ОТЗЫВ

официального оппонента

доктора технических наук, профессора Фрида Аркадия Исааковича

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

В настоящее время качество функционирования промышленных автоматизированных систем управления технологическим процессом (АСУ ТП) в условиях роста числа инцидентов информационной безопасности (ИБ) в значительной степени определяется эффективностью систем защиты информации (СЗИ). Разработка методов и средств обнаружения аномалий, как проявлений инцидентов ИБ, позволяющих оперативно выявлять и реагировать на угрозы безопасности информации (БИ), имеет большое значение для обеспечения непрерывности и безопасности технологических процессов.

Особую актуальность приобретает проблема разработки методов и средств защиты информации в компьютерных сетях (КС) АСУ ТП транспортировки нефтегазового сырья, являющихся одним из лидеров по числу инцидентов ИБ и относящихся к объектам критической информационной инфраструктуры (КИИ). Значимость тематики исследований отражена в ряде нормативных документов, в частности: Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ, ГОСТ Р серии 62443, Приказы ФСТЭК России №№ 31, 235, 239. Рост числа инцидентов ИБ и появление новых требований регуляторов к СЗИ обуславливают необходимость совершенствования

ВХОД. № 5711-2
«28» 08 2024г.

существующих средств защиты информации в промышленных АСУ ТП.

Важнейшим фактором, во многом определяющим сложность решения задачи обеспечения ИБ в реальных условиях эксплуатации КС АСУ ТП, является их распределенность в пространстве и нестационарность информационных потоков. Таким образом, тема диссертационной работы, посвященная вопросам разработки методов 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

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, отмечены научная новизна и практическая значимость 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. Определена целевая функция и выбраны критерии оценки результатов исследования. Проведен анализ структурно-функциональной организации распределенной АСУ ТП как объекта защиты, дана характеристика сетевого трафика системы как источника сведений об аномалиях. Проведен анализ современных решений задачи обнаружения аномалий и нейтрализации угроз БИ в распределенных АСУ ТП. Показаны возможности повышения оперативности и достоверности методов и средств обнаружения, распознавания аномальных состояний АСУ на основе исследования и интеллектуальной обработки сетевых информационных потоков. Разработана концепция исследования.

Во второй главе представлены результаты разработки метода построения математических и имитационных моделей и модельного базиса задачи обнаружения аномалий и нейтрализации угроз БИ на основе данных мониторинга сетевого трафика.

Дана характеристика базовой модели угроз для распределенной АСУ процессом транспортировки нефтегазового сырья предложен метод матричной кластеризации угроз и моделей угроз на основе статистической обработки значений рисков, позволяющий определять характер изменения угрозы на последовательности подсистем распределенной 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, позволяющие повысить производительность и достоверность средств обнаружения аномалий и нейтрализации угроз. Представлены обобщенный алгоритм и структурно-функциональная модель ассоциативного процессора обнаружения аномалий и нейтрализации угроз по данным сетевого трафика

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.

В четвертой главе проведен анализ результатов экспериментальной оценки эффективности от использования разработанных методов, показавший

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. Проведена апробация разработанных программных средств в условиях лабораторного эксперимента. Даны рекомендации по практическому применению результатов диссертационной работы в СЗИ на предприятиях нефтегазовой отрасли.

В заключении приведены основные результаты и выводы по работе.

Приложения содержат акты о внедрении результатов работы, результаты вычислительных и натурных экспериментов, многоаспектного анализа предложенных в работе решений, фрагменты листингов программных средств, справку о получении грантов.

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

Обоснованность научных положений и выводов, сформулированных в диссертации, подтверждается опубликованными по материалам исследования работами, включая 4 статьи в научных изданиях из Перечня рецензируемых научных изданий, рекомендованных ВАК, 1 научную работу в издании, включенном в базу Scopus, 26 статей в других изданиях, 1 коллективную монографию, 1 учебно-методическое пособие, 1 патент и 9 свидетельств о регистрации программ.

Диссертация содержит достаточное для понимания результатов проведенных исследований количество иллюстративного материала. Автореферат полно раскрывает основное содержание диссертации.

Полученные результаты соответствуют паспорту научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Достоверность и новизна полученных результатов подтверждена корректной постановкой задач и выбором методов исследования, обсуждением на научных конференциях, апробацией в процессе проведения экспериментов с использованием разработанных программных средств, публикацией результатов в ведущих рецензируемых научных изданиях.

Научная новизна работы

К новым научным результатам, полученным в диссертационном исследовании, следует отнести:

1. 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. 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. 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

В работе теоретически обоснована концепция исследований, разработан модельный базис задачи обнаружения аномалий и нейтрализации угроз БИ, доказана необходимость совершенствования существующих СЗИ и разработки новых высокопроизводительных и достоверных средств защиты, позволяющих снизить риски ИБ в компьютерных сетях распределенных АСУ.

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 и реализация результатов работы заключается в разработке научно обоснованных методов и средств, позволяющих снизить риски от угроз БИ в распределенных АС, в частности: от угрозы распространения вредоносного кода в КС; от угрозы несанкционированных действий персонала АСУ; от потери информации о состоянии объекта защиты.

Разработанное программное обеспечение передано для внедрения и используется в ряде организаций, что подтверждается актами о внедрении.

К достоинствам диссертационной работы следует отнести:

1. Системность и глубину подхода к решению фундаментальной проблемы исследования – построение целого ряда моделей, позволяющих планомерно решать задачи для достижения поставленной цели

2. Убедительное подтверждение изложенных в работе положений в 8-и приложениях.

Замечания по диссертационной работе

1. В главе 1, на мой взгляд, к перечисленным основным видам рисков следовало бы добавить риски от разрушения инфраструктуры, т.к.

исследуемые системы относятся к системам критической информационной инфраструктуры (КИИ).

2. Не ясно, как учитывается при оценке рисков взаимодействие участков сети, так как наверняка существует влияние изменения состояния одних участков сети на состояние других.

3. Не ясно, как учитывается при оценке рисков возможность одновременного негативного воздействия на нескольких участках сети.

4. На рис. 2.4 приведен пример классификационного кода угрозы 1011100. Не ясно, как получилось это выражение, поскольку не указаны исходные данные для его построения.

5. На стр. 69 предлагается проводить бинаризацию значений аргументов X_i по правилам (2.8, 2.9). Хотя математически эти неравенства не оставляют места для сомнений в принятии решений, при учете неточностей измерений и помех может возникнуть зона неопределенности, приводящая к ошибкам первого и второго рода. Как учитывать это обстоятельство?

6. На стр. 80 говорится, что дихотомический подход позволяет повысить оперативность и достоверность определения аномалии. По сути, дихотомический подход – это округление, и вряд ли эта операция может повысить достоверность.

7. Разработанный метод кластеризации угроз и моделей угроз БИ для подсистем распределенных объектов КИИ ориентирован на АСУ ТП транспортировки нефтегазового сырья. В тексте диссертации недостаточно четко показана возможность распространения полученных результатов на распределенные технические системы иной природы.

8. Замечания по представлению работы. Нет списка условных обозначений, часто одни и те же понятия сопровождаются уже введенными ранее аббревиатурами, есть повторы.

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, обладает научной новизной, теоретической и практической значимостью, является законченной научно-квалификационной работой, в которой решена актуальная задача разработки методов и средств обнаружения аномалий и нейтрализации угроз в распределенных автоматизированных системах управления на основе мониторинга сетевых информационных потоков.

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:
доктор технических наук, профессор,
заместитель директора по научной работе,
закрытого акционерного общества
«Республиканский центр защиты информации»

Фрид Аркадий Исаакович

28.08.2024

Докторская диссертация защищена
по специальности 05.13.01 – Системный анализ, управление и обработка информации.

Даю согласие на обработку персональных данных.

Адрес основного места работы: 450077, г. Уфа, ул. К. Маркса, 12, корп.5, каб.5-408
Рабочий телефон: +79173416834
Адрес эл. почты: frid46@mail.ru

Подпись проф. Фрида А.И. заверяю:
зам. директора ЗАО «РЦЗИ» Т.З. Хисамутдинов