

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**

Диссертационная работа Абрамовой Т.В. посвящена решению актуальной задачи разработки методов, моделей, алгоритмов и методик обнаружения аномалий и нейтрализации угроз безопасности информации (БИ), позволяющих снизить риски от угроз в компьютерных сетях (КС) распределенных автоматизированных систем управления.

Автором проведен анализ современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах критической информационной инфраструктуры с распределенной архитектурой.

Разработан метод матричной кластеризации угроз и моделей угроз на основе статистической обработки значений рисков, позволяющий определять характер изменения угрозы на последовательности подсистем распределенной автоматизированной системы управления технологическим процессом (АСУ ТП), оценивать степень актуальности угроз и приоритетности их нейтрализации.

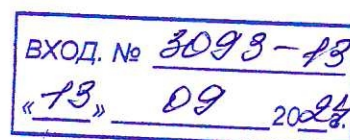
Предложен метод построения математических и имитационных моделей и разработаны модели для обнаружения аномалий и распознавания состояния КС АСУ на основе данных мониторинга сетевого трафика, позволяющий повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз в КС автоматизированных систем.

Разработаны алгоритмы, методики и программная реализация методов и средств обнаружения аномалий и нейтрализации угроз в КС распределенных автоматизированных систем, позволяющие снизить риски от угроз БИ.

Проведена экспериментальная оценка эффективности результатов исследований, показавшая снижение рисков от угроз распространения вредоносного кода в КС, несанкционированных действий персонала АСУ, потери информации о состоянии технологического объекта. Разработаны рекомендации практического применения результатов работы в распределенных автоматизированных системах.

Научная новизна исследований не вызывает сомнений. Полученные результаты обладают достоверностью, теоретической и практической значимостью, что подтверждается их апробацией на научных конференциях, достаточным числом публикаций в ведущих рецензируемых научных изданиях, актами о внедрении и использовании результатов диссертационной работы в организациях и ВУЗах.

По материалам исследования опубликовано 43 работы, в том числе 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 1 научная работа в издании, включенном в базу Scopus, 26 статей в других изданиях, 1 коллективная монография, 1 учебно-методическое пособие. Получен 1



патент и 9 свидетельств о регистрации программ для ЭВМ.

Замечания по автореферату:

1. Обозначения географических объектов и надписи на рисунке 1 автореферата выполнены слишком мелко, что затрудняет его читабельность.


2. При оценке снижения уровня риска недостаточно ясен механизм работы получения численных значений вероятностей (4 глава).

Указанные замечания носят частный характер и не снижают научной и практической ценности диссертации.

По объему и научной значимости полученных результатов диссертационная работа Абрамовой Т.В. на тему «Обнаружение аномалий и нейтрализация угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков», представленная на соискание ученой степени кандидата технических наук, 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 ученой степени кандидата технических наук по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Отзыв составил:

профессор кафедры №1 военного учебного центра имени Героя Советского Союза полковника В.Ф. Шишкова при ФГБОУ ВО «Пензенский государственный университет»

д-р техн. наук, профессор  А. Ю. Малыгин

«02» сентября 2024 г.

Сведения об авторе отзыва:

Малыгин Александр Юрьевич, д-р техн. наук, профессор.

Докторская диссертация защищена по специальности 05.13.01. Системный анализ, управление и обработка информации (технические науки)

Даю согласие на обработку персональных данных

 А. Ю. Малыгин

Адрес основного места работы: 440026, г. Пенза, ул. Красная, 40, ФГБОУ ВО «Пензенский государственный университет»

Рабочий телефон: (88412)20-35-83

Адрес эл. почты: mal890@yandex.ru

Подпись и сведения профессора Малыгина А.Ю. заверяю:

Ученый Секретарь Ученого Совета

к.т.н., доцент

«02» сентября 2024 г.


О.С. Дорофеева

