. Попова,
заведующий кафедрой радиоуправления и связи,
д.т.н., профессор Кириллов С.Н.

Доцент кафедры Радиоуправления и связи
к.т.н., доцент Дмитриев В.Т.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Рязанский государственный радиотехнический университет»

Адрес: 390005, г.Рязань, ул. Гагарина, 59/1

Телефон: 8(4912)460303

Эл.адрес: rgrtu@rsrtu.ru