МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное учреждение науки
«Санкт-Петербургский Федеральный исследовательский центр
Российской академии наук» (СПб ФИЦ РАН)

14-я линия В.О., д. 39, г. Санкт-Петербург, 199178
Тел.:+7 (812) 328-33-11, факс: +7 (812) 328-44-50
e-mail: info@spcras.ru, web: http://www.spcras.ru
ОКПО 04683303, ОГРН 1027800514411, ИНН/КПП 7801003920/780101001

«УТВЕРЖДАЮ»
Директор СПб ФИЦ РАН
доктор технических наук
профессор РАН
Ронжин А.Л.
«20» 08 2024 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию 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

Актуальность темы исследования

Задача обеспечения информационной безопасности является одной из приоритетных для газовой и нефтяной промышленности в связи с большим значением отрасли для глобальной и национальной экономики. Цифровая трансформация приводит к росту числа угроз, кибератак и инцидентов информационной безопасности (ИБ) на предприятиях нефтегазовой отрасли, о чем свидетельствует статистика последних лет. В результате этого предприятия могут столкнуться с остановкой производства, повреждением оборудования, перебоями в работе подсистем автоматизированных систем управления технологическим процессом (АСУ ТП).

Существенно выросли требования регуляторов по обеспечению ИБ

АСУ ТП нефтегазовой отрасли как объектов критической информационной инфраструктуры (КИИ). В связи с этим возникает необходимость совершенствования существующих систем защиты информации (СЗИ) в АСУ и разработки новых высокопроизводительных и достоверных средств защиты, с учетом современных требований.

Таким образом, тема диссертационной работы, посвященная вопросам разработки методов, моделей, алгоритмов и средств обнаружения аномалий и нейтрализации угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков, является актуальной.

Оценка структуры и содержания работы

Диссертационная работа состоит из введения, четырех глав, заключения, списка использованных источников и приложений. Работа изложена на 235 страницах, в том числе: основной текст на 195 страницах, 32 таблицы, 73 рисунка, список использованных источников из 205 наименований, 8 приложений на 40 страницах.

Первая глава посвящена анализу современного состояния исследований в области обнаружения аномалий и нейтрализации угроз безопасности информации (БИ) на объектах КИИ с распределенной архитектурой на примере КС АСУ ТП транспортировки нефтегазового сырья.

Во второй главе представлены результаты разработки метода матричной кластеризации угроз и моделей угроз распределенной АС на основе ортогональных средних значений рисков по угрозам и МУ для сопоставления актуальных угроз, приоритетности их нейтрализации и определения характера изменения актуальности угроз на последовательности подсистем распределенной АСУ ТП; метода построения математических и имитационных моделей для обнаружения аномалий, распознавания состояний КС АСУ на основе дихотомического принципа и разделяющей функции мажоритарного вида с бинарными амплитудными оценками информативных гармоник спектров временных рядов сетевого трафика; модельного базиса задачи обнаружения аномалий и нейтрализации угроз БИ на основе данных

сетевого трафика.

В третьей главе представлены результаты разработки алгоритмов, методик и программной реализации методов и средств обнаружения аномалий и нейтрализации угроз по данным сетевого трафика на основе принципов построения ассоциативных процессоров в подсистемах сетевой защиты, учета действий персонала и защиты доступности технологической информации.

Четвертая глава посвящена экспериментальной оценке эффективности результатов исследований и разработке рекомендаций их практического применения в распределенных АС на примере АСУ ТП транспортировки нефтегазового сырья.

В заключении приведены основные результаты и выводы по работе.

Область исследования диссертации соответствует пунктам паспорта научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»:

п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»;

п. 5 «Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»;

п. 6 «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях»;

п. 15 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Оформление диссертации в целом соответствует ГОСТ Р 7.0.11–2011. Автореферат диссертации выполнен с соблюдением установленных требований, полностью отражает ее содержание, полученные в ней практические и теоретические результаты и выводы.

Новизна полученных результатов

1. Разработан метод матричной кластеризации угроз и моделей угроз (МУ) на основе статистической обработки значений рисков, отличающийся тем, что в качестве исходных данных для кластеризации используются ортогональные средние значения рисков по угрозам и МУ, формализующий описание угроз и МУ в виде вектора бинарных классификационных кодов, что позволяет оценивать степени актуальности угроз, приоритетности их нейтрализации и определять характер изменения угрозы на последовательности подсистем распределенной АСУ ТП, а также применять принципы типового проектирования при построении СЗИ для АСУ с распределенной топологией.

2. Разработан 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, аргументами которой являются бинаризированные амплитудные оценки информативных гармоник спектров временных рядов сетевого трафика, позволяющий повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз в КС АС.

3. Разработаны 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, в которых адресная часть запоминающих блоков соответствует контролируемым признакам аномалий, информационная часть – характеристикам исследуемых образов, а структура и архитектура арифметико-логических блоков определяется назначением этих средств, в частности, для принятия решения по мажоритарному принципу, что позволяет

повысить производительность, достоверность, универсальность средств и снизить риски от угроз БИ. Новизна ассоциативного устройства мониторинга действий персонала АС подтверждена патентом на изобретение.

Степень достоверности результатов исследования

Достоверность научных положений, результатов и выводов подтверждается корректной постановкой задач и выбором методов исследования, обсуждением полученных результатов на научных конференциях, их апробацией в процессе проведения экспериментов с использованием разработанных программных средств, практическим применением разработанных методов, моделей, алгоритмов и методик обнаружения аномалий и нейтрализации угроз БИ при решении ряда прикладных задач.

Публикации. 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.

Теоретическая и практическая значимость результатов, полученных автором диссертации

Теоретическая значимость предложенных результатов заключается в том, что они расширяют методологию построения СЗИ КС распределенных АСУ с использованием усовершенствованных моделей и алгоритмов кластерного описания угроз и развития методов защиты информации на основе дихотомического и ассоциативно-мажоритарного подходов с применением интеллектуальной обработки данных сетевого трафика.

Практическая значимость и реализация результатов работы заключается в разработке научно обоснованных методов и средств, позволяющих снизить риски от угроз БИ в распределенных АС. Результаты диссертационной работы прошли апробацию в ряде организаций, в частности, ООО «Уральский центр систем безопасности», ООО «Газпромнефть-Оренбург», используется в

учебном процессе ФГБОУ ВО «Оренбургский государственный университет», АНО ДО «Просвещение» (г. Оренбург), что подтверждается соответствующими актами о внедрении.

Рекомендации по использованию результатов и выводов диссертации

Результаты диссертационной работы рекомендуются к использованию в подразделениях ИБ, аналитической и проектной деятельности на предприятиях и в организациях, занимающихся нефте-газодобычей, транспортировкой и обработкой нефтегазового сырья, а так же вопросами обеспечения ИБ АСУ ТП нефтегазовой отрасли.

Замечания по диссертационной работе

1. Для четвертого положения, выносимого на защиту, касающегося результатов оценки эффективности предложенных решений, во введении отсутствует описание научной новизны.

2. Список литературы содержит достаточно небольшое количество публикаций на иностранных языках. Учитывая, что представленная в диссертации проблема также активно исследуется на международном уровне, целесообразно было бы рассмотреть больше зарубежных источников, чтобы обеспечить более широкий обзор и учесть достижения мировой науки в данной области.

3. На странице 131 представлен численный эксперимент для оценки возможного ущерба от вирусной атаки. При этом, для оценки ущерба используется стоимость установленного на АРМ ПО (таблица 4.2) При этом, необходимо отметить, что заражение АРМ вирусом-шифровальщиком не уничтожает лицензии на ПО, а лишь временно делает его недоступным. ПО можно переустановить с использованием тех же лицензий без покупки новых. Более значимым является ущерб от нарушения бизнес-процессов, который далеко не всегда зависит от стоимости конкретного ПО.

4. В Приложении Г в разделе «Оценка экономического эффекта от применения разработанных методов» сравнение Kaspersky Industrial CyberSecurity for Networks с разработанным подходом выглядит

некорректным. Сравнивать стоимость коммерческой лицензии и собственную разработку недостаточно обоснованно, поскольку не учитывается различие в функциональности и масштабируемости решений. Продукт от Kaspersky, вероятно, обладает более широкой функциональностью и зрелостью, что требует учитывать не только стоимость, но и качество защиты, поддержку, обновления и другие аспекты, которые влияют на реальную экономическую эффективность.

5. Оформление отдельных элементов диссертационной работы не соответствует ГОСТ Р 7.0.11–2011, а оформление библиографических записей не полностью соответствует ГОСТ 7.1 и ГОСТ 7.80.

Заключение

Приведенные выше замечания в целом не снижают общей положительной оценки работы и не ставят под сомнение основные научные и практические результаты диссертационной работы.

Диссертация Абрамовой Таисии Вячеславовны на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований разработаны методы, модели, алгоритмы и методики обнаружения аномалий и нейтрализации угроз на основе мониторинга сетевых информационных потоков, применение которых позволяет снизить риски информационной безопасности в компьютерных сетях распределенных АСУ ТП.

Диссертация соответствует требованиям п. 9 Положения ВАК о порядке присуждения ученых степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24.09.2013 г. (с последующими изменениями), а её автор – Абрамова Таисия Вячеславовна - заслуживает присуждения ей ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Диссертационная работа Абрамовой Т.В. и отзыв обсуждены на заседании лаборатории проблем компьютерной безопасности Федерального

государственного бюджетного учреждения науки "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук". Протокол заседания № 8 от 14 августа 2024 года.

Главный научный сотрудник, заведующий лаборатории Проблем компьютерной безопасности
д.т.н, профессор,
заслуженный деятель науки РФ Котенко Игорь Витальевич

ведущий научный сотрудник лаборатории Проблем компьютерной безопасности
к.т.н. доцент Чечулин Андрей Алексеевич

Наши реквизиты: Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН); юр.адрес: 14-я линия В.О., д. 39, г. Санкт-Петербург, 199178; тел.: +7 (812) 328 33 11, факс: +7 (812) 328 44 50, электронная почта: info@spcras.ru.

«Я, Ронжин Андрей Леонидович, директор СПб ФИЦ РАН даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку»
доктор технических наук, профессор РАН Ронжин Андрей Леонидович

«Я, Котенко Игорь Витальевич, главный научный сотрудник лаборатории «Проблем компьютерной безопасности» СПб ФИЦ РАН даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку»
доктор технических наук, профессор Котенко Игорь Витальевич

«Я, Чечулин Андрей Алексеевич, ведущий научный сотрудник лаборатории «Проблем компьютерной безопасности» СПб ФИЦ РАН даю согласие на включение своих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку»
кандидат технических наук, доцент Чечулин Андрей Алексеевич

Подписи рук Ронжина А.Л., Котенко И.В. и Чечулина А.А. заверяю

Начальник отдела кадров
Д.В.Токарев
«__» _____ 20__ г.