

ОТЗЫВ

на автореферат диссертационной работы

Жаровой Ольги Юрьевны,

выполненной на тему:

«Моделирование параметров воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия»,
представленной на соискание ученой степени кандидата технических наук
по специальности

2.3.1 – Системный анализ, управление и обработка информации, статистика

В настоящее время автоматизированные системы управления технологическими процессами (АСУ ТП) являются частью информационных систем многих хозяйствующих субъектов. В общем случае технологическая сеть (ТС), включающая сегмент SCADA/HMI, сегмент PLC и сегмент RTU, является частью корпоративной сети (КС). ТС взаимодействует с КС посредством сервера шлюза (демилитаризованная зона, DMZ), блокирующего передачу управляющих команд в направлении «устройства в КС – устройства в ТС», таким образом управление технологическими процессами организуется исключительно в технологической сети.

Так как технологическая сеть входит в состав корпоративной сети, существует вероятность проникновения в ТС посредством вектора атаки: 1. Получение/повышение привилегий в КС; 2. Закрепление в КС; 3. Получение доступа к ТС.

В 2021 г. специалисты по информационной безопасности в ходе тестирования защищенности провели успешные атаки и получили доступ к технологическим сетям 75% отечественных промышленных компаний даже при наличии демилитаризованной зоны за счет уязвимостей операционных систем и программного обеспечения, недостаточной фильтрации трафика в DMZ, создания собственного канала в обход DMZ. При этом успешные атаки на ТС и получение несанкционированного доступа к компонентам АСУ ТП опасны как с точки зрения финансовых потерь, так и с точки зрения возникновения аварийных ситуаций на производстве вплоть до человеческих жертв и техногенных катастроф.

Исходя из вышесказанного, автор отзыва считает, что разработка методов повышения надежности функционирования управляющих узлов технологических сетей промышленного предприятия в условиях угрозы воздействий деструктивных потоков данных является актуальной научно-практической задачей.

Автором диссертационной работы обоснован выбор исходного множества критериев оценки деструктивных потоков данных. На основе анализа взаимосвязей и закономерностей изменения статистических параметров потоков данных предложена методика определения вида воздействия (на уязвимость, интенсификация). Сформирована иерархическая модель, предназначенная для прогнозирования исхода воздействия деструктивных потоков данных на управляющие узлы технологической сети промышленного предприятия. Система правил, составленная автором диссертационной работы при построении иерархической модели, позволила разработать направленный граф воздействия деструктивных потоков данных и алгоритм прогнозирования последствий воздействий на узлы. Предложена универсальная методика определения ущерба и предотвращения последствий воздействий деструктивных потоков данных на управляющие. Методика апробирована для системы вентиляции промышленного предприятия. Предложена принципиальная структура модуля защиты, принцип работы которого заключается в мониторинге статистических параметров потоков данных, выбранных для конкретной технологической сети.

Исходя из вышесказанного, новизна научных исследований, научные положения, практическая значимость диссертационной работы, обозначенные в представленном на отзыв автореферате, не вызывают сомнений. Предложенные автором диссертационной работы решения укладываются в проводимую в Российской Федерации политику разработки и импортозамещения отечественного ПО.

Автореферат оформлен в соответствии с требованиями ВАК, последовательность изложения представленного материала и его научная стилистика позволяют сформировать представление о сути диссертационной работы. Апробация осуществлялась на международной научной конференции, материалы изложены, в том числе, в рецензируемых научных журналах, что в совокупности позволяет говорить о проведении экспертизы работы научным сообществом.

Замечания.

1. Исходя из Рисунка 1 автореферата, имитационная модель строится для ОС Windows, использующей сетевую модель TCP/IP. При этом по тексту автореферата и на Рисунке 6 автором приводится модель OSI.
2. На Рисунке 1 в качестве источника деструктивных потоков данных и цели воздействия обозначены, в том числе, концентраторы (устройства уровня L1 модели OSI). При этом автором работы на Рисунке 7 указывается, что уровень L1 не рассматривается.

3. Автор указывает, что воздействия, направленные на истощение вычислительных ресурсов, имеют своей целью максимально нагрузить процессор узла; не рассматривает при этом, такие атаки на истощение ресурсов как недопустимое распределение оперативной памяти, ее «утечки», истощение; deadlock процессов или их перевод в состояние race condition.

Заключение.

Приведенные замечания не ставят под сомнение достоверность и научную ценность результатов диссертационного исследования. Автор отзыва считает, что диссертация представляет собой законченную научно-квалификационную работу, в которой, на основании проведенных теоретических и экспериментальных исследований, приведено решение актуальной научной и практической задачи повышения эффективности и надежности функционирования управляющих узлов различных уровней технологических сетей промышленного предприятия в условиях угрозы воздействия деструктивных потоков данных. По объему выполненных исследований, научной новизне, достоверности и практической значимости полученных результатов и выводов диссертационная работа «Моделирование параметров воздействия деструктивных потоков данных на технологическую сеть промышленного предприятия» полностью соответствует требованиям «Положения о порядке присуждения ученых степеней» в НИТУ МИСИС, а ее автор Жарова О.Ю. заслуживает присуждение ученой степени кандидата технических наук по специальности 2.3.1 – Системный анализ, управление и обработка информации, статистика.

Доцент кафедры Информатики
и информационных технологий, к.т.н.

В.А. Раевский
07.12.2023

«Подпись Раевского В.А. заверяю»
Руководитель подразделения «Управление кадрами»
ФГБОУ ВО «Калужский государственный
университет им. К.Э. Циолковского»



И.В. Леонтьева
07.12.2023

Адрес: 48023, Калужская область, г. Калуга, ул. Степана Разина, д. 22/48
Телефон: +7 900 574 84 00
E-mail: raevskyva@tksu.ru