ОТЗЫВ

официального оппонента

кандидата технических наук, доцента Соколова Александра Николаевича

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

Статистика последних лет свидетельствует о росте числа инцидентов информационной безопасности (ИБ) в промышленных автоматизированных системах. Качество функционирования промышленных автоматизированных систем управления технологическими процессами (АСУ ТП) в условиях роста числа атак определяется эффективностью систем защиты информации (СЗИ). Это обуславливает необходимость совершенствования существующих средств защиты в АСУ, обеспечивающих своевременное обнаружение аномалий и нейтрализацию угроз безопасности информации (БИ). Немаловажной является проблема разработки методов и средств ЗИ в компьютерных сетях (КС) АСУ ТП транспортировки нефтегазового сырья, которые относятся к объектам критической информационной инфраструктуры (КИИ) и часто становятся целью кибератак. Важность темы исследования отражена в Приказах № 31, № 235 и № 239 ФСТЭК России, в которых отмечается необходимость применения методов и средств оперативного обнаружения аномалий и достоверной идентификации угроз БИ на объектах КИИ.

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

Оценка структуры и содержания работы

Диссертация 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.

Во введении изложена краткая характеристика диссертации, обоснована актуальность темы, определены объект и предмет исследования, сформулированы цель и задачи работы, представлены положения, выносимые на защиту.

Первая глава посвящена анализу современного состояния исследований в области обнаружения аномалий и нейтрализации угроз БИ на объектах КИИ с распределенной архитектурой на примере КС АСУ ТП транспортировки нефтегазового сырья. Представлена концепция снижения риска ИБ за счет высокопроизводительных методов и средств оперативного и достоверного обнаружения, распознавания аномальных состояний АСУ, как проявлений инцидентов ИБ, нейтрализации связанных с ними угроз на основе исследования и интеллектуальной обработки данных сетевого трафика.

Во второй главе представлены результаты разработки метода матричной кластеризации угроз и моделей угроз на основе статистической обработки значений рисков, позволяющего определять характер изменения угрозы на последовательности подсистем распределенной АСУ ТП, оценивать степень актуальности угроз и приоритетности их нейтрализации, в частности, необходимость совершенствования средств защиты в задачах определения источников и восстановления маршрутов распространения вредоносного кода, определения резервных маршрутов передачи данных для нейтрализации блокировки доступа к источникам информации, мониторинга действий персонала в распределенных АС. Предложен метод построения математических и имитационных моделей и разработаны модели для обнаружения аномалий и распознавания состояния КС АСУ на основе данных

мониторинга сетевого трафика, позволяющие повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз.

В третьей главе представлены результаты разработки алгоритмов, методик и программной реализации методов и средств: восстановления маршрутов распространения вредоносного кода по данным сетевого трафика, позволяющих оперативно выявлять маршруты и источники распространения вредоносной информации в КС и принимать превентивные меры по нейтрализации угрозы дальнейшего распространения; определения резервного маршрута с обходом аномальных участков промышленных КС, позволяющих снизить риски от угроз потери информации о состоянии объекта защиты при ее передаче по каналам связи распределенной АСУ и повысить оперативность реагирования на возникновение аварийной ситуации; мониторинга действий персонала в АС на основе логического контроля ассоциативности сигнатур управляющих транзакций, позволяющих снизить риски от угроз нерегламентированных управляющих воздействий на систему.

Четвертая глава посвящена экспериментальной оценке эффективности результатов исследований, показавшей снижение рисков от угроз БИ в распределенных АС при использовании разработанных методов и средств, в частности: от угрозы распространения вредоносного кода в КС; от угрозы несанкционированных действий персонала АСУ; от угрозы потери информации о состоянии объекта защиты. Даны рекомендации по практическому применению результатов диссертационной работы в СЗИ на предприятиях нефтегазовой отрасли.

В заключении приведены основные результаты и выводы по работе.

Структура и содержание диссертации соответствуют поставленным задачам и цели исследования.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Обоснованность научных положений и выводов, сформулированных в диссертации, не вызывает сомнения. Это подтверждается корректной

постановкой цели и задач, выбором методов исследования, анализом широкого круга научной, научно-технической и патентной литературы, публикациями по материалам диссертационной работы. Диссертация имеет четкую и логическую структуру, содержит достаточное число рисунков и таблиц, поясняющих основные результаты работы. Содержание автореферата соответствует основным положениям диссертации.

Полученные результаты соответствуют заявленным автором пунктам паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Достоверность и новизна полученных результатов подтверждается обсуждением основных положений и результатов диссертационной работы на научных конференциях, публикацией в ведущих рецензируемых научных изданиях, апробацией в процессе проведения экспериментов с использованием разработанных программных средств, программного комплекса SCADA TRACE MODE и эмуляторов промышленного сетевого протокола ModBus TCP, а также апробацией разработанных решений в профильных организациях, подтвержденной актами о внедрении.

По результатам диссертационного 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.

Научная новизна работы заключается в следующем:

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.

Теоретическая и практическая значимость полученных автором результатов

Предложенные результаты 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 работы заключается в разработке научно обоснованных методов и средств, позволяющих снизить риски от угроз БИ в распределенных АС. Полученные результаты внедрены и используются в ряде организаций, о чем свидетельствуют соответствующие акты о внедрении.

Замечания по диссертационной работе

1. В главе 1 диссертации автор рассматривает целевую функцию задачи защиты информации, в определении которой фигурируют элементы p_{ij} и U_{ij}, после чего говорит о минимизации параметров p и U, явно их не определяя. Видимо, речь идет о матрицах P и U, составленных из этих элементов. Из текста не ясно, что понимается под минимизацией матрицы, может быть, минимизация ее элементов?

2. В главе 2 диссертации говорится, что вычисление вероятности $P(x)$ производится с помощью функции Гаусса. На основании чего можно считать, что в этом случае имеет место нормальное распределение?

3. Экспериментальная оценка эффективности результатов исследований проводилась на примере характеристик АСУ ТП транспортировки нефтегазового сырья. Вместе с тем, в работе не уделено достаточно внимания вопросам эффективности предложенных решений в составе СЗИ других промышленных объектов.

4. В диссертации недостаточно подробно раскрыт вопрос выбора и обоснования инструментария и средств разработки программных решений.

5. В главе 4 представлено большое количество иллюстративного материала, часть которого можно перенести в приложение без потери информативности и понимания результатов исследования.

Вместе с тем, отмеченные недостатки не носят принципиального характера и не снижают общей положительной оценки работы.

Заключение

Диссертация Абрамовой Т.В., представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, посвященной решению актуальной задачи разработки методов и средствобнаружения аномалий и нейтрализации угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков. Результаты диссертационной работы обладают научной новизной и практической значимостью.

Считаю, что диссертация 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.

Официальный оппонент:
кандидат технических наук, доцент,
заведующий кафедрой защиты информации,
Федеральное государственное автономное
образовательное учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Соколов Александр Николаевич

21.08.2024

Кандидатская диссертация защищена
по специальности 05.12.21 – Радиотехнические системы специального назначения, включая технику СВЧ и технологию их производства.

Даю согласие на обработку персональных данных.

Адрес основного места работы: 454080, г. Челябинск, просп. Ленина, д.87, ауд. 624А/3А
Рабочий телефон: +7(351)2679355
Адрес эл. почты: sokolovan@susu.ru

ВЕРНО
Ведущий документовед
О.В. Брюхова