ОТЗЫВ

на автореферат диссертации Абрамовой Таисии Вячеславовны

на тему «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков», представленную на соискание ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Диссертация Абрамовой Т.В. посвящена вопросам разработки методов, алгоритмов, методик и средств обнаружения аномалий и нейтрализации угроз безопасности информации (далее - БИ) в распределенных автоматизированных системах управления технологическими процессами (далее – АСУ ТП). Тематика работы является актуальной в связи с ростом числа угроз БИ и атак на объекты критической информационной инфраструктуры (далее – КИИ), в том числе АСУ ТП транспортировки нефтегазового сырья, что подтверждается статистикой инцидентов информационной безопасности на предприятиях нефтегазовой отрасли.

В работе четко выделены объект и предмет исследования. Поставлены и решены актуальные задачи. Автором проведен системный анализ современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой на примере компьютерных сетей (далее - КС) АСУ ТП транспортировки нефтегазового сырья. Разработаны: метод кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ; метод построения математических и имитационных моделей и модельный базис задачи обнаружения аномалий и нейтрализации угроз БИ на основе данных сетевого трафика; алгоритмы, методики и программы для реализации методов и средств обнаружения аномалий и нейтрализации угроз в КС распределенных АСУ ТП. Проведена экспериментальная оценка эффективности результатов исследований и разработаны рекомендации их практического применения в распределенных автоматизированных системах на примере АСУ ТП транспортировки нефтегазового сырья.

Среди результатов, обладающих научной новизной, следует выделить:

- метод матричной кластеризации угроз и моделей угроз (далее - МУ) безопасности информации на основе статистической обработки значений рисков,

отличающийся использованием ортогональных средних значений рисков по угрозам и МУ в качестве исходных данных для кластеризации, позволяющий оценивать степени актуальности угроз, приоритетности их нейтрализации и определять характер изменения угрозы на последовательности подсистем распределенной АСУ ТП, применять принципы типового проектирования при построении систем защиты информации для АСУ с распределенной топологией;

- метод построения математических и имитационных моделей для обнаружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика, отличающийся использованием дихотомического принципа разделения исследуемого множества состояний сетевого трафика на нормальные и аномальные на основе разделяющей функции мажоритарного вида, позволяющий повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз в КС АС;

- алгоритмы, методики и программная реализация методов и средств идентификации источников и маршрутов распространения вредоносного кода, определения резервных маршрутов передачи данных в промышленной КС, мониторинга действий персонала АС, отличающиеся тем, что в основу работы средств защиты положены принципы построения ассоциативных процессоров, что позволяет повысить производительность, достоверность, универсальность средств и снизить риски от угроз БИ.

Новизна результатов подтверждается полученным патентом на изобретение, свидетельствами о регистрации программ для ЭВМ, значительным числом публикаций.

Практическую ценность исследования составляют разработанные автором методы и средства, позволяющие снизить риски от угроз БИ в распределенных АС, которые могут быть использованы в подразделениях, занимающихся вопросами обеспечения информационной безопасности АСУ ТП.

Достоверность полученных результатов подтверждена их апробацией в процессе проведения экспериментов, апробацией на научных конференциях, публикацией результатов в ведущих рецензируемых научных изданиях.

Автореферат диссертации грамотно написан, аккуратно оформлен, полностью отвечает требованиям Положения ВАК о порядке присуждения ученых степеней. Из материалов автореферата следует, что диссертационная работа выполнена на высоком научном уровне.

Между тем, по материалам автореферата можно сделать следующие замечания.

1) В тексте автореферата явно не указано, какие меры обеспечения безопасности значимого объекта реализуют разработанные решения, согласно требованиям Приказа ФСТЭК № 239.

2) В автореферате приводится математическая модель, положенная в основу метода обнаружения аномального состояния распределенных АС на базе дихотомического подхода, но не приведена блок-схема соответствующего алгоритма, что позволило бы получить наглядное представление о его работе.

Указанные замечания не являются принципиальными и не снижают научно-практическую ценность диссертационного исследования. Судя по автореферату, представленное диссертационное исследование актуально, обладает достоверностью, научной новизной и практической значимостью, является завершенной научно-квалификационной работой и соответствует требованиям п.9 Положения ВАК о порядке присуждения ученых степеней, а ее автор, Абрамова Таисия Вячеславовна, заслуживает присуждения ей ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Отзыв составил:
Доктор технических наук, доцент
заведующая кафедрой информатики
и информационной безопасности,
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Магнитогорский государственный технический
университет им. Г.И. Носова» Баранкова Инна Ильинична

«3» сентября 2024

Докторская диссертация защищена по специальности:
05.09.10 – Электротехнология

Даю согласие на обработку персональных данных.

Адрес места основной работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова», 455000, г. Магнитогорск, пр. Ленина 38, ауд. 368
Рабочий телефон: +7 (3519) 23-27-51
Адрес эл. почты: inna_barankova@mail.ru

Подпись Баранковой И.И. заверяю:

ПОДПИСЬ ЗАВЕРЯЮ
Начальник отдела делопроизводства
ФГБОУ ВО «МГТУ им. Г.И. Носова»
Д.Г. Семенова