ОТЗЫВ

на автореферат диссертации

Милославской Натальи Георгиевны

на тему «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях»,

представленной на соискание учёной степени

доктора технических наук по специальности

05.13.19 – методы и системы защиты информации, информационная безопасность

Актуальность темы. Интенсивно развивающиеся во всем мире и в России информационно-коммуникационные и сетевые технологии породили широкое использование информационно-телекоммуникационных сетей. Не случайно Национальная программа «Цифровая экономика Российской Федерации» 2019 г. одной из целей ставит создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных на территории Российской Федерации, базирующейся на информационно-телекоммуникационных сетях субъектов критической информационной инфраструктуры. Направлениями обеспечения информационной безопасности указанной инфраструктуры являются: повышение безопасности функционирования ее объектов, обеспечение целостности, устойчивости функционирования и безопасности информационно-телекоммуникационных систем, а также обеспечение безопасности передаваемой по ним информации. Следовательно, появление диссертации по тематике интеллектуального управления сетевой безопасностью в связи с особой актуальностью ее темы не вызывает сомнения.

Оценка содержания и структуры автореферата. Материал автореферата структурирован соискателем в строгом соответствии с ГОСТ и логикой раскрытия темы. Текст написан хорошим литературным и научным языком.

В первой главе традиционно анализируется состояние проблемы, уточняются цель и задачи исследования, определяются его границы. Во второй главе вводятся и разрабатываются системные классификации основных используемых в работе понятий информационной безопасности. В третьей

главе дается формализованное описание процессов управления инцидентами информационной безопасности. В четвертой главе на основе выявленных недостатков центров мониторинга и управления безопасностью прошлых поколений сформулированы требования к создаваемому центру интеллектуального управления сетевой безопасностью для информационно-телекоммуникационных сетей, а также описана разработанная бизнес-логика его функционирования. Пятая глава посвящена изложению научно обоснованной методологии, принципов, трех архитектур, методов использования и выбору решений для реализации типового центра интеллектуального управления сетевой безопасностью. В шестой главе приводятся результаты внедрения. Каждая из глав отражает результаты решения намеченных задач исследования, что гарантированно обеспечивает достижение цели исследования.

В диссертации решена научная проблема формирования научной основы обеспечения информационной защищенности и функциональной устойчивости информационно-телекоммуникационных сетей на всех стадиях жизненного цикла их информационных ресурсов в штатном режиме и в условиях реализации угроз информационной безопасности в едином информационном пространстве организации.

Указанная проблема решена за счет прогнозирования развития событий в области информационной безопасности и применения в центре интеллектуального управления сетевой безопасности для достижений этих целей интеллектуальных подходов обработки больших относящихся к информационной безопасности информационно-телекоммуникационных сетей данных.

Таким образом, в диссертации разрешено противоречие между существующим недостаточным уровнем обеспечения информационной безопасности в информационно-телекоммуникационных сетях организаций и постоянно растущим масштабом и сложностью сетевых атак на них.

Из автореферата можно заключить, что диссертация является законченным научным исследованием и выполнена на высоком научном и методическом уровне.

Основные положения и выводы могут быть в полном объеме использованы в практике внедрения типового центра интеллектуального управления сетевой безопасностью в информационно-телекоммуникационных сетях

субъектов критической информационной инфраструктуры, а также для подготовки будущих специалистов для его разработки, разворачивания и использования.

К недостаткам автореферата следует отнести:

1) отсутствуют математические модели, описывающие функционирование предложенного автором центра интеллектуального управления сетевой безопасностью и позволяющие исследовать влияние различных факторов на характеристики его функционирования;

2) отсутствуют количественные результаты, позволяющие оценить по каким-либо критериям преимущества от использования предложенного центра интеллектуального управления сетевой безопасностью в информационно-телекоммуникационных сетях;

3) в автореферате упомянуто о разработке методологии построения типового центра интеллектуального управления сетевой безопасностью, но не приведено ее описание, критерии и количественные результаты, показывающие ее преимущества, хотя это является одним из положений, выносимых на защиту;

4) не приведены сравнительные характеристики работы указанного в пятом пункте основных положений, выносимых на защиту, средства блокирования попыток компрометации массива накапливаемых в центре интеллектуального управления сетевой безопасностью свидетельств инцидентов информационной безопасности в информационно-телекоммуникационной системе и существующих средств, выполняющих аналогичную функцию;

5) из текста автореферата не ясно, в чем состоит расширение и уточнение временной шкалы, упомянутой в шестом пункте основных положений, выносимых на защиту;

6) в тексте автореферата встречается большое количество аббревиатур, и присутствую грамматические и пунктуационные ошибки.

Как следует из автореферата, результаты работы достаточно полно опубликованы и прошли апробацию на конференциях различного уровня.

Выводы. Изучение автореферата диссертации на тему «Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях» дает веские основания утверждать, что по объему, всестороннему освещению темы, логически последовательному по-

строению, теоретической и практической значимости полученных результатов диссертация полностью отвечает требованиям, предъявляемым ВАК РФ к диссертациям на соискание учёной степени доктора наук, а ее автор – Милославская Наталья Георгиевна – заслуживает присуждения ученой степени доктора технических наук по специальности 05.13.19.

Отзыв заслушан на заседании кафедры «Информационная безопасность систем и технологий», протокол №7 от «29» января 2021 г.

Доцент каф. «Информационная безопасность
систем и технологий», д.т.н.,
05.13.19 «Методы и системы защиты
информации, информационная безопасность»
Тел. +7 8412 20-84-35, e-mail: ibst@pnzgu.ru
Наталья Алексеевна Егорова

«29» января 2021 г.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет» (ФГБОУ ВО ПГУ), ул. Красная, д. 40, г. Пенза, Россия, 440026
Тел/факс: (841-2) 56-51-22, e-mail: cnit@pnzgu.ru, http://www.pnzgu.ru

ЛИЧНУЮ ПОДПИСЬ Егорову Н.А.
ЗАВЕРЯЮ
Начальник управления кадров