«УТВЕРЖДАЮ»
Первый проректор, проректор
по научной и инновационной работе ВлГУ,
д.ф-м.н., проф.
_____ В.Г. Прокошев
_____ 2016 г.

ЗАКЛЮЧЕНИЕ

федерального государственного бюджетного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

Диссертация «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети» выполнена во Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых.

В период подготовки диссертации соискатель Монахова Мария Михайловна обучалась в заочной аспирантуре Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых.

В 2014 году закончила магистратуру Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых по направлению «Информационные системы и технологии».

Кандидатские экзаменов по иностранному языку сданы в 2012 году, по истории и философии науки в 2013 году, по специальной дисциплине в 2016 году.

Научный руководитель - Никитин Олег Рафаилович, доктор технических наук, профессор, заведующий кафедрой радиотехники и радиосистем Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых.

в диссертационной работе изложены результаты разработки моделей, алгоритмов и процедур контроля инцидентов информационной безопасности (ИБ), направленных на повышение эффективности обеспечения ИБ в системах и сетях телекоммуникаций. Поставлены и решены следующие задачи:

1. Выполнен анализ процессов, методов и средств обеспечения контроля инцидентов ИБ в корпоративной телекоммуникационной сети, на основе которого предложена классификация инцидентов по характеру нарушения технической политики ИБ.

2. Разработана методика определения множества существенных факторов возникновения инцидентов ИБ, определяющих параметры контроля.

3. Разработаны модели и алгоритмы формирования пакетов контролируемых параметров, процедур обнаружения инцидентов ИБ в корпоративной телекоммуникационной сети.

4. Синтезирована структурная схема системы контроля инцидентов ИБ в корпоративной телекоммуникационной сети. Реализованы функциональные модули системы контроля, которые нашли практическое внедрение в корпоративных телекоммуникационных сетиях предприятий и организаций.

Личный вклад автора. Монаховой М.М. на основе проведенного анализа сформулированы задачи диссертационного исследования, выполнен отбор способов и средств для решения поставленных задач, произведено теоретическое обобщение результатов исследования, что представлено в диссертации и опубликованных работах.

Достоверность полученных в диссертационной работе результатов подтверждается с помощью исследований корпоративной сети, выполненных на экспериментальной установке, воспроизводящей условия возникновения инцидентов в КТС, а также в ходе практического использования разработанных средств.

Научная новизна результатов, полученных Монаховой М.М., заключается в следующем:

1. Предложена формальная модель инцидента ИБ, как специфичного со-

стояния корпоративной телекоммуникационной сети, 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 корпоративной телекоммуникационной сети, 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.

Практическая значимость работы.

Разработано информационное и программное обеспечение системы контроля инцидентов ИБ, включающее программные комплексы для расчета значимости элементов корпоративной телекоммуникационной сети, документированного обеспечения, администрирования корпоративной сети, регистрации инцидентов ИБ, мониторинга состояния элементов корпоративной телекоммуникационной сети, АРМ диспетчера. Результаты опытной эксплуатации модулей системы контроля инцидентов на ряде предприятий показали: среднее время ожидания заявки пользователей, обнаруживших проявление инцидента ИБ, на обработку снижается на 33%, среднее время выполнения функции устранения инцидента снижается до 25%, снизилось время назначения исполнителя на решения инцидента. Кроме того, уменьшается общее количество инцидентов.

Результаты исследования внедрены и реализованы:

- в корпоративной сети ОАО ВЗ «Электроприбор» г. Владимир, что позволило повысить уровень автоматизации при оценке защищенности телекоммуникационных и информационных ресурсов;

- в сети передачи данных администрации Владимирской области, что позволило сократить затраты на восстановительные работы по устранению инцидентов ИБ;

- в ООО «НПП «ИНПРОКОМ» г. Балакирево Владимирской области при проведении плановых технических мероприятий по обеспечению защиты информации, что позволило выявить дополнительные уязвимости сетевой инфраструктуры предприятия;

- в ФГБОУ ВО ВлГУ для обеспечения учебного процесса при подготовке бакалавров по направлению 11.03.02 - «Инфокоммуникационные технологии и системы связи» на кафедре радиотехники и радиосистем.

Опубликованные научные работы полностью отражают основное содержание диссертационного исследования. По результатам исследования опубликовано 28 работ, 5 в изданиях из перечня ВАК, из них 1 проиндексирована в международной базе Scopus. Получено 9 свидетельств о государственной регистрации программ для ЭВМ.

Диссертация «Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети» Монаховой Марии Михайловны рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.12.13 - «Системы, сети и устройства телекоммуникаций».

Заключение принято на заседании кафедры радиотехники и радиосистем ВлГУ.

Присутствовало на заседании 14 человек. Результаты голосования: «за» - 14 человек; «против» - 0 человек; «воздержалось» - 0 человек. Протокол №10 от 17 февраля 2016 г.

Заведующий кафедрой радиотехники
и радиосистем ВлГУ д.т.н., проф. О.Р. Никитин