ОТЗЫВ

официального оппонента к.т.н., доцента Ложникова Павла Сергеевича 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

Актуальность работы. Диссертационная работа направлена на решение научно-технической задачи повышения эффективности обеспечения информационной безопасности (ИБ) в системах и сетях телекоммуникаций за счет построения новых моделей, методов и средств контроля инцидентов информационной безопасности.

Складывающаяся в Российской Федерации организационно-правовая конъюнктура, а также все возрастающее влияние глобальной информационной инфраструктуры, являющейся благоприятной средой для осуществления разного рода угроз ИБ, подталкивает руководство организаций и предприятий к использованию более строгих, формализованных подходов к составлению, актуализации и контролю за исполнением политик ИБ. В связи с этим появилась масса методов и инструментальных средств, автоматизирующих разные аспекты деятельности специалиста по безопасности телекоммуникационных и информационных систем (системы обнаружения атак, DLP-системы, системы автоматизации протоколирования и т.д.). Вместе с тем существенно возросла роль службы технической поддержки, занимающейся сбором, обработкой и реагированием на сообщения пользователей информационно-телекоммуникационной системы предприятия о разного рода сбоях, ошибках и аномалиях. Как правило, такого рода службы для автоматизации своей деятельности используют ERP-систему, напрямую не связанную с системой защиты информации в организации.

С другой стороны, понятие инцидента ИБ как нарушения политики ИБ предполагает соотнесение технического регламента и конфигурации инстру-

ментальных средств анализа информации об информационно - телекоммуникационной системе с конкретными требованиями политики как документа. Само по себе срабатывание, скажем, системы обнаружения атак, равно как и поступление заявки от пользователя в службу технической поддержки, не означает факт того, что на предприятии имел место инцидент ИБ. Следует также упомянуть, что количество параметров, которые необходимо контролировать для выявления инцидента, крайне велико в силу большого размера современных информационно - телекоммуникационных систем. Более того, методы, лежащие в основе функционирования службы технической поддержки, имеют низкую эффективность в условиях ограниченных ресурсов. Таким образом, ключевой задачей в рамках проблемы повышения эффективности обеспечения ИБ в корпоративных телекоммуникационных системах представляется задача создания производительных методов контроля инцидентов ИБ, позволяющих при заданных ресурсах (в т.ч. и временных) успешно выявить и локализовать произошедшее нарушение политики ИБ предприятия.

Содержание работы в целом соответствует названию и обозначенной проблематике. В диссертацию входят: обзорная глава, в которой анализируются стандарты и инструментальные средства сетевого управления и обеспечения ИБ, описывается формальная модель инцидента ИБ в телекоммуникационной сети; глава, которая посвящена разработке методики определения существенных факторов нарушения технической политики ИБ; глава, в которой разрабатываются математические и алгоритмические модели формирования пакетов контроля инцидентов ИБ в КТС; глава, посвященная описанию системы контроля инцидентов ИБ и примеров реализации функциональных блоков системы контроля.

Новизна исследования и полученных результатов:

1. Предложена формальная модель инцидента ИБ, как специфичного состояния корпоративной телекоммуникационной сети (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.

Степень обоснованности и достоверности научных положений, выводов и заключений, сформулированных в диссертации. Все положения, выносимые на защиту, являются строго обоснованными и логически увязанными друг с другом. Выводы и рекомендации, отражающие теоретическое и прикладное значение диссертационной работы, не вызывают сомнений в их правильности и обоснованности. Новизна и достоверность научных положений и выводов, сформулированных в диссертации, подтверждены апробацией на представительных всероссийских и международных научных конференциях, исследованиями КТС, выполненными на экспериментальной установке, воспроизводящей условия возникновения инцидентов в КТС, а также в ходе практического использования разработанных средств.

Опубликование основных результатов диссертации в научной печати**.** Автором 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.

Ценность для науки и практики. Ценность для науки определяется перечисленными ранее научными результатами. Они позволяют повысить эффективность обеспечения ИБ телекоммуникационной сети предприятия. Особый интерес для решения задачи оптимального обнаружения инцидентов представляют алгоритмы формирования пакета контролируемых параметров,

которые позволяют исключать из рассмотрения некоторые особенности сетевого взаимодействия и функционирования узлов сети, при этом сохраняя приемлемые статистические характеристики обнаружения инцидента. Внедрение этих алгоритмов в широкий класс систем автоматизации деятельности администратора безопасности позволит существенно снизить время и затраты ресурсов, требуемых для мониторинга и контроля за состоянием телекоммуникационной системы.

Развитие тематики в диссертационном исследовании имеет существенное теоретическое и практическое значение как для проектирования систем и средств защиты информации в телекоммуникационных системах и сетях, так и для разработки методов автоматизации технической поддержки крупномасштабных информационно - телекоммуникационных систем. Результаты исследований внедрены в корпоративной телекоммуникационной сети ряда предприятий и организаций, а также были использованы при разработке учебных курсов во Владимирском государственном университете.

Замечания:

1. В алгоритме экспертного анализа (раздел 2.2 диссертации) проверяется условие «если согласованность (экспертов) не соблюдена, то необходимо изменить исходные факторы». Каким образом это можно сделать, если Политика уже существует?
2. Системе контроля приходится проверять значения многих параметров во многих узлах телекоммуникационной сети. Какую «нагрузку» на сеть дает система контроля? Не страдают ли пользователи.
3. В алгоритме формирования пакета контроля инцидента пропущен шаг 4
4. Не приведены временные оценки решения процедуры назначения контролируемым параметрам минимально допустимого времени на контроль и их распределение по узлам сети. Процедура решается полным перебором и затраты времени решения могут быть существенными.

Указанные недостатки существенным образом не снижают достоинств работы, которая в целом заслуживает положительной оценки.

Заключение

Работа представляет собой законченное научное исследование, включающее постановку проблемы, теоретические исследования и новые научные и практические результаты. Основные положения и выводы, сформулированные в работе, теоретически обоснованы, проверены в ходе экспериментальных исследований, достаточно отражены в научных публикациях и апробированы. Диссертационная работа соответствует паспорту заявленной специальности.

Автореферат правильно отражает основное содержание диссертации. Диссертация Монаховой Марии Михайловны соответствует требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.12.13 – Системы, сети и устройства телекоммуникаций.

Официальный оппонент

Ложников Павел Сергеевич, к.т.н., доц., заведующий кафедрой «Комплексная защита информации» Федерального государственного бюджетного образовательного учреждения высшего образования «Омский государственный технический университет»

644050, г. Омск, пр. Мира 11,

телефон (3812) 21-77-02, e-mail: lozhnikov@gmail.com

30.05.16 П.С.Ложников

Подпись заверяю

И.о. начальника Управление кадров