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

Методы и средства обнаружения аномалий и нейтрализации угроз безопасности информации (БИ) являются необходимой составляющей в современных системах защиты информации (СЗИ) автоматизированных систем управления технологическими процессами (АСУ ТП), как объектов критической информационной инфраструктуры (КИИ). Они позволяют повысить уровень безопасности технологических процессов и защитить промышленные объекты от внутренних и внешних угроз БИ. Таким образом, тематика представленного диссертационного исследования является актуальной и востребованной.

Автором диссертации предложена оригинальная концепция снижения рисков информационной безопасности на объектах КИИ с распределенной архитектурой за счет разработки высокопроизводительных методов и средств оперативного обнаружения и достоверного распознавания аномальных состояний АСУ на основе дихотомического и ассоциативно-мажоритарного подходов с применением интеллектуальной обработки данных сетевого трафика.

К наиболее значимым результатам диссертационной работы, обладающим научной новизной, относятся метод матричной кластеризации угроз и моделей угроз распределенной АС на основе ортогональных средних значений рисков, метод построения математических и имитационных моделей для обнаружения аномалий, распознавания состояний КС АСУ на основе дихотомического принципа и разделяющей функции мажоритарного вида, алгоритмы, методики и программная реализация методов и средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика на основе принципов построения ассоциативных процессоров.

Новизна результатов подтверждается полученным патентом на изобретение, свидетельствами о регистрации программ для ЭВМ. Материалы диссертационного исследования неоднократно обсуждались на научных и научно-практических конференциях различного уровня, опубликованы в ведущих рецензируемых научных изданиях из Перечня ВАК и в издании, включенном в базу Scopus.

Практическая значимость и достоверность работы подтверждается результатами проведенных вычислительных и натурных экспериментов с использованием разработанных программных средств и специализированного программного обеспечения, актами о внедрении в ООО «Уральский центр систем безопасности», ООО «Газпромнефть-Оренбург», в учебный процесс ФГБОУ ВО «Оренбургский государственный университет», АНО ДО «Просвещение» (г. Оренбург).

Автореферат диссертации соответствует требованиям Положения ВАК о порядке присуждения ученых степеней, однако при прочтении возникает несколько замечаний:

- в тексте автореферата не представлено обоснование выбора ассоциативно-мажоритарной модели для идентификации аномального состояния автоматизированных систем;

- в автореферате не раскрыты детали внедрения предложенных решений в подсистемы сетевой защиты, учета действий персонала и защиты доступности технологической информации.

Перечисленные замечания не снижают общей положительной оценки работы.

Учитывая вышеизложенное, считаю, что диссертационная работа Абрамовой Т.В. является завершенной научно-квалификационной работой и выполнена на высоком уровне. Представленные в работе результаты достоверны, выводы обоснованы.

Диссертация 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:
заведующий кафедрой
«Информационная безопасность»
ФГБОУ ВО «Ижевский государственный
технический университет
имени М.Т. Калашникова»,
д-р техн. наук, доцент _____ Вологдин Сергей Валентинович
«8» 08 2024

Даю согласие на обработку персональных данных. _____
подпись

Вологдин Сергей Валентинович
ФГБОУ ВО «Ижевский государственный технический университет имени М.Т. Калашникова»
Адрес: 426069, Удмуртская Республика, г. Ижевск, ул. Студенческая, д. 7
Тел.: 8 (3412) 77-60-55, доб. 7194
E-mail: vologdin_sv@mail.ru
Докторская диссертация защищена по специальности 05.13.01 «Системный анализ, управление и обработка информации».

Подпись д.т.н., доцента Вологдина С.В. заверяю: