Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

ОПТИМИЗАЦИЯ МЕТОДОВ КОНТРОЛЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Монография

Рекомендовано к изданию ученым советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет»

Оренбург
2019

УДК 004.73
ББК 32.971.35
О 62

Рецензенты:
профессор, доктор технических наук А. М. Пищухин
профессор, доктор технических наук А. И. Сердюк

Авторы: Т. З. Аралбаев, Г. Г. Аралбаева, Т. В. Абрамова, Р. Р. Галимов, А. В. Манжосов

О 62 Оптимизация методов контроля технического состояния распределенных автоматизированных систем: монография / Т. З. Аралбаев, Г. Г. Аралбаева, Т. В. Абрамова, Р. Р. Галимов, А. В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2019.
ISBN

В монографии представлены результаты научных исследований и обоснованные разработки методов повышения эффективности контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков. Выводы и рекомендации основываются на реальных результатах и могут быть внедрены в практике деятельности предприятий промышленного комплекса и в процессе реализации образовательных программ высшего образования по направлениям подготовки 10.03.01 Информационная безопасность и 09.04.01 Информатика и вычислительная техника.

УДК 004.7
ББК 22.1

ISBN

Содержание

Введение

Одним из основных факторов повышения эффективности производства является обеспечение работоспособности промышленного оборудования и оптимальных технологических режимов с использованием автоматизированных систем мониторинга и диагностирования (СМД) состояния объектов. Стремление получить максимальную прибыль за счет эффективного использования промышленного оборудования, продления ресурса его использования, обеспечение безопасных для человека и окружающей среды условий производства - обуславливает новые требования к системам контроля, оперативной оценки, прогнозирования и выбора оптимальной стратегии по предупреждению аварийных ситуаций и ликвидации их последствий.

Особую актуальность в настоящее время приобретает проблема разработки методологических принципов построения распределенных автоматизированных систем мониторинга и диагностирования протяженных промышленных объектов (ППО). Это обусловлено сложностью организации СМД, предназначенных для решения задач непрерывного контроля, диагностирования, прогнозирования и принятия решений по устранению нерегламентированных состояний.

Вопросам построения систем мониторинга посвящен обширный перечень работ отечественных и зарубежных ученых, представляющих организации и производственные предприятия различного профиля. К этому перечню относятся работы Мозгалевского А.В., Пархоменко П.П., Согомоняна Е.С., Биргера И.А., Фомина Я.А., Глазунова Л.П., Павлова Б.В. - заложивших основы теории технической диагностики. Следует особо отметить работы Глушкова В.М, Ивахненко А.Г., Бусленко В.Н., Клира Д., Ту Д., Гонсалес Р., Горелика А.Л., в которых большое внимание уделено теоретическим принципам построения автоматизированных систем. Вопросам практической разработки, внедрения и эксплуатации средств контроля и диагностики в составе АСУ ТП нефтедобычи посвящены работы Абдуллаева А.А., А.В., Кузякина В.И., Алиева Т.М., Султанова Б.З., Храмова Р.А., Шаммазова А.М. и целого ряда других ученых.

Анализ известных работ показал, что в теории управления и мониторинга промышленных объектов известны методологии построения систем распознавания, прогнозирования, принятия решений, однако они не полностью учитывают специфику построения распределенных систем мониторинга технического состояния распределенных АСУ, работающих в условиях пространственных и временных возмущений, обусловленных антропологическими, климатическими и техногенными угрозами.

Цель работы – повышение оперативности и достоверности методов контроля технического состояния распределенных управляющих систем в условиях воздействия пространственно-временных угроз на основе мониторинга информационных потоков. **Объект исследования** – АСУ протяженными промышленными объектами. **Предмет исследования** – методы и средства мониторинга технического состояния АСУ протяженными промышленными объектами.

Для достижения цели в работе поставлены следующие задачи:

1 Разработать пространственно-временную модель угроз для АСУ протяженным в пространстве объектом.

2 Построить структурно-функциональные, математические и имитационные модели, позволяющие исследовать объекты защиты, оптимизировать традиционные методы и средства идентификации технических состояний АСУ управления транспортным нефтепроводом в условиях воздействия пространственно-временных угроз.

3 Построить модель сетевого трафика как информационного пространства условно бесконечного объема.

4 Разработать метод оценки технического состояния распределенной АСУ на основе мониторинга сетевых потоков информации (на примере системы транспортировки нефтегазового сырья).

5 Разработать и исследовать метод контроля директивных установок в распределенной АСУ распределенным объектом.

6 Разработать метод повышения живучести телекоммуникационной подсистемы АСУ ТП в условиях распределенной пространственно-временной модели угроз.

7 Провести анализ технико-экономической эффективности результатов исследований.

8 Разработать рекомендации по внедрению методов и средств контроля технического состояния распределенных АСУ ТП транспортировки нефтегазового сырья на предприятиях Оренбургской области.

Методы исследования. Использованы методы теории вероятности, теории принятия решений, теории оптимизации систем автоматизированного управления, теории распознавания образов.

Научную новизну работы составляют:

− модель распознавания технического состояния протяженного промышленного объекта на основе ассоциативно-мажоритарного подхода;

− метод контроля поведения пользователя, позволяющий в режиме реального времени анализировать и предупреждать несанкционированные действия оператора в АСУ;

− метод ранжирования угроз на основе ассоциативного подхода, позволяющий определять степень актуальности угрозы в ряду угроз в момент регистрации ее характеристик.

Новизна аппаратно-программных разработок подтверждается полученным положительным решением на изобретение и свидетельствами о регистрации программных средств в университетском фонде программ.

Практическая значимость и реализация результатов работы.

Результаты разработки могут быть использованы в системе информационной безопасности в различных организациях и фирмах для мониторинга сетевого трафика, выявления сетевых аномалий и идентификации протекающих в сети событий. При использовании в сетевом администрировании подобный подход позволит повысить оперативность в принятии решений в задачах анализа ситуаций в трафике большого объема по доступной совокупности фрагментов сведений.

Разработанный метод и программное средство может использоваться для идентификации ситуаций и поиска аномалий в больших объемах сетевого трафика. При этом нет необходимости в проверки каждого хоста сети и просмотра всего потока сетевого трафика на предмет выявления нежелательного содержимого.

Полученные результаты рекомендованы для использования на предприятиях Оренбургской области, в частности Газопромысловое управление "Газпром добыча Оренбург", Оренбургский газоперерабатывающий завод, ООО "Газпром переработка", Предприятие «Газпром трансгаз Екатеринбург», Компания «Уральский центр систем безопасности» (УЦСБ), ООО "Газпромнефть-Оренбург".

Достоверность результатов исследований обеспечена апробированием их в процессе поведения экспериментальных исследований с использованием инструментальных средств системы SCADA/TraseMod и эмуляторов протоколов промышленного сетевого протокола TCP/ModBus.

Публикации. Основные положения работы отражены в трудах трех международных конференций, одной статье из перечня ВАК РФ, в полученных свидетельствах на программные средства и одном положительном решении на получение патента на изобретение.

Работа содержит 4 раздела, введение, заключение, список использованных источников из 120 наименований и приложения.

Перечень сокращений и обозначений

В монографии применены следующие сокращения и обозначения.

IP-адрес - уникальный сетевой адрес узла в компьютерной сети

АМП – ассоциативно-мажоритарный подход

АП – ассоциативная память

АСУ ТП – автоматизированная система управления технологическими процессами

БКЭС - блочно-комплектная электростанция

БПЛА – беспилотный летательный аппарат

ВОЛС – волоконно-оптическая линия связи

ИБ – информационная безопасность

ИМ – исполнительный механизм

ИС – информационная система

КСИИ - ключевая система информационной инфраструктуры

ЛЭП – линии электропередач

НСД – несанкционированный доступ

ОС – операционная система

ПВЭМ - персональная электронно-вычислительная машина

ПЛК – программируемый логический контроллер

ПО – программное обеспечение

ППО – протяженный промышленный объект

ПЭМИН - побочные электромагнитные излучения и наводки

СЗИ – средство защиты информации

СМД - система мониторинга и диагностирования

СТ – сетевой

ТС – техническое состояние

1 Задача контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз и определение требований к методам и средствам контроля

1.1 Актуальность задачи контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз

Рассматриваемые в работе распределенные системы мониторинга технического состояния (РСМ ТС) протяженных промышленных объектов относятся к категории ключевых систем информационной инфраструктуры (КСИИ). Системы данного класса, в соответствии с положениями ФСТЭК РФ, представляют собой информационно-управляющие или информационно-телекоммуникационные системы, которые осуществляют управление критически важными объектами (процессами), в результате деструктивных информационных воздействий на которые может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями [25].

Специфика КСИИ, как защищаемого объекта, определяется следующими характеристиками:

- протяженность промышленного объекта в пространстве, в частности, общая протяженность нефте- и газопроводов по Оренбургской области составляет более 6600 км, а по России в целом – более 250 тыс. км;
- распределенность в пространстве подсистем АСУ транспортировкой нефте-газопродуктов по трубопроводам;
- переменный во времени и в пространстве характер угроз на объекты информатизации АСУ, обусловленные различными географическими и

климатическими особенностями регионов, определяющий различные параметры подсистем по периодичности, сезонности и стохастичности их проявления.

Для рассматриваемого типа АСУ наиболее характерны различия в характеристиках угроз антропогенного, техногенного и природного типов, что определяет специфику задач построения модели угроз под каждую подсистему АСУ, топологически распределенную в заданном географическом регионе.

Существенная часть рисков при использовании информационных подсистем АСУ для организации возникает вследствие несанкционированных действий с информацией со стороны сотрудников. Данные действия являются, в первую очередь, следствием получения лицом, проводящим такие операции, несанкционированного доступа к информационным ресурсам и системам.

Основная часть убытков организации являются следствием вполне определенных действий персонала. Причиной этих действий могут быть ошибки персонала, умысел, халатность, либо безответственное отношении к своим обязанностям.

Так, согласно исследованию аналитической службы компании «Код безопасности», угроза НСД со стороны сотрудников (пользователей компьютерной системы) занимает первое место среди угроз информационной безопасности компьютерной системе. Статистика угроз представлена на рисунке 1 [10]. Согласно исследованиям, наиболее актуальными угрозами информационной безопасности для большинства российских компаний остаются внутренние факторы.

В частности, 25 % опрошенных считают, что наибольшую опасность для компании представляют несанкционированные действия сотрудников при обработке технологической информации (первое место).

Второе место занимает потеря/кража конфиденциальной информации (23 %). Третье место в рейтинге угроз (19 %) занимает такая внешняя угроза, связанные с распространением вредоносных программ. 14% опрошенных считают, что серьезные риски для компании несут атаки из сети Интернет. Пятое место поделили между собой шпионские программы и спам [10].

Рисунок 1 – Статистика актуальных угроз информационной безопасности компьютерной системы

Проведенный анализ теоретических и прикладных работ по проблеме обеспечения надежности функционирования АСУ протяженными объектами показал следующее:

- в настоящее время рассматриваемой проблеме уделяется большое внимание со стороны научно-исследовательских и производственных организаций в России и за рубежом, примером этому являются разработки таких организаций как: ООО «Уральский Центр Систем Безопасности», ЗАО «ОМЕГА», предприятие «ПетроЛайт» и целый ряд других;

- несмотря на повышенное внимание со стороны исследователей и разработчиков, а также специалистов по эксплуатации этих систем существуют резервы повышения эффективности используемых методов и средств на основе повышения производительности и достоверности методов идентификации состояния АСУ с применением доступных информационных ресурсов каналов передачи данных и повышением эффективности использования существующих средств передачи данных;

- анализ современных методов и средств обеспечения эффективной работы систем управления выявил аспекты совершенствования базовой

методологии построения систем управления, реализация которых позволяет повысить производительность, достоверность, надежность и полноту контроля технического состояния элементов систем, а также контроля изменения их технологического состояния;

- большинство существующих методов решения проблемы контроля технического состояния в автоматизированных системах управления узконаправлены, зачастую, посвящены вопросам поддержания конкретного технологического процесса и не учитывают ряд проблем, связанных с распределенностью автоматизированных систем, большим объемом циркулирующей в них информации, затрудняющих процессы ее передачи и анализа, воздействия различных антропогенных, климатических и техногенных факторов, создающих угрозы безопасности работы этих систем;

- меры обеспечения функциональной безопасности, реализованные для систем управления технологическими процессами, как правило, не рассчитаны на намеренное нарушение удаленным нарушителем или злоупотребление внутренним пользователем. Это может привести к пагубным последствиям для технологического процесса, оборудования или даже жизни и здоровья людей и безопасности окружающей среды;

- пространственная распределенность автоматизированных систем управления увеличивает вероятность воздействия различных как антропогенных, так и техногенных и климатических угроз.

Перечисленные выше факторы приводят к необходимости оптимизации методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз. Это обусловлено необходимостью достоверно идентифицировать возникновение нерегламентированных ситуаций, оперативно реагировать на инциденты в АСУ ТП и принимать решения по их нейтрализации.

Также немаловажно отметить, что автоматизированные системы управления технологическими процессами активно используются на множестве предприятий Оренбургской области как производственных, так и непроизводственных секторов

экономики. Зачастую, подобные системы состоят из множества территориально распределенных модулей. Такое распределение обусловлено ростом количества контролируемых параметров, увеличением территории, на которой должна функционировать АСУ ТП, а также усложнением алгоритмов управления.

По этой причине для Оренбуржья, как одного из ведущих регионов нефтегазовой промышленности в России, задача оптимизации методов контроля технического состояния распределенных АСУ ТП объектов нефте- и газодобычи является актуальной.

1.2 Аналитический обзор публикаций по теме работы

Цель проведенного обзора: на основе анализа актуальной информации по теме работы определить концепцию ее исследований.

Анализ современного состояния рассматриваемых задач по материалам современной научной, технической периодики, патентной литературы, конференций и других актуальных Интернет ресурсов позволил разбить перечень публикаций на группы, содержащие:

- сведения, определяющие современный уровень рассматриваемой проблемы;
- сведения, являющиеся аналогами проведенных исследований;
- сведения, позволяющие выявить инструментальный и методический аспекты исследований;
- сведения концептуального характера, определяющие стратегию, тактику и перспективы исследований;
- сведения, используемые при решении частных задач оптимизации методов и средств системы мониторинга.

К первой группе публикаций отнесены труды известных ученых и разработчиков систем мониторинга состояния нефтегазового оборудования и транспортных трубопроводов. В частности, к ним отнесены работы Абдуллаева А.А. [1], Васютинской С.И. и Ханс-Христина Штубера [31], Гаспарянца Г.С. [35],

Латышева Л.Н., Насырова З.Р. [54], Остиану В.М. [65], Вайнштока С.М., Новоселова В.В., Прохорова А.Д., Шаммазова А.М. [102].

Анализ этих работ позволил определить особенности построения рассматриваемых систем для различных объектов автоматизации, выявил динамику развития методов и средств мониторинга.

Ко второй группе публикаций отнесены публикации, характеризующие конкретные методы, средства и технические решения, направленные на повышение технико-экономических характеристик систем мониторинга.

К ним отнесены труды авторских коллективов, представленных в работах [11, 46, 48, 51], диссертационные исследования [55, 59] и ряд патентных материалов [68, 71, 74, 76]. Анализ этой группы публикаций позволил определить современное состояние и направленность научных и практических исследований по теме проекта. В частности, патентный анализ технических решений позволил определить и обосновать степень новизны полученных авторами решений при разработке аппаратно-программных средств распознавания образов.

К третьей группе отнесены публикации, позволившие определить методическую направленность исследований. К ним отнесены положения ГОСТов, касающиеся предмета исследования, в частности, материалы, представленные в работах [37, 38], руководящие материалы ФСТЭК РФ [25, 58, 62, 79, 81, 85, 96], а также целый ряд публикаций методического характера по теории надежности, спектрального анализа, массового обслуживания, анализа и прогнозирования временных рядов, организации систем защиты информации и анализа их эффективности [24, 26, 27, 34, 41, 43, 47, 50-52, 64, 77, 84, 93, 104-108].

К четвертой группе отнесены публикации, позволившие определить основную концепцию и перспективы исследований. В частности, в работах [9, 12, 14-17, 31, 109] на основе анализа перечня задач, решаемых в системах мониторинга сложных промышленных объектов, определена в качестве одной из основных, задача распознавания образов и вопросы, связанные с повышением эффективности методов и средств оперативной идентификации технических состояний АСУ управления этими объектами.

Вопросы повышения эффективности методов и средств распознавания образов входят в перечень актуальных в теории и практике управления, поскольку от качества оценки состояния объектов зависит общая эффективность работы управляющих систем. Неслучайно эта область находится в зоне особого внимания ученых, представляющих различные аспекты этой проблемы. В работе использованы научные и практических положения, представленные в трудах: А.Г. Ивахненко - по самоорганизации распознающих систем; Симанкова В.С. и Луценко Е.В. - по применению распознающих средств в системах управления; У. Пирса - по вопросам обеспечения надежности компьютерных систем; в технических решениях отечественных и зарубежных разработчиков.

Одной из задач настоящих исследований является систематизация принципов повышения эффективности методов распознавания образов на основе ассоциативно-мажоритарного подхода (АМП).

По мнению авторов, этот аспект недостаточно представлен в современной литературе по теории и практике распознавания образов, что не позволяет в должной мере использовать высокий технически-экономический потенциал этого подхода в современных системах распознавания образов.

Актуальность выбранного направления оптимизации средств распознавания образов определена, как это показано ниже, широкими возможностями совершенствования средств распознавания образов на базе АМП.

К пятой группе из рассмотренных публикаций отнесены работы, используемые при решении частных задач оптимизации методов и средств системы мониторинга. В частности, публикации, посвященные вопросам имитационного моделирования сетевого трафика как источника информации с использованием протоколов, используемых в системах связи АСУ ТП; публикации, связанные с контролем поведения пользователя в сетевых структурах. Актуальность данных исследований определена спецификой управления различных промышленных объектов и, соответственно, особенностями исследования их состояний. К перечню этих публикаций относятся, как работы коллег по данной области исследований,

например: [29,30,36,40,42,44,45, 57, 60, 63], так и авторские разработки, в частности [1-8, 17-22, 32-33, 56, 67,69, 72,73, 75, 90,91].

Результаты аналитического обзора представленных работ определили цель, основные задачи исследований.

1.3 Пространственно-временная модель угроз для распределенных автоматизированных систем мониторинга технического состояния протяженных в пространстве объектов

Под угрозой безопасности информации в КСИИ понимается совокупность условий и факторов, создающих потенциальную или реальную существующую опасность несанкционированных и (или) непреднамеренных воздействий на информацию, обрабатываемую в КСИИ, и способных привести к возникновению чрезвычайных ситуаций или к нарушению выполняемых системой функций со значительными негативными последствиями [25].

Классификация угроз информационной безопасности (ИБ) КСИИ в соответствии с документами ФСТЭК РФ представлена в Приложении **А** [25].

Согласно этой классификации угрозы ИБ в КСИИ классифицируются по следующим признакам:

- по объекту воздействия;
- по характеру нарушаемого свойства защищаемой информации (содержанию деструктивного воздействия);
- способу (типу канала).

Угрозы ИБ, реализуемые в отношении информации информационно-измерительной подсистемы, влияют на процессы, проходящие в управляющей подсистеме, так как нарушение целостности (подлинности), доступности этой информации может повлиять на ход и правильность принятия управляющей подсистемой решений по управлению технологическими процессами или элементами КСИИ.

Специфика защищаемого объекта определяется следующими характеристиками:

- протяженностью промышленного объекта в пространстве;

- распределенностью в пространстве подсистем АСУ транспортировкой нефте-газопродуктов по трубопроводам;

- переменным во времени и в пространстве характером угроз на объекты информатизации АСУ, обусловленным различными географическими и климатическими особенностями регионов, определяющим различные параметры периодичности, сезонности и стохастичности их проявления.

Для рассматриваемого в работе типа АСУ наиболее характерны различия в характеристиках угроз антропогенного, техногенного и природного типа, что определяет специфику задач построения модели угроз для каждой подсистемы АСУ, топологически распределенную в заданном географическом регионе.

В таблице Б.1 в приложение **Б** представлен перечень актуальных угроз из разработанной авторами работы модели угроз. Нумерация угроз в таблице имеет регистрационный характер, не связанный со степенью их актуальности. Анализ угроз показал, что в отношении информации измерительно-исполнительной подсистемы актуальны следующие угрозы ИБ:

– нарушения целостности информации, содержащей команды управления объектом (процессом);

– блокирования информации, содержащей команды управления объектом (процессом);

– нарушения целостности (подлинности информации), относящейся к программному обеспечению измерительно-исполнительной подсистемы с целью нарушения или изменения логики её работы.

В отношении информации подсистемы внешнего управления актуальны угрозы ИБ [58]:

– нарушения целостности информации, содержащей команды управления от внешних объектов (процессов);

– блокирования информации, содержащей команды управления от внешних объектов (процессов);

– нарушения целостности (подлинности) информации, содержащей актуальные данные о состоянии КСИИ и его компонентов, предоставляемой управляющей подсистемой внешним объектам (процессам);

– нарушения доступности (актуальности) информации, содержащей актуальные данные о состоянии КСИИ и его компонентов, предоставляемой управляющей подсистемой внешним объектам (процессам).

Через программно-аппаратные компоненты этой подсистемы возможна реализация:

– угроз несанкционированного подключения к каналам передачи данных и транзитным устройствам в целях: съёма, модификации, блокирования передачи, циркулирующей в этих каналах информации и (или) реализации угроз несанкционированного доступа (НСД);

– угроз НСД с удалённых узлов КСИИ (в том числе узлов, входящих в подсистему внешнего управления);

– угроз непреднамеренных действий санкционированных пользователей КСИИ на защищаемую информацию.

Несанкционированное подключение к данной подсистеме может осуществляться через сетевые интерфейсы транзитных сетевых устройств (узлов) или иных компонентов подсистем или путём воздействия на канал передачи данных. В КСИИ, в которых для решения задач подсистемы передачи данных арендуются каналы передачи данных у оператора, предоставляющего услуги связи, или используется транспортная инфраструктура сетей общего пользования, становится возможной реализация угроз НСД с удалённых, не входящих в состав КСИИ, узлов, имеющих подключение к той же сети. Чаще всего эти подсистемы имеют подключения к глобальным сетям общего пользования Internet. Это приводит к опасности реализации угроз сетевых атак из сети общего пользования.

В приложении **Б** в таблице Б.1 в первом столбце представлены, соответственно, нумерация актуальных угроз для КСИИ и их наименования.

Жирным шрифтом выделены угрозы, источники которых и характер реализации связаны с сетевыми каналами связи.

Как видно из изложенного, сетевые угрозы составляют 56 % (46 видов) из перечня актуальных угроз, нейтрализация которых является одной из основных задач настоящей работы.

Перечень актуальных угроз определяет особенности и требования к методам и средствам защиты распределенных АСУ протяженными промышленными объектами и формирует «стратегию природы» в модели принятия оптимальных решений при разработке соответствующей стратегии системы мониторинга состояния объектов и противодействия угрозам.

1.4 Построение целевой функции и выбор критериев оценки результатов исследований

Одной из главных задач мониторинга является поиск и анализ совокупности данных о процессах, протекающих в распределенной информационно-вычислительной системе и выявление аномалий в работе системы. Под аномальным состоянием понимается техническое состояние АСУ, не соответствующее регламентированным режимам ее работы. Главной целью анализа является обнаружение, прогнозирование и принятие мер по предупреждению и оперативному устранению последствий аномального состояния. Причем принятие мер должно минимизировать величину риска $\boldsymbol{R}$ от возникновения аномалий при соответствующих временных $\boldsymbol{T_{огр}}$ и стоимостных $\boldsymbol{Z_{огр}}$ ограничениях.

Целевая функция риска с учетом ограничений представлена в выражении (1.1).

$$R=P*U \rightarrow min;$$
$$T_{реал} \leq T_{огр};\ Z_{реал} \leq Z_{огр}; \qquad (1.1)$$

где P – вероятность возникновения аномального состояния;

U –ущерб от возникновения аномального состояния;

$T_{реал}$ и $Z_{реал}$ – соответственно реальное время идентификации аномалии и затраты на систему идентификации.

Анализ выражения (1.1) показал, что параметр $\boldsymbol{P}$ зависит от достоверности распознавания и принятия решения системы мониторинга состояний, а величина $\boldsymbol{U}$ - от степени оперативности этой системы [21], т.е., чем дольше длится процесс распознавания, тем больше величина $\boldsymbol{U}$.

Для представления конкретных технико-экономических показателей эффективности методов и средств мониторинга представим задачу мониторинга, как задачу распознавания состояний, решением которой является указание принадлежности идентифицируемого образа $\boldsymbol{q}^x$ к одному из двух классов, например, классу $\boldsymbol{A}$, представители которого относятся к нормальным, с точки зрения характера протекания, процессам, или классу $\boldsymbol{B}$, представляющему категорию аномальных состояний. В этих случаях решение связано с ошибками распознавания первого и второго рода, оцениваемых вероятностями, соответственно $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$.

Целевая функция задачи повышения эффективности $\boldsymbol{E_c}$ метода контроля состояния системы определяется минимизацией ошибок первого и второго рода при реальных приведенных затратах на систему мониторинга $\boldsymbol{Z}$, меньших, чем допустимые, $Z \leq Z_{\text{доп}}$, и представлена формулой (1.2) [14]:

$$E_c = e_A\ 1-\alpha\ + z_A\alpha\ P_A + e_B\ 1-\beta\ + Z_B\beta\ P_B, \qquad (1.2)$$

где e_A и e_B – экономия и возможный денежный доход от верного распознавания образа;

z_A и z_B – затраты от неверного распознавания образа, зависящие от временных характеристик системы;

α и β – соответственно ошибки первого и второго рода при определении состояния объекта;

P_Aи P_B – соответственно априорные вероятности образов $\boldsymbol{A}$ и $\boldsymbol{B}$.

Стоимостной критерий эффективности $\boldsymbol{E_c}$ является одновременно и критерием оценки качества системы мониторинга, а его аргументы α и β – частными критериями качества работы ее отдельных подсистем.

Анализ выражения (1.2) позволяет сделать вывод о том, что основными требованиями к методам мониторинга технического состояния объектов являются высокая достоверность результатов, определяемая параметрами α и β, при допустимых параметрах производительности и затрат для их достижения.

1.5 Концепция оптимизации контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков

Одной из основных моделей в теории и практике принятия решений является модель игры с природой, позволяющая в системах управления по определенной методике и системе критериев оптимизации выбрать стратегию управления в ответ на случайно заданную стратегию природы [27, 106].

Эта модель использована при выборе оптимальной стратегии защиты информации в ответ на случайные угрозы информационной безопасности автоматизированных систем (АС), представленные в модели угроз.

Для противодействия стратегиям природы согласно принципу Эшби мощность множества возможных стратегий управления ***Q2*** должна быть не меньше мощности возможных стратегий природы ***Q1***, т.е.:

$$Q2 \geq Q1 \qquad (1.3)$$

Изучение условий задачи о выборе управляющей стратегии распределенной системы мониторинга (РСМ) позволяет свести ее к задаче из теории игр с природой, в которой природа случайным образом определяет характеристики угроз в интервале времени ***T***, а подсистема принятия решений РСМ в соответствии со

стратегией природы выбирает собственную оптимальную стратегию защиты. Модель выбора оптимальной стратегии в настоящей работе определена в виде матрицы исходов стратегий размером $n \times m$, представленной в таблице 1.

Строки матрицы соответствуют стратегиям защиты C, а столбцы – прогнозируемым стратегиям природы S на перспективу T. Каждый элемент матрицы содержит оценки параметра эффекта ef_{nm}, соответствующие экономическому (или другому эффекту) для конкретной стратегии, представленные в виде дроби e_{ij}/z_{ij}, числитель которой характеризует сэкономленное качество от правильно выбранной стратегии защиты, а знаменатель – затраты от применения i-ой стратегии при ликвидации j-ой угрозы (i=1-n, j=1-m).

Таблица 1 – Матрица исходов стратегий

C	S				
	s_1	s_2	…	s_m	E
c_1	ef_{11}	ef_{12}	…	ef_{1m}	E_1
c_2	ef_{21}	ef_{22}	…	ef_{2m}	E_2
…	…	…	…	…	…
c_n	ef_{n1}	ef_{n2}	…	ef_{nm}	E_n

В качестве стратегий природы в модели использованы актуальные угрозы из модели угроз, представленной в приложении **Б**. В качестве возможных стратегий для системы мониторинга использовано множество методов обнаружения, прогнозирования и нейтрализации угроз. Выбор стратегии c_i из множества C производится с учетом условия каждой задачи, например - по максимуму экономии или минимуму затрат с учетом следующего выражения:

$$c \in C : \max | \min \sum_{j=1}^{m} ef_{ij,} \quad i = 1, n; \quad j = 1, m. \tag{1.4}$$

В выражении (1.4) принят некоторый критерий из четырех возможных критериев модели.

Эффект от каждой стратегии, в случае ее использования, определяется экспертами и закладывается в матрицу ***C***. В случае несоответствия стратегий множества ***C*** требуемой величине эффекта ставится вопрос о поиске и разработке новых стратегий мониторинга.

В условиях риска выбор стратегии РСМ производится на основе критериев минимакса, минимина, максимакса или максимина. В данной работе для обеспечения минимального риска от возникновения аномальной ситуации использован критерий минимина, который предусматривает выбор стратегии, обеспечивающий минимальный риск при нейтрализации угроз для всех стратегий природы и лица, принимающего решение в соответствии с выражением (1.3).

Следует отметить, что в данной задаче также возможно применение критерия Гурвица, т.е. максимакса при условии получения максимальной величины стоимостного эффекта по выражению (1.4).

Проведенный анализ модели актуальных угроз на АС определил в качестве оптимальной стратегии использование методов защиты на основе мониторинга сетевого трафика, включающей в себя методы обнаружения, прогнозирования и предупреждения аномального состояния АСУ трубопроводом и контроль директивных установок пользователя при управлении объектом. Данная стратегия позволяет контролировать и нейтрализовать большинство актуальных угроз из модели угроз (около 56 %) и решать задачи обнаружения и предупреждения вторжений в информационную систему АС и утечки информации.

Определенная выше стратегия контроля наряду с результатами исследований, представленными в пунктах 1.1-1.4, позволила определить общую концепцию исследований в работе, основными положениями которой являются:

- решение задачи оптимизация методов мониторинга технического состояния распределенных автоматизированных систем производится на основе разработанной с учетов документов ФСТЭК РФ модели угроз;

- принятие решений по выбору оптимальной стратегии контроля состояния объектов осуществляется на основе системного подхода, предполагающего анализ всех актуальных угроз на объект информатизации, выбор и обоснование целевой функции и критериев оценки качества контроля;
- выбор оптимальной стратегии производится на основе классической модели теории игр;
- в качестве источника исходной информации для идентификации технического состояния АСУ протяженным промышленным объектом используется сетевой трафик, как доступный поток информации обо всех подсистемах АСУ;
- в качестве инструментального аппарата использованы математические и имитационные модели, построенные на основе теории распознавания образов, вероятности, графов, множеств, автоматов;
- одним из основных предметов исследований является поток технологической информации, представленный протоколом обмена информацией в АСУ TCP/ModBus;
- основными результатами исследования являются эффективные аппаратно-программных средств идентификации, прогнозирования и предупреждения аномальных состояний в АСУ, отвечающие требованиям высокой достоверности и производительности.

1.6 Основные задачи исследований и требования к результатам

Цель исследований**:** повышение оперативности и достоверности методов контроля технического состояния распределенных управляющих систем в условиях воздействия пространственно-временных угроз на основе мониторинга информационных потоков.

Для достижения цели поставлены следующие задачи:

1) Разработать пространственно-временную модель угроз для АСУ протяженным в пространстве объектом;

2) Построить структурно-функциональные, математические и имитационные модели, позволяющие исследовать объекты защиты, оптимизировать традиционные методы и средства идентификации технических состояний АСУ управления транспортным нефтепроводом в условиях воздействия пространственно-временных угроз;

3) Построить модель сетевого трафика как информационного пространства условно бесконечного объема;

4) Разработать метод оценки технического состояния распределенной АСУ на основе мониторинга сетевых потоков информации (на примере системы транспортировки нефтегазового сырья);

5) Разработать и исследовать метод контроля директивных установок в распределенной АСУ распределенным объектом;

6) Разработать метод повышения живучести телекоммуникационной подсистемы АСУ ТП в условиях распределенной пространственно-временной модели угроз;

7) Провести анализ технико-экономической эффективности результатов исследований;

8) Разработать рекомендации по внедрению методов и средств контроля технического состояния распределенных АСУ ТП транспортировки нефтегазового сырья на предприятиях Оренбургской области.

Основные требования к результатам разработок и исследований:

- выполнение требований руководящих документов ФСТЭК РФ и регламентирующих документов по созданию АСУ в защищенном исполнении;
- создание технических решений, отвечающих уровню конкурентоспособности по сравнению с известными аналогами;
- разработка технических решений, максимально учитывающих специфику используемых в современных АСУ ТП сетевых ресурсов и аппаратно-программных средств.

2 Моделирование и исследование информационных процессов в распределенной системе мониторинга протяженного промышленного объекта

2.1 Структурно-функциональная модель распределенной управляющей системы транспортировки нефте-газопродуктов

Структурно-функциональная модель распределенной информационно-управляющей системы (РИУС) транспортировки нефте-газопродуктов предназначена для представления ее состава, информационных потоков и описания функций составляющих подсистем РИУС с целью дальнейшего анализа и определения параметров технического состояния системы в условиях воздействия пространственно-временных угроз.

На рисунке 2 представлена ее схема. Модель состоит из следующих структурных подсистем: подсистема промышленного объекта **T**; совокупность информационно-управляющих подсистема нижнего уровня **PSL1-PSLN;** информационно-управляющая подсистема верхнего **PSH;** подсистема средств связи между информационно-управляющими подсистемами **PSC** и подсистема мониторинга **PSM.**

Информационными входами и выходами для подсистем **PSL1-PSLN** являются, соответственно, данные о промышленном объекте **T** и потоки измерительной информации **F1-FN**. Управляющими входами и выходами для подсистем **PSL1-PSLN** являются, соответственно, потоки директивной информации от подсистемы верхнего уровня и управляющие потоки на исполнительные механизмы объекта **T**. Информационный поток в подсистеме **PSC** представляет собой сетевой трафик, обычно описываемый протоколом TCP/ModBus [113].

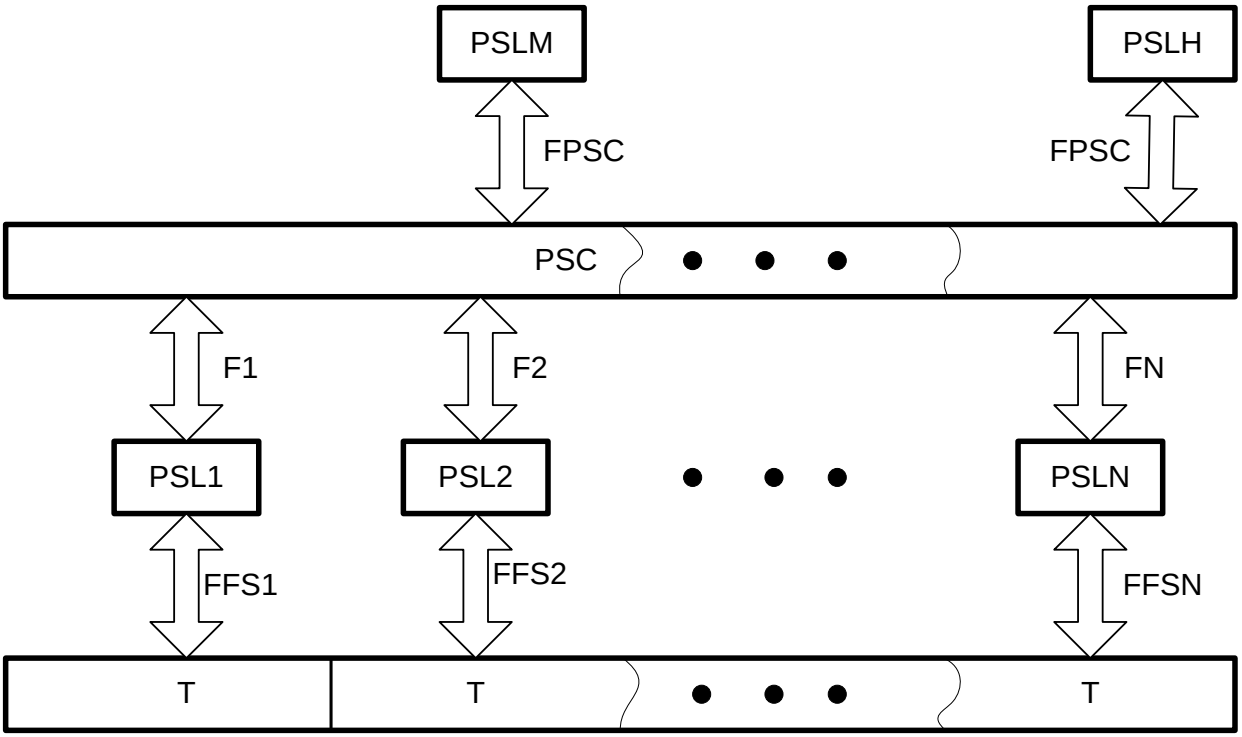


Рисунок 2 – Структурно-функциональная схема распределенной системы управления протяженным промышленным объектом

Предметом исследования в задаче моделирования являются информационные потоки системы, как потоки сведений о состоянии ее подсистем. На рисунке 2 представлены следующе информационные потоки:

- **FFS1-FFSN** – потоки физических сигналов о параметрах ППО и сигналов о воздействии на изменение этих параметров;
- **F1-FN** – потоки измерительной и управляющей информации в подсистемах нижнего уровня;
- **FPSC** – информационные потоки сетевого трафика в подсистеме средств связи.

Анализ потоков сетевого трафика позволил представить его составляющие в следующем виде:

FPSC={**T, A, K, D, C**},

где потоки в фигурных скобках обозначают, соответственно, потоки данных о текущем времени, об адресах сетевых узлов, о командах, о данных и об информации служебного характера.

Совокупность данных, зарегистрированных в конкретный момент времени характеризует текущее состояние системы. Временные ряды параметров сетевого трафика позволяют получать информацию о динамике изменения состояний системы. В общем случае множество состояний системы можно разделить на два класса: класс регламентированных (нормальных) состояний **QN** и класс аномальных состояний **QA**. Классы **QN** и **QA** содержат некоторые множества состояний (образов), определяемых значениями параметров сетевого трафика, являющихся характерными признаками для идентификации каждого состояния.

Анализ структурно-функциональной модели позволяет подвести задачу оптимизации методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз к задаче совершенствования методов и средств распознавания состояний сложных распределенных систем на основе исследования и интеллектуальной обработки доступной информации, циркулирующей между сетевыми узлами системы.

2.2 Ассоциативно-мажоритарная модель распознавания аномалий в системе мониторинга технического состояния протяженных промышленных объектов

Вопросы повышения эффективности методов и средств распознавания образов входят в перечень актуальных в теории и практике управления, поскольку от качества оценки состояния объектов зависит общая эффективность работы управляющих систем. Неслучайно эта область находится в зоне особого внимания ученых, представляющих различные аспекты этой проблемы. В настоящем разделе использованы научные и практические положения, представленные в трудах: А.Г. Ивахненко - по самоорганизации распознающих систем; Симанкова В.С. и Луценко Е.В. - по применению распознающих средств в системах управления; У. Пирса - по вопросам обеспечения надежности автоматизированных систем; в технических

решениях отечественных и зарубежных разработчиков. Основные аспекты этих положений представлены в аналитической части публикаций из приведенного в работе списка литературы.

Целью настоящего раздела работы является систематизация принципов повышения эффективности методов распознавания образов на основе ассоциативно-мажоритарного подхода (АМП).

По мнению авторов, этот аспект недостаточно представлен в современной литературе по теории и практике распознавания образов, что не позволяет в должной мере использовать высокий технически-экономический потенциал этого подхода в современных системах распознавания образов.

Актуальность выбранного направления совершенствования средств распознавания образов определена, как это показано ниже, широкими возможностями совершенствования средств распознавания образов на базе АМП.

Концептуально процесс повышения эффективности методов распознавания образов (МРО) основан на следующих положениях. В процессе создания МРО использован системный подход и принцип тотальной последовательной оптимизации, причем последовательность решения задач оптимизации определена выставленными приоритетами исследований, а принцип тотальности – стремлением усовершенствования МРО по всем их операциям:

- операции поиска альтернативных решений;
- выбору наиболее достоверного результата;
- оптимизации операций обучения и управления распознаванием.

Определение требований к МРО зависит от постановки конкретной задачи. Основными критериями и ограничениями при разработке и оценке качества УРО являются: достоверность, производительность, универсальность, алгоритмическая или конструктивная сложность реализации, стоимость изготовления, автоматизация технологических процедур, связанных со сбором исходных данных, обучения и анализа результатов. Анализ современных тенденций развития теории и практики средств распознавания образов, представленный в работах [5, 6, 8, 11], определил в качестве основной концепции исследований настоящей работы использование

ассоциативно-мажоритарного подхода, обеспечивающего максимально возможную производительность средств на этапе определения альтернативных решений и максимальную достоверность принятия окончательных решений на основе принципов мажоритарности.

Разработка и оптимизация методов и средств распознавания образов представляют собой сложный непрерывный процесс, включающий в себя ряд задач, связанных единой целевой функцией и ограничениями, в частности, таких, как:

- разработка математической модели процесса распознавания;
- разработка высокопроизводительного алгоритма работы распознающего средства (РС);
- оптимизация сложности вычислений математических выражений РС;
- обеспечение универсальности РС относительно различных исходных данных и требований задачи распознавания;
- оптимизация управления процессом распознавания образов;
- оптимизация структуры и архитектуры средств распознавания;
- разработка рекомендаций по эффективному использованию РС.

Для формализации задачи распознавания образов при построении математической модели использованы следующие условные обозначения [5]:

– $\boldsymbol{Q=\{Q_1, Q_2, \dots, Q_N\}}$ – множество классов распознаваемых образов;

– $\boldsymbol{q^x}$ – неизвестный образ, подлежащий распознаванию;

– $\boldsymbol{Q^*}$ – класс образов, к которому отнесен $\boldsymbol{q^x}$;

– $\boldsymbol{P = \{p_1, p_2, \dots, p_M\}}$ – множество признаков распознавания образов;

– $\boldsymbol{<s_i>}$ – зарегистрированное значение $\boldsymbol{i}$-го признака, $\boldsymbol{i = 1, M}$;

– $\boldsymbol{<S^x>}$ – вектор зарегистрированных значений признаков $\boldsymbol{q^x}$;

– $\boldsymbol{D=\{D_1, D_2, \dots, D_N\}}$ – множество диапазонов изменения признаков, состоящее из множеств поддиапазонов признаков для каждого образа;

– $\boldsymbol{V\{q^x, Q_j\}}$ – мера близости между $\boldsymbol{q^x}$ и $\boldsymbol{j}$-ым образом из множества $\boldsymbol{Q}$, $\boldsymbol{j= 1, N}$;

– $\boldsymbol{v_{ij}\{<s_i>, Q_j\}}$ – частный параметр (коэффициент) ассоциативности значения $\boldsymbol{<s_i>}$ признака $\boldsymbol{s_i}$ из множества $\boldsymbol{S^x}$ для образа $\boldsymbol{Q_j}$;

– $M\{<S^x>, Q\}$ – матрица коэффициентов ассоциативности значений признаков $<S^x>$ и всех классов образов из множества Q;

– $\Phi\{<S^x>, Q_j\}$ – разделяющая функция для вычисления меры близости $V\{q^x, Q_j\}$;

– $W_j\{<S^x>, D_j\}$ – вектор коэффициентов оценок ассоциативности, характеризующих состояние принадлежности зарегистрированных значений q^x диапазонам значений признаков j-го образа из множества Q, $j = 1, N$;

– $R\{(v_{ij})_k, k, p_k, P\}$ – правило определения очередности выбора приоритетных признаков из множества P для $(k+1)$-ого шага в цикле распознавания, исходя из текущей ситуации распознавания.

Модель распознавания q^x имеет следующий вид:

$$V\{q^x, Q_j\} = \Phi\{< S^x >, Q_j\},\ j = 1, N; \tag{2.1}$$

$$\Phi\{< S^x >, Q_j\} = \sum_{i=1}^{M} v_{ij}\{< s_i^{\ x} >, Q_j\}, i = 1, M; \tag{2.2}$$

$$v_{ij}\{< s_i^{\ x} >, Q_j\} = \begin{cases} 1, & \text{если} \quad < s_i^{\ x} > \in D_{ij}; \\ 0, & \text{если} \quad < s_i^{\ x} > \notin Q_j; \end{cases} \tag{2.3}$$

$$M\{< S^x >, Q\} = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1j} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2j} & \dots & v_{2n} \\ \dots & \dots & \dots & v_{ij} & \dots & \dots \\ v_{m1} & v_{m2} & \dots & v_{mj} & \dots & v_{mn} \end{pmatrix}; \tag{2.4}$$

$$q^x \in Q^* \in Q : V\{q^x, Q^*\} \equiv \max V\{q^x, Q_j\}, Q_j \in Q. \tag{2.5}$$

В выражениях (2.1) и (2.2) параметры N и M соответствуют числу образов и числу признаков. В матрице (2.4) каждый столбец соответствует частным мерам близости v_{ij} множества $<S^x>$ для каждого класса образов по всем признакам. Сумма элементов каждой строки соответствует сумме в выражении (2.2).

Выражение (2.5) представляет собой правило отнесения q^x к одному из образов множества Q по принципу простого большинства с использованием меры Хемминга, либо по принципу превышения суммы ассоциаций более половины признаков. В обоих случаях выбор правила принятия решения по мажоритарному

принципу определяется на основании метода группового учета аргументов, разработанного А.Г. Ивахненко и его учениками [43]. Мажоритарный принцип повышает достоверность распознавания образов.

При обучении модели производится вычисление элементов матрицы (2.5) по выражениям (2.1) - (2.3). Обучение модели основано на принципе работы амплитудных анализаторов сигналов, что обеспечивает высокое быстродействие, обусловленное простотой алгоритма формирования произвольных распределений.

Представленная выражениями (2.1) - (2.5) модель реализована в виде аппаратных и программных средств и использована в ряде задач распознавания образов различной природы [2, 3, 9, 11].

На рисунке 3 представлена обобщенная структурная схема устройства, построенного в соответствии с описанной математической моделью [14,75] .

Устройство содержит: блоки коммутаторов К1 и К2, подключенные, соответственно к информационным входам кодов образов и к информационным входам каналов признаков; блок преобразования кода признаков (БПК) в адрес блока ассоциативной памяти (БАП); блок обучения (БО); мажоритарный блок (БМ); блок анализа текущего результата распознавания (БАТР).

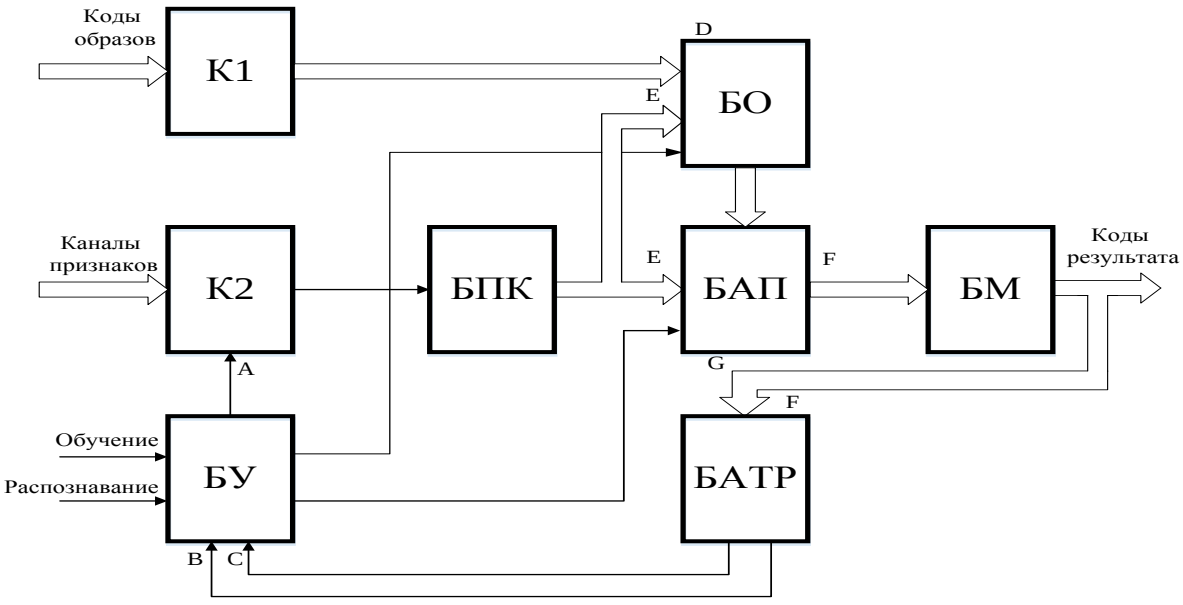


Рисунок 3 – Обобщенная структурная схема устройства распознавания образов ассоциативно-мажоритарного типа

Концепция повышения производительности МРО основана на принципах параллельно-конвейерной технологии организации процедур поиска альтернативных образов, соответствующих признакам исследуемого образа и передаче результата поиска для обработки в мажоритарный блок. Альтернативные решения распознавания образов, рассмотренные, в частности, в работах [14,75], предусматривали последовательное вычисление коэффициентов ассоциативности v_{ij} для каждого признака и каждого образа, что увеличивало общее число операций вычисления до величины, определяемой произведением $M*N$. Разработанные авторами технические решения позволили сократить число этих операций до минимума, т.е. до M, за счет того, что при поступлении очередного значения некоторого признака из P производится определение всех v_{ij} за один такт. Это достигается использованием ассоциативной памяти, в которой адреса ячеек с коэффициентами ассоциативности соответствуют значениям соответствующего признака.

В основу оптимизации сложности вычислений математических выражений положены принципы представления коэффициентов ассоциативности в двоичном виде и уменьшения вычислительной сложности выражений (2.2) и (2.3). При этом в качестве разделяющей функции использована мажоритарная функция, позволяющая оценивать степень близости совокупности признаков для каждого образа на основе меры Хемминга, представленной выражениями (2.2) и (2.3) [14, 67, 69,70,75].

Сравнение методов распознавания образов на основе АМП с другими, например, построенными на основе аналитических выражений Байеса, показало, что при снижении достоверности распознавания на 2 % производительность ассоциативно – мажоритарных средств выросла на порядок [21].

Универсальность средств распознавания образов на основе АМП обеспечена возможностью использования признаков распознавания с различными распределениями вероятностей изменения значений и автоматизацией процедуры обучения. Данное решение представлено в работе [67,70].

В основу концепции оптимизация управления процессом распознавания образов положены принципы сокращения числа операций цикла распознавания ***M*** на основе оценки текущего состояния процесса, прогнозирования результата распознавания и принятии окончательного решения. Эта ситуация определяется в случае, когда мера Хемминга для одного из образов претендентов на некотором ***k***-ом шаге распознавания имеет преимущество по сравнению с другими образами, достаточное для досрочного принятия окончательного решения. Данное решение, в частности, реализуется применением блоков БАТР, БУ и К2 на рисунке 3 и представлено в работе [75]. Оно позволяет сократить цикл распознавания образов в среднем на 15 %.

Представленные принципы повышения эффективности МРО нашли широкое применение в задачах распознавания образов различной природы, и представлены в работах [3-5, 12, 13, 16,17]. Применение АМП в задачах оценки качества дорожного полотна, как протяженного объекта, позволило на основе данных датчиков дорожного покрытия оперативно определять категорию дорожного покрытия и выбирать безопасную скорость движения транспортных средств [70]. Эти результаты рекомендованы для применения в бортовых системах автомобилей.

Особую актуальность приобретают рассмотренные технические решения в системах информационной безопасности, требующих высокой достоверности и оперативности принятия решения при обнаружении сетевых вторжений, защиты доступа и учета поведения пользователей в распределенных вычислительных системах различного назначения. В работах [3-5,12,13,16,17], в частности, изложены результаты идентификации личности и поведения пользователя на основе биометрических характеристик ладони, лица, клавиатурного почерка.

В работах [3-5] в процессе исследований доказано преимущество ассоциативного подхода перед традиционными средствами последовательного поиска информации в базах данных о сетевом трафике. В частности, результаты исследований показали увеличение производительности поисковых систем в среднем на 20 %. Эти результаты рекомендованы для использования в системах

мониторинга технического состояния распределенных промышленных объектов, в частности транспортных нефтепроводов [3-5].

Представленный перечень приложений АМП является подтверждением перспективности подхода в задачах различного профиля и является залогом дальнейшего развития и усовершенствования его в теории и практике систем распознавания образов. Результаты использования АМП представлены в разделах 3, 4 настоящей работы в пунктах 3.5., 4.1.

2.3 Модель сетевого трафика как информационного пространства условно бесконечного объема

Интенсивный рост автоматизации процесса транспортировки нефтегазового сырья влечет за собой ряд проблем. Сложность контроля технического состояния распределенного объекта заключается в том, что большинство искомых параметров о состоянии АСУ ТП оператор получает удаленно, из сетевого трафика при передаче данных в корпоративной информационной системе. Соответственно, перед современными системами контроля состояния АСУ ТП стоит задача оперативного поиска и анализа информации о состоянии распределенного объекта в сетевом трафике.

Развитие технологий мониторинга и анализа сетевого трафика должно опираться на адекватные модели и инструменты моделирования сетевых процессов. Характер сетевого трафика определяется рядом факторов – от поведения пользователей до протоколов передачи, особенностей монтажа и используемого оборудования. Таким образом, моделирование сетевого трафика и сетевых процессов, является актуальной задачей.

Целью разработки моделей сетевого трафика является выявление особенностей трафика как источника информации о состоянии АСУ ТП. Для достижения данной цели необходимо провести обзор существующих моделей сетевого трафика, разработать классификацию моделей сетевого трафика,

определить модель, применимую для мониторинга состояния АСУ ТП и разработать модель сетевого трафика как пространства условно-бесконечного объема.

В ходе обзора существующих моделей [90, 91, 116-120] были рассмотрены модели сетевого трафика, представленные на рисунке 4.

Ранние стохастические модели. Стохастические модели трафика, широко использовавшиеся в прошлом, в основном представляли марковские процессы, то есть обладали кратковременной зависимостью.

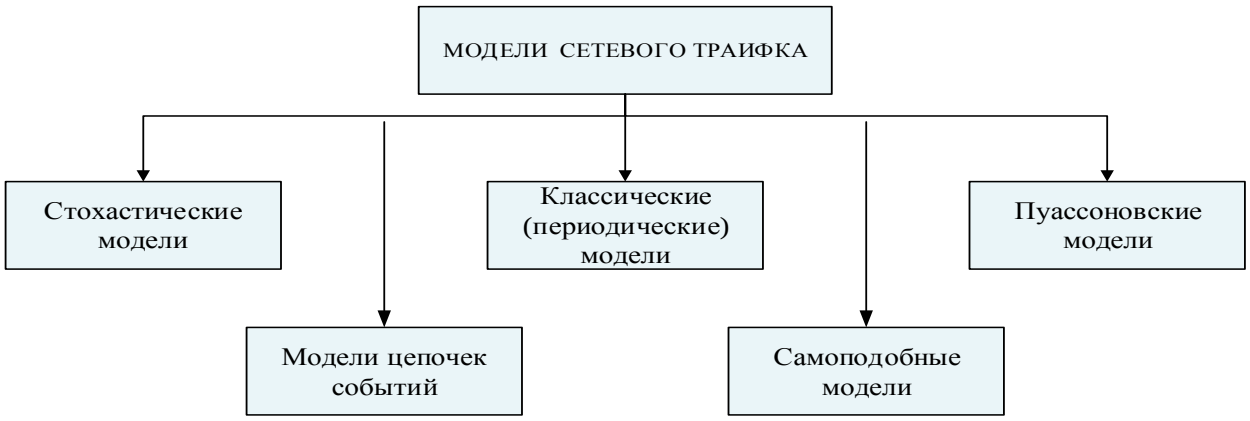


Рисунок 4 – Классификация моделей сетевого трафика

Такие модели описывались распределением Пуассона с длиной сообщения, изменявшейся по экспоненциальному закону, и основывались на теории массового обслуживания. *Пуассоновская модель* не учитывает того, что реальный сетевой трафик обладает периодами сильных всплесков активности. Для классической модели автокорреляционная функция стремится к нулю для больших отсчетов, в то время как наличие всплесков активности в реальном исследуемом трафике приводит к положительной автокорреляции.

В рамках *классической модели* трафика считается, что источники данных работают переменно. То есть периоды высокой активности сменяются длительными задержками. Таким образом, было заключено, что время поступления сообщений и длина сообщений подчиняются экспоненциальному распределению, а процесс

поступления сообщений от источников данных - пуассоновский процесс. Все процессы стационарные и независимые.

Модель цепочки сообщений. Модель трафика была сформулирована и стала популярной в 80-е гг. XX в.. В рамках модели подразумевается, что пакеты трафика передаются вместе и могут обрабатываться как одно целое. Сетевое оборудование в каждой точке сети может принимать решение о дальнейшей обработке цепочки по первому сообщению. Подобный алгоритм предохранил бы сеть от бесполезных операций по анализу кадров. Однако стоит отметить, что это модель источников сообщений. Модель применима только для сообщений, обладающих одним пунктом назначения. Очевидно, что реализация транспортных протоколов и сетевого оборудования для модели цепочки сообщений и классической модели будет кардинально отличаться.

Самоподобная модель. Во многих современных работах отмечается, что объединение трафика от нескольких переменных источников приводит к тому, что трафик становится сильно автокоррелированным с долговременной зависимостью. Это приводит к тому, что совокупность множества источников данных, проявляющих синдром бесконечной дисперсии, в результате дает самоподобный объединенный сетевой трафик, стремящийся к фрактальному броуновскому движению. Кроме того, исследование различных источников трафика показывает, что существенное изменчивое поведение – это свойство, присущее архитектуре клиент/сервер.

Проведенные исследования [19] показали, что сетевой трафик – это сложный набор слабоструктурированных данных, характеризующийся большими объемами информации. Для получения полной информации об исследуемых процессах в ходе моделирования невозможно использовать ограниченный класс моделей, что приводит к необходимости использования нескольких видов моделей одновременно.

Наиболее объективным подходом к моделированию сетевого трафика для мониторинга состояния протяженных в пространстве АСУ является использование стохастических моделей и моделей цепочек событий, так как данные о состоянии АСУ чаще всего представляют собой детерминированные цепочки событий с

элементами случайных отклонений. Такие характеристики пакета, как, например, адреса и порты субъектов взаимодействия, стохастичны, заранее не предопределены и определяются в процессе сетевых взаимодействий и установления сеанса связи. А данные сеанса представляют собой цепочки событий, отражающие информацию о сетевых взаимодействиях.

Под потоками данных в АСУ ТП понимается передача данных в виде некоторого количества пакетов ***I*** определенного типа, регистрируемого в дискретный момент времени ***t,*** как показано на рисунке 5. Регистрация передаваемых данных происходит периодически в заданные моменты времени, либо при возникновении нерегламентированных ситуаций.

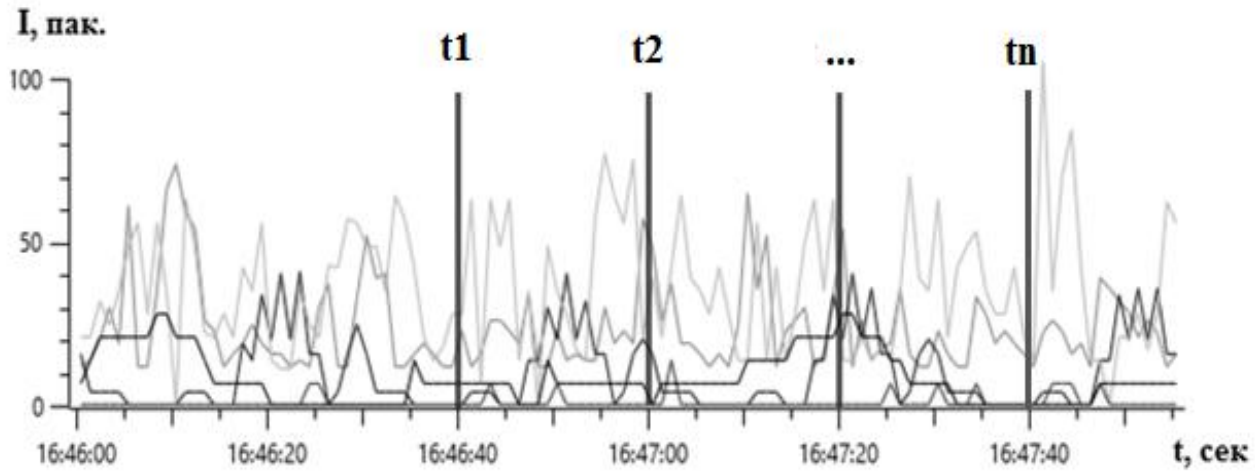


Рисунок 5 – График информационных процессов в сетевом трафике

Анализ потоков сетевого трафика позволил представить его составляющие в следующем виде:

$$FPSC=\{T, A, K, D, C\}, T \to \infty, \quad (2.6)$$

где потоки в фигурных скобках обозначают, соответственно, потоки данных о текущем времени, об адресах сетевых узлов, о командах, о данных и об информации служебного характера.

Время регистрации пакета ***T*** необходимо для определения выборки событий, удовлетворяющих интервалу анализа. Его устанавливает администратор системы в зависимости от преследуемых целей. Анализируемая статистика может быть как текущей или частной (при малых значениях ***T***), так и долговременной или глобальной (при значении ***T*** от нескольких часов или суток).

На рисунке 6 представлена обобщенная информационная модель сетевого трафика. На вход модели поступает технологическая, административная (управляющая) и служебная информация, а также информация о нерегламентированных действиях пользователей АСУ представлена на рисунке 6. Пользователем может быть как оператор, так и нарушитель, получивший несанкционированный доступ к системе.

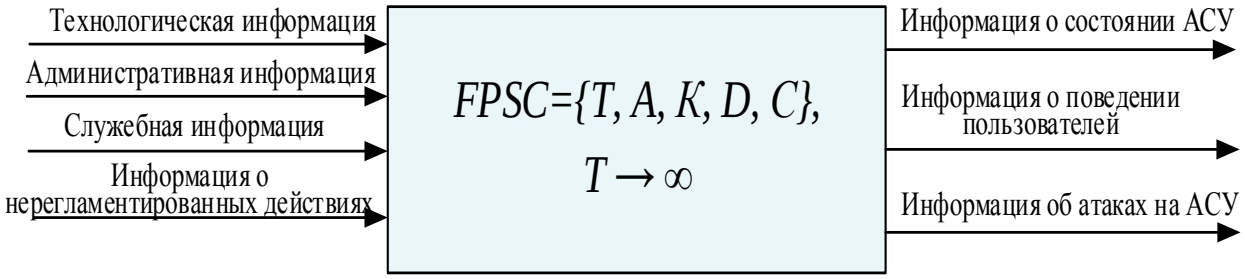


Рисунок 6 – Обобщенная информационная модель сетевого трафика

В ходе анализа регистрируются основные данные пакета, содержащие информацию о состоянии объекта мониторинга: о текущем времени, об адресах сетевых узлов, о командах, о данных и об информации служебного характера. Подобная информация может содержаться как в заголовке пакета (адреса, порты, время), так и в информационной части (например, значения регистров управляющего устройства). Более подробно структура пакета сетевого трафика промышленных протоколов представлена в приложении **В.**

Совокупность данных, зарегистрированных в конкретный момент времени характеризует текущее состояние системы. Временные ряды параметров сетевого трафика позволяют получать информацию о динамике изменения состояний системы. В общем случае множеств состояний системы можно разделить на два

класса: класс регламентированных (нормальных) состояний ***QN*** и класс аномальных состояний ***QA***. Классы ***QN*** и ***QA*** содержат некоторые множества состояний (образов), определяемых значениями параметров сетевого трафика, которые являются характерными признаками для идентификации каждого состояния. Совокупность нескольких признаков идентификации образует сигнатуру состояния, по которой текущее состояние может быть отнесено к классу ***QN***, либо ***QA***.

Сигнатура состояния по данным сетевого трафика на момент времени t, согласно формуле (2.7), имеет следующий вид:

$$\Phi(t) = <t, A, K, D, C>. \quad (2.7)$$

Каждый из перечисленных параметров, регистрируемый в дискретный момент времени ***t***, имеет свою природу, диапазон значений и значительное количество возможных значений в этом диапазоне. Например, количество возможных IP-адресов по протоколу IPv4 – 256^4 – более 4 млрд. значений. Так как состояние системы, определяется несколькими параметрами одновременно и, зачастую, анализируется в течение некоторого диапазона времени, число возможных состояний системы, регистрируемых в логических файлах сетевого трафика, является условно-бесконечным и определяется по формуле:

$$N\text{сост} = \quad NDP_i \,, \quad (2.8)$$

где $\boldsymbol{NDP_i}$ – количество возможных значений ***i*** – го параметра в диапазоне его изменения. Ввиду непрерывности мониторинга состояния АСУ ТП, время регистрации данных сетевого трафика не ограничено. Соответственно, объем регистрируемых данных о состоянии АСУ также является условно-бесконечным.

В ходе исследований авторами были проанализированы данные лог-файлов сетевого трафика нескольких предприятий нефтегазовой отрасли. Средний объем трафика, регистрируемого одним узлом системы мониторинга, составлял около 0,2 - 0,5 Гб (около 1,5 - 2 млн. пакетов) в час. Соответственно, при непрерывном

мониторинге требуется около 12 Гб памяти в сутки для каждого узла системы мониторинга. При этом даже при использовании аппаратно-программных средств мониторинга с высокой пропускной способностью (4 Гбит/сек) и высокой производительностью [112] необходимы значительные объемы памяти для хранения получаемых данных и значительные вычислительные мощности для их обработки.

Этот факт создает определенные трудности при хранении и обработке информации, так как объем памяти и скорость обработки данных аппаратно-программными средствами мониторинга сетевого трафика ограничены: зачастую, время поиска и анализа данных о произошедшем инциденте превышает допустимое время реакции на него. Соответственно, необходимы новые подходы, позволяющие компактно и оперативно хранить и обрабатывать получаемую информацию.

В ходе анализа основных способов представления данных в памяти компьютера [12], сделан вывод о том, что наиболее эффективным решением проблемы обработки и хранения больших объемов трафика является ассоциативный подход к организации данных при регистрации информации о пакетах, циркулирующих в сети. При использовании ассоциативной организации данных с увеличением объемов сетевого трафика и количества поисковых признаков время доступа к данным существенно не изменяется, а скорость доступа значительно превышает скорость, достигнутую методом полного перебора. При этом сложность метода заключается только в построении ассоциаций и не зависит от объемов трафика и сложности организации данных.

Одной из главных задач процесса мониторинга сетевого трафика на основе ассоциативного подхода является оперативное формирование кода о состоянии АСУ, как показано на рисунке 7, и сигнализирование диспетчера о возникновении аварийной ситуации при обнаружении кодов нерегламентированных состояний. Функции диспетчера представлены в приложении **Г**.

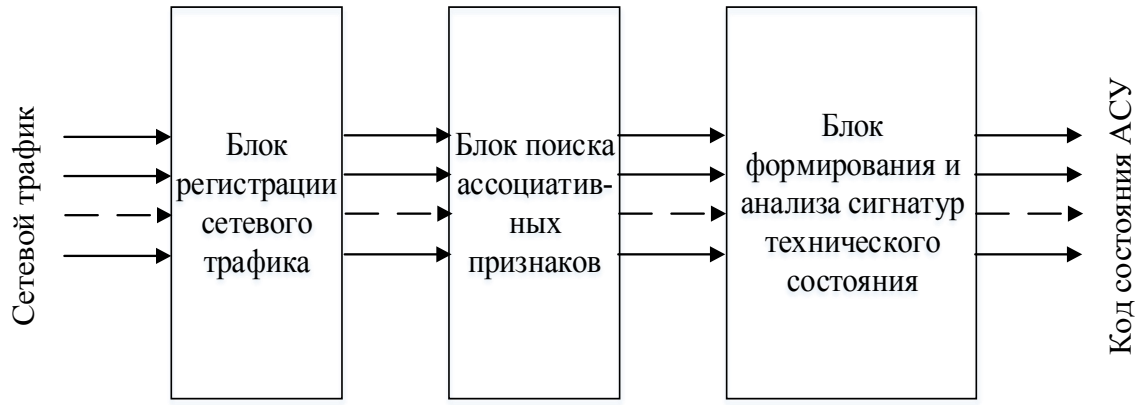


Рисунок 7 – Технологическая схема процесса преобразования информации о сетевых потоках в системе мониторинга сетевого трафика

Согласно представленной схеме данные сетевого трафика регистрируются с помощью блока регистрации сетевого трафика, после чего передаются в ассоциативную память. При этом, в качестве адреса задаются необходимые для анализа данные пакетов (IP-адреса, порты, время регистрации и т.д.). После анализа зарегистрированных данных по содержащимся в памяти сигнатурам в поле данных записывается код состояния АСУ. Сигнатуры задаются оператором и определяются в контексте конкретной ситуации. Примеры ассоциативного анализа данных сетевого трафика, характеризующих возникновение аномальных ситуаций, более подробно рассмотрены в пункте 3.2 раздела 3.

Таким образом, с учетом непрерывности мониторинга состояния АСУ, значительного количества возможных состояний и большого числа анализируемых параметров, объем данных о состоянии АСУ ТП, регистрируемых в виде потока сетевого трафика, является условно-бесконечным, что приводит к необходимости компактного хранения и оперативного анализа полученных данных. В качестве решения данной проблемы авторами предложен ассоциативный подход к организации и поиску данных, позволяющий компактно хранить и оперативно анализировать данные о состоянии АСУ, что сокращает время реакции на аномальное состояние системы.

3 Исследование и разработка методов повышения эффективности контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков

3.1 Имитационное моделирование аномалий в информационной системе мониторинга состояния нефтепровода по данным сетевого трафика

Одной из основных задач построения АСУ сложными промышленными объектами является исследование их режимов, близких к экстремальным, в частности в предаварийных состояниях [11, 42, 61, 82, 83]. Особую актуальность эта задача имеет для распределенных АСУ ТП, работающих в условиях пространственно-временных возмущений. Это обусловлено спецификой топологии управляемых объектов, динамикой изменения их состояний, условиями их эксплуатации, требованиями к модернизации и рядом других факторов, что приводит к необходимости моделирования и разработки новых систем мониторинга состояния АСУ транспортировкой нефтегазового сырья. Решение задач исследования в действующей системе нежелательно из-за большого риска нежелательного вмешательства в отлаженный технологический процесс.

В настоящем разделе представлены результаты разработки имитационных моделей, позволяющих в лабораторных условиях генерировать информационное пространство сетевого трафика, соответствующее типовым состояниям системы управления протяженным промышленным объектом. В частности:

- построена мнемосхема системы мониторинга технического состояния нефтепровода;
- разработана классификация аномальных состояний системы мониторинга нефтепровода;

- разработана структурная схема имитационной модели подсистемы мониторинга участка трубопровода;

- проведены эксперименты по моделированию аномальных состояний системы с регистрацией и поиском информации по данным сетевого трафика.

Для получения достоверных оценок выбраны два вида инструментальных средств: разработанная авторами имитационная модель на базе средств автоматизации SCADA и система имитации сетевого трафика на базе программного эмулятора сетевого промышленного протокола ModBus. Основные результаты исследований опубликованы в работах [6-7]. Особенности имитационного моделирования на базе программного эмулятора представлены в приложении **В**.

Для моделирования нефтепровода, датчиков, ПЛК и исполнительного механизма в системе автоматизации технологических процессов «SCADA TRACE MODE» была построена мнемосхема подсистемы мониторинга технического состояния нефтепровода, представленная на рисунке 8, и разработан программный комплекс для формирования промышленного сетевого трафика. Разработанный авторами программный комплекс для формирования сетевого трафика состоит из программ: PLC_Simulator [6] и Scada_pipeline. Программа PLC_Simulator имитирует работу удаленного ПЛК, контролирующего давление в трубопроводе до и после задвижки, а также управляющего открытием/закрытием задвижки. Программа Scada_pipeline реализована в среде Trace Mode 6.0 и позволяет контролировать и управлять состоянием ТО через удаленный ПЛК. Подключение к удаленному ПЛК производится по протоколу ModBus TCP.

Подсистема мониторинга, мнемосхема которой приведена на рисунке 8, обеспечивает контроль основных технологических параметров участка трубопровода: давления, температуры, загазованности, расхода нефти и т.д. Давление на данном участке нефтепровода регулируется задвижкой, переключаемой исполнительным механизмом. Измерение значений давления происходит с помощью датчиков, устанавливаемых до и после задвижки. Команды на исполнительный механизм поступают от контроллера после получения им соответствующих команд от диспетчера.

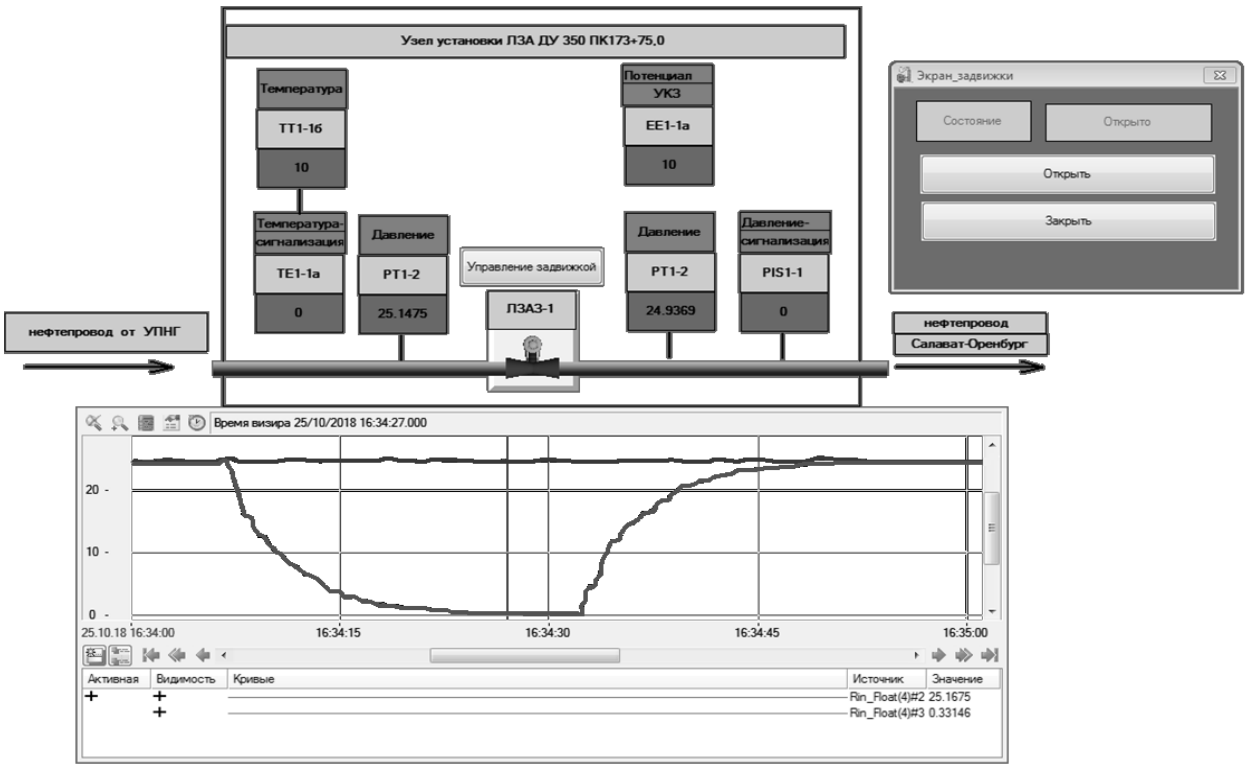


Рисунок 8 – Мнемосхема подсистемы мониторинга технического состояния отдельного участка нефтепровода

На экране компьютера диспетчера в режиме реального времени отражаются основные параметры участка трубопровода, в частности, значения и графики изменения давления. При выходе контролируемых параметров за границы допустимых значений оператор должен получать извещение об аномальном состоянии системы.

На рисунке 9 представлена классификация основных состояний АСУ ТП. Причинами возникновения аномального состояния могут быть: техногенные факторы (обрыв линии связи, поломка оборудования, сбои в работе сети), антропогенные условия (нерегламентированные действия пользователя, атаки на АСУ ТП и т. п.), а также природные явления в виде снегопада, резких порывов ветра и других. Одной из главных задач мониторинга состояния АСУ ТП является выявление и предупреждение инцидентов в автоматизированных системах, приводящих к нарушению их работы.

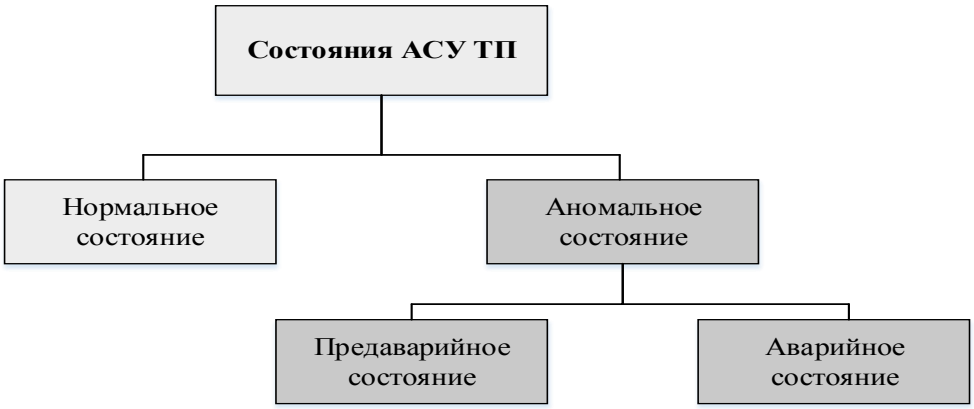


Рисунок 9 – Классификация состояний АСУ ТП

Особенность контроля технического состояния системы мониторинга распределенного объекта заключается в том, что большинство искомых параметров о состоянии АСУ оператор получает из сетевого трафика при передаче данных в корпоративной информационной системе. Большинство современных АСУ ТП для организации передачи информации используют протокол Modbus [114]. Сетевые узлы при этом взаимодействуют, используя клиент-серверную модель, основанную на транзакциях, состоящих из запроса и ответа, как показано на рисунке 10.

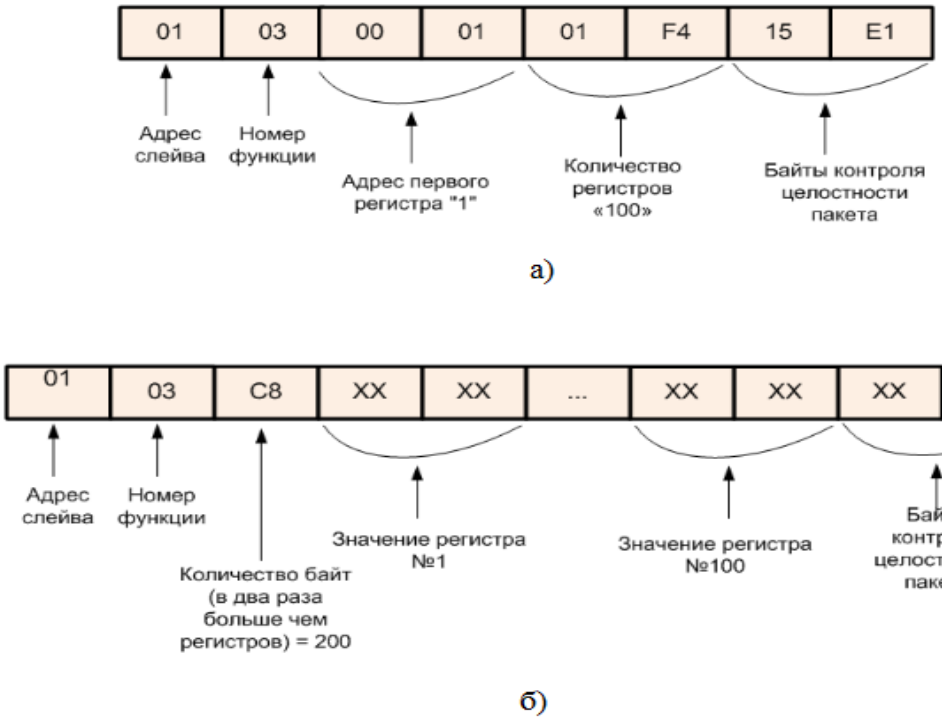


Рисунок 10 – Структура пакета Modbus (а) - запрос от ведущего устройства, б) – ответ от подчиненного устройства) [114]

Для передачи данных на дальние расстояния по сетям Ethernet используется протокол ModBus TCP [78, 114], представляющий собой стандартный пакет ModBus с добавлением данных стека TCP/IP (адресов и портов взаимодействия и т.п.). При обнаружении инцидентов, связанных с некорректной работой полевого оборудования в сетевом трафике в первую очередь анализируются коммуникационные протоколы этого типа.

Для моделирования системы мониторинга технического состояния АСУ трубопроводом по данным сетевого трафика была построена локальная сеть, имитирующая взаимодействие оператора и Modbus-устройств в режиме управления участком трубопровода. Структурная схема сети представлена на рисунке 11.

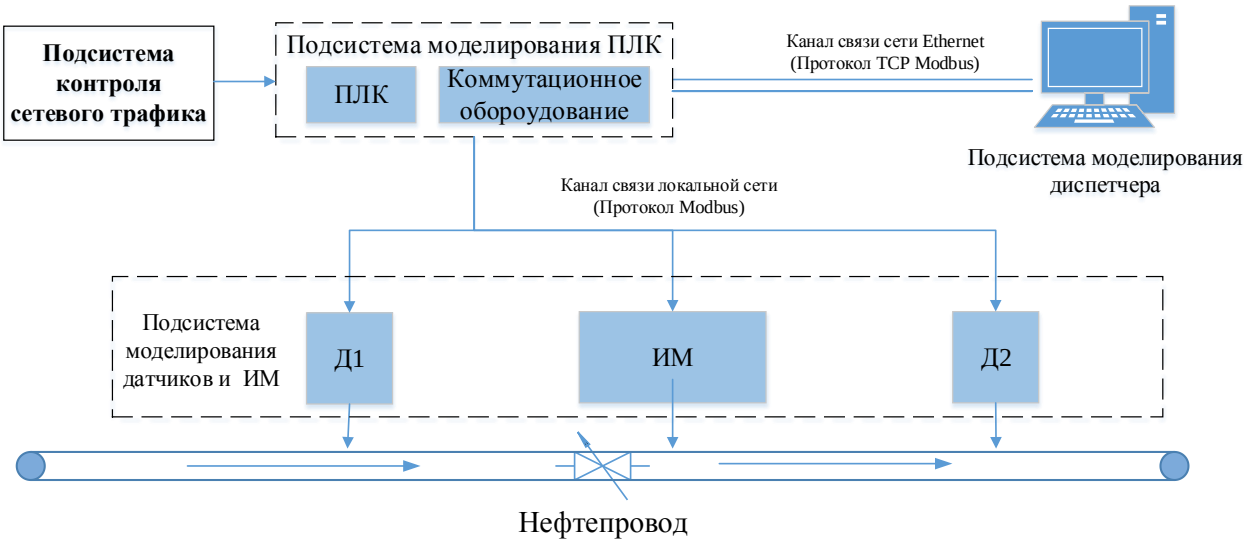


Рисунок 11 – Структурная схема имитационной модели исследования сетевого трафика в системе сбора и регистрации данных о состоянии трубопровода

В ходе проведения эксперимента моделировались различные варианты воздействия на техническое состояние автоматизированной системы и нефтепровода. Для моделирования были выбраны следующие распространенные инциденты: обрыв линии связи и нерегламентированные действия оператора (закрытие задвижки нефтепровода). Результаты эксперимента представлены на рисунках 12 - 13.

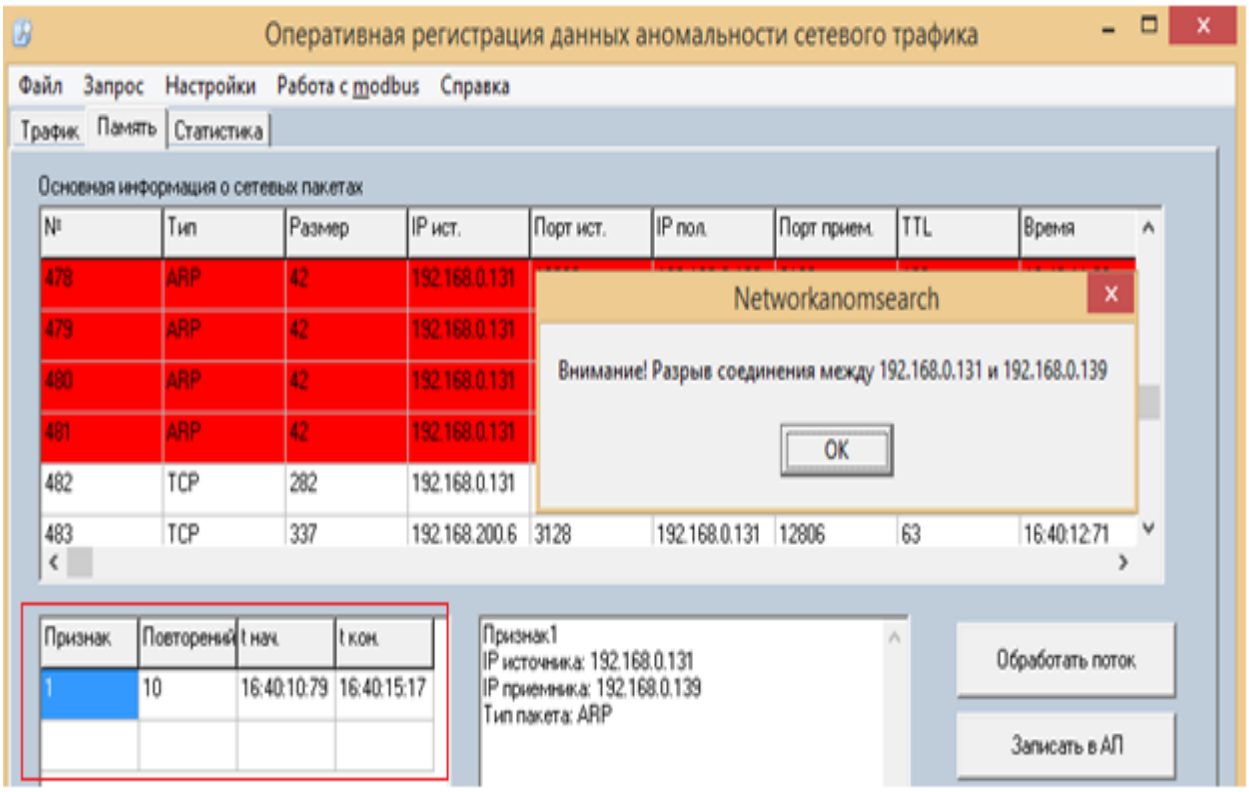


Рисунок 12 – Обнаружение обрыва линии связи

В случае обрыва линии связи в качестве сигнатуры было использовано повторение запроса на соединение, поступающего от оператора к ПЛК. Например, в случае повторения в течение 5 секунд более 10 запросов на соединение, система сигнализирует о разрыве связи.

В ходе эксперимента также была смоделирована ситуация с отправкой оператором команды на закрытие задвижки. В реальных условиях такая команда может привести к изменению давления в нефтепроводе до критических значений.

Для обнаружения команды закрытия задвижки использовалась сигнатура изменения данных соответствующего регистра ПЛК, считываемая из данных протокола Modbus. В регистр 2 управляющего устройства посылались команды для исполнительного механизма «открыть/закрыть задвижку», представленные в виде логических команд «0» - открыть и «1» - закрыть, как представлено на рисунке 13. При этом, значения давления, хранящиеся в регистрах 5 и 7 возрастают и убывают, соответственно показаниям датчиков, расположенным до и после задвижки.

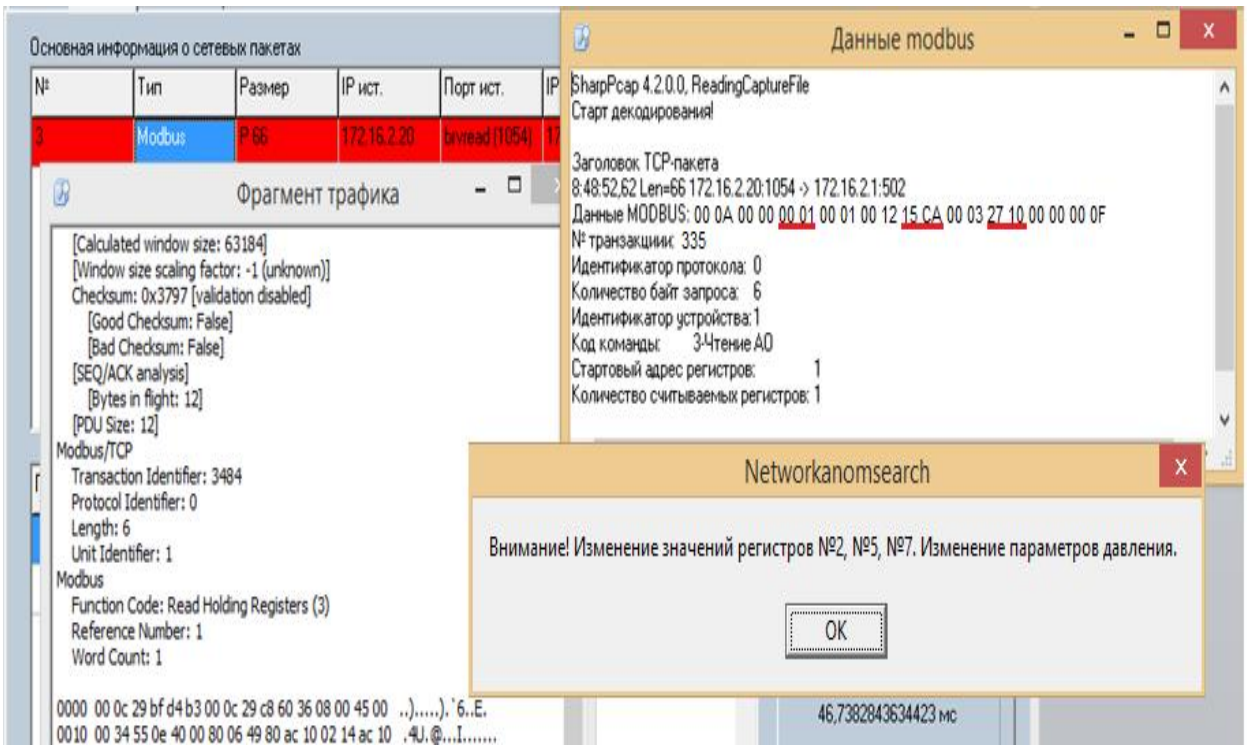


Рисунок 13 – Обнаружение несанкционированных действий оператора (закрытия задвижки)

Получение оператором подобного сообщения от подсистемы контроля сетевого трафика сигнализирует о необходимости немедленного реагирования на инцидент в соответствии с предоставленными данными.

Разработанная имитационная модель позволяет осуществлять генерацию и передачу информации по протоколу Modbus без использования специализированного оборудования и вмешательства в реальный производственный процесс. Подсистема анализа сетевого трафика позволяет контролировать доступ к объектам управления транспортировкой нефтегазового сырья и протекание технологического процесса, оперативно выявлять и реагировать на инциденты в АСУ ТП. В реальных условиях разработанная модель может быть реализована стандартным сетевым оборудованием и средствами обеспечения сетевой безопасности, что повлечет снижение риска от угроз аномального технического состояния АСУ транспортировкой нефтегазового сырья.

3.2 Метод обнаружения аномалий в системе мониторинга технического состояния протяженного промышленного объекта по данным сетевого трафика

В результате моделирования и исследований информационных процессов в распределенной системе мониторинга протяженного промышленного объекта разработан метод обнаружения аномалий в системе мониторинга технического состояния протяженного промышленного объекта по данным сетевого трафика. Особенностью метода является использование ассоциативного подхода к организации и поиску данных о техническом состоянии системы мониторинга ППО на основе мониторинга сетевого трафика.

Алгоритм обнаружения аномалий в системе мониторинга ТС ППО на основе ассоциативного подхода представлен на рисунке 14. Исходными данными являются данные потока сетевого трафика. По протоколу Modbus выделяется информация о времени регистрации пакета, адресах, командах и данных об объектах. По полученным данным формируется совокупный адрес, по которому происходит обращение к ассоциативной памяти (АП). Данные в АП хранятся в следующем виде. Адрес включает в себя код времени, код команды, код порта и код данных. В поле данных АП по конкретному адресу хранится сигнатура состояния системы мониторинга ППО.

По сформированному совокупному адресу из АП считывается сигнатура состояния системы. После анализа полученных данных происходит идентификация состояния. В случае обнаружения аномалии оператору выводится сообщение об аномальном состоянии системы. Если аномалии не обнаружены, то происходит захват и анализ новых данных.

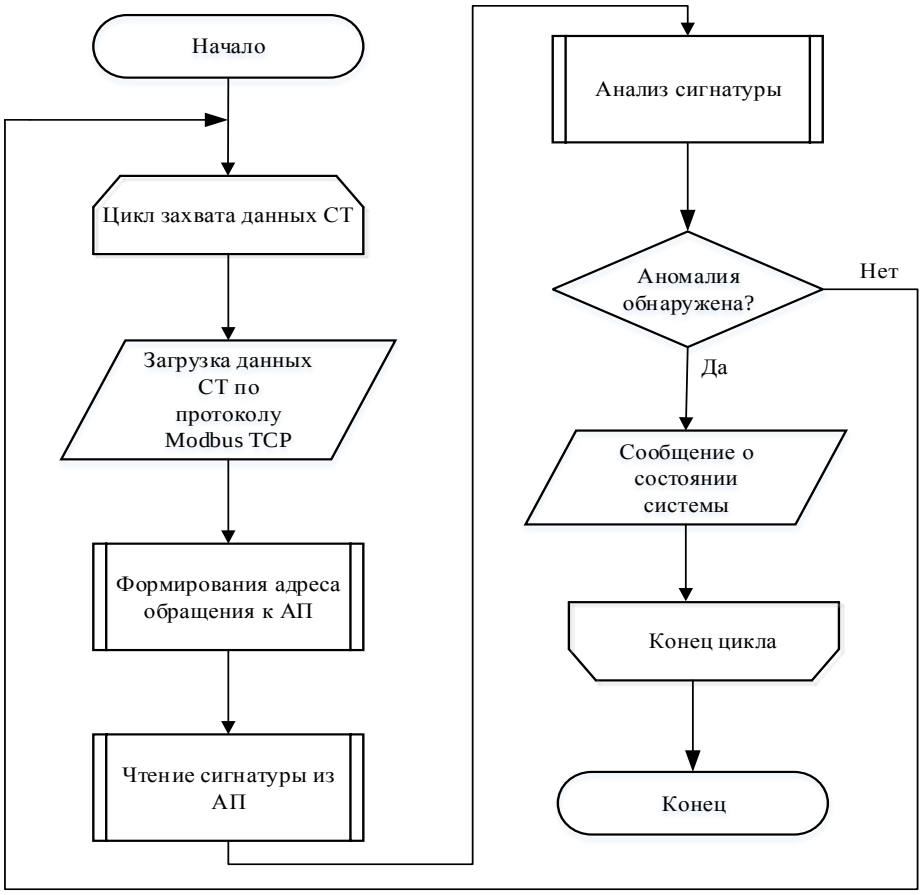


Рисунок 14 – Схема алгоритма обнаружения аномалий в системе мониторинга ТС ППО на основе ассоциативного подхода

Ввиду непрерывности мониторинга технического состояния алгоритм выполняется циклически до тех пор, пока не поступит команда об остановке мониторинга информационных потоков АСУ.

Сигнатуры, по которым происходит идентификация аномального состояния, задаются оператором и определяются в контексте конкретной ситуации. Например, сигнатура обрыва линии связи формируется следующим образом: в АП фиксируется число повторения одного и того же адреса за некоторый интервал времени (**T**). Если число повторений (**N**) запросов на соединение от определенного адреса (**A**) за некоторый промежуток времени (**T**) больше заданного порога, то это свидетельствует об обрыве линии связи, как показано на рисунке 15.

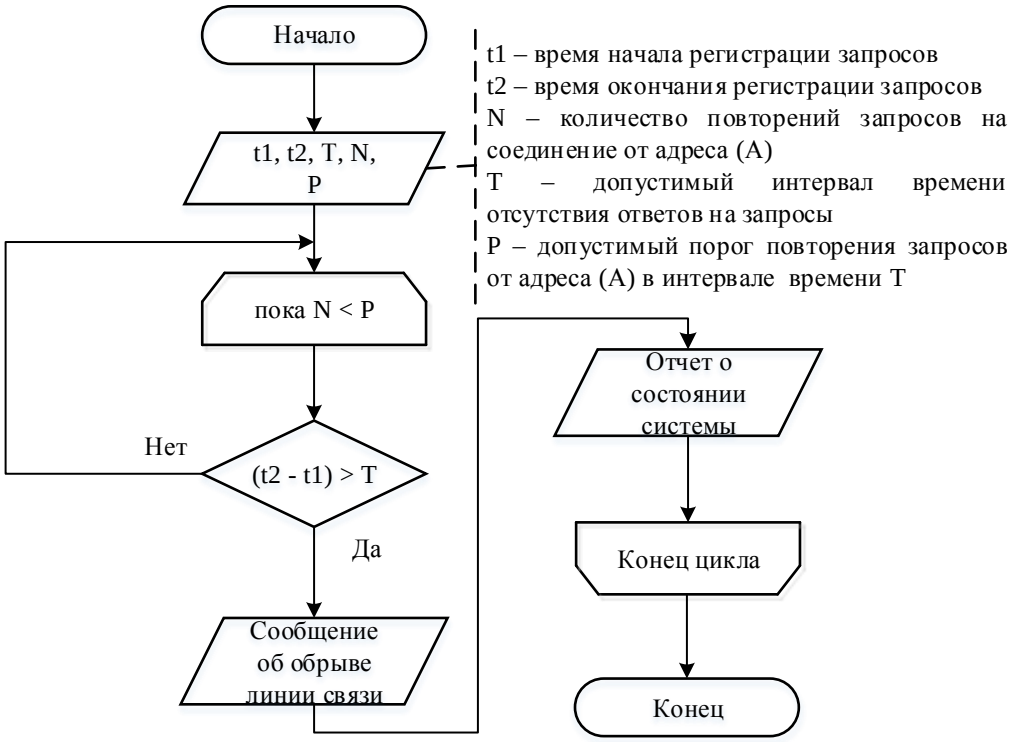
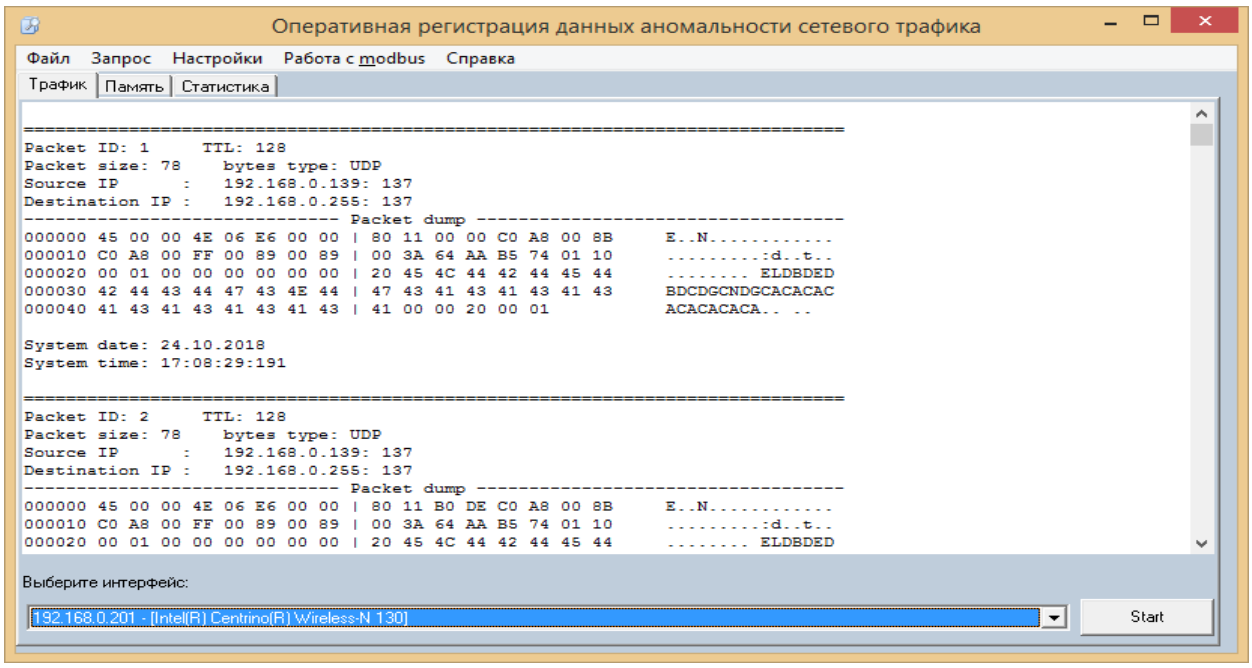


Рисунок 15 – Алгоритм формирования сигнатуры обрыва линии связи

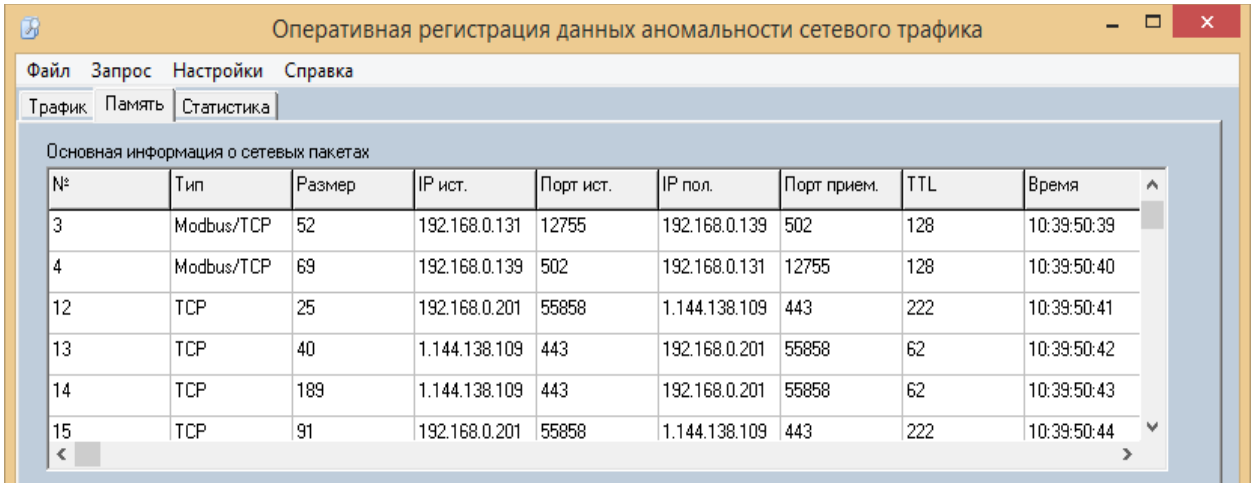
При обнаружении нерегламентированных состояний выдается сигнал о необходимости оперативного реагирования на инцидент.

Разработанный алгоритм реализован в виде программного средства поиска информации и обнаружения аномалий на основе мониторинга сетевых информационных потоков [6,88], осуществляющего автоматизированный поиск и обнаружение аномалий в системе мониторинга технического состояния протяженного промышленного объекта по данным сетевого трафика.

Входными данными для работы программы является поток сетевого трафика, в котором производится поиск информации о проходящих через сетевой интерфейс пакетах. На первом этапе производится регистрация данных сетевого трафика, как показано на рисунке 16, и запись зарегистрированных данных в ассоциативную память.



а) регистрация данных сетевого трафика;



№	Тип	Размер	IP ист.	Порт ист.	IP пол.	Порт прием.	TTL	Время
3	Modbus/TCP	52	192.168.0.131	12755	192.168.0.139	502	128	10:39:50:39
4	Modbus/TCP	69	192.168.0.139	502	192.168.0.131	12755	128	10:39:50:40
12	TCP	25	192.168.0.201	55858	1.144.138.109	443	222	10:39:50:41
13	TCP	40	1.144.138.109	443	192.168.0.201	55858	62	10:39:50:42
14	TCP	189	1.144.138.109	443	192.168.0.201	55858	62	10:39:50:43
15	TCP	91	192.168.0.201	55858	1.144.138.109	443	222	10:39:50:44

б) запись зарегистрированных данных в ассоциативную память

Рисунок 16 – Экранная форма регистрации сетевого трафика

Далее, в автоматическом режиме, либо по запросу оператора происходит поиск данных о техническом состоянии системы с выводом сообщения об аномалии и содержимого трафика по протоколу Modbus.

В ходе моделирования различных вариантов воздействия на техническое состояние системы, описанных в пункте 3.1., производился поиск и анализ данных в сетевом трафике о следующих распространенных инцидентах: обрыв линии связи и нерегламентированные действия оператора (закрытие задвижки нефтепровода).

При анализе полученных данных с помощью разработанного программного средства производился ассоциативный поиск данных по содержащимся в базе данных сигнатурам.

На рисунке 17 в полученных лог-файлах сетевого трафика виден разрыв соединения на 545 транзакции (область 1) и попытки оператора (адрес 192.168.0.131) связаться с управляющим устройством (ПЛК, адрес 192.168.0.139) – область 2.

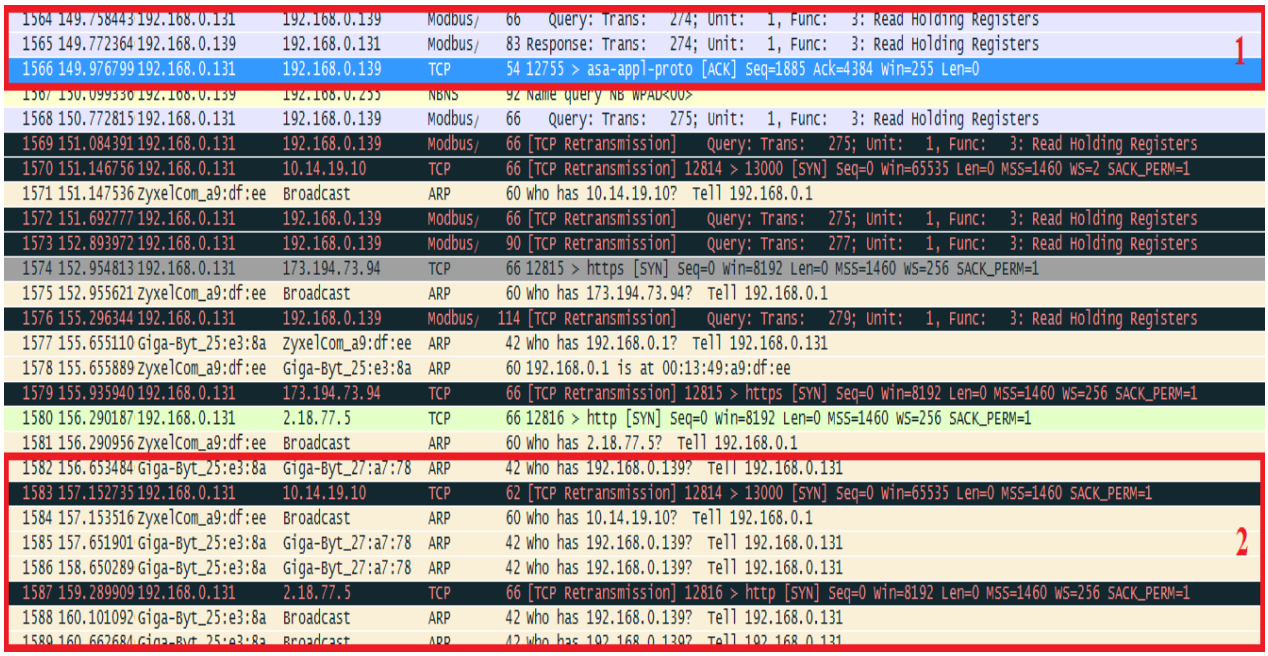


Рисунок 17 – Экранная форма данных сетевого трафика при обрыве линии связи

В случае обрыва линии связи в качестве сигнатуры используется повторение запроса на соединение, поступающем от оператора к ПЛК. Если количество повторений запросов от одного адреса в течение определенного интервала времени превышает установленный порог, то выводится сообщение об инциденте.

На рисунке 18 приводится экранная форма работы программы при обнаружении обрыва лини связи в случае регистрации в течение 5 секунд более 10 запросов на соединение.

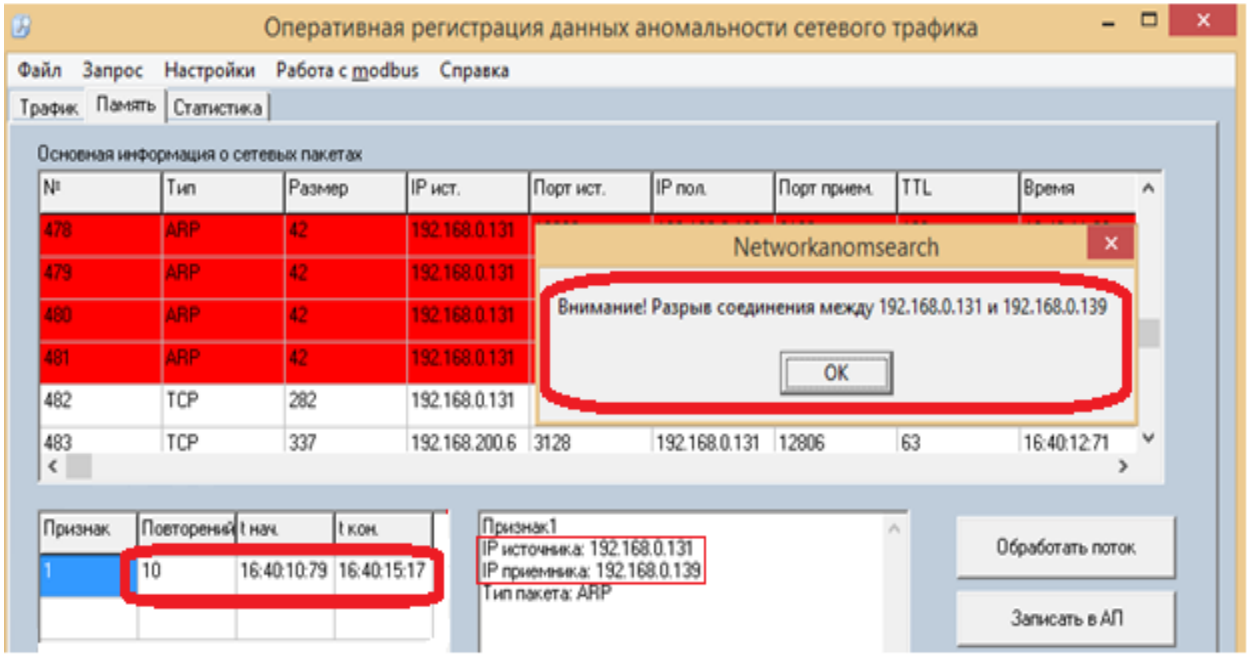


Рисунок 18 – Экранная форма работы программы при обнаружении обрыва линии связи

В ходе моделирования также была воспроизведена ситуация с записью в регистр контроллера команды на закрытие задвижки. Закрытие задвижки определяется по совокупному адресу в ассоциативной памяти, в котором данные соответствуют закрытой задвижке, т.е. по этому адресу в АП хранится сигнатура (сигнальный код) для оператора, что трубопровод закрыт. Код сигнатуры формируется из адреса и данных соответствующих регистров управляющего устройства, считываемых по протоколу Modbus.

В перехваченных данных сетевого трафика видно, что в регистр 2 управляющего устройства посылались команды для исполнительного механизма, представленные в виде логических команд «0» - открыть и «1» - закрыть задвижку, как представлено на рисунке 19. При этом значения давления в регистрах 5 (15CA) и 7 (2710) возрастают и убывают, соответственно показаниям датчиков до и после задвижки.

Получение оператором подобного сообщения от подсистемы контроля сетевого трафика сигнализирует о необходимости оперативного реагирования на инцидент в соответствии с предоставленными данными.

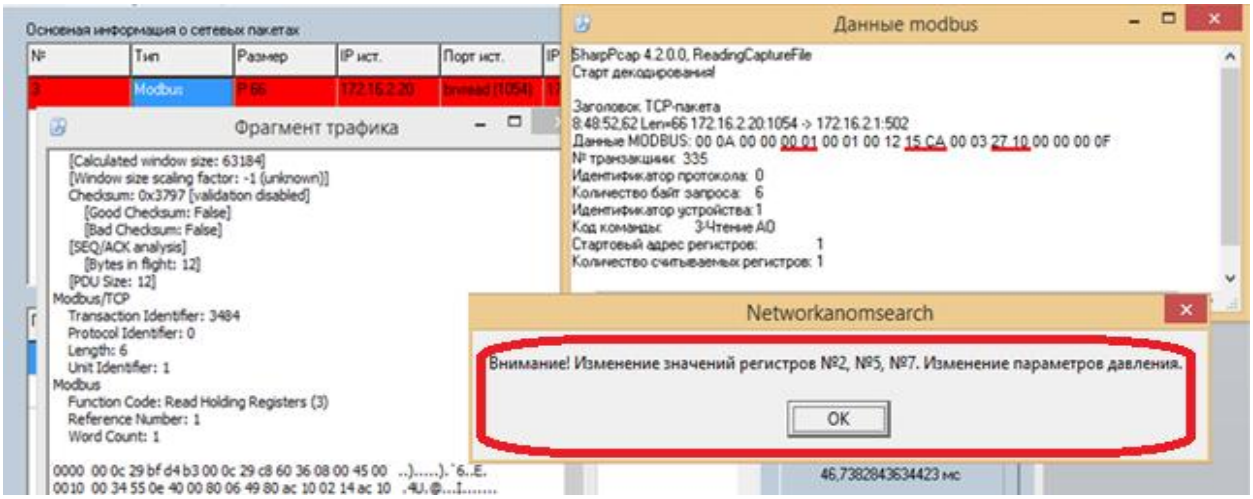


Рисунок 19 – Экранная форма работы программы при обнаружении изменения параметров давления при закрытии задвижки

Экспериментальная оценка эффективности разработанного метода, представленная на рисунке 20, показала высокую оперативность его работы, в сравнении со стандартным методом полного просмотра сетевого потока.

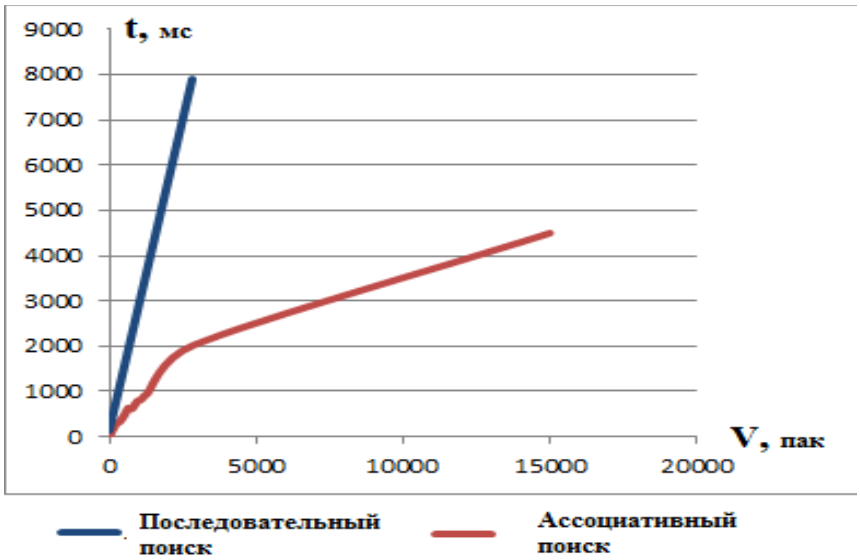


Рисунок 20 – График временных затрат на поиск аномалий в потоке трафика

При анализе полученных результатов можно увидеть, что с увеличением объема трафика время, затрачиваемое на поиск данных с использованием

ассоциативного подхода, значительно меньше, вследствие обращения в каждом случае лишь к конкретному участку памяти, содержащему соответствующие поисковым признакам сигнатуры, в то время как метод полного перебора последовательно анализирует весь поток трафика.

Уже на второй секунде анализа потока прослеживается сокращение времени поиска более чем в 5 раз. Это свидетельствует о значительном повышении эффективности поиска информации в больших объемах трафика при использовании ассоциативного подхода.

Проведенные исследования показали высокую производительность разработанного метода, обусловленную значительным сокращением времени обнаружения аномалий за счет применения ассоциативного подхода. Значительное сокращение времени сбора информации и сигнализирования об инциденте позволяет оперативно реагировать на возникновение аномальной ситуации и принимать решения для ее нейтрализации. Разработанный метод позволяет контролировать техническое состояние объекта, оперативно выявлять и реагировать на инциденты в АСУ ТП.

3.3 Метод прогнозирования временных рядов по данным сетевого трафика на основе полигармонического полинома

Актуальность рассматриваемой задачи определяется необходимостью принятия оперативного достоверного решения в условиях большого объема обработки исходных данных и ограничений на временные ресурсы.

Задачи такого типа часто встречаются при создании различных расчетно-аналитических прогнозирующих систем. Особую актуальность имеет эта задача при разработке стратегии защиты информации в информационных системах АСУ различного назначения, функционирующих в режиме реального времени в условиях воздействия различных угроз. В проведенных авторами исследованиях рассматривались информационные системы мониторинга протяженных

промышленных объектов, в частности, трубопровода по транспортировке нефтепродуктов, компьютерные системы мобильных объектов: автомобилей и летательных аппаратов. Проведенный обзор публикаций по данной теме показал, что, несмотря на достаточно представительный их перечень, проблема повышения производительности средств прогнозирования и ранжирования рисков для рассмотренных объектов информатизации является актуальной [21-34].

При обработке данных, полученных с объектов различной природы, широко используются их спектральные характеристики, получаемые на основе Фурье-преобразования. Это можно объяснить доступной для понимания физической интерпретацией процессов и результатов обработки во многих практически важных случаях, включая их прогнозирование. Решение задачи прогноза, опирается на принцип сохранения закономерностей, выявленных на интервале предыстории и сохранившихся на интервале прогноза. Закономерности, выявленные на основе спектральных составляющих, доступно формулируются и реализуются.

В основу модели прогнозирования рисков $P_{\text{mod}}(t)$ положен полигармонический полином вида [3], дополненный моделями линейной и случайной составляющей [2]:

$$P_{\text{mod}}(t) = a_0 + \sum_{k=1}^{K}(a_k \cdot \cos(2 \cdot \pi \cdot k \cdot \frac{t}{N}) + b_k \cdot \sin(2 \cdot \pi \cdot k \cdot \frac{t}{N})) + d_0 + d_1 \cdot t + c_0 + c_1 \cdot e(t-1);$$

$$a_0 = \frac{\sum_{t=1}^{N} P(t)}{N}; \qquad a_k = \frac{2 \cdot \sum_{t=1}^{N} P(t) \cdot \cos(2 \cdot \pi \cdot k \cdot \frac{t}{N})}{N};$$

$$b_k = \frac{2 \cdot \sum_{t=1}^{N} P(t) \cdot \sin(2 \cdot \pi \cdot k \cdot \frac{t}{N})}{N}; \qquad (3.1)$$

где ***a,b,c,d*** - индексированные коэффициенты модели;

k – номер гармоники из выбранного ряда из ***K*** гармоник;

P(t) – значения временного ряда в дискретный момент времени ***t***;

N – число элементов временного ряда.

Процедура синтеза данной модели реализуется с использованием компьютерной программы до получения случайного остатка, соответствующего критериям случайности, нормальности, критериям Стьюдента и Дарбина-Уотсона.

Апробация модели (1), проведенная на временных рядах развития технологических нарушений на объектах металлургического производства, в частности алюминиевых электролизеров, объектах нефтегазодобычи, при прогнозировании процесса износа долота буровой установки, прогнозировании пожаров, интенсивности вирусных атак в компьютерных сетях - показала результаты, по точности, удовлетворяющие требованиям соответствующих производств и систем. В частности, проверка работы модели при прогнозировании временных рядов активности вирусных атак по ежедневным данным сайта Касперского выявила погрешности прогноза модели с перспективой на неделю не более 15 %.

3.4 Метод ранжирования угроз на основе ассоциативного принципа

В основу модели ранжирования рисков положен принцип ассоциативности значения величины риска $<zR_i>$ от угрозы с индексом $\boldsymbol{i}$ - с порядковым номером ранга этой величины $\boldsymbol{J}$ в ранжированном ряду рисков $\boldsymbol{S}$. В терминах теории распознавания образов процедура определения номера риска $\boldsymbol{Q^*}$ в ранжированном ряду $\boldsymbol{S}$ для исследуемого значения риска $\boldsymbol{q^x}$ описывается следующим образом:

$$Q = \{Q_1, Q_2, \dots, Q_N\};\ D(<zR_i>) = \{d_1, d_2, \dots, d_N\};\ P = \{<zR_i>\};$$
$$KP: q^x \in Q^* \in Q: <zR_i> \in dQ^*,$$
(3.2)

где $\boldsymbol{Q}$, $\boldsymbol{P}$, $\boldsymbol{D}$ и $\boldsymbol{KP}$ – соответственно: множество номеров рангов в ряду $\boldsymbol{S}$, множество признаков распознавания, множество поддиапазонов значений рисков, соответствующих порядковому номеру $\boldsymbol{J}$, и классифицирующее правило.

В соответствии с выражением (3.2) исследуемый образ $\boldsymbol{q}^{x}$ (или же некоторое значение риска $<\boldsymbol{zR_i}>$) относится к классу $\boldsymbol{Q}^{*}$ (или рангу $\boldsymbol{Q}^{*}$) из множества рангов $\boldsymbol{Q}$, если это значение риска $<\boldsymbol{zR_i}>$ входит в диапазон значений, ранжируемых под номером $\boldsymbol{Q}^{*}$.

В процессе идентификации параметра $\boldsymbol{J}$ учитывается, что нескольким значениям рисков, принадлежащих одному диапазону, присваивается один и тот же номер в ряду $\boldsymbol{J}$. В этом случае при определении $\boldsymbol{J}$ учитывается номер по порядку поступления значения риска. Применение ассоциативного принципа позволяет определять ранг риска за один такт времени, синхронный с его поступлением. Метод ранжирования рисков реализован в виде разработанного авторами программного средства, представленного в работах [5].

Программа «Ранжирование рисков от угроз на основе ассоциативного принципа» предназначена для имитационного моделирования и исследования устройства ранжирования рисков. Программа также может найти применение в системах реального времени, где требуется высокая оперативность построения ранжированного ряда. Высокая производительность работы программы обеспечивается применением ассоциативного принципа ранжирования, позволяющего в отличие от известных алгоритмов при поступлении данных по риску одновременно определять ранг этих данных в ранжированном ряду. Основной функцией программы «Ранжирование рисков от угроз на основе ассоциативного принципа» является сортировка рисков по убыванию. Входными данными алгоритма являются количество обрабатываемых рисков, максимальное значение риска и непосредственно оценки рисков. Значения рисков обрабатываются последовательно и на основе ассоциативного принципа их номера размещаются в матрице, имитирующей память. В конце работы алгоритма выводится ранжированный список индексов рисков угроз информации в исследуемой системе представлено на рисунке 21.

Достоинством метода, основанного на разработанных моделях, является высокая производительность, позволяющая в режиме реального времени определять

ранжированный ряд рисков, управлять принятием решений в соответствии с приоритетами угроз.

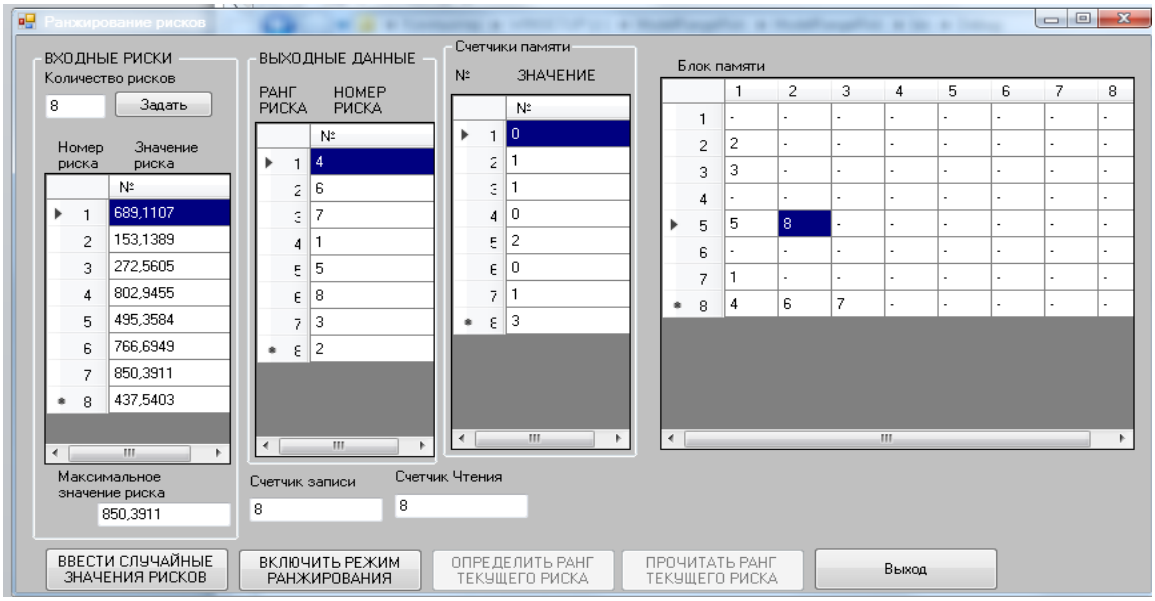


Рисунок 21 – Экранная форма программы ранжирования угроз по величинам их рисков

Программный комплекс, включающий в себя программу ранжирования угроз в совокупности с рассмотренной ранее программой прогнозирования временных рядов на основе полигармонического полинома, позволяет строить динамическую модель угроз объекта информатизации, что обеспечивает оперативный выбор средств защиты информации в условиях изменения пространственно-временных условий эксплуатации системы мониторинга протяженных промышленных объектов.

3.5 Метод выбора базовой функции при автоматизированной идентификации временных рядов сетевого трафика на основе ассоциативно-мажоритарного подхода

В ходе современных научных исследований все чаще возникает необходимость наглядного представления статистического материала о значениях

каких-либо параметров исследуемого процесса. Очень часто такая информация представляется в виде временных рядов, которые могут быть проанализированы и изучены аналитическими и программными способами. Но, такие данные характеризуются сложными зависимостями, которые часто трудны для определения. Примером таких зависимостей могут являться данные интенсивности сетевого трафика, представленные на рисунке 22. Так как подобные зависимости зачастую являются основой для построения прогнозных моделей, возникает необходимость в определении вида функции временного ряда.

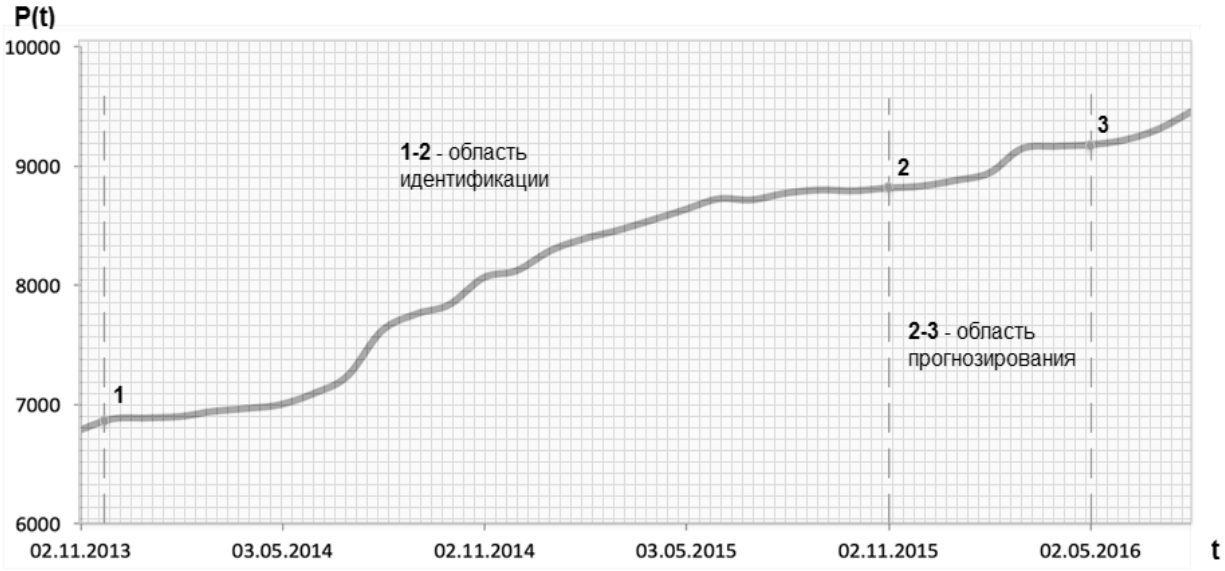


Рисунок 22 – Фрагмент сетевого трафика: t – время, $P(t)$ – функция зависимости интенсивности сетевого трафика от времени

В основе моделирования и прогнозирования большинства динамических процессов лежит операция идентификации базовой функции (БФ), характеризующей основные зависимости в исследуемом процессе. В известной литературе, касающейся методов моделирования и прогнозирования процессов [21, 34, 55, 63, 107, 110], распознавание БФ в большинстве случаев производится либо визуально, либо путем последовательного сравнения с эталонами.

При этом достоверная идентификация БФ занимает значительное количество времени, что является проблемой в случае необходимости быстрой реакции на возникновение нерегламентированной ситуации (например, сетевой атаки), распознаваемой и прогнозируемой с помощью тренда процесса.

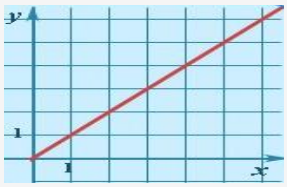
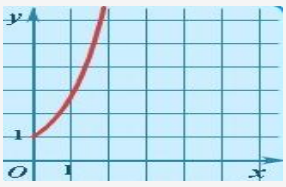
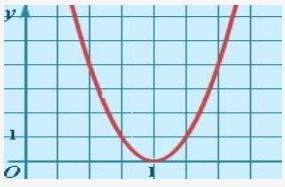
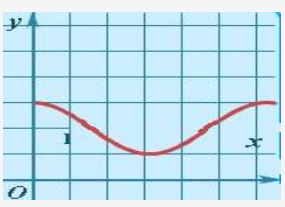
По этой причине автоматизированная идентификация базовых зависимостей является одной из актуальных задач при прогнозировании процессов.

Целью данной работы является автоматизация процесса выбора базовой функции при идентификации временных рядов.

Для достижения данной цели были разработаны: модель распознавания БФ, алгоритм и программное средство, осуществляющее выбор БФ, и исследована программа при работе с реальными данными временных рядов. Для повышения оперативности идентификации в алгоритме выбора БФ использован ассоциативно-мажоритарный подход к хранению и поиску идентификационных данных в электронной памяти. За счет поиска данных по ассоциациям ассоциативный подход увеличивает скорость доступа и сокращает время поиска информации [109].

В основе алгоритма идентификации тренда временного ряда лежит оценка степени соответствия исходного образа временного ряда эталонным образам элементарных базовых функций. Формулы и графики основных элементарных функций, используемых для прогнозирования, представлены в таблице 2.

Таблица 2 – Базовые функции, используемые для прогнозирования

Название и формула функции	**График функции**	**Название и формула функции**	**График функции**
Линейная $y = kx+b$		Показательная $y = e^x$	
Квадратичная $y = a(x-1)^2$		Логарифмическая $y = \log_a x$	
Степенная $y = x^n$		Периодическая $y = cosx+1$	

Задача идентификации БФ, как правило, решается с использованием классической теории распознавания образов. Известны:

– $Q = Q_1, Q_{2,\ldots}, Q_N$ – множество образов (эталонов) базовых функций;

– ***N*** – количество образов БФ;

– ***X*** – множество ассоциативных признаков распознавания $X = \{x_1, x_2, \ldots, x_M\}$, характеризующих исходный временной ряд;

– ***M*** – количество элементов временного ряда;

– $D = \{D_{11}, D_{12}, \ldots, D_{ij}\}$ – диапазон изменения *i*-го признака для *j*-го класса функций, в пределах которого лежат логические значения функций определенного эталона БФ: $D_{ij} = 0,1$;

– ***RP*** – разделяющее правило для идентификации;

– ***RF*** – разделяющая функция идентификации БФ, определяющая меру близости распознаваемого образа с эталоном;

– ***v*** – коэффициент ассоциативности.

Необходимо идентифицировать вид базовой функции исходного временного ряда для получения прогнозных оценок его изменения.

Для проведения идентификации на первом этапе необходимо составить библиотеку эталонов базовых функций (БФ), с каждым из которых будет проводиться сравнение исходного образа. В качестве данных эталонов могут использоваться эталоны одной из элементарных функций, представленных в таблице 2.

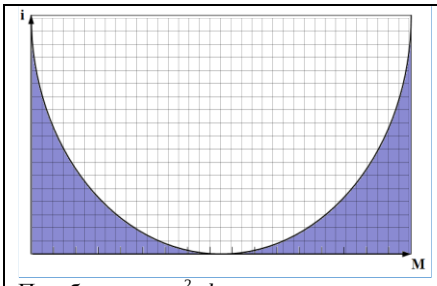
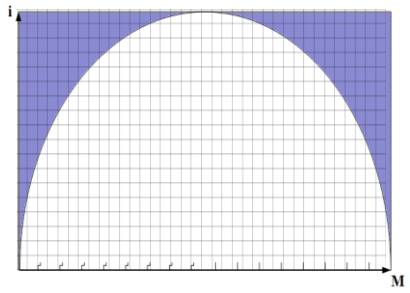
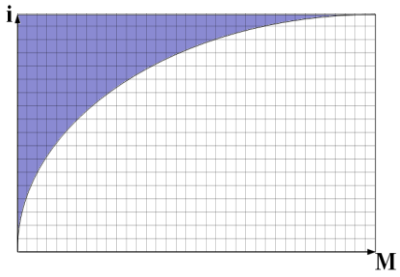
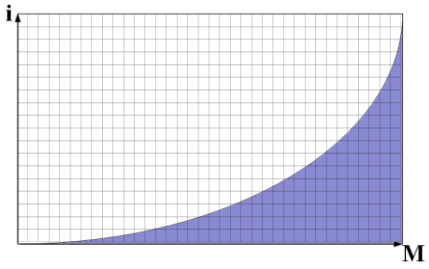
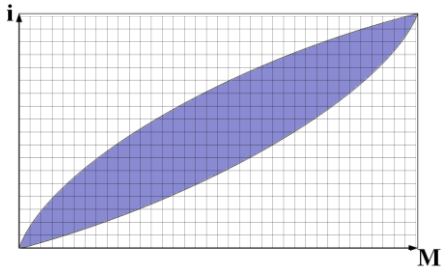
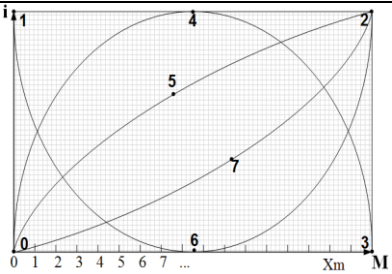
Графическая модель эталона представляет собой квадратную матрицу размерностью ***n*n***, заполняемую единицами в случае присутствия значения исходной функции в конкретной ячейке матрицы эталонов. Диапазоны изменения некоторых видов БФ представлены в таблице 3. Для примера были выбраны линейная, параболическая и экспоненциальная функции.

Все образы БФ хранятся в одном участке памяти, и идентификация того или иного вида функции производится в зависимости от степени нахождения исходного графика функции в диапазоне определенного образа. В правой нижней ячейки

таблицы 3 представлена схема пространства образов и показаны диапазоны нахождения базовых функций в едином пространстве образов: 0-5-2-7-0 – линейной функции, 1-6-2-3-6-0-1 и 0-4-3-2-4-1-0 – параболической и обратной параболической функций, 0-5-2-4-1-0 и 0-7-2-3-6-0 – экспоненциальной и обратной экспоненциальной функции.

Пространство образов представляет собой область памяти устройства, на котором производится идентификация. В качестве ЗУ для хранения эталонов используются микросхемы ассоциативной памяти, в которых в адресных полях записываются координаты каждой из клеток матрицы, а в полях данных значения 1 (в случае заполненной клетки матрицы) или 0 (в случае пустой клетки матрицы).

Таблица 3 – Графические образы БФ

 Парабола $y = ax^2+bx+c$	 Обратная парабола $y = -ax^2+bx+c$	 Экспонента $y = e^x$
 Обратная степенная $y = e^{-x}$	 Линейная $y = kx+b$	 Схема пространства образов БФ

Для распознавания подается неизвестный образ $\boldsymbol{q}^{\boldsymbol{x}}$, для удобства распознавания предварительно масштабированный в соответствии с размерами пространства образов, и сравнивается с хранящимися в нем образами.

В результате сравнения исходного тренда временного ряда с эталонами в пространстве образов определяется процентное соотношение вероятности совпадения с каждой базовой функцией по числу ассоциаций (единиц в матрицах). Вид функции исходного временного ряда определяется по полученным процентным

соотношениям: если значение вероятности совпадения по конкретному виду БФ наибольшее – данному виду и принадлежит исходная функция.

В предложенной модели идентификации вида БФ используется разделяющая функция (3.3), позволяющая оценить степень соответствия исходного образа с эталонными образами базовых функций. Задача распознавания ставится следующим образом: необходимо идентифицировать неизвестный образ функции $\boldsymbol{q}^x$, отнеся его к одному из известных эталонов $\boldsymbol{Q}^x$ множества образов $\boldsymbol{Q}$.

$$RP: q^x \in Q^x \in Q;$$
$$RF^* \equiv RF_{max}\ RF\ ; \qquad (3.3)$$
$$RF_i = \sum_{j=1}^{M} v_{ij}, \qquad v_{ij} = \begin{matrix} 1, \text{если } x_j \in d_{ij} \\ 0, \text{если } x_j \notin d_{ij} \end{matrix};$$

Вид базовой функции ***RF**** определяется по наибольшему числу соответствий значений $\boldsymbol{RF}_{\mathbf{max}}$ исходного образа со значениями диапазона определенного эталона *D*.

Функциональная схема модели распознавания на основе ассоциативно-мажоритарного подхода представлена на рисунке 23.

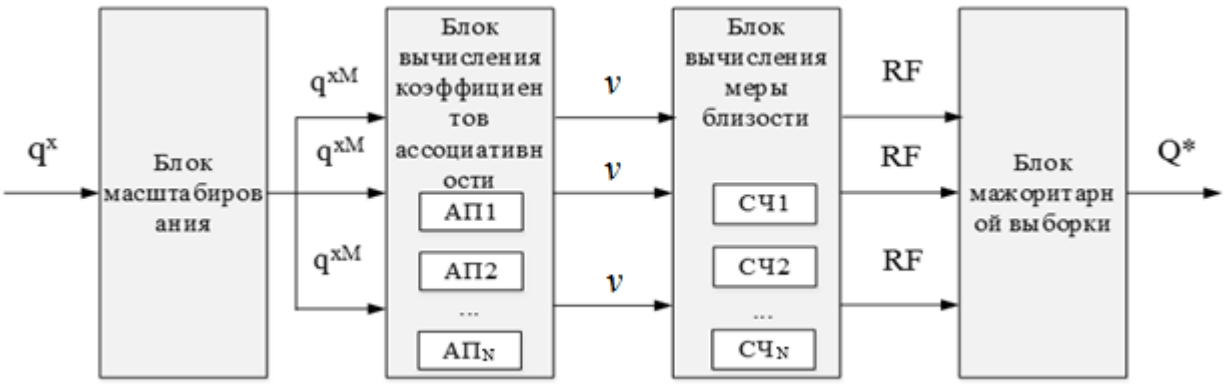


Рисунок 23 – Функциональная схема модели распознавания на основе ассоциативно-мажоритарного подхода

На вход устройства подается исходный идентифицируемый образ $\boldsymbol{q}^x$. Для реализации предложенного алгоритма используется сглаженный ряд данных

исходной функции, то есть линия тренда функции. Ввиду неограниченности размеров временных рядов исходный образ масштабируется в соответствии с размерностью пространства эталонов ($\boldsymbol{q}^{xM}$), после чего сравнивается с каждым из эталонов в ассоциативных ЗУ (АП). В результате сравнения этих двух образов счетчиком (СЧ) подсчитывается суммарное значение совпадений (ассоциаций) между исходным образом и эталоном, после чего определяет вид идентифицируемой функции $\boldsymbol{Q}^*$. Блок мажоритарной выборки производит идентификацию исходного образа по большинству ассоциаций исходного образа с эталонами. Критерий выбора базовой функции основан на мере близости Хемминга.

Особенностью предложенной модели является оперативность сравнения исходных образов с образами эталонов за счет использования единого признакового пространства и возможности сравнения всех образов за один такт.

Для исследования работы предложенного алгоритма идентификации было разработано программное средство, осуществляющее выбор базовой функции при идентификации временных рядов на основе ассоциативно-мажоритарного подхода.

Исходными данными для работы прикладной программы являются: зарегистрированный временной ряд, образы базовых функций (БФ) эталонов трендов, представленные в матричной форме. Для проведения идентификации используется библиотека эталонов базовых функций. В качестве примеров выбраны линейная, параболическая и экспоненциальная функции.

При загрузке исходного образа (файла данных временного ряда) для корректной работы программы производится масштабирование исходных данных в требуемом диапазоне. Далее производится сглаживание графика функции с целью получения тренда. Полученный тренд переводится в матричную форму для последующего сравнения с эталонами базовых функций. Матрица тренда имеет размерность 100×100 и заполняется единицами в зависимости от формы тренда.

Результатом выполнения программы является вывод о принадлежности функции временного ряда одному из эталонных образов, с указанием оценки вероятности принадлежности к каждому образцу. После сравнения матрицы исходного тренда сетевого трафика и матриц базовых функций эталонов на форме

отображается процентное соотношение вероятности совпадения с каждой базовой функцией. В качестве условия достоверности идентификации функции принят порог совпадения более чем на 50 %. Экранная форма работы программы представлена на рисунке 24.

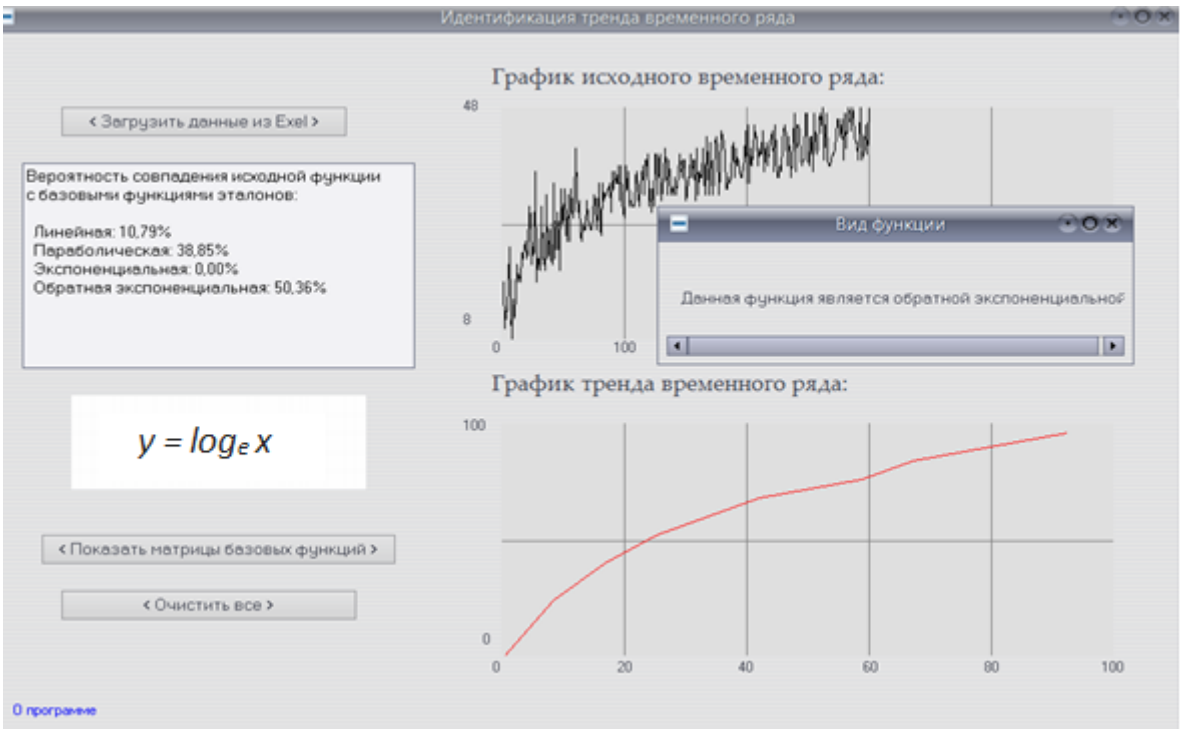


Рисунок 24 - Экранная форма программы идентификации БФ

Достоинствами разработанной программы являются: оперативность распознавания исходной функции временного ряда за счет автоматизации процесса идентификации и достоверность распознавания вида базовой функции за счет подсчета процентного соотношения исходной функции временного ряда с базовыми функциями эталонов. Прикладная программа также может быть использована в учебном процессе при проведении лабораторных работ, связанных с моделированием и прогнозированием динамических процессов.

Предложенный алгоритм и программное средство являются универсальными, так как позволяют идентифицировать вид базовой зависимости в любом динамическом процессе, независимо от специфики исследуемой предметной области. Автоматизированная идентификация вида БФ позволит оперативно прогнозировать дальнейшие варианты протекания процесса.

3.6 Метод контроля поведения пользователя на основе мониторинга информационных потоков сетевого трафика

3.6.1 Разработка алгоритма контроля поведения пользователя на основе мониторинга информационных потоков сетевого трафика

Система контроля поведения пользователя - программный или аппаратный комплекс, позволяющий отслеживать действия пользователя. Такая система осуществляет мониторинг рабочих операций пользователя на предмет их соответствия политике безопасности.

В основу разработанного метода контроля поведения пользователя положена ассоциативная модель, представленная в пункте 2.2 работы.

К исходным данным задачи контроля поведения пользователя отнесены:

- множество $\boldsymbol{Q}$ контролируемых транзакций, выполняемых пользователем: $\boldsymbol{Q} = \{q_1, q_2, \ldots, q_j, \ldots q_N\}$;
- множество $\boldsymbol{P}$ информативных признаков: $\boldsymbol{P} = \{p_1, p_2, \ldots, p_i, \ldots p_M\}$;
- код транзакции $\boldsymbol{K}$;
- номер операции в транзакции $\boldsymbol{NO}$,
- код операции транзакции $\boldsymbol{KOT}$.

Математическая модель мониторинга поведения пользователя описывает процедуру контроля действий пользователя, представляемую параметрами: ***K, NO, KOT*** в конкретный момент времени ***t.***

При этом совокупный признак ***P(t)*** имеет следующий вид:

$$\boldsymbol{P(t)=(K\_NO\_KOT)_t}\,.$$

В каждый момент времени *t* совокупный признак ассоциируется (≡) с кодом соответствующей легитимной (правомерной) операции $\boldsymbol{<KOT>_t}$, хранящейся в ассоциативной памяти (АП):

$$(K\_NO\_KOT)_t \equiv <KOT>_t$$

В случае отсутствия ассоциации производится запрет на ввод следующей операции.

Технически контроль поведения реализуется подачей совокупного кода на адресные входы блока ассоциативной памяти. При наличии ассоциации с выходов АП поступает код легитимной операции *KLO*, который сравнивается с кодом операции *KOT*, набираемым пользователем. При равенстве *KLO=KOT* санкционируется ввод следующего совокупного признака *P(t+1)*. После выполнения всех операций транзакции режим контроля завершается. Процесс контроля поведения пользователя для наглядности целесообразно представить в виде схемы алгоритма, которая представлена на рисунке 25.

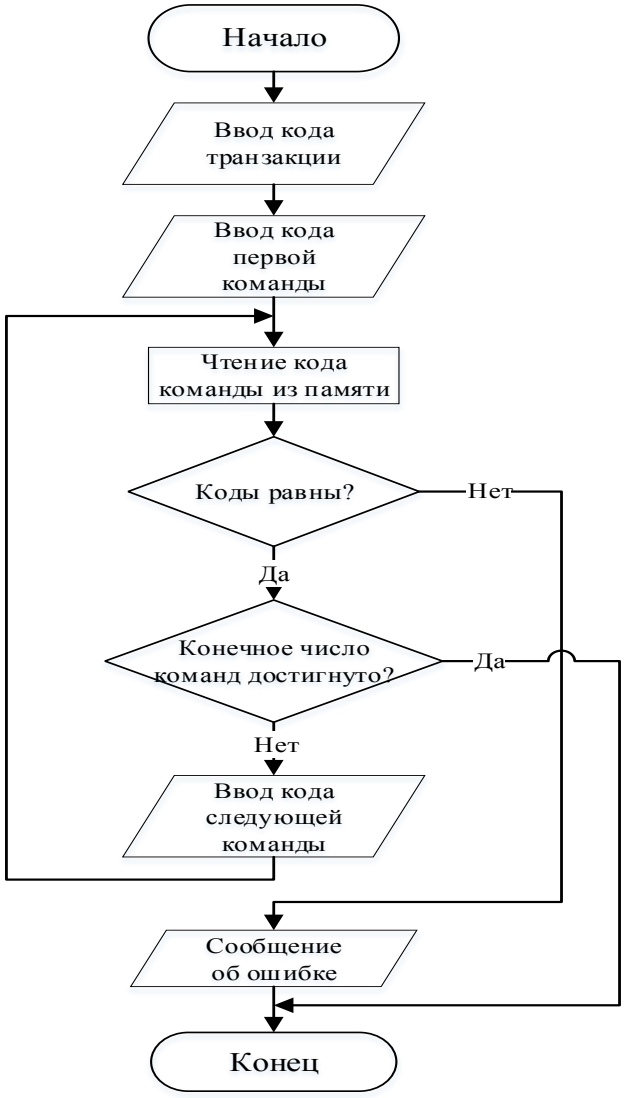


Рисунок 25 – Схема алгоритма контроля поведения пользователя

Как показано на рисунке 25, вначале осуществляется ввод пользователем кода транзакции и кода первой команды этой транзакции. Затем производится чтение соответствующего кода команды из блока памяти, который сравнивается к кодом введенной команды пользователя. При несовпадении кодов процедура контроля завершается. При совпадении кодов проверяется, достигнуто ли конечное число команд транзакции. Если достигнуто, то процедура контроля завершается успешно. Если нет, то происходит ввод пользователем последующих кодов команд транзакции и их сравнение с соответствующими кодами команд из памяти, пока не будет достигнуто конечное число команд транзакции.

3.6.2 Разработка аппаратно-программного обеспечения метода контроля поведения пользователя на основе мониторинга информационных потоков сетевого трафика

В рамках исследования, на основании разработанной математической модели и алгоритма контроля, было разработано аппаратное средство для реализации метода контроля поведения пользователя [75].

Изобретение относится к автоматике и вычислительной технике и предназначено для контроля управляющих действий пользователя в вычислительных системах.

Техническим результатом настоящего изобретения является повышение уровня универсальности устройства.

Устройство для контроля предназначено для использования в системах защиты информации, в частности, для защиты ее от несанкционированного доступа на основе контроля действий пользователя.

Недостатком устройства-прототипа является недостаточная универсальность, связанная с отсутствием возможности распознавания и анализа поведения объекта, как взаимосвязанной последовательности образов, а также с отсутствием возможности процедуры обучения пользователя при выполнении требуемой последовательности операций.

На рисунке 26 представлена структурная схема предлагаемого устройства.

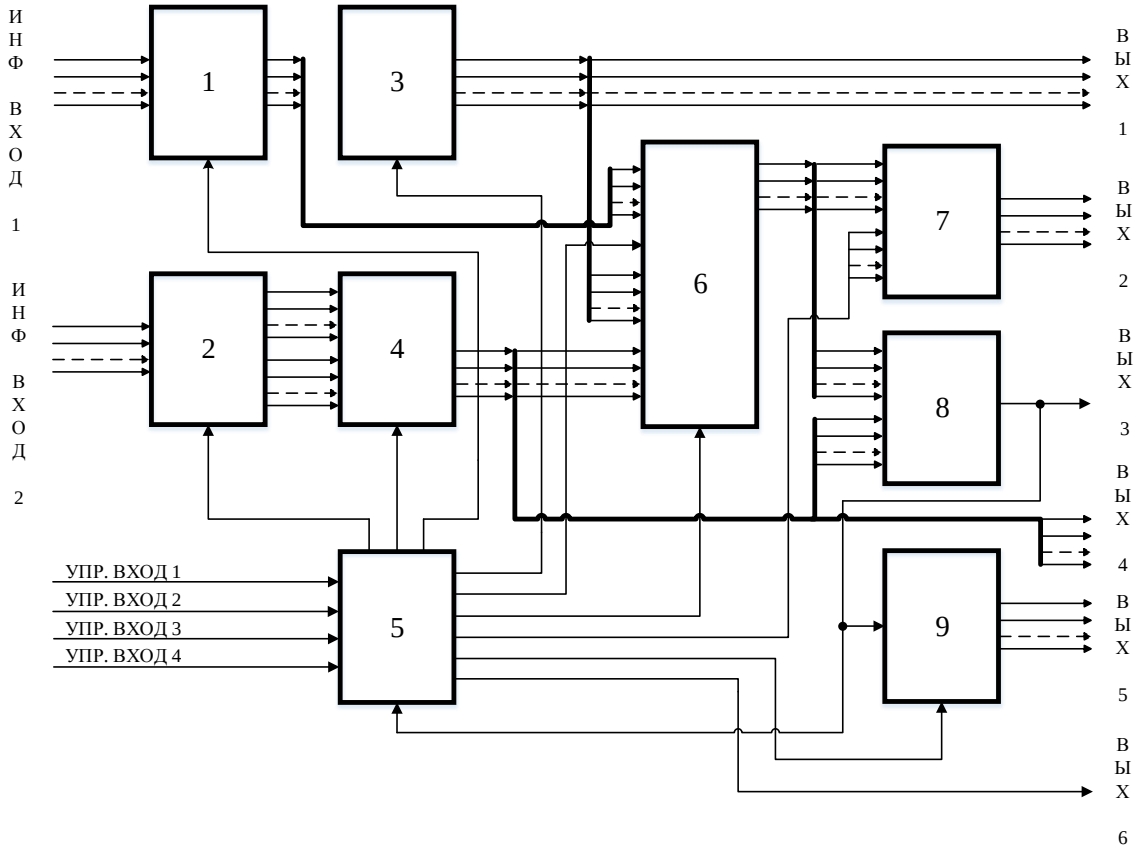


Рисунок 26 – Структурная схема устройства для контроля поведения пользователя

Цифрами на схеме обозначены: 1 – регистр кода транзакции, 2 – блок сдвиговых регистров; 3 – счетчик адресов; 4 – многоканальный коммутатор; 5 – блок управления; 6 – блок памяти; 7 – блок логических элементов И; 8 – схема сравнения; 9 – сдвиговый регистр результатов сравнения.

Устройство для контроля поведения пользователя функционирует в трех режимах:

- режим контроля поведения пользователя;
- режим анализа поведения;
- режим обучения.

В режиме контроля на входы устройства подается код транзакции и код команды. В блоке памяти, при этом, содержится информация, соответствующая санкционированной последовательности команд. При этом код каждой команды,

поданной пользователем, инициирует чтение соответствующего кода из блока памяти. После чего на вход блока сравнения поступает код первой команды пользователя и контрольные коды этой команды из блока памяти. При неравенстве этих кодов режим контроля завершается. При равенстве кодов разрешается ввод последующей команды и по достижении конечного числа команд режим контроля завершается.

Инициализация режима анализа осуществляется путем подачи команды на соответствующий управляющий вход устройства. Режим анализа поведения пользователя предназначен для выявления характера ошибок в поведении пользователя при выполнении транзакции. Режим анализа поведения работает аналогично режиму контроля за исключением того, что при возникновении ошибки ввод команд пользователем продолжается. Код корректности команд фиксируется в сдвиговом регистре результатов сравнения, и по достижении конечного числа команд режим анализа завершается.

Режим обучения предназначен для ознакомления пользователя с составом команд транзакции и порядком их задания. Исходное состояние устройства в режиме обучения соответствует конечному состоянию его в режиме анализа. Ознакомление с командами транзакции осуществляется путем считывания контрольных команд из блока памяти независимо от кодов, сформированных в адресной части блока памяти.

Адресный код блока памяти состоит из 4 групп двоичных разрядов: A, B, C и D. Первая адресная группа A содержит код транзакции. Она определяет содержание блока памяти для конкретной транзакции. Код B – одноразрядный, он представляет вторую адресную группу и определяет содержание блока памяти для конкретного режима работы устройства, причем значение разряда равно единице, если устройство работает в режиме контроля и анализа. Значение разряда равно нулю, если устройство работает в режиме обучения. Группа C определяет номер операции в транзакции, а группа D – код операции транзакции, вводимой пользователем.

В качестве примера заполнения блока памяти была взята последовательность действий, совершаемых оператором при управлении паровыми котлами, а именно:

- открыть задвижку газа;
- открыть задвижку воды;
- установить значение давления в 2.3 атм;
- установить значение температуры в 70 градусов.

Выбранная транзакция вместе с кодами показана в таблице 4.

Таблица 4 – Коды команд транзакции

Номер по порядку	1	2	3	4
Обозначение команды	Откр/газ	Откр/вода	P=2.3	T=70
Код команды	0 0 1	0 1 0	0 1 1	1 0 0

В таблице 5 представлено содержимое блока памяти в режиме контроля без ошибок. Достоинством предлагаемого устройства также является возможность контроля содержимого памяти, самого устройства со стороны администратора системы контроля, когда он по специальной проверочной процедуре по гарантированно корректным командам транзакции инспектирует работу самого устройства.

Таблица 5 – Содержимое блока памяти в режиме контроля без ошибок

№ строки	Адресная часть										Данные			Корректность	Команда
	A			B	C			D			E			F	G
0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	не исп.
1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	Откр/газ
2	0	0	1	1	0	1	0	0	1	0	0	1	0	0	Откр/вода
3	0	0	1	1	0	1	1	0	1	1	0	1	1	0	P=2.3
4	0	0	1	1	1	0	0	1	0	0	1	0	0	0	T=70

Устройство может быть реализовано на доступной элементной базе электронных микросхем.

3.6.3 Разработка программного эмулятора контроля поведения пользователя

Прикладная программа «Эмулятор устройства для контроля поведения пользователя» ориентирована на использование в системах защиты информации, в частности, для защиты информации от несанкционированного доступа и учета действий пользователя в компьютерной системе [57, 89].

Разработанное программное средство осуществляет контроль вводимых пользователем команд путем их сравнения с эталонными командами, хранящимися в базе транзакций, а также производит обучение пользователя путем его ознакомления с составом команд транзакции и порядком их задания.

Актуальность разработки программы определяется двумя факторами:

- необходимостью снижения риска от несанкционированных действий пользователя в компьютерной системе;
- необходимостью эмуляции (моделирования) работы средства контроля проведения пользователя, выполненного в виде аппаратного устройства, что позволяет исследовать более детально режимы его функционирования.

Программа позволяет повысить оперативность контроля и принятия решений в задачах распознавания аномального поведения пользователя в компьютерной системе.

Программа работает в трех режимах: режим контроля, анализа и обучения.

На начальном этапе задается номер транзакции и режим работы устройства. Например, выбирается режим «Контроль».

Далее необходимо осуществить ввод первой команды транзакции 1 в поле «Входной сигнал» и нажать кнопку «Отправить. В случае правильного ввода всех команд транзакции режим контроля завершается.

Для работы с программой в режиме анализа необходимо ввести всю последовательность команд транзакции. При этом в окне «Сдвиговый регистр результатов сравнения» можно наблюдать код корректности ввода последовательности команд, где 1 – команда введена верно; 0 – ошибка при вводе команды.

В режиме «Обучение» необходимо выбрать транзакцию, команды которой нужно узнать. Затем необходимо нажать кнопку «Отправить». Во всплывающем окне будет отображаться правильная команда выбранной транзакции.

Общий вид экранной формы программы «Эмулятор устройства для контроля поведения пользователя» представлен на рисунке 27.

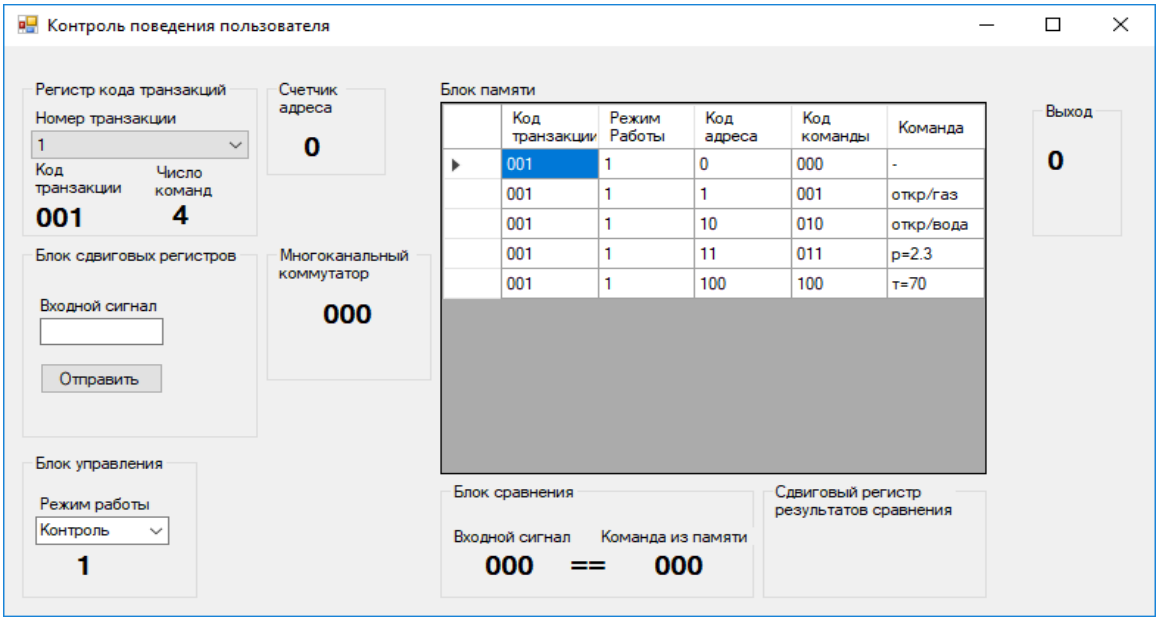


Рисунок 27 – Экранная форма главного окна программы

При вводе неверной команды возникает ошибка, и режим контроля прекращается, как показано на рисунке 28 [89].

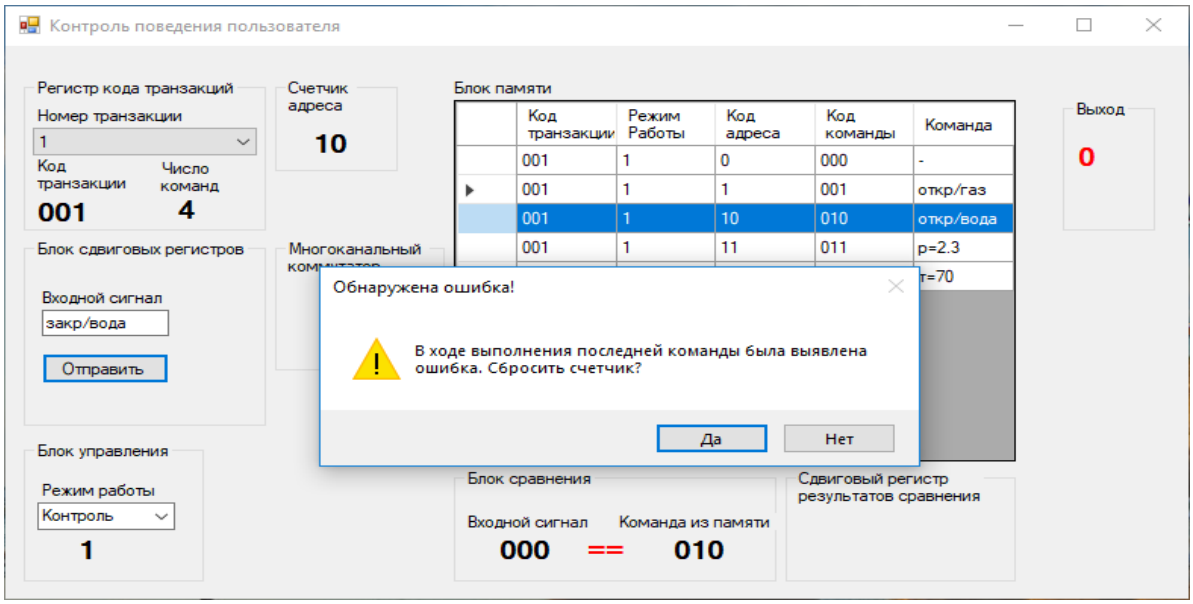


Рисунок 28 – Ошибка при вводе команды в режиме «Контроль»

Результат работы программы в режиме анализа представлен на рисунке 29.

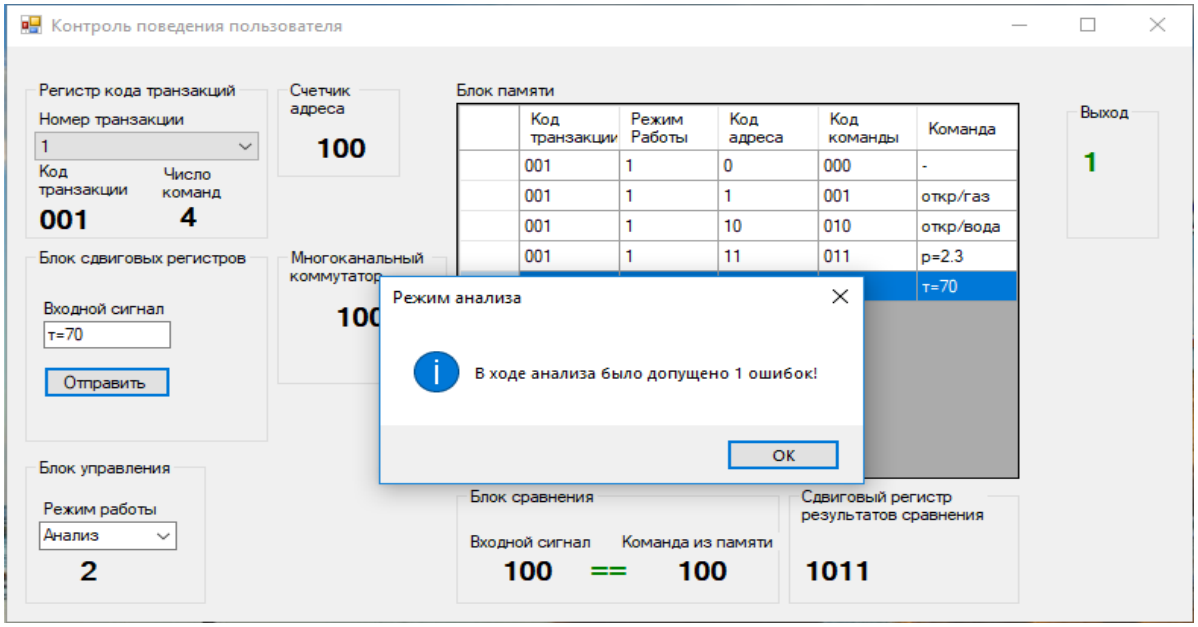


Рисунок 29 – Результат работы программы в режиме «Анализ»

Пример работы программы в режиме «Обучение» представлен на рисунке 30. [89].

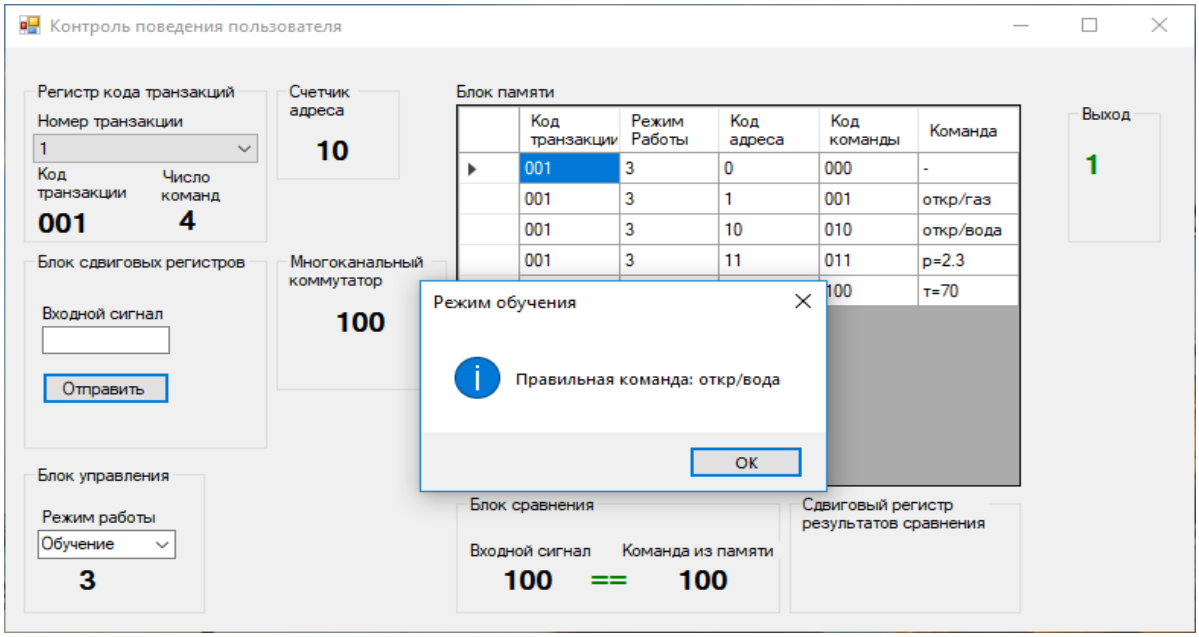


Рисунок 30 – Пример работы программы в режиме «Обучение»

По достижении конечного числа команд транзакции режим обучения завершается, о чем пользователя уведомляет соответствующее сообщение.

3.6.4 Исследование метода контроля поведения пользователя на примере системы управления режимами работы паровых котлов

Разрабатываемый метод контроля поведения пользователя может быть применен в автоматизированных системах управления технологическими процессами, где в качестве пользователя выступает оператор АСУ ТП.

Рассмотрим применение метода на примере автоматизированной системы управления паровыми котлами. В процессе управления оператор совершает определенные действия (открытие и закрытие задвижек, изменение значений давления газа и температуры воды).

Для моделирования системы управления паровыми котлами был использован программный комплекс SCADA Trace Mode 6. [6, 84, 116]. На рисунке 31 представлена мнемосхема системы управления паровыми котлами.

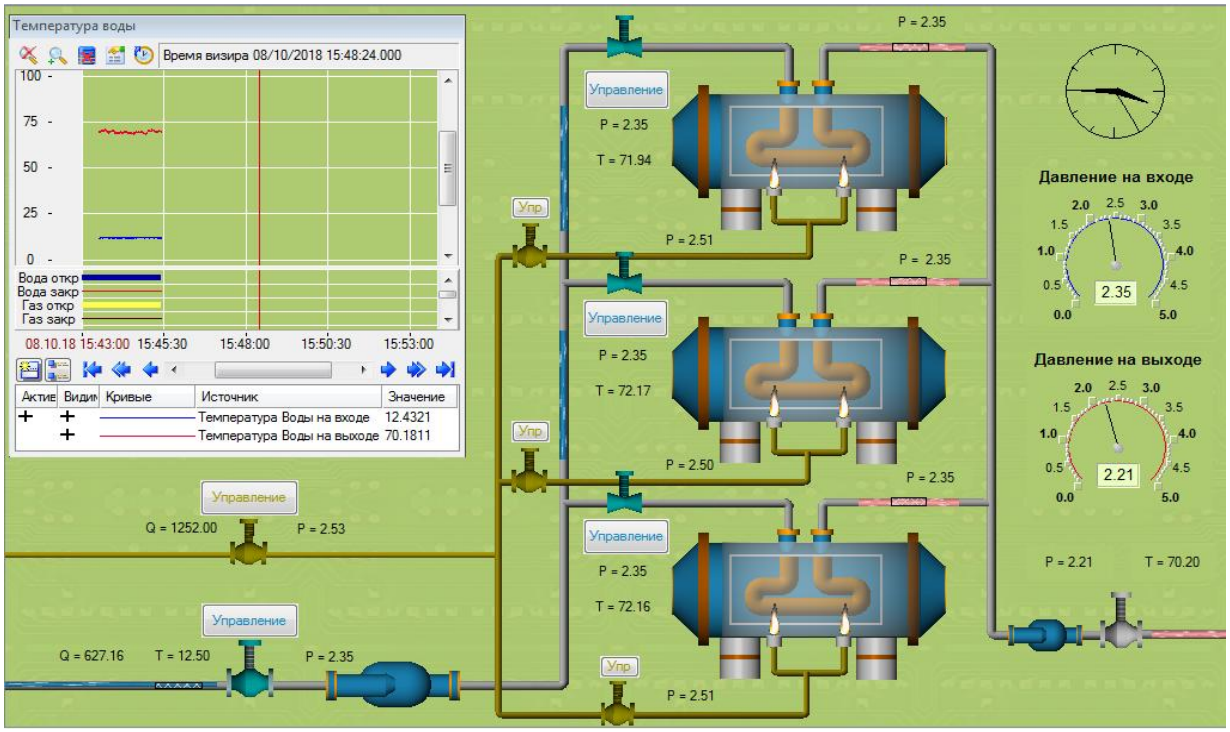


Рисунок 31 – Мнемосхема системы управления паровыми котлами

Как видно из рисунка 31, оператор осуществляет управление состоянием задвижек воды и газа, а также изменение значений параметров, таких как давление и температура нагрева воды.

Для проведения эксперимента два компьютера были соединены по локальной сети. На одном из компьютеров оператор совершал управление задвижками и изменение значений параметров, при этом все изменения отображались на мнемосхеме, отражаемой на другом компьютере. В процессе моделирования информационные процессы между компьютерами отражались и регистрировались в сетевой трафике в виде сетевых пакетов с использованием программы Wireshark [61].

В результате имитационного моделирования был получен сетевой трафик, представленный на рисунке 32.

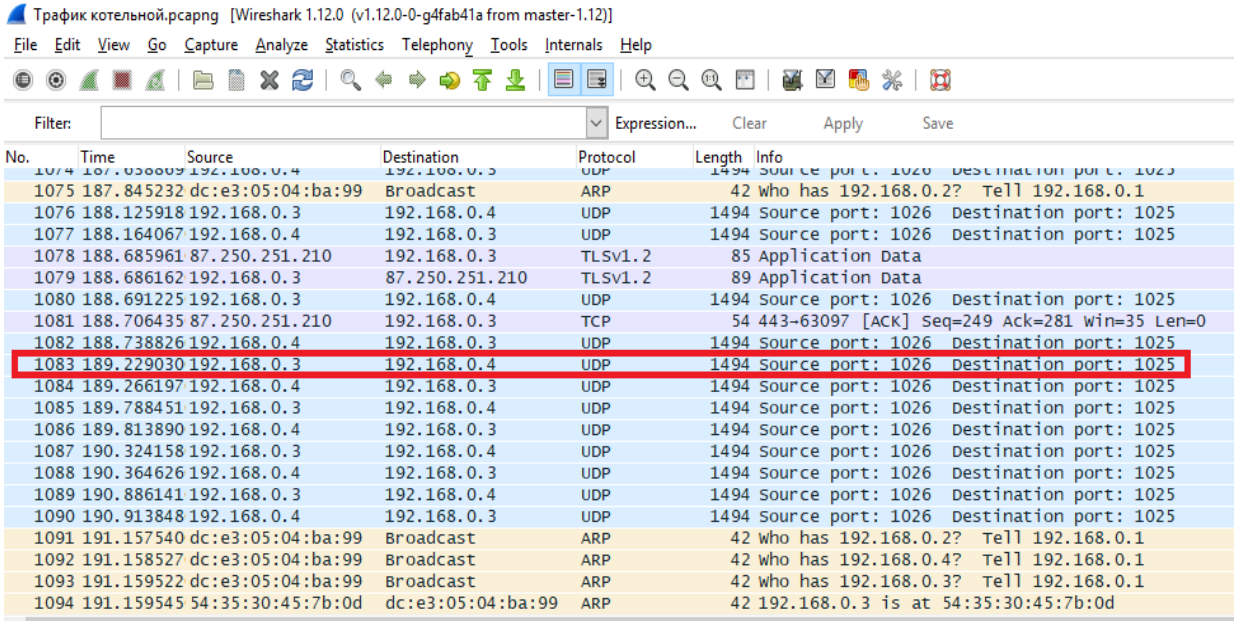


Рисунок 32 – Сетевой трафик при сканировании локальной сети

IP-адреса компьютеров локальной сети имеют следующий вид: 192.168.0.3 и 192.168.0.4, поэтому исследовались пакеты только между этими IP-адресами. Выберем сетевой пакет, который обозначен на рисунке 8, и выделим из него

признаки, по которым будем определять правомерность того ли иного сетевого пакета:

– IP-адрес компьютера, с которого происходит управление паровыми котлами: 192.168.0.3;

– IP-адрес компьютера, на котором запущена программа индикации мнемосхемы паровых котлов: 192.168.0.4;

– протокол, по которому происходит передача между ПК: UDP;

– длина пакета: 1494;

– порт источника: 1026;

– порт назначения: 1025.

Таким образом, была сформирована транзакция, которая определяет правомерный сетевой пакет, передаваемый по сети при управлении паровыми котлами. Параметры транзакции представлены в таблице 6.

Таблица 6 – Исследуемая транзакция

Команда 1	Команда 2	Команда 3	Команда 4	Команда 5	Команда 6
192.168.0.3	192.168.0.4	UDP	1494	1026	1025

Процесс контроля действий оператора по выбранной транзакции представлен в виде алгоритма на рисунке 33.

Воспользуемся программным эмулятором устройства для контроля поведения пользователя и проверим его работоспособность на примере определения правомерности того или иного сетевого пакета, передаваемого по сети при управлении паровыми котлами.

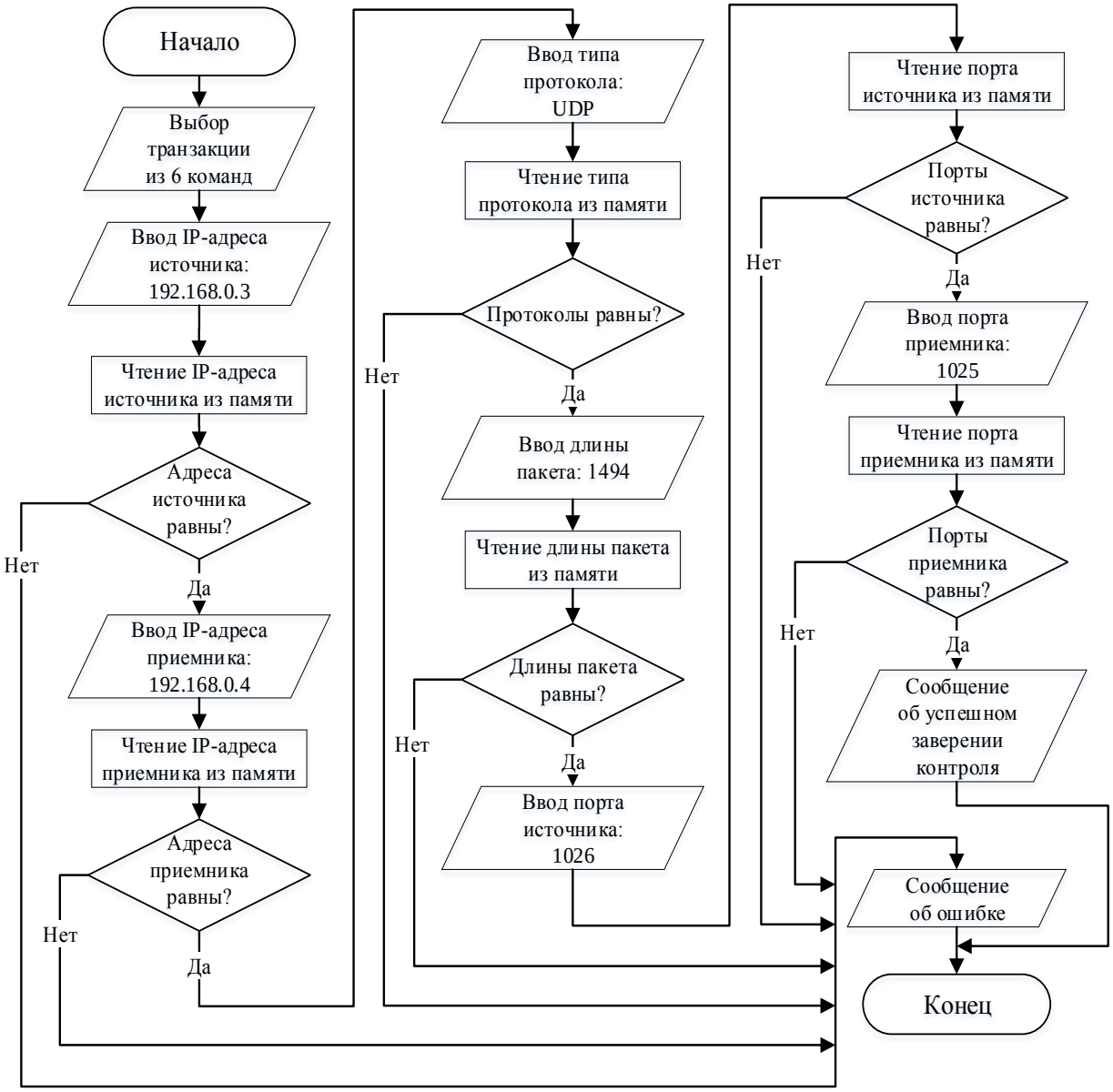


Рисунок 33 – Схема алгоритма контроля поведения оператора по выбранной транзакции

Для этого исследуемая транзакция была внесена в базу транзакций программы «Эмулятор устройства для контроля поведения пользователя».

На рисунке 34 представлен процесс ввода команд транзакции в режиме контроля.

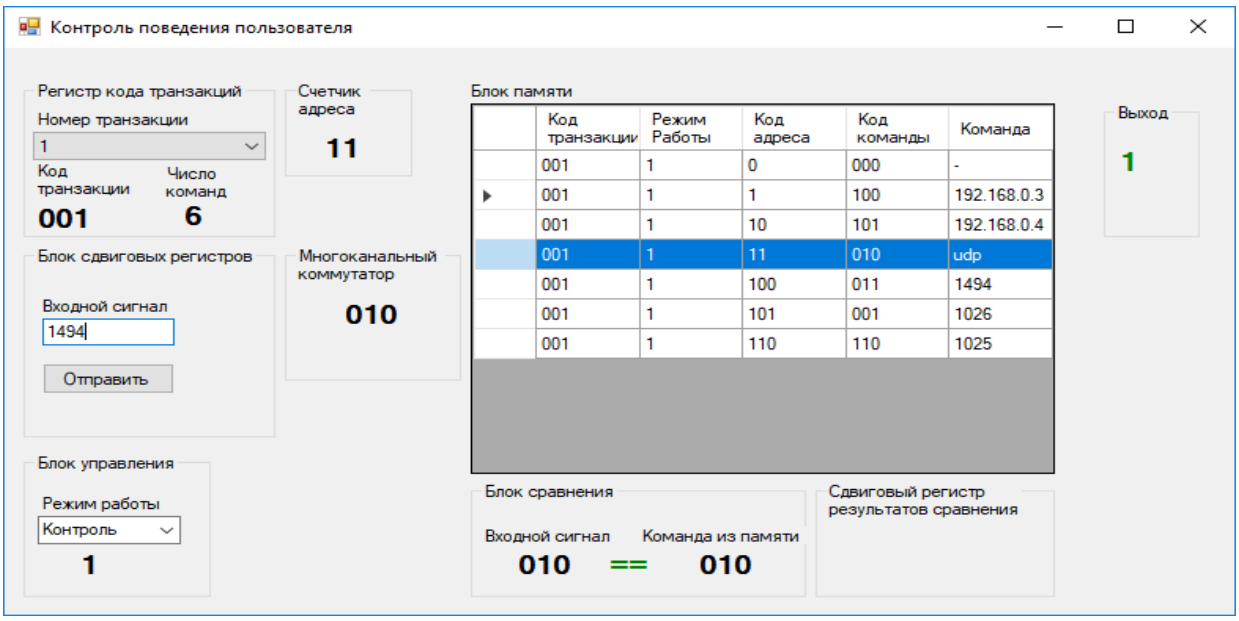


Рисунок 34 – Экранная форма работы программы в режиме контроля

Намеренно введем неправильную длину пакета, в результате чего режим контроля завершится, как показано на рисунке 35.

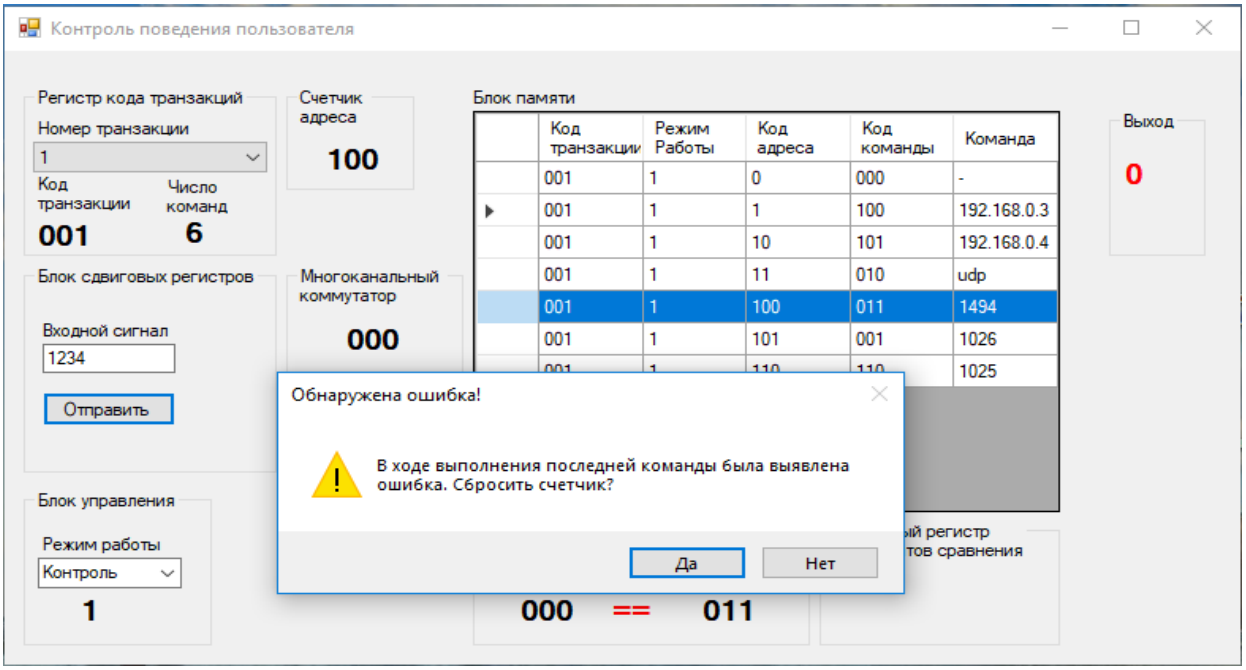


Рисунок 35 – Экранная форма режима обнаружения ошибки при вводе длины пакета

Таким образом, любой сетевой пакет, который отличается от эталонного, хранящегося в базе транзакций, будет считаться несанкционированным.

3.6.5 Оценка эффективности и рекомендации по применению метода контроля поведения пользователя в АСУ нефтепроводом

Разрабатываемый метод контроля поведения пользователя также применим в автоматизированной системе управления нефтепроводом.

Рассмотрим мнемосхему нефтепровода, построенную в Trace Mode 6 [6, 84], которая представлена на рисунке 36.

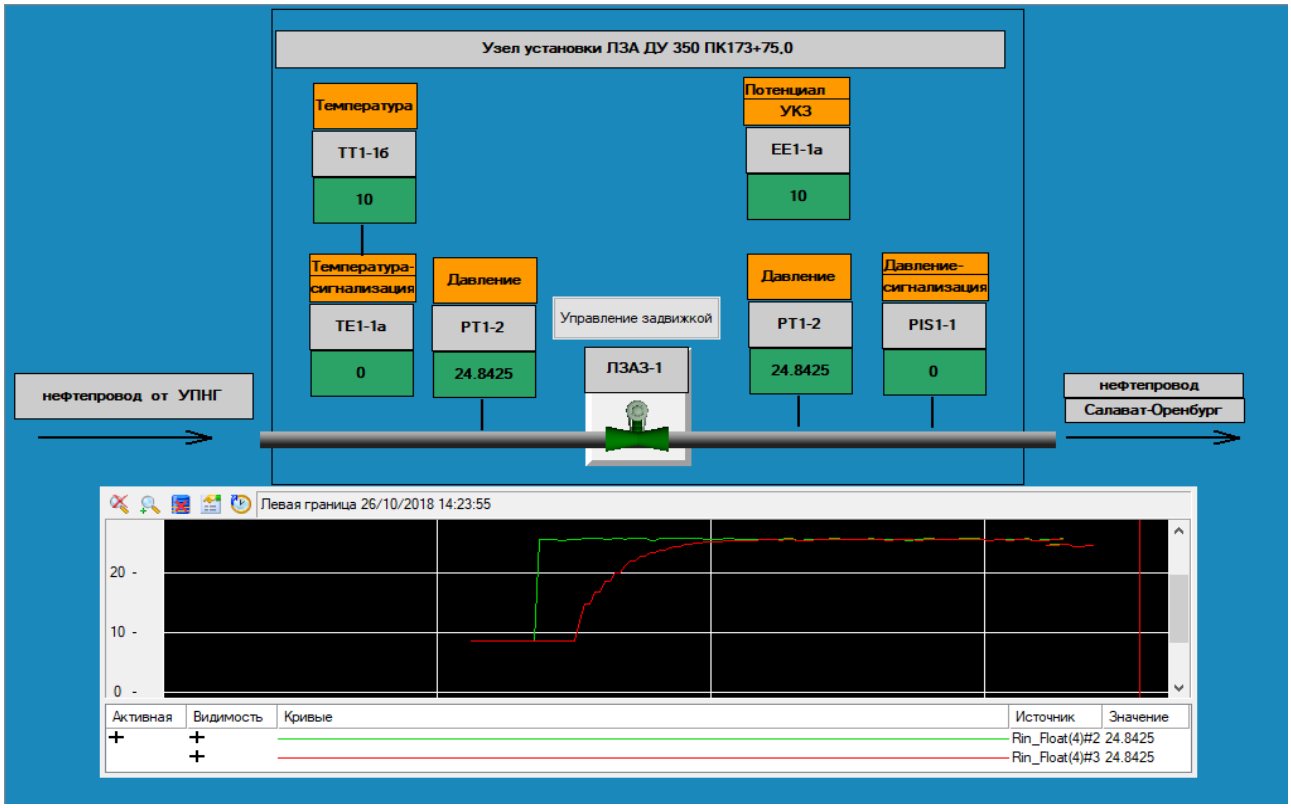


Рисунок 36 – Мнемосхема нефтепровода в SCADA Trace Mode 6

На рисунке 37 представлена экранная форма главного окна программы, эмулирующей работу автоматизированного рабочего места (АРМ) оператора.

Управление нефтепроводом осуществляется по протоколу Modbus/TCP [78] с АРМ оператора путем открытия/закрытия задвижки, изменения значения давления на входе. Для проведения эксперимента было использовано два компьютера, подключенных к одной сети.

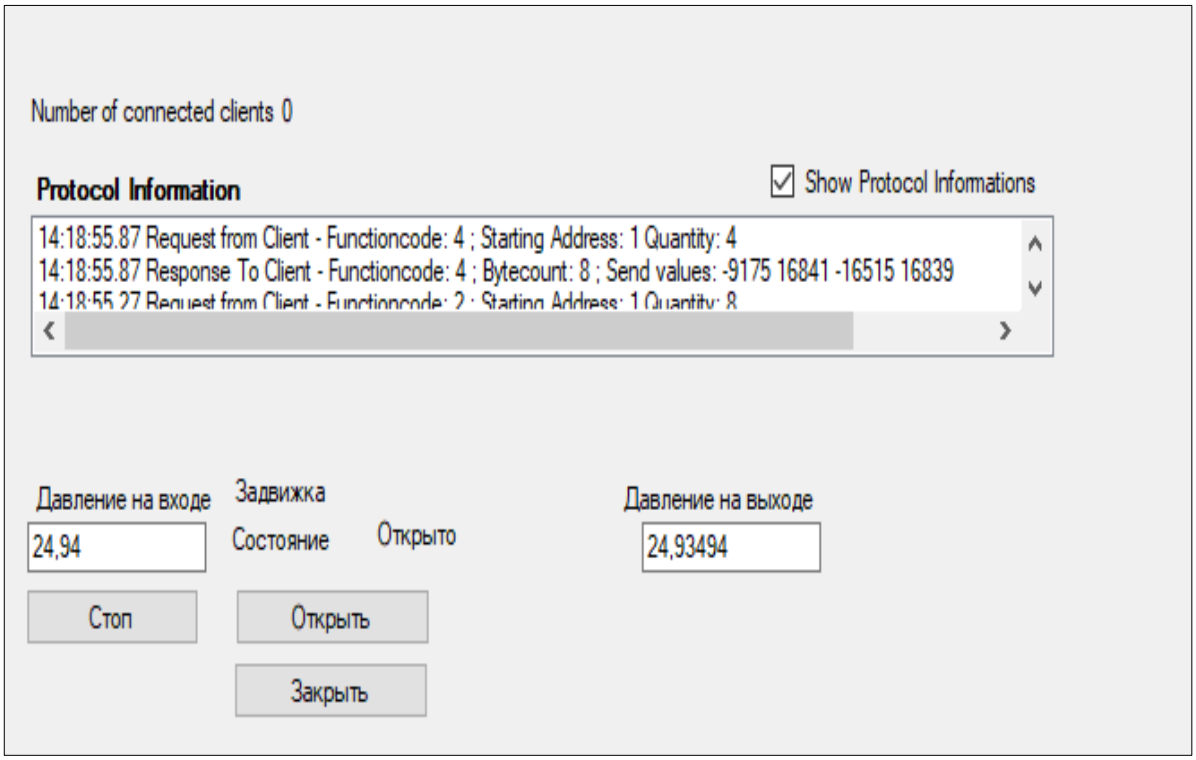


Рисунок 37 – Экранная форма программы АРМ оператора

На одном через Trace Mode запущена программа имитации мнемосхемы нефтепровода, на другом – управляющая программа АРМ оператора.

Управление состоянием задвижки осуществляется кнопками «Открыть» и «Закрыть». При открытии задвижки осуществляется процесс перекачки нефти. При этом задается режим, при котором давление в трубопроводе, заданное на входе, должно равняться давлению на выходе. Все управляющие действия, совершаемые оператором, отображаются в сетевом трафике. В окне «Protocol Information» отображается основная информация о сетевых пакетах, передаваемых по протоколу Modbus/TCP.

В ходе эксперимента была использована программа захвата сетевого трафика Wireshark и получен сетевой трафик, передаваемый при управлении нефтепроводом.

Рассмотрим пакет запроса, представленный на рисунке 38, на чтение входных регистров с управляющего контроллера нижнего уровня.

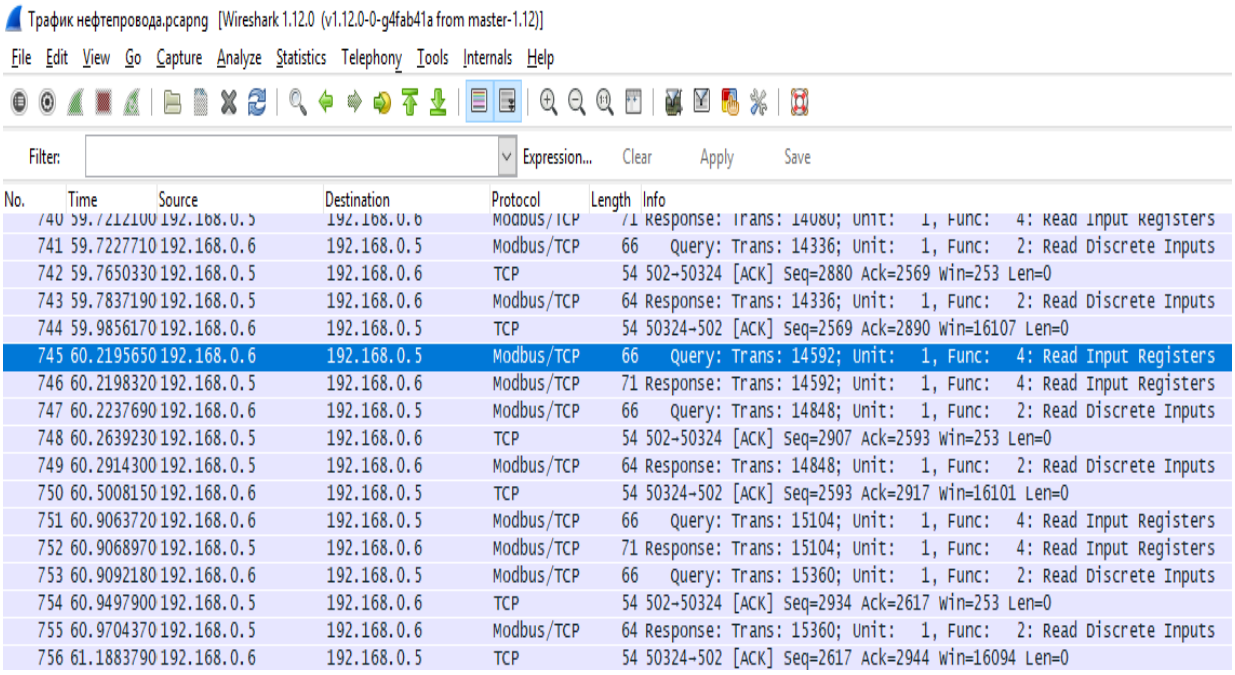


Рисунок 38 – Экранная форма сетевого трафика, отражающая пакет запроса на чтение входных регистров программируемого контроллера

Содержимое пакета представлено на рисунке 39.

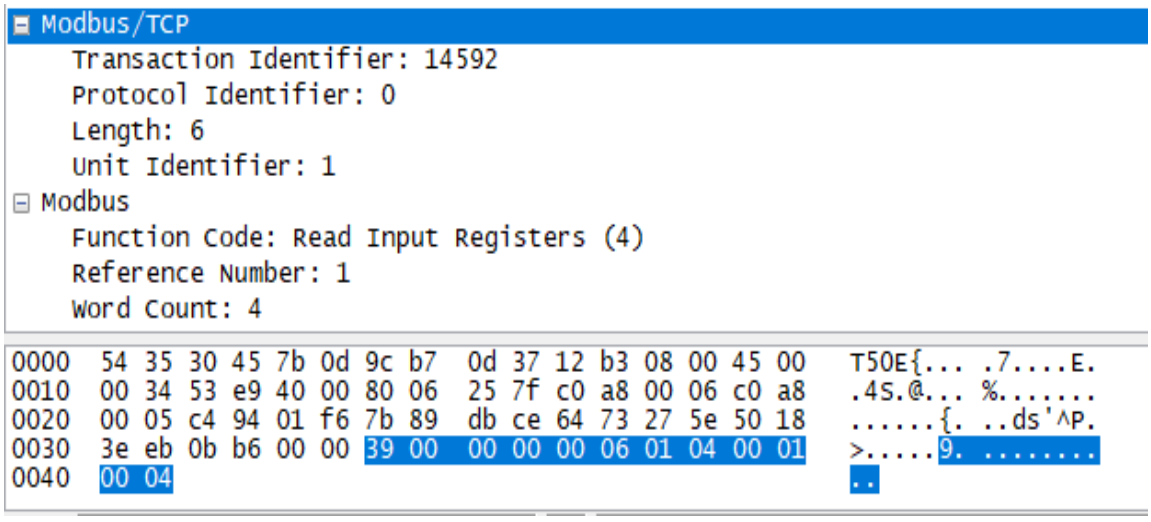


Рисунок 39 – Содержимое пакета запроса на чтение входных регистров программируемого контроллера

На рисунке 39 обозначены [114]:

– Transaction Identifier - идентификатор транзакции;
– Protocol Identifier - идентификатор протокола;
– Length - длина;
– Unit Identifier - идентификатор блока или адрес устройства;
– Function Code - код функции;
– Reference Number - начальный номер регистра;
– Word Count - количество регистров.

Выделим из сетевого пакета признаки, по которым будем определять его правомерность:

– IP-адрес компьютера, на котором установлена программа АРМ оператора: 192.168.0.6;
– IP-адрес компьютера, на котором запущена мнемосхема нефтепровода: 192.168.0.5;
– протокол, по которому происходит передача между ПК: Modbus/TCP;
– длина пакета: 66;
– идентификатор транзакции: 14592;
– адрес устройства: 1;
– код функции: 4.

Сформируем транзакцию из 7 команд, которую представим в таблице 7.

Таблица 7 – Исследуемая транзакция

Команда 1	Команда 2	Команда 3	Команда 4	Команда 5	Команда 6	Команда 7
192.168.0.6	192.168.0.5	Modbus/TCP	66	14592	1	4

Внесем получившуюся транзакцию в базу транзакций программы «Эмулятор устройства для контроля поведения пользователя» и проведем эксперимент по определению правомерности данной транзакции.

На рисунке 40 представлен пример безошибочного ввода команд транзакции.

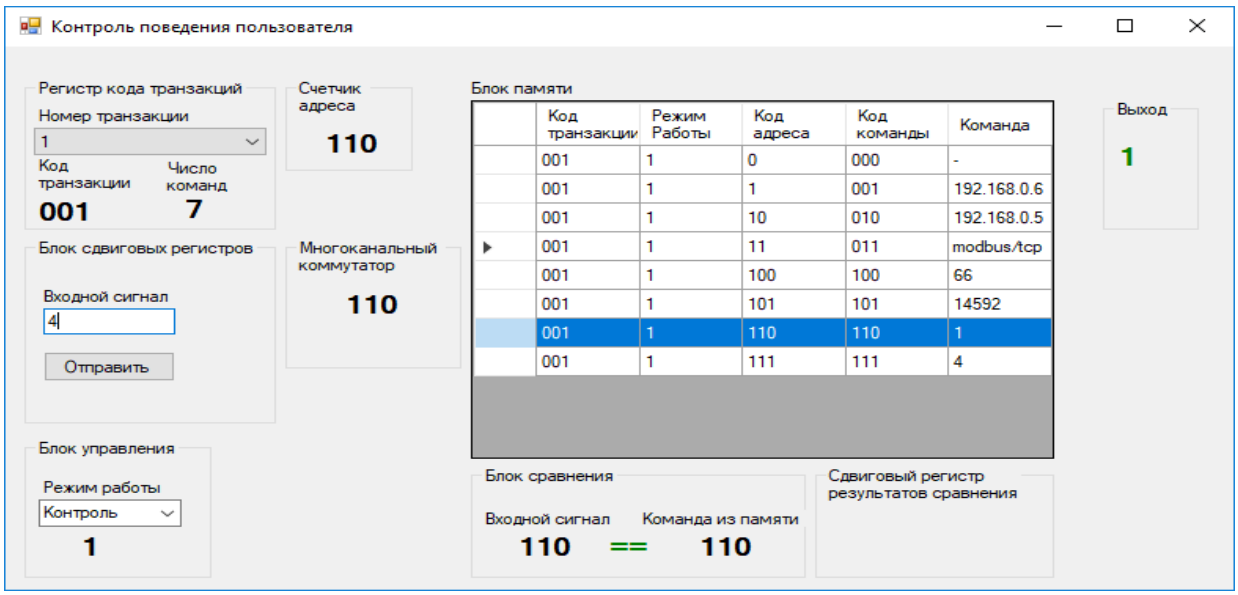


Рисунок 40 – Пример безошибочного ввода команд транзакции

Намеренно допустим ошибку при вводе последней команды транзакции (вместо кода функции: 4, введем код функции: 2), в результате чего возникнет ошибка, как показано на рисунке 41.

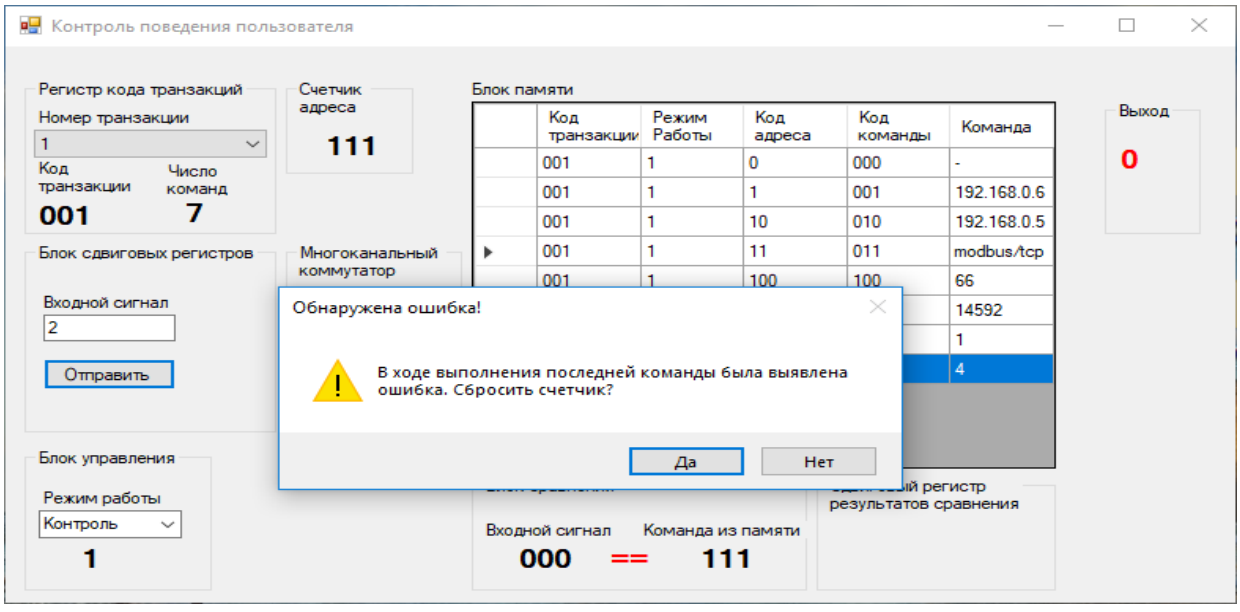


Рисунок 41 – Ошибка при вводе последней команды

Таким образом, применение в автоматизированной системе управления нефтепроводом протокола Modbus/TCP позволяет более подробно раскрыть

содержимое сетевого пакета и более точно определить совершаемые оператором действия (например, запрос на запись или чтение значения регистров).

Эффективность разработанного метода оценивается с учетом анализа рисков в системах защиты информации [30,41,64]. Риск определяется как произведение финансовых потерь (ущерба), связанных с несанкционированными операциями, и вероятностями реализации этих операций.

Графовая модель последовательности выполнения команд (операций) оператором в исходной автоматизированной системе, в которой переходы пользователя от одной команды к другой осуществляются без каких-либо проверок, показана на рисунке 42.

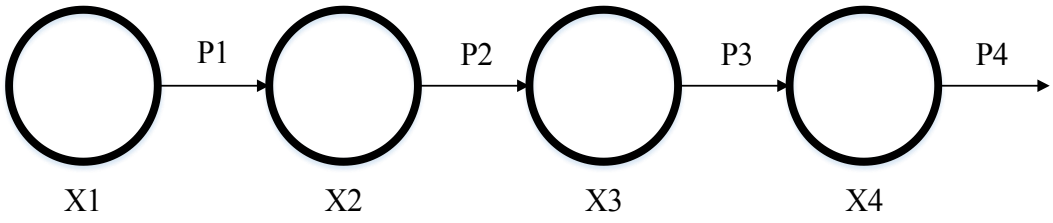


Рисунок 42 – Графовая модель последовательности операций пользователя без проверок

Модель, представленная на рисунке 43, описывает разрабатываемый метод. В этом случае при выполнении каждой операции производится проверка ее санкционированного выполнения, а также проверка всех предыдущих операций с использованием соответствующих сигнатур. Данный алгоритм позволяет контролировать каждый переход состояния компьютерной системы с учетом санкционированности всех предыдущих переходов [22,45].

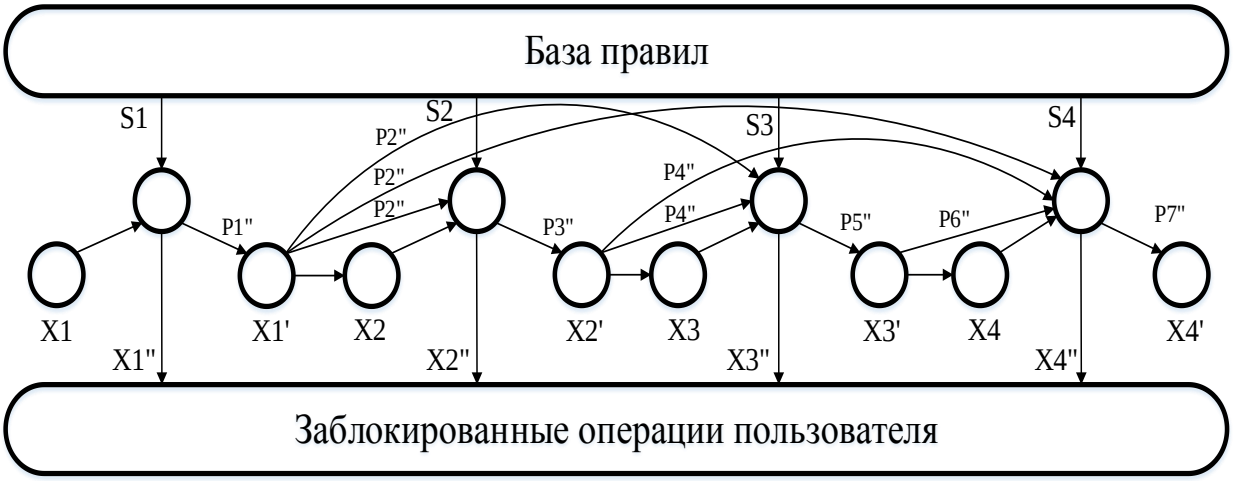


Рисунок 43 – Графовая модель контроля операций пользователя на основе сигнатурного метода

На рисунках 42-43 приняты следующие обозначения:

– X1- X4 – сигналы запроса на выполнение операций пользователя;

– X1'-X4' – сигналы разрешения выполнения операций пользователя;

– X1"-X4" – сигналы блокировки выполнения операций пользователя системой мониторинга;

– S1-S4 – коды сигнатур операций пользователя;

Величина «P» с индексами - оценки вероятностей ошибки при обнаружении несанкционированной операции.

В том случае, если величина ущерба равна для рассматриваемых вариантов контроля, представленных на рисунке 42, в рассматриваемой задаче оценка риска определяется вероятностями реализации угрозы выполнения несанкционированной операции [22,45].

Для исходной модели, представленной на рисунке 42, оценка реализации угрозы равна произведению (*M1*) вероятностей *P1–P4*:

$$M1=P1\cdot P2\cdot P3\cdot P4$$

В предложенном методе вероятность несанкционированной реализации всей последовательности операций равна произведению вероятностей *P1"- P7"* (*M2*):

$$M2=P1''\cdot P2''\cdot P3''\cdot P4''\cdot P5''\cdot P6''\cdot P7''$$

Допустим, что оценка вероятности ошибки при обнаружении несанкционированной операции (P) составляет 0.2.

Подставим это значение в выражения и получим:

$$M1 = 0.2 \cdot 0.2 \cdot 0.2 \cdot 0.2 = 0{,}0016$$

$$M2 = 0.2 \cdot 0.2 \cdot 0.2 \cdot 0.2 \cdot 0.2 \cdot 0.2 \cdot 0.2 = 0{,}0000128$$

$$0{,}0000128 < 0{,}0016$$

Таким образом:

$$M2 < M1$$

Величина *M2* значительно меньше *M1,* так как по мере выполнения каждой последующей операции, как это видно на рисунке 43, осуществляется дополнительно контроль выполнения всех предшествующих операций.

Предложенный метод позволяет снизить вероятность несанкционированного подключения нарушителя в последовательность выполняемых операций за счет непрерывного текущего контроля санкционированности всех предыдущих операций. Внесенная при этом некоторая избыточность проверок при использовании средств автоматизации контроля не снижает производительности выполнения операций, а алгоритмическая избыточность снижает риск несанкционированного доступа.

3.7 Метод защитного резервирования информационного канала системы управления трубопроводом с использованием высоковольтной линии электропередач

Для магистральных нефтепроводов, как критически важных распределённых технологических объектов, необходимо организовывать надёжную высокоскоростную связь для всех подсистем, включая каналы выделенной сети, телефонной и диспетчерской связи, трансляции с камер видеонаблюдения, систем обнаружения утечек и систем мониторинга технического состояния, а также средств обеспечения технической безопасности. В случае обрыва канала передачи

информации, время восстановления связи будет равняться времени физического восстановления коммуникаций [33].

В рамках данной работы рассматривается протяжённый технологический объект [86]. Источники информации (ИИ), в которых установлено оборудование электропитания и средства собора информации о состоянии технологического объекта, передают данные по линии связи приёмнику информации (ПИ), как показано на рисунке 44. Риск ***R*** не доставить информацию от ИИ, число которых задается параметром ***i,*** до приёмника определяется как сумма произведений вероятности (***P***) обрыва основного канала передачи на ущерб (***U***) от обрыва основного канала передачи информации.

$$R = \sum_i P_i \cdot R_i \tag{3.4}$$

Целевая функция в данном случае определяется как функция минимизации риска не доставить информацию от ИИ до ПИ при ограничении стоимостных затрат на систему сбора технологической информации.

$$R = \sum_i P_i \cdot R_i \rightarrow min \tag{3.5}$$

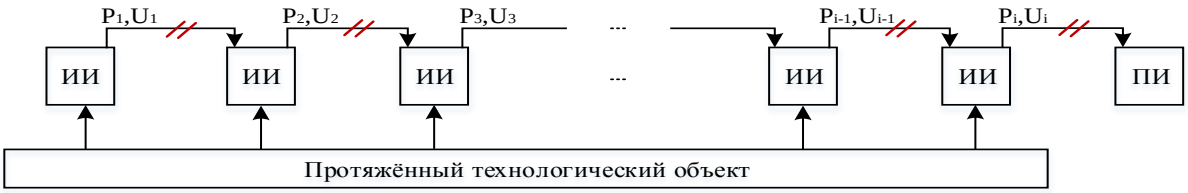


Рисунок 44 – Структурно-функциональная схема распределённой системы мониторинга протяжённого объекта

Чрезвычайной ситуацией системы передачи информации в распределённой системе мониторинга технологического объекта (РСМТО) является состояние, при котором имеется повреждение канала связи. Обрыв возможен при повреждении протяжённого объекта, выполнении земельных работ, а также несанкционированной врезке в канал передачи данных [54, 80, 86].

При сбоях в работе основной сети, система передачи данных автоматически переключается на резервный канал связи и функционирует в этом режиме до восстановления нормальной работы поврежденного участка основного канала передачи данных. Связь основного и резервного каналов осуществляется с помощью коммутатора (К). Модем (М) передаёт информации по резервному каналу связи ИИ и ПИ. На рисунке 45 представлена структурно-функциональная схема самоорганизующейся системы информационного обмена между узлами РСМТО с использованием резервного канала.

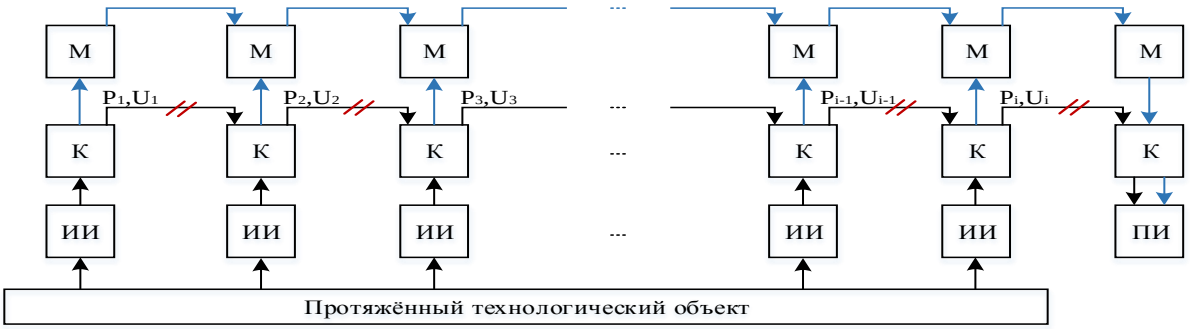


Рисунок 45 – Структурно-функциональная схема самоорганизующейся системы информационного обмена между узлами РСМТО с использованием резервного канала

Использование резервного канала позволяет ПИ продолжать контролировать состояние протяжённого технологического объекта даже при обрыве участка основного канала передачи данных.

Для предотвращения аварий на распределённом промышленном объекте предусмотрена система мониторинга технического состояния, управление системой производится в диспетчерских пунктах. Как известно, для принятия решений диспетчер использует информацию от датчиков, системы видеонаблюдения за факелами и т.д. [80, 86].

Одной из самых актуальных угроз протяжённого промышленного объекта является угроза обрыва канала связи. Предполагается, что при потере связи с объектом, задействуется резервный канал передачи данных. Инициатором переключения на резервную может быть как диспетчер, так и контроллер

телеметрии, используя сигнатуры обрыва канала связи. При успешном переключении системы мониторинга технического состояния на резервный канал, система возвращается в штатный режим.

Алгоритм работы системы управления технологическим процессом при возникновении аварийной ситуации представлен на рисунке 46.

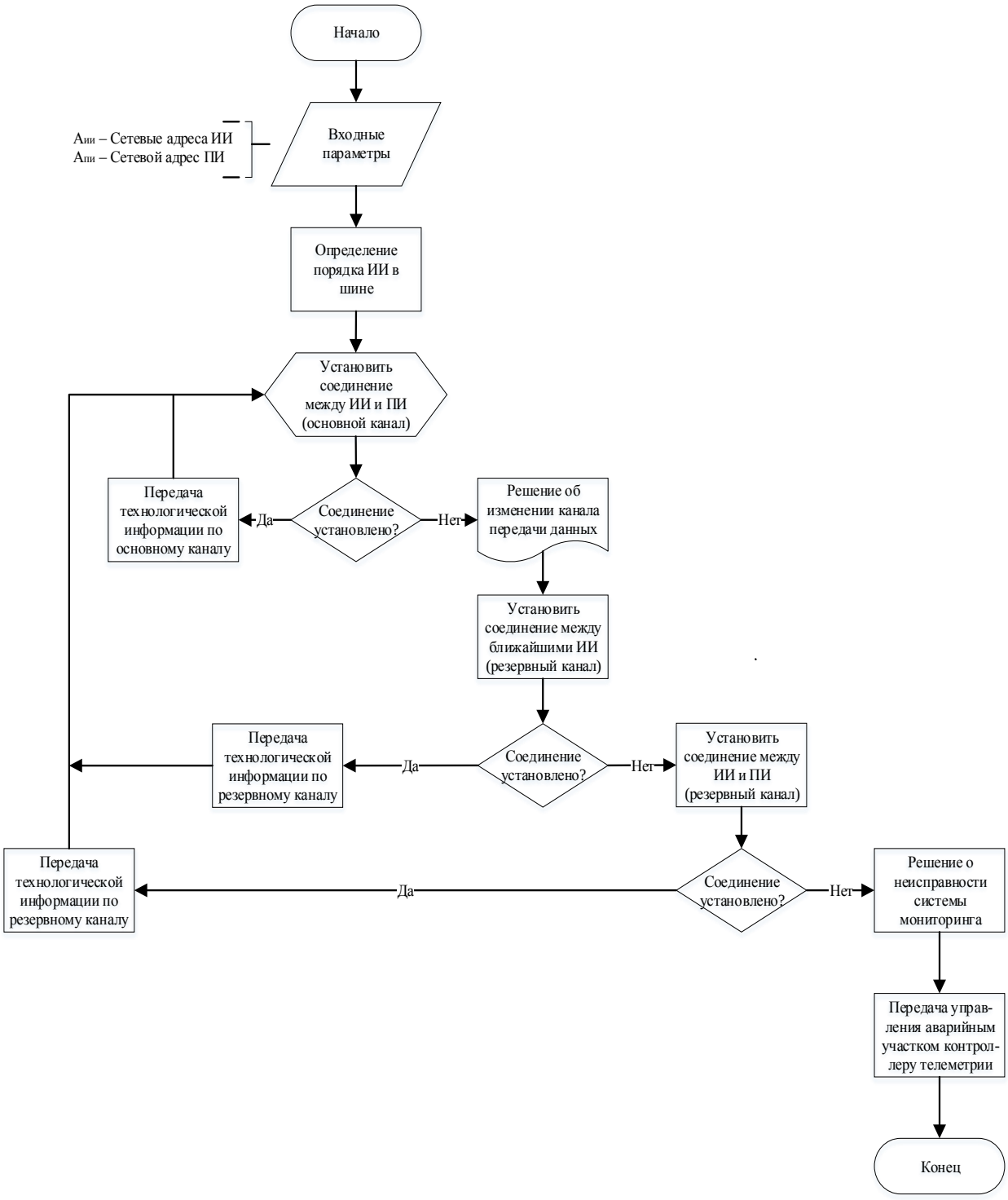


Рисунок 46 – Алгоритм работы системы управления технологическим процессом при возникновении аварийной ситуации

Если на резервный канал переключиться невозможно, контроллер телеметрии берёт на себя управление аварийным участком протяжённого технологического объекта до восстановления связи с диспетчером [56].

Топологическая модель РСМТО с использованием ЛЭП в качестве резервного канала представлена на рисунке 47.

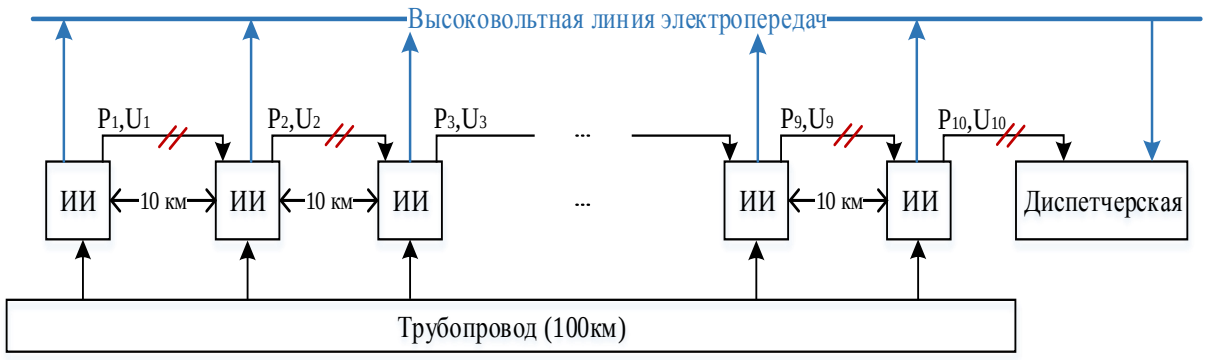


Рисунок 47 – Топологическая модель РСМТО с использованием резервного канала

Согласно алгоритму, источники информации, оказавшиеся между местом обрыва и диспетчерской, будут работать в обычном режиме, продолжая передавать информацию по основному каналу. После обнаружения обрыва линии связи источники, расположенные до места обрыва, воспользуются резервным каналом передачи информации. Это позволит диспетчерам продолжать контролировать состояние трубопровода Таким образом, контроль за состоянием трубопровода будет непрерывным.

Для реализации данного метода необходим модем приёма-передачи информации, выполняющий функции модулятора-демодулятора сигналов [99]. Для подключения модема передачи информации к ВЛЭП, необходимы фильтр присоединения и конденсатор связи, защищающие оборудование приёмо-передачи и сглаживающие помехи. В таблице 8 представлена спецификация программного и аппаратного обеспечения, необходимого для реализации резервного канала передачи информации по ВЛЭП. В соответствии со спецификацией стоимость дополнительных капитальных вложений составляет 523088 рублей. Продолжительность эксплуатации модема приёма-передачи информации AMIS-

49587 с наработкой на отказ равна 87600 часов, что соответствует почти 10 годам службы. Диапазон рабочих температур выбранного оборудования варьируется от -30°C до +35°C. Учитывая, что оборудование устанавливается в помещениях с контролем климата, температурный порог пригоден для эксплуатации системы.

Таблица 8 – Спецификация программного и аппаратного обеспечения, необходимого для реализации резервного канала передачи технологической информации по ВЛЭП

Наименование	Наработка на отказ (часов)	Диапазон рабочих температур (°C)	Ед. измерения	Количество	Стоимость единицы (руб.)	Общая стоимость (руб.)	В т.ч. НДС 18% (руб)
Модем приёма-передачи информации AMIS-49587	87600	от –40 до +60	шт.	12	14000	168 000	30240
Фильтр присоединения и конденсатор связи ФП-Рс	113 880	от -60 до +110	шт.	12	17900	214 800	38664
Кабель КВВ Unipump 4х2,5	-	от –60 до +70	м.	70	216,5	15 155	2727,8
Кабель COM 9pin – COM 9pim (3м)	-	от –30 до +35	шт.	12	200	4800	864
Кабель заземления ПВ3 (ПуГВ) 1х16	-	от –50 до +35	м.	20	127	2540	457,2
Программное обеспечение для управления очередями сетевого трафика (разработка)	-	-	шт.	1	38000	38000	6840
Всего:						443 295	79 793
						523 088	

Для определения загруженности резервного канала передачи информации были рассчитаны требования к пропускной способности. За основу был взят один

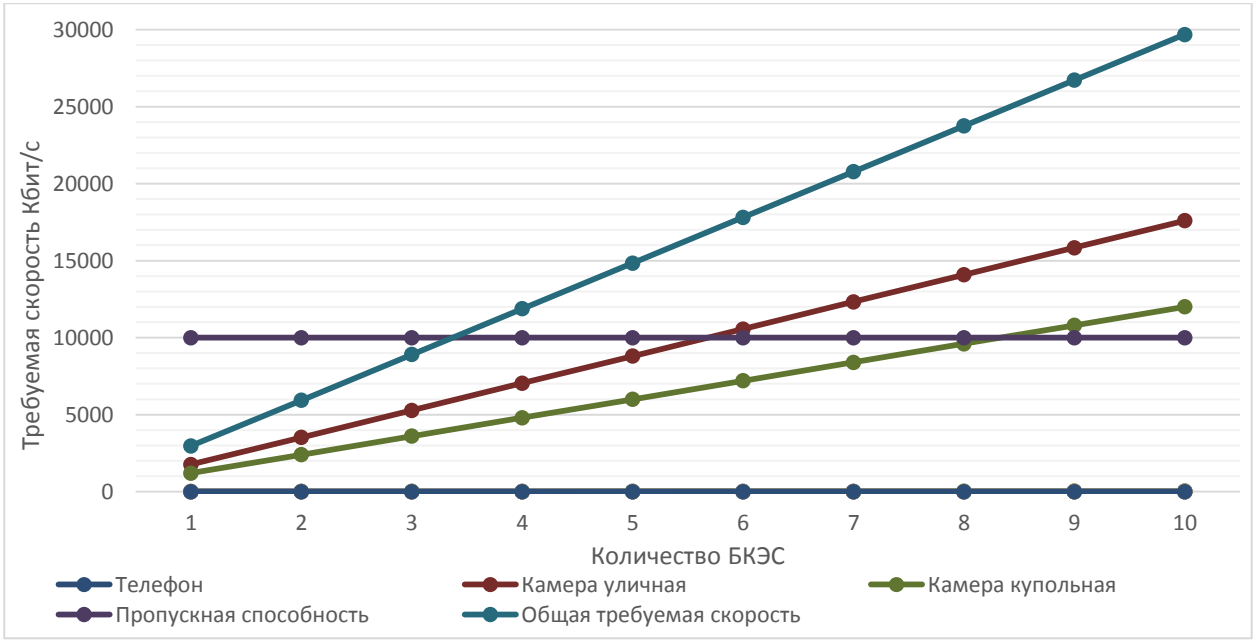
участок протяжённого технологической объекта и учтены все устройства, использующие канал передачи. В таблице 9 определено, какой процент занимает каждый из потоков информации, передаваемый одним БКЭС в диспетчерский пункт.

Таблица 9 – Сравнение занимаемой пропускной способности канала передачи данных каждым из информационных потоков для одного БКЭС

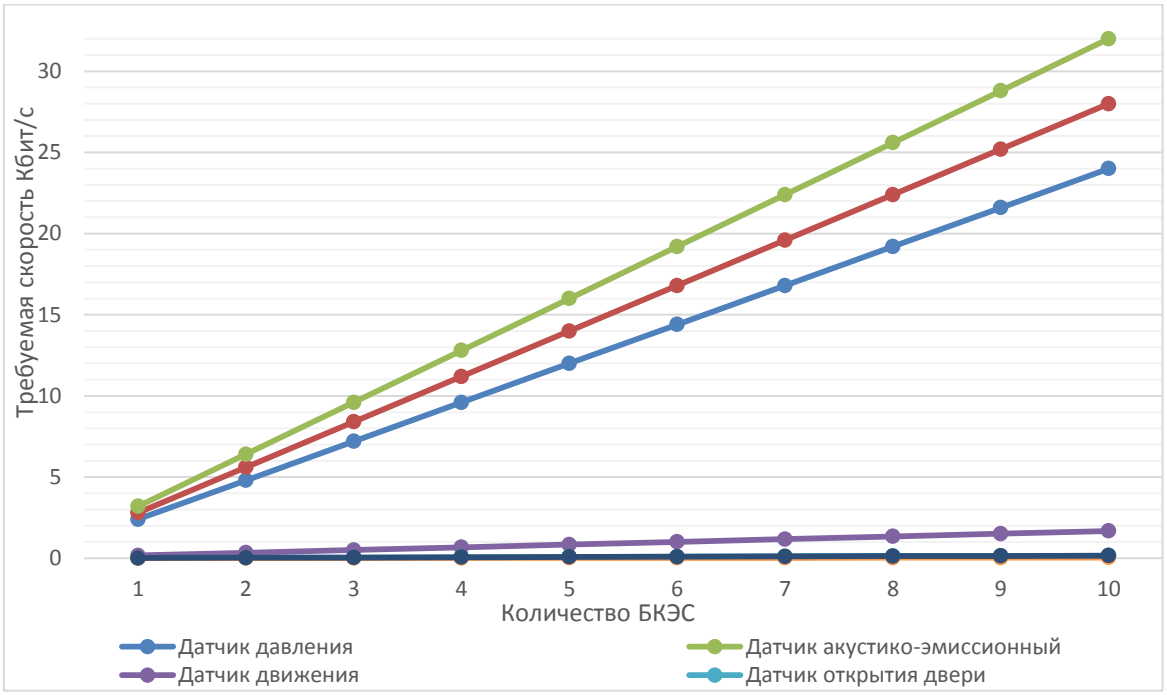
Оборудование	Требуемая скорость	Загруженность канала		Приоритет передачи
1	2	3		4
Датчик давления	2,400 Кбит/с	0,081%	1,093%	Очень высокий
Датчик вибрации	2,800 Кбит/с	0,094%		
Датчик акустико-эмиссионный	3,200 Кбит/с	0,108%		
Датчик движения	0,168 Кбит/с	0,005%	0,007%	Высокий
Датчик открытия дверей	0,016 Кбит/с	0,001%	0,007%	Высокий
Датчик температуры	0,004 Кбит/с	0,001%		
Телефон	0,016 кбит/с	0,001%	0,001%	Средний
Видеокамера уличная	1 760 Кбит/с	58,476%	98,899%	Низкий
Купольная видеокамера уличная	1 200 Кбит/с	40,423%		

На рисунке 48 представлена зависимость пропускной способности канала передачи данных от количества блоков контроля электрических сигналов (БКЭС), использующих этот канал.

Резервный канал передачи будет полностью отвечать требованиям объёма передаваемой информации для трёх участков протяжённого объекта при обрыве основного канала передачи данных. При обрыве основного канала передачи информации после четырёх и более БКЭС, появляется дефицит пропускной способности резервного канала передачи информации.



а)



б)

Рисунок 48 – Зависимость пропускной способности канала передачи данных от количества подключённых к ней БКЭС до использования механизма управления очередями (при различных масштабах)

На рисунке 49 представлена структурная схема механизма управления очередями для приёмо-передающего оборудования резервного канала передачи технологической информации.

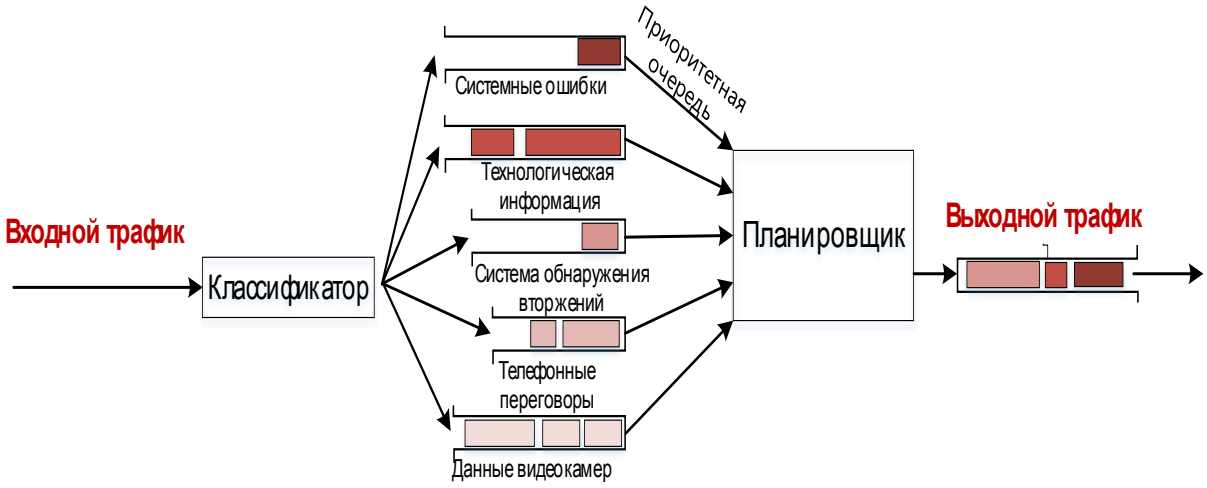
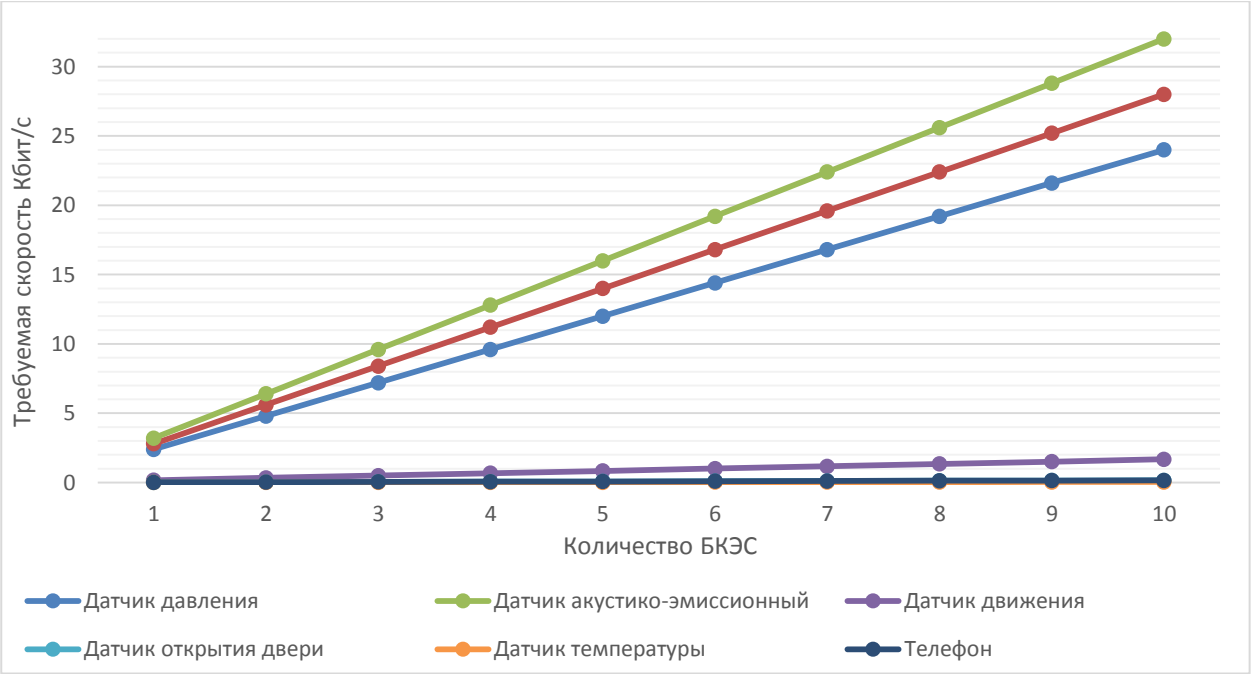


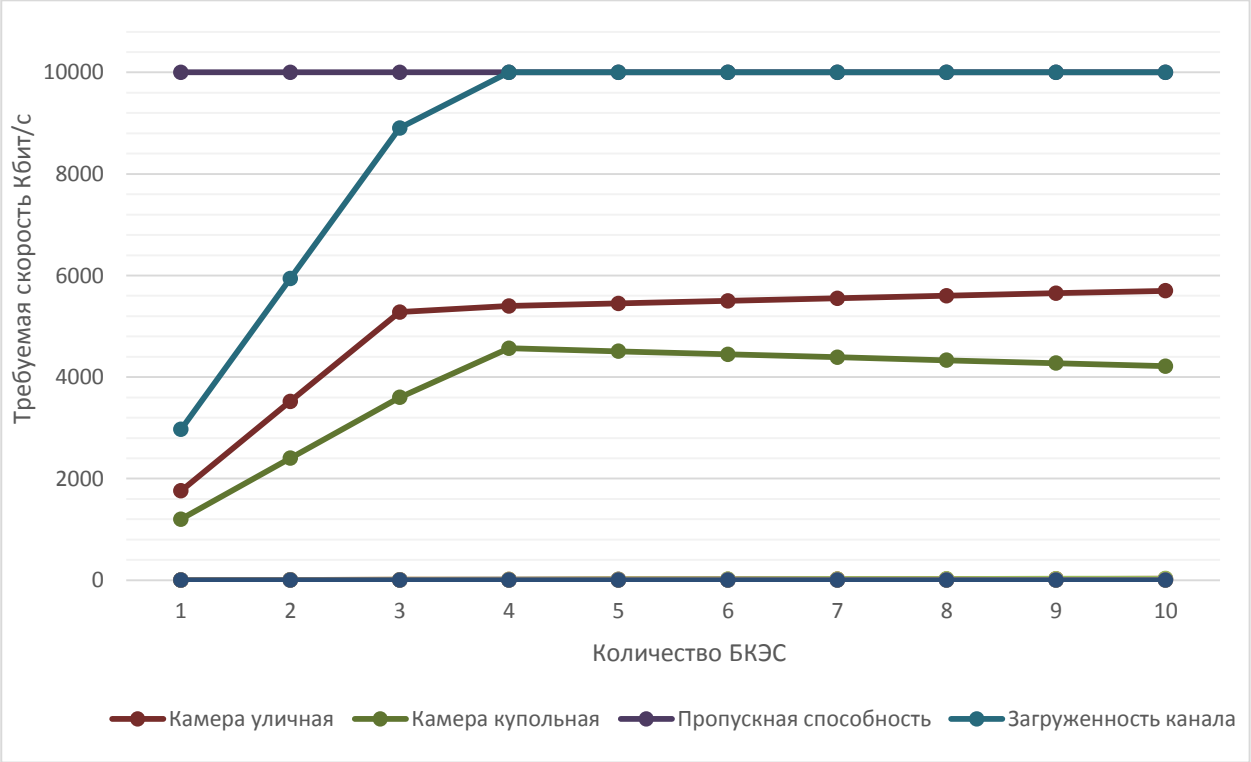
Рисунок 49 – Структурная схема механизма управления очередями для приёмо-передающего оборудования резервного канала передачи технологической информации

При такой организации передачи технологической информации, резервный канал будет загружен полностью при подключении к нему более чем трёх обслуживающих блоков. На рисунке 50 представлена зависимость загруженности канала от количества БКЭС, использующих этот канал.

По приоритету передаваемой информации, это: 100 % объёма информации о состоянии трубопровода (0,84 % от общего объёма технологической информации), 100 % объёма информации о состоянии обслуживаемого объекта (0,019 % от общего объёма технологической информации), 100 % в данных телефонных переговоров (0,01 % от общего объёма технологической информации) и 32,815 % от объёма данных с видеокамер (29,6 % от общего объёма технологической информации).



а)



б)

Рисунок 50 – Зависимость загруженности канала от количества БКЭС после использования механизма управления очередями (при различных масштабах)

Техническим эффектом от внедрения резервного канала является повышение надёжности работы автоматизированной системы мониторинга технического

состояния, благодаря чему информация о состоянии объекта будет доступна в любой момент времени. Оценки ожидаемого технического эффекта представлены в таблице 10.

Таблица 10 – Оценки ожидаемого технического эффекта от внедрения резервного канала передачи технологической информации

Угроза	До внедрения		После внедрения	
	Вероятность аварийной ситуации	Уровень доступности информации	Вероятность аварийной ситуации	Уровень доступности информации
Отсутствует	0	100%	0	100%
Низкая	0,2	80%	0,2	100%
Средняя	0,4	60%	0,4	90%
Высокая	0,6	40%	0,6	70%
Угрожающая	0,8	20%	0,8	50%
Катастрофическая	1	0%	1	30%

Для оценки ожидаемого экономического эффекта используем методики, представленные в работах [51, 104]:

Показатель ожидаемых потерь ***ALE*** вычисляется согласно формуле (3.6) [104]:

$$ALE = f \cdot L, \tag{3.6}$$

где f – частота возникновения потенциальной угрозы, уровень которой определяется на основании оценок вероятности возникновения угрозы в заданный интервал времени;

L – величина потерь в рублях, которая определяется на основании степени тяжести нарушения информационной безопасности.

В качестве показателей безотказности технических систем применяют следующие количественные характеристики:

– вероятность отказа;

- вероятность безотказной работы;
- интенсивность отказов;
- средняя наработка до отказа (до первого отказа).

В таблице 11 представлены уровни вероятности угроз и их частота.

Таблица 11 – Уровни вероятности угроз и частота событий

Уровень вероятности	Описание	Частота
Незначительный	Вряд ли произойдет	0,05
Очень низкий	Событие происходит два-три раза в пять лет	0,6
Низкий	Событие происходит не более раза в год	1,0
Средний	Событие происходит реже раза в полгода или раз в полгода	2,0
Высокий	Событие происходит реже раза в месяц или раз в месяц	12,0
Очень высокий	Событие происходит несколько раз в месяц	36,0
Экстремальный	Событие происходит несколько раз в день	365

В таблице 12 представлены степени тяжести угроз и потери от их реализации.

Таблица 12 – Степень тяжести угроз и потери от их реализации

Степень тяжести	Описание	Потери, руб.
Несущественная	Авария не повлечёт за собой никаких последствий	0
Низкая	Авария не ведет к финансовым потерям, но выяснение характера происшествия потребует незначительных затрат	150 000
Существенная	Происшествие принесет некоторый материальный и моральный вред	700 000
Угрожающая	Потеря репутации, конфиденциальной информации. Затраты на ремонт коммуникаций, проведение расследований	6000000
Серьезная	Устранение последствий разлива нефтепродуктов, ремонт трубопровода, расследование происшествия	15000000
Критическая	Вывод из строя протяжённого технологического объекта, капитальный ремонт	60000000

Угроза типа «Отказ в обслуживании» относится к «Серьёзной» угрозам по степени тяжести, а частота возникновения угрозы примерно раз в год, то есть коэффициент $\boldsymbol{f}$ будет равен 1.

Таким образом, показатель $\boldsymbol{ALE}$ будет равен (3.7):

$$ALE = 1 \cdot 15\,000\,000 = 15\,000\,000 \text{ руб.} \quad (3.7)$$

В свою очередь затраты на внедрение разрабатываемой концепции ($\mathbf{Z_{вн}}$) включают в себя приобретение оборудования для дублирования линии связи, включая монтаж, подключение, настройку, а также затраты на техническое обслуживание ($\boldsymbol{Z}_{\text{ТО}}$) (3.8, 3.9).

$$\text{Z}_{\text{вн}} = \text{Z}_{\text{АРМ}} + \text{Z}_{\text{уст}} = 523\,088 + 156\,926 = 680\,014 \text{ руб.} \quad (3.8)$$

$$\text{Z}_{\text{ТО}} = 0{,}1 * \text{Z}_{\text{вн}} = 68\,001{,}4 \text{ руб./год} \quad (3.9)$$

Таким образом, внедрение резервного канала передачи технологической информации считается экономически выгодным, так как затраты на его использование значительно ниже, чем затраты от реализации угрозы типа «Отказ в обслуживании».

К социальному эффекту от внедрения отнесены снижение обеспокоенности близким расположением распределённого промышленного объекта у населения, проживающего в непосредственной близости от него. Жители близлежащих населённых пунктов будут знать, что мониторинг технического состояния производится в режиме реального времени и не может возникнуть ситуации, когда распределённый промышленный объект останется без контроля из-за обрыва информационного канала.

4 Оценка эффективности и рекомендации по применению методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз

4.1 Анализ технико-экономической эффективности методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз

В таблице 13 представлен анализ эффективности разработанных методов контроля технического состояния распределенных автоматизированных систем

Таблица 13 – Оценки эффективности методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз

Метод	**Эффект**		
	Технический	Экономический	Социальный или иной эффект
1	2	3	4
Метод обнаружения аномалий в системе управления трубопроводом на основе мониторинга информационных потоков сетевого трафика	Обнаружение аномальной сигнатуры состояния в момент ее регистрации в сетевом трафике	Затраты определяются стоимостью аппаратно-программных средств устройства распознавания ситуаций	сокращение времени сбора информации и оповещения об инциденте, что позволяет оперативно реагировать на возникновение аномальной ситуации и принимать решения для ее нейтрализации

Продолжение таблицы 13

1	2	3	4
Метод прогнозирования временных рядов по данным сетевого трафика на основе полигармонического полинома	Полученная экспериментально точность прогноза интенсивности распространения вредоносного кода по данным сайта Касперского с перспективой на семь дней не превышает 15%	Стоимость программы – 10 тыс. р	-
Метод ранжирования угроз на основе ассоциативного принципа	Ранжирование угрозы происходит за один такт в момент ее регистрации	Стоимость программы – 10 тыс. руб..	-
Метод выбора базовой функции при автоматизированной идентификации временных рядов сетевого трафика на основе ассоциативно-мажоритарного подхода	Идентификация базовой функции производится в автоматизирован-ном режиме непосредственно в момент ее регистрации	Стоимость программы – 10 тыс. р.	-
Метод контроля директивных установок в распределенной АСУ протяженным промышленным объектом	Снижение вероятности несанкционированных действий оператора АСУ более, чем на порядок	Стоимость программных средств для реализации устройства около 10 тыс. руб.	-
Метод повышения живучести телекоммуникаци-онной подсисте-мы АСУ ТП в условиях распределенной пространственно-временной модели угроз на основе защитного резервирования информационного канала системы управления трубопроводом с использованием высоковольтной линии электропередачи (ЛЭП)	Технические характеристики представлены в пункт 3.7	Расчет ожидаемого экономического эффекта представлен в рразделе 3 в п. 3.7	Социальный эффект представлен в разделе 3, в п. 3.7 Улучшение экологии окружающей среды

Проведенный анализ технико-экономической эффективности результатов исследований подтвердил эффективность исследований, в частности, оценки доступности к информации в АСУ в зависимости от степени аварии на объекте существенно повысились: в случае катастрофической ситуации – на 30%, в случае угроз с низкой и средней степенью ущерба, соответственно – на 90 и 100%.

По данным ожидаемого экономического эффекта от внедрения метода защиты каналов передачи информации в АСУ нефтепроводом при дополнительных капитальных вложениях в средства защиты в 680 тыс.р. возможно устранение ущерба в размере порядка 15 млн. р.

4.2 Рекомендации по внедрению методов и средств контроля технического состояния распределенных АСУ ТП транспортировки нефтегазового сырья на предприятиях Оренбургской области

Как уже отмечалось, общая протяженность нефте- и газопроводов по данным Интернет ресурсов (Интернет ресурс: http://orenpriroda.ru/экономическая-география/инфраструктура-оренбургской-области/744-трубопроводный-транспорт-оренбургской-области) в Оренбургской области составляет более 6600 км, что свидетельствует об актуальности использования результатов разработки на предприятиях и в организациях области, занимающихся нефте-газодобычей, транспортировкой и обработкой нефтегазового сырья. К таким предприятиям относятся:

1) Газопромысловое управление «Газпром добыча Оренбург»;
2) Оренбургский газоперерабатывающий завод ООО «Газпром переработка»;
3) Предприятие «Газпром трансгаз Екатеринбург»;
4) Компания «Уральский центр систем безопасности» (УЦСБ);
5) ООО «Газпромнефть-Оренбург»;
6) ООО «ВолгоУралНИПИгаз»;
7) Оренбургский гелиевый завод ООО «Газпром переработка»;
8) Управление по эксплуатации соединительных продуктов ООО «Газпром добыча Оренбург»;
9) ПАО «МРСК Волги» - «ОренбургЭнерго».

Представленные в работе разработки касаются различных этапов жизненного цикла систем мониторинга технического состояния распределенных промышленных

объектов, в частности – вопросов их разработки, эксплуатации, внедрения и модернизации. В связи с этим результаты разработок имеют разную степень актуальности для каждой из перечисленных организаций. Тем не менее, все они могут быть востребованы в аналитических и проектных подразделениях перечисленных выше организаций.

Следует отметить, что в некоторых исследованиях, связанных с имитационным моделированием промышленного протокола сетевого трафика были использованы результате совместного обсуждения выбора инструментальных средств исследований со специалистами Компании «Уральский центр систем безопасности» в рамках совместного договора о сотрудничестве. Эти исследования могут найти продолжение в рамках совместного договора о сотрудничестве между Оренбургским государственным университетом и этой организацией. Это касается разработки средств мониторинга сетевого трафика на основе принципов ассоциативно-мажоритарного подхода. Особую актуальность для предприятий нефте-газодобычи представляет разработанный метод защитного резервирования каналов передачи информации на основе ЛЭП.

Результаты, касающиеся прогнозирования временных рядов и ранжирования угроз, кроме перечисленных организаций, могут найти применение в ООО «ГлобалМониторинг» (г. Оренбург) при организации перевозок ценных грузов для их охраны с применением пространственно-временной модели угроз, адаптированной к особенностям маршрутов передвижения транспортных средств.

Особую актуальность имеют полученные в проекте результаты для ВУЗов, выпускающих специалистов по разработке автоматизированных систем в защищенном исполнении, частности для Оренбургского государственного университета и его филиалов, а также Оренбургского филиала Российского государственного университета имени И.М. Губкина.

Перечисленные результаты нашли отражение и доступны в виде Интернет ресурсов по реквизитам и адресным ссылкам, представленным в списке источников работы.

4.3 Перспективы использования средств спутниковой навигации и беспилотных летательных объектов в системах мониторинга протяженных промышленных объектов

Одним из актуальных перспективных направлений в теории и практике построения современных систем мониторинга протяженных промышленных объектов является применение беспилотных летательных аппаратов (БПЛА), в частности квадрокоптеров [23,28,31].

Перечень задач мониторинга, решаемых БПЛА, весьма широк и разнообразен. Помимо функций визуального наблюдения за пространством, в котором проложен трубопровод, актуальными являются задачи наблюдения за полевым оборудованием АСУ, сбором и передачей информации на пункты наблюдения. В связи с этим появляются новые задачи, связанные с защитой самого квадрокоптера, как объекта информатизации, с вопросами точного позиционирования его в трехмерном пространстве и управления режимами регистрации и распознавания видеоизображений. Эти задачи могут быть предметом перспективных исследований. На рисунке 51 представлен перспективный вариант концептуальной схемы управления и защиты БПЛА, как мобильного объекта информатизации (МОИ), на основе средств спутниковой навигации, разрабатываемый при участии авторов настоящей работы.

Для решения задачи защиты МОИ выбран модуль повышенной точности определения местоположения «NEO-M8P» на плате «C94-M8P» производителя «u-blox». Семейство модулей спутниковой навигации NEO-M8P является разработкой швейцарской компании u-blox. Модули обладают небольшими габаритами и умеренным энергопотреблением. Модули дают пользователю доступ к многочисленным внутренним настройкам, позволяя выполнять гибкую конфигурацию под каждую конкретную разновидность конечного оборудования. NEO-M8P – технология высокой точности при малых размерах для таких приложений, как беспилотные транспортные средства и роботизированные системы управления. Модули NEO-M8P поддерживает работу как в совмещенном режиме,

принимая в расчет данные с нескольких навигационных систем, например, GPS и ГЛОНАСС, так и с одной отдельно взятой системы. Главной особенностью модулей NEO-M8P является поддержка технологии RTK, позволяющая определять координаты с точностью до единиц сантиметров. Принцип работы технологии заключается в следующем: один модуль выполняет функции неподвижной базовой станции, вычисляет свои координаты и рассылает так называемые дифференциальные поправки в широковещательном режиме по радиоканалу. Все остальные модули выполняют функции подвижных объектов и принимают дифференциальные поправки, рассылаемые базовой станцией, с их помощью определяют свои координаты с точностью до сантиметров.

Real Time Kinematic (RTK, кинематика реального времени) – совокупность приёмов и методов получения плановых координат и высот точек местности сантиметровой точности с помощью спутниковой системы навигации посредством получения поправок с базовой станции, принимаемых аппаратурой пользователя во время съёмки. На основе данной технологии в задаче защиты МОИ предлагается разместить в защищаемой области (на территории организации) один GPS-модуль, который выступать в роли неподвижной базовой станции. Установка модуля в роли базовой станции на защищаемой территории организации позволит обеспечить защиту модуля от физического несанкционированного доступа. Первый навигационный модуль, расположенный на защищенной территории организации определяет координаты и передаёт по каналу радиосвязи набор данных, называемых поправками. В прикладной плате C94-M8P используется встроенный радиомодем HM-TRP с прошивкой, имеющей открытый исходный код «SiK», которая поддерживает вариант подмножества команд модема Hayes «AT» для предварительной настройки. Второй приёмник «ровер», расположенный на автомобиле, принимает дифференциальные поправки, рассылаемые базовой станцией, с их помощью определяет свои координаты с точностью до сантиметров (до 1 см в плане и 2 см по высоте).

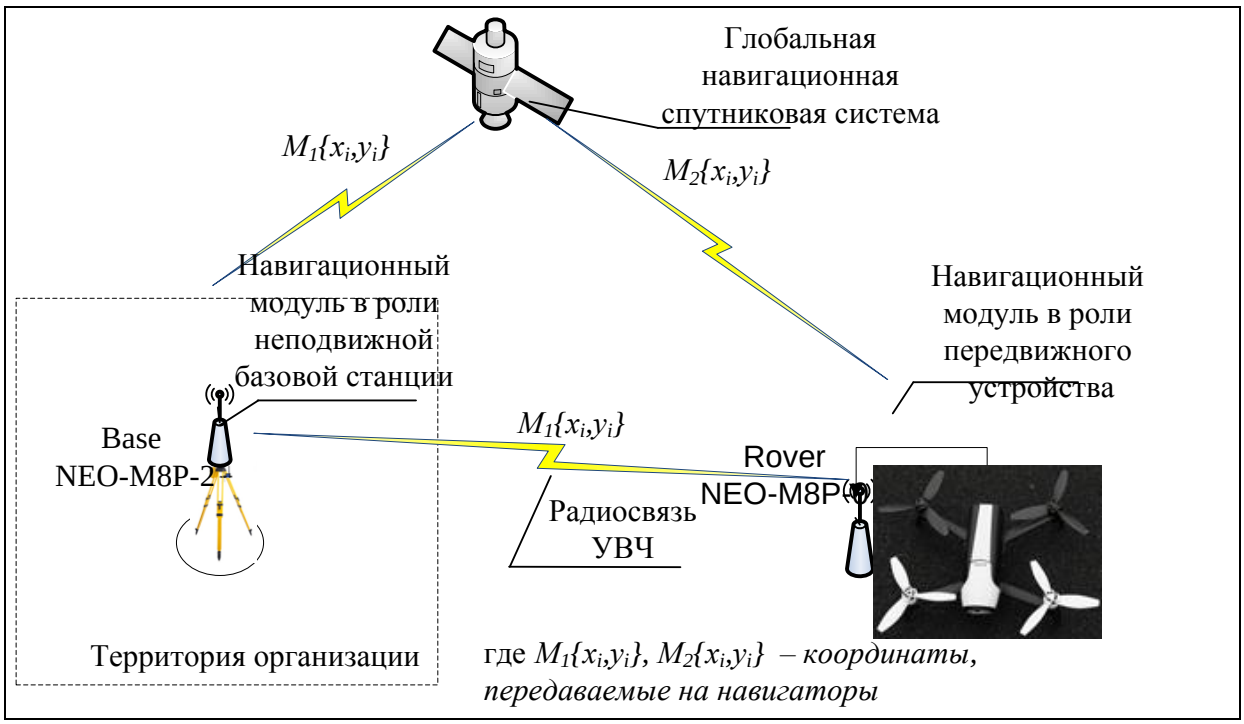


Рисунок 51 – Структурная схема системы защиты БПЛА с использованием отладочного комплекса модуля позиционирования «С94-М8Р»

В случае если корректировочные поправки от модуля базовой станции станут недоступными, второй модуль (ровер) будет работать как автономный приемник стандартной точности. Но для усиления процедуры проверки доступа возможно реализовать в программном средстве дополнительную проверку на условие получения поправочных данных от базовой станции: если данные будут получены, то доступ при совпадении навигационного ключа может быть предоставлен, в ином случае – в доступе будет отказано.

Передача корректировочных поправок осуществляется радиосигналом в УВЧ диапазоне посредством электромагнитных волн. Канал передачи корректировочных поправок по умолчанию не зашифрован, т.е. существует уязвимость канала связи в виде фальсификации данных при передаче или глушения самого сигнала. В случае использования мобильных объектов с навигационными модулями повышенной точности вероятность ошибочного предоставления доступа (ошибка второго рода) будет снижена.

В приложении **Д** представлен фотоматериал по предварительным испытаниям квадрокоптера типа Parrot BEBOR 2 по сбору видеоинформации полевого оборудования АСУ нефтепровода. Испытания показали устойчивую работу БПЛА в реальных условиях и определили перспективу дальнейших исследований в этом направлении.

Заключение

Проведенный анализ выводов и рекомендаций позволяет констатировать то, что в результате проведенных разработок и исследований поставленная цель: повышение оперативности и достоверности методов контроля технического состояния распределенных управляющих систем в условиях воздействия пространственно-временных угроз на основе мониторинга информационных потоков – достигнута.

Для достижения цели в работе поставлены следующие задачи:

1) В соответствии с руководящими и методическим документами ФСТЭК разработана пространственно-временная актуальных модель угроз для АСУ протяженным в пространстве объектом, которая позволила определить основную концепцию мониторинга технического состояния и стратегию защиты информации для исследуемого в проекте класса промышленных объектов. В частности, выявлено, что более 56 % угроз реализуются через сетевые информационные каналы, что определило сетевой трафик как основной источник исследований в работе;

2) Построены структурно-функциональные, математические и имитационные модели, позволяющие исследовать объекты защиты, оптимизировать традиционные методы и средства идентификации технических состояний АСУ управления транспортным нефтепроводом в условиях воздействия пространственно-временных угроз.

В частности:

- построена структурно-функциональная модель АСУ протяженным промышленным объектом, выявлены основные функциональные подсистемы и информационные потоки, определен состав качественный состав сетевого трафика, как предмета исследования;
- построена математическая модель системы распознавания образов на основе ассоциативно-мажоритарного подхода (АМП), предназначенная для

достоверного и оперативного распознавания технического состояния АСУ протяженного объекта н основе признакового пространства сетевого трафика;

3) Построена модель сетевого трафика как информационного пространства условно бесконечного объема, включающая в себя математическое, графическое и численное представление процесса изменения информационных потоков и способов их регистрации. Модель позволила: выявить особенности сетевого трафика; недостатки существующих систем регистрации, последовательного поиска и обработки данных об информационном обмене между сетевыми узлами; подтвердила актуальность повышения производительности и достоверности идентификации сетевых процессов на основе АМП;

4) Разработан метод оценки технического состояния распределенной АСУ на основе мониторинга сетевых потоков информации (на примере системы транспортировки нефтегазового сырья). В основу разработки положены результаты исследования имитационных моделей отдельных участков нефтепровода, построенных на базе инструментальных средств системы SCADA/TraseMod, позволившие получить адекватные реальным условиям модели сетевого трафика, реализующие промышленные протоколы информационного обмена TCP/ModBus и позволяющие идентифицировать аномальные состояния в системе передачи данных. В процессе имитационного моделирования подтвердилась концепция использования сигнатур технического состояния АСУ для мониторинга состояния на основе АМП;

5) Разработан и исследован метод контроля директивных установок оператора в распределенной АСУ распределенным объектом на основе АМП. Новизна метода подтверждена положительным решением на изобретение, позволяющем производить контроль и анализ действий оператора в АСУ в режиме реального времени.

6) Разработан метод повышения живучести телекоммуникационной подсистемы АСУ ТП в условиях распределенной пространственно-временной модели угроз на основе. В основу метода положена концепция использования ЛЭП, как резервного канала связи в случае обнаружения обрыва связи по основному

каналу передачи информации между подсистемами нижнего и верхнего уровня АСУ;

7) Проведен анализ технико-экономической эффективности результатов исследований, который подтвердил эффективность исследований, в частности, оценки доступности к информации в АСУ в зависимости от степени аварии на объекте существенно повысились: в случае катастрофической ситуации – на 30 %, в случае угроз с низкой и средней степенью ущерба, соответственно – на 90 и 100 %. При дополнительных капитальных затратах на создание резервной линии связи в 680 тыс. рублей оценочный эффект от избежания возможного ущерба составляет около 15 млн. рублей;

8) По результатам исследований разработаны рекомендации по внедрению методов и средств контроля технического состояния распределенных АСУ ТП транспортировки нефтегазового сырья на предприятиях Оренбургской области.

Список использованных источников

1 Абдулаев, А. А. Телемеханические комплексы для нефтяной промышленности/ А. А. Абдулаев. – М.: Недра. 1982. – 200 с.

2 Абрамова, Т. В. Моделирование аномалий в информационной системе мониторинга состояния нефтепровода по данным сетевого трафика гипотез / Т. В. Абрамова, Т. З.Аралбаев, Р. Р. Галимов, А. В. Манжосов, М. Д. Хаеев // Безопасность: Информация, Техника, Управление: Материалы международной научной конференции (Октябрь 2018). – Санкт-Петербург: Изд-во ГНИИ «НАЦРАЗВИТИЕ». 2018. – С.5.

3 Абрамова, Т. В. Метод оперативного прогнозирования и ранжирования рисков информационной безопасности на основе ассоциативного подхода/ Т. В. Абрамова, Т. З. Аралбаев, Г. Г. Аралбаева, Р. Р. Галимов // Вопросы развития современной науки и практики в период становления цифровой экономики: Материалы международной научно-практической конференции (18 октября 2018 г.). – Санкт-Петербург : Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова. 2018. - URL: http://www.konferenc.ru/konferenc10_10_18_3.html (дата обращения 10.11.2018).

4 Абрамова, Т.В. Исследование эффективности метода оперативного поиска информации о сетевом трафике на основе ассоциативного принципа/ Т. В. Абрамова, Т. З. Аралбаев // Компьютерная интеграция производства и ИПИ-технологии: Материалы VII Всероссийской научно-практической конференции. – Оренбург, 2015. – С. 235-239.

5 Абрамова, Т.В. Программное средство «Ранжирование рисков от угроз на основе ассоциативного принципа»/ Т. В. Абрамова, Т. З. Аралбаев // Свидетельство о регистрации электронного ресурса. Рег. № 1646. Дата регистрации: 01.10.2018. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

6 Абрамова, Т. В. Программный комплекс «Моделирование сетевого трафика на базе протокола TCP/ModBUS»/ Т. В. Абрамова, Т. З. Аралбаев, Р. Р.

Галимов// Свидетельство о регистрации электронного ресурса. Рег. № 1657. Дата регистрации: 10.11.2018. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

7 Абрамова, Т. В., Моделирование системы мониторинга технического состояния АСУ трубопроводом по данным сетевого трафика/ Т. В. Абрамова, Т. З. Аралбаев, Р. Р. Галимов, А. В. Манжосов, М. Д. Хаеев // Безопасность: Информация, Техника, Управление: Материалы международной научной конференции (Октябрь 2018). – Санкт-Петербург: Изд-во ГНИИ «НАЦРАЗВИТИЕ». 2018. – С.4.

8 Абрамова, Т.В. Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности компьютерной сети/ Т. В. Абрамова, Т. З. Аралбаев// Свидетельство о регистрации электронного ресурса. Рег. № 1109. Дата регистрации: 20.05.2015. Оренбургский государственный университет. Университетский фонд электронных ресурсов.

9 Аграновский, А. В. О недостатках современных систем обнаружения вторжений/ А. В. Аграновский, С. А. Репалов, Р. А. Хади, М.Б., Якубец // Информационные технологии. – 2005. – № 5. – С. 39-43.

10 Аналитическая служба компании «Код безопасности» [Эл. ресурс]. / Российский разработчик программных и аппаратных средств защиты информации. 2008-2018 «Код Безопасности». – Режим доступа: https://www.securitycode.ru/documents/analytics/. - 12.03.2014.

11 Анохин, А. Н. Сбор данных о надежности выполнения управляющих действий оператором АСУ ТП/ А. Н. Анохин, Р. И. Машковцева, Ю. Н. Анохин, А. Ю. Захаркив / Обнинск: Обнинский институт атомной энергетики Национального исследовательского ядерного университета «МИФИ». – 2016. – С. 141-146.

12 Аралбаев, Т. З. Исследование эффективности методов мониторинга сетевого трафика на основе последовательного и ассоциативно последовательного принципов поиска актуальной информации/ Аралбаев Т. З., Абрамова Т. В. // СТИН,2017. - № 11. - С. 2-5. . - 4 с.

13 Аралбаев, Т. З. Выбор базовой функции при автоматизированной идентификации временных рядов на основе ассоциативно-мажоритарного подхода / Т. З. Аралбаев, Т. В. Абрамова, Р. Р. Галимов, Д. А. Гайфулина, Э. Р. Хакимова// Вестник Ижевского государственного технического университета имени М. Т. Калашникова. – 2018. – Т. 21. – № 4. – 3 с.

14 Аралбаев, Т. З. Контроль и управление доступом в АСУ ТП на основе биометрических характеристик пользователя/ Т. З. Аралбаев, А. Г. Африн. – Уфа: Гилем. 2008. – 124 с.

15 Аралбаев, Т.З. Структурно-параметрический и структурно-топологический синтез распределённых систем контроля и управления объектами нефтегазодобычи/ Т. З. Аралбаев, Р. Р. Галимов. – Уфа: Гилем. 2010. – 144с.

16 Аралбаев, Т.З. Исследование эффективности метода оперативного поиска информации о сетевом трафике на основе ассоциативного принципа/ Т. З. Аралбаев, Т. В. Абрамова // Современные информационные технологии в науке, образовании и практике : Материалы VII Всероссийской научно-практической конференции. – Оренбург: Оренбургский государственный университет. – 2015. – С. 235-239.

17 Аралбаев, Т. З. Исследование эффективности методов мониторинга сетевого трафика на основе последовательного и ассоциативно последовательного принципов поиска актуальной информации/ Т. З. Аралбаев, Т. В. Абрамова // СТИН. – 2017. – № 11. – С. 2-5.

18 Аралбаев, Т. З. Моделирование сетевых атак на ресурсы вычислительных систем с использованием принципов самоорганизации/ Т. З. Аралбаев, Т. В. Абрамова // Современные информационные технологии в науке, образовании и практике: Материалы XI Всероссийской научно-практической конференции. – Оренбург: ООО ИПК «Университет». – 2014. – С. 109-114.

19 Аралбаев, Т. З. Особенности оперативного поиска информации о сетевом трафике по первичным данным аномальной активности компьютерной сети/ Т. З. Аралбаев, Т. В. Абрамова // Информационная безопасность: Материалы XIV

международной научно-практической конференции. − Таганрог: Изд-во ИКТИБ ЮФУ. 2015. − С. 76 – 81.

20 Аралбаев, Т. З. Комбинаторная семантическая модель генерации гипотез / Т. З. Аралбаев, Т. В. Абрамова, Р. Р. Галимов // Информация и безопасность. – 2016. – Т. 19. – №. 3. – С. 379-384.

21 Аралбаев, Т. З. Построение адаптивных систем мониторинга и диагностирования сложных промышленных объектов на основе принципов самоорганизации/ Т. З. Аралбаев. – Уфа : Гилем. 2003. – 248 с.

22 Аралбаев, Т. З. Сигнатурный метод контроля поведения пользователя на основе теории автоматов/ Т. З. Аралбаев, И. И. Каскинов // Наука и мир, –2017. – № 1(41). – С. 27-30.

23 Ароян, З. А. Мониторинг магистральных нефтепроводов с помощью беспилотных летательных аппаратов/ З. А. Ароян, О. А. Коркишко, Г.В. Сухарев. – URL: https://russiandrone.ru (дата обращения 10.11.2018).

24 Бади, Б. Методы оптимизации. Вводный курс/Б. Бади. – М.: Радио и связь, 1988. – 128 с.

25 Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007). – URL: https://zlonov.ru/laws/ics/ (дата обращения 10.11.2018).

26 Белов, Е. Б. Основы информационной безопасности: Уч. пособие для вузов/ Е. Б. Белов. – М.: Горячая линия – Телеком. 2006. – 544 с

27 Блекуэлл, Д. Теория игр и статистических решений /Д. Блекуфлл, М. А. Гиршик// Под редакцией В. А. Севастьянова. — М.: Издательство иностранной литературы, 1958. — 376 с.

28 Боев, Н.М. Анализ командно-телеметрической радиолинии связи с беспилотными летательными аппаратами // Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. – 2012. – № 2 (42). – Красноярск: СибГАУ. – С.86–91.

29 Бояркин, М. А., Моделирование деятельности операторов АСУ ТП НТК/ М. А. Бояркин, В. А. Шапцев // Вестник кибернетики. – 2006. – № 5. – С.77-87.

30 Брицов, Р. А. Ранжирование информации на основе оценок и поведения пользователей/Р. А. Брицов // T-Comm: Телекоммуникации и транспорт. – 2016. – Том 10. – № 1. – С. 62-66.

31 Васютинская, С. И. Комбинированная система мониторинга трубопроводов PROVISTA, использующая преимущества волоконных технологий и БЛА при аэросъемке потенциально опасных событий/С. И. Васютинская, Х. Х. Штубер// Известия ВУЗов. Геодезия и аэрофотосъемка. № 4, 2015 г. – С.1140117.

32 Галимов, Р. Р. Комбинаторная семантическая модель генерации гипотез/Р. Р. Галимов, Т. З. Аралбаев, Т. В. Абрамова// Прикладная программа. – Оренбург: ОГУ. - 2016. - 14 с.

33 Галимов, Р. Р. Распределённая система мониторинга технологических объектов как система массового обслуживания // Прикладная математика и информационные технологии в науке и образовании : Материалы науч.-практ. конф.– Уфа: КИЦ БашГУ. 2008. – С. 29-34.

34 Гамбаров, Г. М. Статистическое моделирование и прогнозирование: Учебное пособие для экономических специальностей вузов / Под ред. А.Г. Гранберга. – М.: Финансы и статистика. 1990. – 382 с.

35 Гаспарянц, Р. С. Организационно-технологическая система обеспечения эксплуатационной надёжности магистральных нефтепроводов: автореф. дис. … д-ра техн. наук/Р. С. Гаспарянц. — Уфа 2008. — 50 с.

36 Гольянов, А. А. Анализ методов обнаружения утечек на трубопроводах/ А. А. Гольянов // Транспорт и хранение нефтепродуктов, . – 2002. – № 10-11. – С. 5-14.

37 ГОСТ 24.701-86. Надёжность автоматизированных систем управления. Основные положения [Электронный ресурс]. – URL: http://docs.cntd.ru/document/1200022035 (дата обращения 10.11.2018).

38 ГОСТ Р 51028-97. Устройство защиты от ошибок аппаратуры передачи данных. Методы защиты. – Москва: Издательство стандартов. 1997. – 38с.

39 Грицай, Г. Positive Technologies. Безопасность промышленных систем в цифрах/ Г. Грицай, А. Тиморин, Ю. Гольцев. - URL:

https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/SCADA-analytics-rus.pdf (дата обращения 23.01.2018).

40 Елисеев, Н. П. GSM-Модули: области применения и производители/Н. П. Елисеев // Электроника: Наука, технология, бизнес. – 2012. – № 7(121). – С. 50-59..

41 Зегжда, Д. П. Информационная безопасность: учебник для вузов. / Д. П. Зегжда; М.: МГТУ им. Н.Э. Баумана, 2010. — 236 с. - ISBN 5-935170-18-3 .

42 Иванов, И. П., Бойченко М.К. Мониторинг ресурсов узлов корпоративной сети // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2010. № 2. С. 114-120.

43 Ивахненко, А. Г. Индуктивный метод самоорганизации моделей сложных систем/А. Г. Ивахненко. – Киев: Наукова думка. 1982. - 296 с.

44 Каскинов, И. И. Ассоциативно-мажоритарная модель системы контроля поведения пользователя на основе теории автоматов/ И. И. Каскинов // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. XXII междунар. студ. науч.-практ. конф. № 11(22). URL: https://sibac.info/archive/meghdis/11(22).pdf (дата обращения 11.11.2018).

45 Каскинов, И. И. Концепция мониторинга аномального поведения пользователей в распределенных сетях на основе автоматной модели по результатам аналитического обзора / И. И. Каскинов // Вектор развития современной науки : сборник материалов X Международной научно-практической конференции. (Москва, 03 апреля 2016). – С. 496-504.

46 Качков, В. П. Ассоциативная память и ассоциативные процессоры в интеллектуальных системах / В. П. Качков, И. Я. Доморадов, Р. Е. Сердюков// Под науч. ред. В. В. Голенкова. – Минск : БГУИР, 2009. – 188 с.

47 Кендалл, М. Дж. Многомерный статистический анализ и временные ряды / М. Дж. Кендалл, А. Стюарт// Пер. с англ. – М.: Наука. 1976. – 736с.

48 Коробкина, Н. Н. Исследование и разработка информационно-поисковых интерфейсов на основе типологии поведения пользователей: автореф. дис. … канд. тех. наук./ Н. Н. Коробкина; Рос. гос. гуманитар. ун-т (РГГУ). 2014. - 18 с.

49 Котарев, С. Н. Использование беспилотных летательных аппаратов для обеспечения безопасности на объектах транспорта/ С. Н. Котарев, О.В. Котарева, А.Н. Александров // Вестник Восточно-Сибирского института министерства внутренних дел. – 2017. - № 4(83). – С. 199-204.

50 Кохонен, Дж. Ассоциативные запоминающие устройства/ Дж. Кохонен. – Москва: Мир. 1982. – 384 с.

51 Криволапов, В. Г. Комплексная методика моделирования рисков информационной безопасности открытых систем : автореф. дис. на соиск. учен. степ, канд. техн. наук : специальность 05.13.19 Методы и системы защиты информ., информ. Безопасность/ В. Г. Криволапов; Центр информ. технологий и систем внутрен. власти. – М., 2009. – 23 с.

52 Круг, Г. К. Планирование эксперимента в задачах идентификации и экстраполяции/ Г. К. Круг. – М.: Наука, 1977. – 208с.

53 Курицын, Е.М. Сценарии организации цифровых трактов для ВЧ-связи по высоковольтным линиям электропередачи/Е. М. Курицын, Ю. А. Сосулин, В. А. Фатуев // Технология и конструирование в электронной аппаратуре. – 2007. – № 1. – С. 3-12.

54 Латышев, Л. Н. Система обнаружения несанкционированных врезок в магистральный нефтепровод / Л. Н. Латышев, З. Р. Насырова // Нефтегазовое дело. – 2006. – С. 1-10.

55 Леонович, И. А. Разработка методики прогнозирования возникновения аварийных ситуаций на компрессорных станциях магистральных газопроводов. Диссертация на соискание учёной степени кандидата технических наук/ И. А. Леонович. – Москва: Российский государственный университет нефти и газа имени И.М. Губкина, 2016. – 181 с..

56 Манжосов, А. В. Организация системы передачи информации в распределенной системе мониторинга протяженного технологического объекта/ А. В. Манжосов, Т. З. Аралбаев, Т. В. Абрамова // «Инновационные, информационные и коммуникационные технологии: сборник трудов XV международной научно-практической конференции; Сочи, 2018. − С. 386 – 390.

57 Машечкин, И. В. Мониторинг и анализ поведения пользователей компьютерных систем/ И. В. Машечкин, М. И. Петровский, С.В. Трошин // Проблемы программирования. – 2008. – № 2-3. – С. 541-549.

58 Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007). URL: https://www.securitylab.ru/blog/personal/zlonov/144489.php. (дата обращения 11.11.2018).

59 Наинг, Л. З. Исследование и разработка методов передачи данных в системах управления технологическими процессами с использованием PLC сети: диссертация ... кандидата технических наук : 05.13.06 [Место защиты: Нац. исслед. ун-т МИЭТ]/ Л. З. Наинг. – Москва, 2015. – 132 с.

60 Никифоров, А. В. Технология PLC – телекоммуникации по сетям электропитания / А. В. Никофоров// Сети и системы связи.– 2002.– № 5.– С. 89-96.

61 Обзор программ анализа и мониторинга сетевого трафика. – URL: http://pi.314159.ru/volotka/volotka1.htm (дата обращения 10.11.2018).

62 Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007). URL: https://www.securitylab.ru/blog/personal/zlonov/144489.php. (дата обращения 11.11.2018).

63 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 г. № 17. URL : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 11.11.2018).

64 Основы информационной безопасности: Уч. пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком. 2006. – 544 с.

65 Остиану, В. М. Характеристики распределённых автоматизированных систем управления ПТК // Промышленные АСУ и контроллеры. – 2002. - № 10. – С. 5 - 9.

66 Пантелеев, В. В. Образование транспорта интегрированной сети доступа на существующей первичной сети электросвязи/ В. В. Пантелеев, А. К. Громовой // Сценарии связи по ВЛЭП. – 1999. – № 8. – С. 51-55.

67 Патент 2306605 Российская Федерация. Устройство для распознавания образов / Аралбаева Г. Г., Аралбаев Т. З., Хасанова С. В., Хасанов Р. И.; заявитель и патентообладатель ОГУ. – № 2014102726/08; заявл. 28.01.2014; опубл. 10.12.2014, Бюл. №34. – 18 с.

68 Патент 2306605 Российская Федерация, МПК 7 G11C15/00. Ассоциативная память / Кабак И. С., Суханова Н. В: заявитель и патентообладатель Кабак И. С., Суханова Н. В; заявл. 2007-12-24; опубл. 20.10.2008.

69 Патент 2430415 Российская Федерация, МПК G 06 K 9/00. Устройство для распознавания образов / Р.И. Хасанов, М.З. Масягутов, Т.З. Аралбаев; заявитель и патентообладатель Оренбургский государственный университет. – №2010116601/08; заявл. 26.04.2010 – опубл. 27.09.2011, Бюл. № 27. – 21 с.

70 Патент 2533064 Российская Федерация, МПК G 06 K 9/62. Устройство для распознавания образов / Сарайкин А.И., Хасанов Р.И., Аралбаев Т.З.; заявитель и патентообладатель Оренбургский государственный университет. – № 2013149729/08; заявл. 06.11.2013 – опубл. 20.11.2014, Бюл. № 32. – 16 с.

71 Патент 2534935. Российская Федерация, МПК G06Q90/00 Система и способ адаптивного управления и контроля действий пользователя на основе поведения пользователя / Леденев А.В., Колотинский Е.Б., Игнатьев К.С.; заявитель и патентообладатель Закрытое акционерное общество «Лаборатория Касперского». - № 2012156444/08; заявл. 25.12.2012; опубл. 10.12.2014, Бюл. № 34.

72 Патент 2540818 Российская Федерация. Устройство для распознавания образов / Аралбаев Т.З., Хасанов Р.И., Сарайкин А.И., Закревский Г.В. / заявитель и патентообладатель ОГУ. – № 2013138762/08; заявл. 20.08.2013; опубл. 10.02.2015, Бюл. № 4. – 19 с.

73 Патент 77483 Российская Федерация, МПК G06K9/62. Устройство для распознавания образов / Аралбаев Т.З, Африн А.Г. заявитель и патентообладатель Государственное образовательное учреждение высшего профессионального

образования «Оренбургский государственный университет»; заявл. 2006-02-28; опубл. 20.09.2007.

74 Патент 2193797 Российская Федерация, G06G007/60, Устройство ассоциативной памяти и способ распознавания образов / Сутерланд Дж. МПК. / заявитель и патентообладатель Сутерланд Дж. № 92016491/14; опубл. 27.11.2002.

75 Патент Российская Федерация Устройство для контроля поведения пользователя / Абрамова Т.В., Аралбаев Т.З., Каскинов И.И., Хатеев М.Д. Положительное решение о выдаче патента на изобретение. Заявка № 2018100997/08(001266). Дата подачи 10.01.2018.

76 Патент № 2025795 Российская Федерация, МПК G11C 15/00. Иерархическая система ассоциативной памяти / В.В. Борисов, И.В. Огнев, приоритет / патентообладатель Борисов В.В.; опубл. 30.12.1994.

77 Пищик, Б. Н. Безопасность АСУ ТП/ Б. Н. Пищик // Вычислительные технологии Том 18, Специальный выпуск, – 2013. – С. 170-175.

78 Подробное описание протокола Modbus TCP с примерами команд [Электронный ресурс]. –URL: https://ipc2u.ru/articles/prostye-resheniya/modbus-tcp/. (дата обращения 10.11.2018).

79 Положение о Реестре ключевых систем информационной инфраструктуры (утв. приказом ФСТЭК России от 04.03.2009). URL: https://www.securitylab.ru/blog/personal/zlonov/144489.php. (дата обращения 11.11.2018).

80 Почкалов, А. АСУ ТП добычи нефти «Регион-2000» / А. Почкалов // IT-решения в нефтегазовой промышленности. – 2002. - № 8. – С. 57-60.

81 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ от 11 февраля 2013 г. № 17. – М., 2013.

82 Программно-аппаратное средство «Ланграф-БИТ» [Электронный ресурс]. – Магазин Nag, 1995-2010 – URL : http://shop.nag.ru/catalog (дата обращения 11.11.2018).

83 Программно-аппаратный комплекс СКАТ [Электронный ресурс]. – Магазин Nag, 1995-2010 – Режим доступа: http://shop.nag.ru/catalog/14605.SKAT – 04.06.2015 (дата обращения 11.11.2018).

84 Пьявченко, Т. А. Проектирование АСУТП в SCADA-системе: учебное пособие. – Таганрог: Изд-во Технологического института ЮФУ. 2007. – 78 с.

85 Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 19.11.2007). URL : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 11.11.2018).

86 Савина, А. В. Аварийность на отечественных и зарубежных магистральных трубопроводах // Безопасность труда в промышленности. – 2014. - № 2. – С. 14-17.

87 Савинова, В. М. Осадчая Идентификация пользователей корпоративной системы с помощью поведенческого анализа с использованием модели искусственной нейронной сети/ В. М. Савинова, Е.С. Бесхмельницкий, А.Д. Бибина // Транспортное дело России. – 2017. – № 5. – С. 65-68.

88 Оперативный поиск информации о сетевом трафике по первичным данным аномальной активности компьютерной сети: свидетельство о рег. прогр. ср-ва № 1109 / Т. В. Абрамова, Т. З. Аралбаев; правообладатель Оренбургский государственный университет. – зарег. 20.05.2015.

89 Эмулятор устройства для контроля поведения пользователя: свидетельство о рег. прогр. ср-ва № 1547 / Т. З. Аралбаев, М. Д. Хатеев; правообладатель Оренбургский государственный университет. – зарег. 12.04.2018.

90 Синергетическая имитационная модель сетевых атак на ресурсы вычислительных систем: свидетельство о рег. прогр. ср-ва № 970 / Т. В. Абрамова, Т. З. Аралбаев, М. С. Гаврилов; правообладатель Оренбургский государственный университет. – зарег. 3.06.2014.– 2540 Кбайт.

91 Комбинаторная семантическая модель генерации гипотез: свидетельство о рег. прогр. ср-ва № 1236 / Т.В. Абрамова, Т.З. Аралбаев, Р. Р. Галимов; правообладатель Оренбургский государственный университет. – зарег. 29.03.2016.

92 Семенов, А. Б. Волоконно-оптические подсистемы современных СКС/ А. Б. Семенов. – М. : Академия АйТи; ДМК. 2007. – 632 с.

93 Сергиенко, А. Б. Цифровая обработка сигналов/ А. Б. Сергиенко. – СПб.: Питер, 2003. – 608 с.

94 Сережин, Д. В. Обоснование выбора контроллера телеметрии для передачи продуктов нефтегазовой отрасли: Материалы межвузовской научно-технической конференции/ Д. В. Сережин. – 2004 г. - Ч.7: - С.86-87,

95 Система мониторинга работы пользователей с информационными ресурсами корпоративной компьютерной сети на основе моделирования поведения пользователей с целью поиска аномалий и изменений в работе [Электронный ресурс]. – URL: http://poleznayamodel.ru/model/10/105042.html (дата обращения 12.04.2018).

96 Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий (утв. Секретарем Совета Безопасности от 08.11.2005) URL : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 11.11.2018).

97 Скакун, С. В. Математическое моделирование поведения пользователей компьютерных систем // Математические машины и системы, - 2005. - № 2. - С. 122–129.

98 Сонькин, Д. М. Мобильные оперативные группы в системах связи и управления/ Д. М. Сонькин, М. А. Сонькин, А. А. Шамин, В. З. Ямпольский // Моделирование, оптимизация и информационные технологии – Томск: Томский политехнический университет, - 2017. - № 2. [Электронный ресурс]. – URL: https://moit.vivt.ru/ (дата обращения 11.11.2018).

99 Способ передачи информации: [Электронный ресурс]. - URL: http://www.nrtb.ru/about_firm/patenty_detail.php?ELEMENT_ID=1801 - (дата обращения 11.11.18).

100 Транспортный уровень. Протоколы TCP и UDP [Электронный ресурс].– URL: http://opds.sut.ru/old/electronic_manuals/it_emd/tema_2/index.htm - (дата обращения 11.11.2018).

101 Трошин, С. В. Мониторинг работы корпоративных пользователей // Вопросы современной науки и практики. Университет им. В. И. Вернадского,- 2009. - № 2(16). - С. 59-72.

102 Трубопроводный транспорт нефти / С.М. Вайншток, В.В. Новоселов, А.Д. Прохоров, А.М. Шаммазов и др.; Под ред. С.М. Вайнштока: Учеб. для вузов: В 2 т. – М.: ООО «Недра-Бизнесцентр». 2004. – Т.2. – 621 с.

103 Ужинский, А. В. Методы и средства мониторинга сервисов передачи данных в глобальных распределенных инфраструктурах : автореф. дис. … канд. техн. наук: автореферат дис. ... кандидата технических наук : 05.13.01 / Ужинский Александр Владимирович; [Место защиты: Междунар. ун-т природы, общества и человека «Дубна»]. – Дубна. 2010. – 20 с.

104 Цуканова, О. А. Экономика защиты информации: учебное пособие / О. А. Цуканова. – СП6. : СП6 ГУИТМО. 2007. – 59 с.

105 ЦЭР: Обзор программ анализа и мониторинга сетевого трафика [Электронный ресурс]. – Наука, техника, образование, 1999-2015 – Режим доступа: http://pi.314159.ru/volotka/volotka1.htm - 04.06.2015

106 Черноруцкий, И. Г. Методы принятия решений/ И. Г. Черноруцкий. – СПб.: БХВ – Петербург. 2005. – 736 с.

107 Шелупанов, А. А. Прогнозирование в системе мониторинга локальных сетей / А. А. Шелупанов, С. Ю. Исхаков, С. В. Тимченко // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012, – № 1-2. – С. 100-103.

108 Якубец, М. Б. Обнаружение сетевых атак методом поиска аномалий на основе вероятностного и верификационного моделирования/ М. Б. Якубец // Искусственный интеллект. – 2006. – № 3. – С. 816 - 823.

109 Aralbaev T. Z., Abramova T.V. Network Traffic Monitoring on the Basis of Sequential and Associative–Sequential Search Principles // Russian Engineering Research.

– 2018. Vol. 38, - №. 5, - pp. 381–383. © Allerton Press, Inc., 2018. ISSN 1068-798X Original Russian Text © T.Z. Aralbaev, T.V. Abramova, 2017, published in STIN, - 2017, №. 11. - pp. 2–5.

110 Chevaleyre Y., Endriss U., Maudet N. Simple negotiation schemes for agents with simplepreferences: sufficiency, necessity and maximality. Autonomous Agents and Multi //Agent Systems. - № 20(2). - 2010. - pp. 234-259.

111 Christopher M. Talbot, Michael A. Temple, Timothy J. Carbino, J. Addison Betances, Detecting rogue attacks on commercial wireless Insteon home automation systems, Computers & Security, In press, corrected proof, Available online 13 October 2017. DOI: 10.1016/j.cose.2017.10.001.

112 DATAPK: программный комплекс для полноценной защиты АСУ ТП. [Электронный ресурс]: – URL: http://www.pressreader.com/russia/ekspert-ural/20140929/281947426075740.

113 Abdo H., Kaouk M., Flaus J.-M., Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis, Computers & Security, Volume 72, January 2018, - p. 175-195. DOI: 10.1016/j.cose.2017.09.004.

114 ModBus TCP. Промышленный протокол для TCP/IP-сетей. [Электронный ресурс]. – LAZY SMART, 2015–2018 – URL: http://lazysmart.ru/osnovy-avtomatiki/modbus-tcp-promy-shlenny-j-protokol-dlya-tcp-ip-setej/ (дата обращения 22.10.2018).

115 NEO-M8P Глонасс/GPS модуль повышенной точности определения местоположения [Электронный ресурс]: – URL: http://ultran.ru/neo-m8p (дата обращения 31.08.2018).

116 Niv Goldenberg, Avishai Wool, Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems, International Journal of Critical Infrastructure Protection, Volume 6, Issue 2, June 2013, - pp. 63-75. DOI: 10.1016/j.ijcip.(2013.05.001).

117 Rafael Ramos Regis Barbosa, Ramin Sadre, Aiko Pras, Flow whitelisting in SCADA networks, International Journal of Critical Infrastructure Protection, Volume 6, Issues 3–4, December. - 2013, - pp. 150-158. DOI: 10.1016/j.ijcip.(2018.08.03).

118 Ramakrishnan P. Self-Similar Traffic Models. Technical research report. 1999. Available at: http://www.isr.umd.edu/TechReports/ISR/1999/TR_99-12/TR_99-12.phtml , accessed 09.07.2018.

119 Reporter Analyzer - программно-аппаратный комплекс для мониторинга, анализа, учета сетевого трафика [Электронный ресурс]. – Магазин Nag, 1995-2010 – URL: http://shop.nag.ru/catalog (дата обращения 10.11.2018).

120 Song X. Conditional anomaly detection / X. Song et al. //Knowledge and Data Engineering, IEEE Transactions on. – 2007. – Vol. 19, - №. 5. – pp. 631-645.

Приложение А

(обязательное)

Классификация угроз информационной безопасности

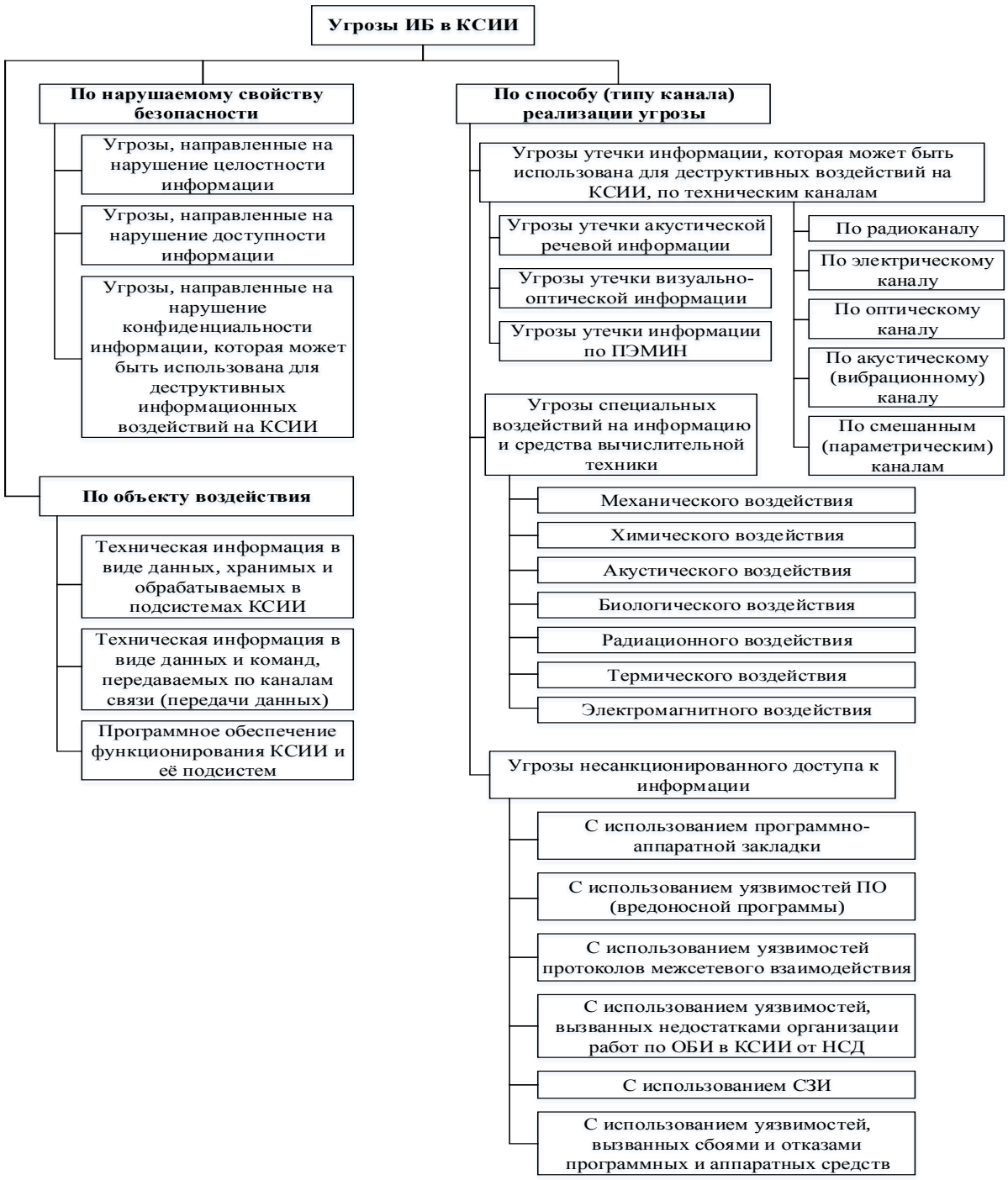


Рисунок А.1 – Классификация угроз ИБ системы управления транспортным трубопроводом

Приложение Б

(обязательное)

Модель угроз информационной безопасности

Таблица Б.1 – Модель актуальных сетевых угроз ИБ

Наименование угрозы	Вероятность реализации угрозы	Коэффициент опасности угрозы	Актуальность угрозы
1	2	3	4
Физического проникновения на территории без возможности проникновения в помещения с техническими средствами обработки и носителями информации Физического проникновения на территорию (в помещении)	Высокая	Средняя	Актуальная
Потеря носителя информации	Средняя	Средняя	Актуальная
Подбора пароля BIOS путём перебора вручную на основе предварительно собранных данных о пользователе	Низкая	Высокая	Актуальная
Обхода заданного пароля BIOS	Низкая	Высокая	Актуальная
Обход заданного пароля BIOS путём обесточивания материнской платы (съём аккумулятора)	Низкая	Высокая	Актуальная
Обход заданного пароля BIOS путём переключения «джамперов» с целью обнуления BIOS	Низкая	Высокая	Актуальная
Обход заданного пароля BIOS путём подмены микросхемы BOIS	Низкая	Высокая	Актуальная
Подбора пароля доступа посредством ввода учётного имени и пароля, заданных по умолчанию, для используемой ОС	Средняя	Высокая	Актуальная

Продолжение таблицы Б.1

1	2	3	4
Перебор вариантов пароля вручную на основе предварительно собранных данных о пользователе	Средняя	Высокая	Актуальная
Запуск программного продукта, выявляющего пароль, записанного на гибкий магнитный диск	Низкая	Высокая	Актуальная
Запуск программного продукта, отключающего пароль, записанного на компакт-диске с функцией автозапуска	Низкая	Высокая	Актуальная
Перезагрузка ПВЭМ	Низкая	Высокая	Актуальная
Выявление пароля BIOS при загруженной ОС, посредством использования программ выявления пароля	Низкая	Высокая	Актуальная
Выявление пароля доступа путём запуска утилит декодирующих файлы хранения паролей	Низкая	Высокая	Актуальная
Выявление пароля доступа путём извлечения паролей из оперативной памяти	Низкая	Высокая	Актуальная
Выявление пароля доступа путём хищения (копирования) файлов паролей	Низкая	Высокая	Актуальная
Редактирование системного реестра с целью запуска программ, меняющих привилегии пользователя	Низкая	Высокая	Актуальная
Инсталляция программного обеспечения «шпион клавиатуры»	Низкая	Очень высокая	Актуальная
Инсталляция программного обеспечения, расширяющего привилегии пользователя	Низкая	Высокая	Актуальная
Инсталляции и запуска вируса	Средняя	Очень высокая	Актуальная
Перезагрузка ОС с целью загрузки альтернативной ОС с нештатного носителя для расширения привилегий	Низкая	Высокая	Актуальная

Продолжение таблицы Б.1

1	2	3	4
Определение сетевого адреса (IP адреса)	Средняя	Высокая	Актуальная
Определение открытых портов удалённого хоста	Средняя	Высокая	Актуальная
Идентификация запущенных сетевых служб	Средняя	Высокая	Актуальная
Определение типа ОС удалённого хоста	Средняя	Высокая	Актуальная
Определение типа ОС маршрутизатора	Высокая	Высокая	Актуальная
Определение сетевых ресурсов, открытых для совместного пользования	Средняя	Высокая	Актуальная
Выявление маршрутов прохождения пакетов информации	Высокая	Высокая	Актуальная
Определение имён пользователей и групп	Средняя	Высокая	Актуальная
Получение информации об используемых приложениях, установленных на ПЭВМ	Средняя	Высокая	Актуальная
Удалённый подбор пароля доступа посредством ввода имени и пароля, заданных по умолчанию	Низкая	Высокая	Актуальная
Подбора имени и пароля посредством перебора	Низкая	Высокая	Актуальная
Удалённый подбор пароля доступа посредством ввода имени и пароля, заданных по умолчанию для используемой ОС	Средняя	Высокая	Актуальная
Подбор имени и пароля посредством перебора	Низкая	Высокая	Актуальная
Получение доступа к программам удалённого администрирования посредством ввода имени и пароля, заданных по умолчанию для используемой ОС	Высокая	Высокая	Актуальная

Продолжение таблицы Б.1

1	2	3	4
Получение доступа к программам удалённого администрирования путём подбора имени и пароля посредством перебора	Средняя	Высокая	Актуальная
Внедрение ложного доверенного объекта путём подмены таблицы преобразования адресов (ARP spoofing)	Высокая	Высокая	Актуальная
Внедрение ложного доверенного объекта путём подмены сетевого адреса (IP spoofing)	Высокая	Высокая	Актуальная
Внедрение ложного доверенного объекта путём подмены сервера доменной системы имён (DNS spoofing)	Высокая	Высокая	Актуальная
Получение необходимой (защищаемой) информации пользователя	Средняя	Высокая	Актуальная
Получение хэш-кода пароля	Средняя	Высокая	Актуальная
Получения пароля, передаваемого по сети в явном (не зашифрованном) виде	Средняя	Высокая	Актуальная
Поиск ресурсов, доступных для записи, запуска ПО	Средняя	Высокая	Актуальная
Анализ комментариев к учётным записям	Средняя	Высокая	Актуальная
Инсталляция программного обеспечения, расширяющего привилегии пользователя	Высокая	Низкая	Актуальная
Переполнение буфера с запуском исполняемого кода	Высокая	Высокая	Актуальная
Инсталляция программного обеспечения «шпион клавиатуры»	Средняя	Очень высокая	Актуальная
Инсталляция программного обеспечения, разрушающего аппаратное обеспечение компьютера	Средняя	Очень высокая	Актуальная
Инсталляция и запуск вируса	Средняя	Высокая	Актуальная

Продолжение таблицы Б.1

1	2	3	4
Инсталляция программ удалённого управления	Средняя	Очень высокая	Актуальная
Подмена системного программного обеспечения	Низкая	Очень высокая	Актуальная
Редактирование системного реестра с целью запуска программ, меняющих привилегии пользователя	Низкая	Очень высокая	Актуальная
Перехвата внутрисегментного сетевого трафика	Низкая	Очень высокая	Актуальная
Перехват трафика маршрутизатора	Высокая	Очень высокая	Актуальная
Перенаправление сетевого трафика посредством изменения таблиц маршрутизации на сетевых устройствах	Низкая	Высокая	Актуальная
Перенаправление сетевого трафика посредством передачи ложных пакетов протокола маршрутизации (RIP)	Средняя	Высокая	Актуальная
Внедрение ложного доверенного объекта путём подмены таблицы преобразования адресов (ARP spoofing)	Высокая	Очень высокая	Актуальная
Внедрение ложного доверенного объекта	Высокая	Очень высокая	Актуальная
Внедрение ложного доверенного объекта путём подмены сервера доменной системы имён (DNS spoofing)	Высокая	Очень высокая	Актуальная
Копирования информации на нештатные носители информации	Средняя	Очень низкая	Актуальная
Подбор пароля к электронному почтовому ящику	Низкая	Очень высокая	Актуальная
Перехват пароля к электронному ящику	Низкая	Очень высокая	Актуальная
«Шторм» ложных сообщений для почтового ящика (spam)	Высокая	Низкая	Актуальная

Продолжение таблицы Б.1

1	2	3	4
Перехват почтовых сообщений	Средняя	Высокая	Актуальная
Посылки скрытых вредоносных программ («троянов»)	Высокая	Очень высокая	Актуальная
Атаки, основанные на уязвимостях Web-браузеров	Низкая	Очень высокая	Актуальная
Запуск программ с удалённого узла	Высокая	Очень высокая	Актуальная
Сохранение (запись) файлов на жёсткий диск пользователя	Средняя	Очень высокая	Актуальная
Атаки, основанные на уязвимостях Web-серверов	Высокая	Очень высокая	Актуальная
Использование ошибок в сценариях автоматизации	Высокая	Очень высокая	Актуальная
Обход межсетевого экрана посредством инкапсуляции данных в заголовки пакетов протокола обмена управляющими сообщениями (ICMP)	Высокая	Очень высокая	Актуальная
Обход межсетевого экрана посредством перенаправления портов	Средняя	Очень высокая	Актуальная
Ошибки при проектировании программных средств	Низкая	Очень высокая	Актуальная
Ошибки при проектировании технических средств	Низкая	Очень высокая	Актуальная
Ошибки при изготовлении программных средств	Низкая	Очень высокая	Актуальная
Ошибки при изготовлении технических средств	Низкая	Очень высокая	Актуальная
Ошибки при эксплуатации технических средств	Низкая	Очень высокая	Актуальная
Ошибки при эксплуатации программных средств	Низкая	Очень высокая	Актуальная
Сбой, отказ технических средств	Средняя	Очень высокая	Актуальная

Продолжение таблицы Б.1

1	2	3	4
Отказ оборудования связи	Средняя	Очень высокая	Актуальная
Обрыв линии связи	Средняя	Очень высокая	Актуальная
Сбой, отказ программных средств	Средняя	Очень высокая	Актуальная

Приложение В

(обязательное)

Построение и исследование имитационной модели передачи информации с использованием программного эмулятора протокола Modbus

Особенность контроля технического состояния системы мониторинга распределенного объекта заключается в том, что большинство искомых параметров о состоянии АСУ оператор получает из сетевого трафика при передаче данных в корпоративной информационной системе. Большинство современных АСУ ТП для организации передачи информации используют протокол Modbus. При обнаружении инцидентов, связанных с некорректной работой полевого оборудования также в первую очередь анализируются коммуникационные протоколы, в частности, ModBus.

Соответственно, перед современными системами контроля состояния АСУ ТП стоит задача оперативного поиска и анализа информации о состоянии распределенного объекта в сетевом трафике по данным протокола Modbus. Моделирование подобных систем позволяет исследовать процесс передачи информации в АСУ ТП без вмешательства в работу реальной системы.

Цель исследования – повышение оперативности обнаружения неисправностей промышленного оборудования за счёт анализа сетевого трафика. Объект исследования – протокол передачи данных Modbus. Предмет исследования – возможность использования протокола Modbus для анализа состояния распределённых промышленных объектов. Гипотеза исследования – чтение Modbus-трафика позволяет анализировать состояние промышленного оборудования и предсказывать аварийные ситуации.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Проанализировать структуру пакета протокола Modbus.
2) Описать процесс передачи кадра Modbus по уровням модели OSI.

3) Организовать передачу данных по протоколу Modbus между двумя имитационными программными средствами;

4) Отследить в сетевом трафике обмен данными по протоколу Modbus;

5) Зафиксировать в сетевом трафике обрыв соединения между устройствами, использующими протокол Modbus.

Modbus — коммуникационный протокол, основанный на архитектуре ведущий-ведомый (master-slave). Для передачи данных использует интерфейсы RS-485, RS-422, RS-232, а также Ethernet сети TCP/IP (протокол Modbus TCP). Элементы сети Modbus взаимодействуют, используя клиент-серверную модель, основанную на транзакциях, состоящих из запроса и ответа. Для передачи данных да дальние расстояния по сетям о Ethernet используется протокол ModBus TCP [78, 114], представляющий собой стандартный пакет ModBus с добавлением данных стека TCP/IP (адреса и порты взаимодействия и т.п.).

Протокол Modbus предполагает, что только одно ведущее устройство (контроллер) и до 247 ведомых (модулей ввода-вывода) могут быть объединены в промышленную сеть. Обмен данными всегда инициируется ведущим. Ведомые устройства никогда не начинают передачу данных, пока не получат запрос от ведущего. Также ведомые устройства не могут обмениваться данными друг с другом. Адреса с 1 по 247 являются адресами Modbus-устройств в сети, а с 248 по 255 зарезервированы. Ведущее устройство не должно иметь адреса, и в сети не должно быть устройств с двумя адресами.

RTU (remote terminal unit) – удалённое терминальное устройство. Формат кадра протокола Modbus показан на рисунке В.1.

Рисунок В.1 – Формат кадра протокола Modbus RTU

Модель OSI (базовая эталонная модель открытых систем) для протокола Modbus представлена в таблице В.1.

Таблица В.1 – Модель OSI протокола Modbus

№ уровня	Название уровня	Реализация
7	Прикладной	Modbus application protocol
6	Уровень представления	Нет
5	Сеансовый	Нет
4	Транспортный	Нет
3	Сетевой	Нет
2	Канальный (передачи данных)	Протокол «Ведущий-ведомый». Режимы RTU и ASCII
1	Физический	RS-485 или RS-232

PDU (protocol data unit) – элемент данных протокола; ADU (application data unit) – элемент данных приложения.

Поле «Адрес» всегда (даже в ответах на команду, посланную ведущим) содержит только адрес ведомого устройства. Благодаря этому ведущее устройство понимает, от какого устройства пришёл ответ. Поле «Код функции» сообщает о том, какое действие нужно выполнить. В поле «Данные» ведущее устройство указывает параметры запроса для выполнения функции поля «Код функции». Поле данных может содержать значения состояния дискретных входов/выходов, адреса регистров, количество байтов данных, ссылки на переменные, количество переменных, код подфункций и т.п. Если ведомое устройство нормально выполнило принятую от ведущего функцию, то в ответе поле «Код функции» содержит ту же информацию, что и в запросе. В противном случае ведомый выдаёт код ошибки. В случае ошибки код функции в ответе равен коду функции в запросе, увеличенному на 128.

Коды функций являются числами в диапазоне от 1 до 127, причём коды в диапазоне от 65 до 72 и от 100 до 110 относятся к задаваемым пользователем функциям. Коды в диапазоне от 128 до 255 зарезервированы для пересылки кодов

ошибок в ответном сообщении. Код 0 не используется. Коды ошибок используются ведомым устройством, чтобы определить какое действие предпринять для их обработки. Четыре возможные реакции ведомого устройства на запрос ведущего представлены в таблице В.2.

Таблица В.2 – Виды реакций ведомого устройства на запрос ведущего

Запрос ведущего			
Реакция 1	Реакция 2	Реакция 3	Реакция 4
Ведомое устройство получает запрос, обрабатывает его и возвращает ответ	Ведомое устройство не получает запрос (обрыв связи) и ведущее устройство не получает ответ	Ведомое устройство получает запрос, но в запросе находятся повреждённые данные, или не хватает байт. Такой запрос игнорируется, ответ не посылается.	Ведомое устройство получает запрос без ошибок, но из-за некоторых условий не может его обработать. В таком случае ведомое устройство отвечает при помощи «Ответа с исключением» и отсылает ведущему код ошибки.

В сети с протоколом Modbus TCP устройства взаимодействуют по типу клиент-сервер, где в качестве клиента выступает ведущее устройство, в качестве сервера – ведомое. Основное отличие, которое накладывает TCP/IP на ModBus при их совместном использовании — непосредственное подключение к определённому адресу. Протокол TCP/IP устроен по принципу «клиент-сервер». Для обмена данными клиент открывает сеанс связи с сервером, указывая его адрес.

Переходя на терминологию протокола ModBus ведущее устройство (мастер) в TCP-сети становится клиентом (т.к. именно клиент является инициатором обмена данными), а подчинённое устройство (слейв) — сервером. Таким образом, для того чтобы передать запрос подчинённому устройству в TCP-сети мастер должен сначала открыть сеанс связи с ним. Причём открытие сеанса реализуется не на уровне протокола ModBus, а на уровне TCP/IP. Поэтому ведущее устройство не может средствами ModBus передавать запросы разным устройствам, так же, как это происходит в ModBus RTU или ASCII.

Протокол ModbusTCP (или ModbusTCP/IP) используется для подключения устройств с протоколом Modbus к Ethernet или сети Internet. Он использует кадры Mudbus RTU на 7-ом прикладном уровне модели OSI, протоколы Ethernet на 1-м и 2-

м уровнях модели OSI и TCP/IP на 3-м и 4-м уровнях. Можно сказать, что Ethernet TCP/IP используется для транспортировки модифицированного кадра Modbus RTU (Рисунок В.2). При такой передаче, кадр Modbus RTU не имеет поля контрольной суммы и поля адреса, поскольку используется стандартная контрольная сумма Ethernet TCP/IP. Таким образом только два поля из блока RTU встраиваются в Ethernet TCP/IP: «Код функции» и «Данные». На рисунке В.2 изображён формат кадра протокола Modbus TCP.

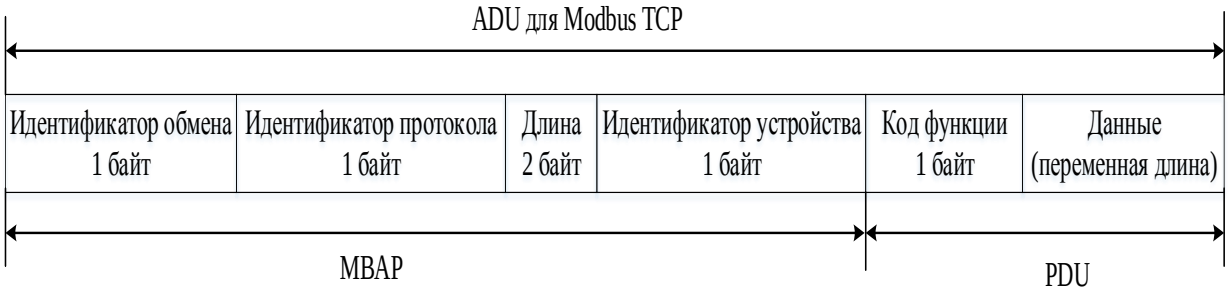


Рисунок В.2 – Формат кадра протокола Modbus TCP

MBAP (Modbus application protocol) – прикладной протокол Modbus

Поле «Идентификатор обмена» используется для идентификации сообщения в случае, когда в пределах одного TCP-соединения клиент посылает сверху несколько сообщений без ожидания ответа после каждого сообщения. Поле «Идентификатор протокола» содержит нули и зарезервировано для будущих применений. Поле «Длина» указывает количество следующих за ним байтов. Поле «Идентификатор устройства» идентифицирует удалённый сервер, расположенный вне сети Ethernet (например, в сети Modbus RTU, которая соединена с Ethernet с помощью межсетевого моста). ADU для Modbus TCP встраивается в поле «Данные» фрейма Ethernet и посылается через TCP-порт 502, специально зарезервированный для Modbus TCP.

Процесс передачи кадра Modbus RTU по уровням модели OSI через стек протоколов Ethernet TCP/IP в сетях с протоколом Modbus TCP представлен на рисунке В.3.

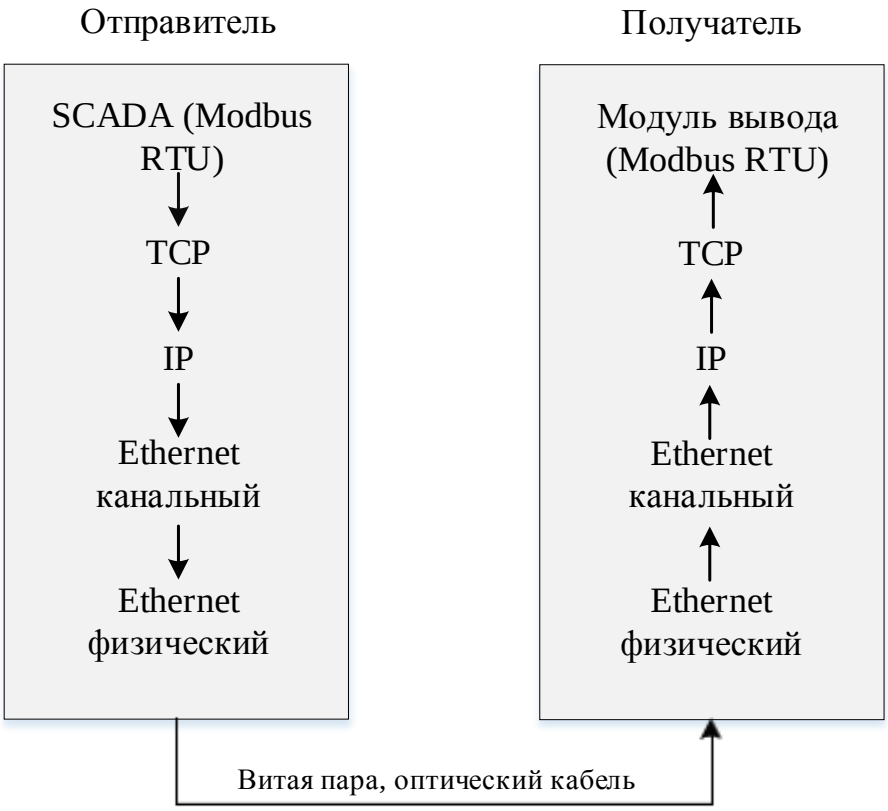


Рисунок В.3 - Процесс передачи кадра Modbus RTU по уровням модели OSI через стек протоколов Ethernet TCP/IP в сетях с протоколом Modbus TCP

Для построения имитационной модели передачи информации по протоколу Modbus TCP с использованием эмулятора, необходимо ведущее и ведомое устройство объединить в локальную сеть. В рамках эксперимента в качестве ведущего и ведомого устройства выступали АРМ-1 и АРМ-2, имитирующие работу исполнительного механизма и котроллера в составе системы, представленной на рисунке 11, с помощью программы Modbus TCP/RTU эмулятор. АРМ-1 выступает в роли ведущего, АРМ-2 выступает в роли ведомого. С помощью сниффера (программы Wireshark) проводился мониторинг сетевого трафика между ведущим и ведомым.

Modbus TCP/RTU эмулятор – программа, имитирующая работу Modbus TCP/RTU ведомых устройств. На рисунке В.4 представлена экранная форма программы-эмулятора трафика Modbus TCP/RTU.

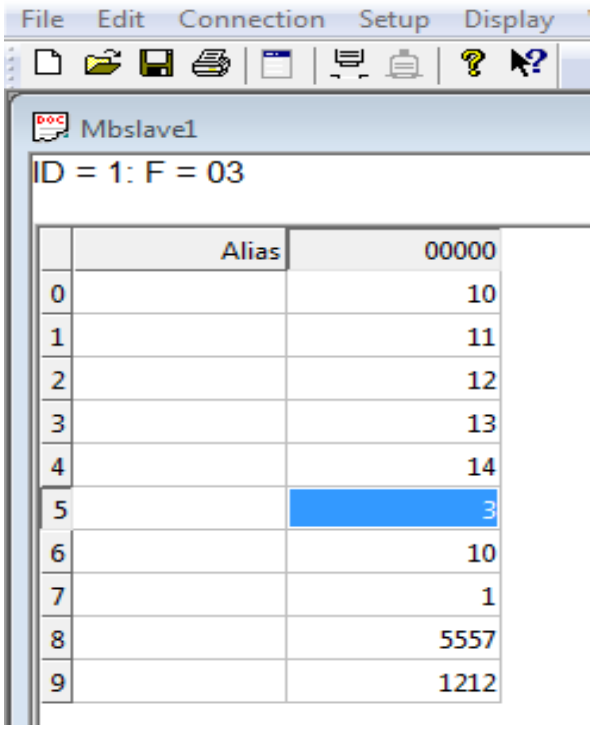


Рисунок В.4 - Экранная форма программы-эмулятора трафика Modbus TCP/RTU

При моделировании команды закрытия задвижки так же, как и в предыдущем эксперименте, производилась запись команды закрытия задвижки в один из девяти регистров устройства, представленного на рисунке В.5.

При анализе данных сетевого трафика на рисунке 17 в первой строке виден запрос на запись в регистр (Func: 6) ведомого (192.168.0.221) устройства. Вторая строка - ответ от ведомого (192.168.0.221) для ведущего (192.168.0.164) об успешной записи значения в регистр. Третья строка - запрос на чтение регистров (Func: 3) ведущего устройства (192.168.0.164) у ведомого (192.168.0.221). За ним - ответ от ведомого (192.168.0.221) для ведущего (192.168.0.164).

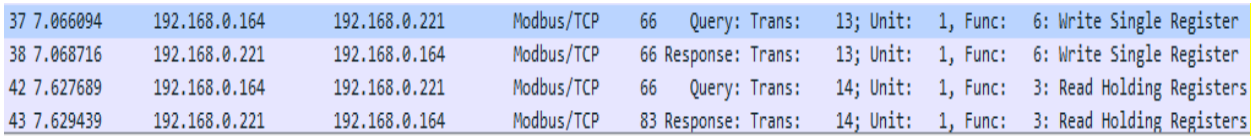


Рисунок В.5 – Экранная форма данных сетевого трафика при записи информации в регистр

При детальном анализе пакета с функцией записи (Func: 6) от ведущего (192.168.0.164) ведомому (192.168.0.221), можно определить содержимое полей ADU Modbus TCP. На рисунке В.6 представлено содержимое пакета с функцией записи (Write Single Register) регистра.

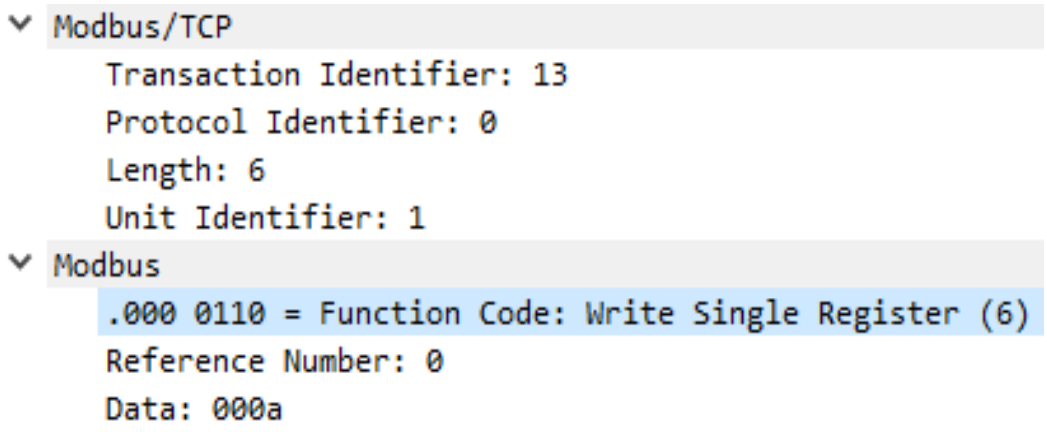


Рисунок В.6 – Содержимое пакета с функцией записи

На рисунке видна функция записи (Write Single Register) в регистр с номером 0 (Reference Number), записываемое значение (Data) - 0a. В ответ на подобный запрос ведомое устройство отправляет пакет, также содержащий в ответе функцию записи (Func: 6). Содержимое пакета-ответа на функцию записи представлено на рисунке В.7.

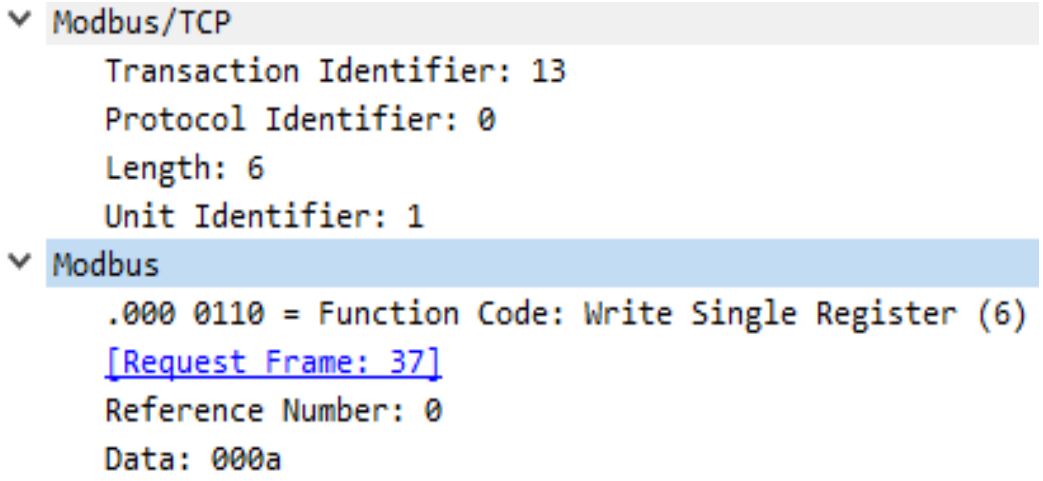


Рисунок В.7 – Содержимое пакета-ответа на функцию записи

После того, как была проведена запись в регистр, выполнился запрос чтения (Func: 3) регистров ведомого устройства, после чего был зафиксирован ответ на запрос чтения регистров. Содержимое пакета ответа на запрос чтения регистров представлено на рисунке В.8.

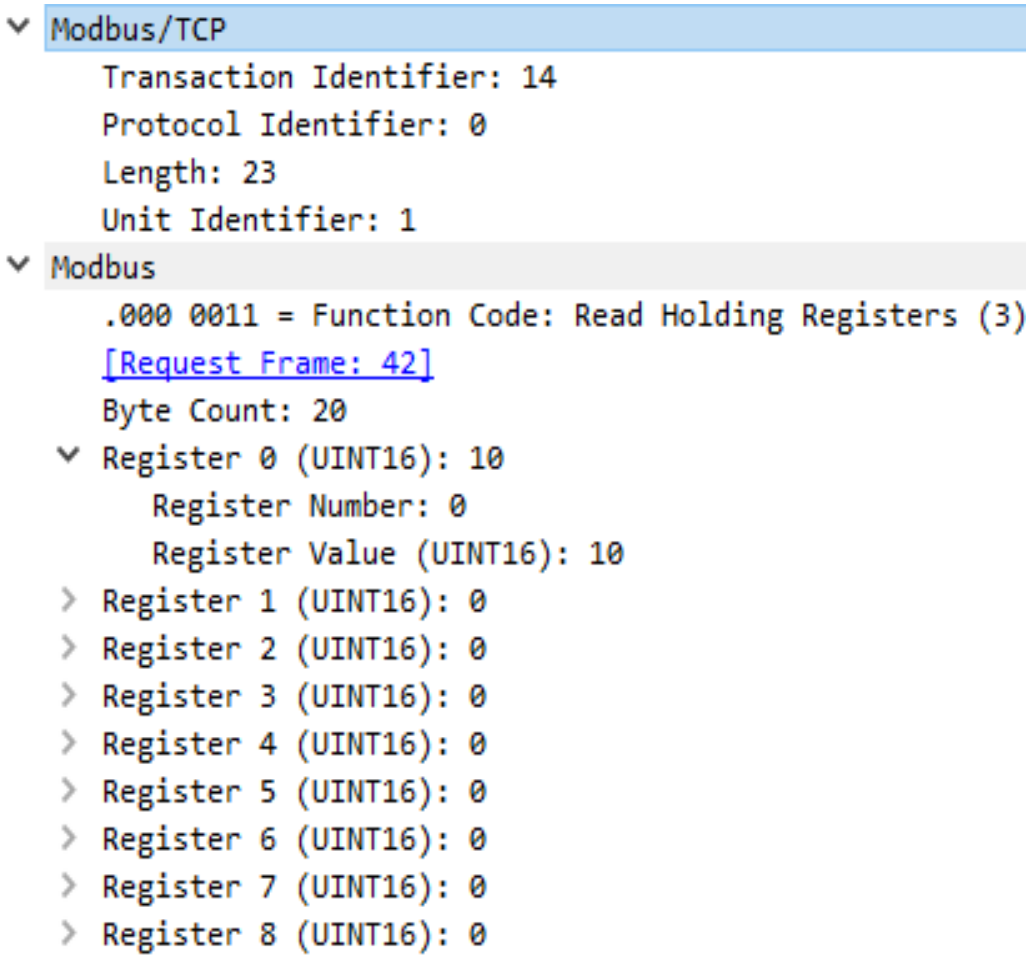


Рисунок В.8 – Содержимое пакета ответа на запрос чтения регистров

На рисунке видно, что значение регистра 0 (Register Value) равно 10 (0a – в шестнадцатеричной системе исчисления).

При проверке журнала событий ведущего устройства, удалось установить соответствие передаваемого трафика и записей в лог-файл. Результат записи и последующего чтения регистров в журнал ведущего устройства представлен на рисунке В.9. Лог-файл содержит данные о принимаемых пакетах (Rx - Receive Data) и отправляемых пакетах (Tx - Transmit Data) данные.

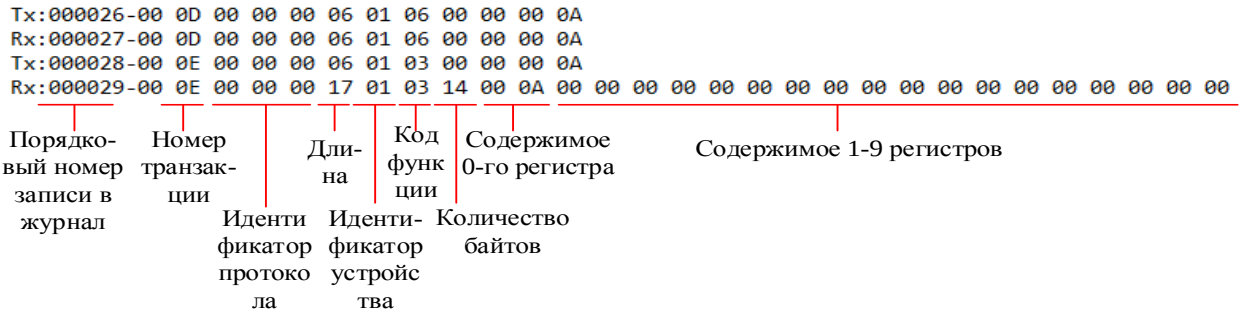


Рисунок В.9 – Данные лог-файла ведущего устройства при записи и последующего чтения значений регистров в журнал

Следующим шагом стала имитация разрыва соединения между АРМ-1 и АРМ-2 (имитация обрыва кабеля или выхода из строя оборудования). Результат зафиксирован в журнале событий ведущего устройства и представлен на рисунке В.10.

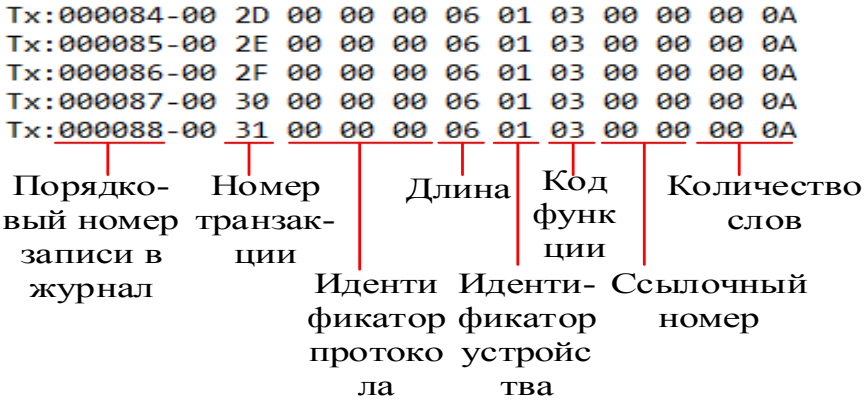


Рисунок В.10 – Данные лог-файла ведущего устройства при разрыве соединения

На рисунке видно, что ведущее устройство отсылает ведомому запрос на чтение регистров, но не получает ответов.

Более подробно результаты экспериментов по обнаружению аномалий в системе мониторинга технического состояния протяженного промышленного объекта по данным сетевого трафика, проведенных на базе разработанных моделей и программных средств, представлены в пункте 3.2.

Основными достоинствами протокола ModBus при использовании его для анализа в сетях TCP/IP являются простота реализации, доступность информации о

работе протокола, благодаря поддержки протокола большинством устройств, применяемых при построении АСУ ТП, высокая надёжность и достоверность при передаче данных.

Построенная имитационная модель продемонстрировала возможность передачи информации по протоколу Modbus без использования специализированного оборудования и позволила смоделировать обмен между ведущим и ведомым устройствами по протоколу Modbus при возникновении аномальных ситуаций без вмешательства в работу реальной промышленной системы. Были зафиксированы команды чтения и записи в регистрах. Также удалось зафиксировать в сетевом трафике разрыв соединения между двумя устройствами.

Приложение Г

(справочное)

Функции диспетчера АСУ ТП

Состав функций диспетчера и системы управления на верхнем технологическом уровне представлен в таблице Г.1.

Таблица Г.1 – Состав функций диспетчера и системы управления на верхнем технологическом уровне

Наименование функции	Перечень функциональных задач	Режим и регламент выполнения функций
Управление производством	Выдача режимных заданий	По инициативе диспетчера
Контроль за работой производства	Опрос систем среднего уровня Прием информации от систем нижнего уровня Обработка и представление информации о работе технологического оборудования. Формирование и выдача учетных и отчетных документов. Протоколирование событий.	Автоматический Автоматизированный Автоматический
Защита информации от несанкционированного доступа	Регистрация диспетчерского персонала по личному номеру и паролю. Проверка регистрации персонала перед выдачей информации и выполнением директив управления.	Автоматический
Ведение технологической базы данных	Корректировка и обновление информации в базе данных. Поиск информации в базе данных Ведение архива технологической информации	Автоматический, с обновлением информации по мере поступления

Состав функций диспетчера и контроллеров БКЭС на среднем технологическом уровне приведён в таблице Г.2

Таблица Г.2 – Состав функций диспетчера и контроллеров БКЭС на среднем технологическом уровне

Наименование функции	Перечень функциональных задач	Режим и регламент выполнения функций
1	2	3
Управление технологичским оборудованием	Управление ИМ по командам от оператора. Прием и обработка установок и управляющих сигналов для исполнительных механизмов.	Автоматизированный, по командам с АРМ
Измерение и сигнализация технологических параметров и положений исполнительных механизмов	Периодический опрос датчиков, характеризующих положение исполнительных механизмов, датчиков сигнализации предельных значений параметров. Периодический опрос датчиков для измерения параметров. Передача по запросу либо инициативно-аналоговых и дискретных сигналов о текущих значениях измеряемых и контролируемых параметров, состоянии исполнительных механизмов. Передача сигналов о предельных значениях технологических параметров и срабатываниях исполнительных механизмов.	Автоматический, в режиме реального времени
Регулирование режимных технологических параметров	Сравнение текущих значений режимных параметров, с заданными установками. Расчет управляющих воздействий на регулирующие устройства. Формирование и выдача управляющих сигналов на регулирующие устройства. Поддержание режимных параметров в заданных технологических границах (по соответствующим алгоритмам).	Автоматический, в режиме реального времени

Продолжение таблицы Г.2

1	2	3	4
4.	Аварийная защита техно-логического оборудования.	Выявление аварийной ситуации при поступлении информации от датчиков аварийной сигнализации по анализу информации от датчиков сигнализации предельных значений параметров и положений исполнительных механизмов. Выдача оператору световой, звуковой сигнализации. Отработка команд аварийной защиты (по соответствующему алгоритму).	Автоматический, в режиме реального времени

В автоматическом режиме (нижний и средний уровень АСУ ТП) выполняются:

– сбор и первичная обработка информации с датчиков, регулирование режимов работы технологического оборудования с целью поддержания оптимальных параметров технологического процесса;

– известительная, предупредительная и аварийная сигнализация, регистрация отклонений параметров от регламентных норм;

– защита технологического процесса и оборудования;

– формирование и печать журнала аварийных и технологических сообщений (ЖАТС);

– архивирование информации о ходе технологического процесса и состоянии оборудования;

– формирование видеокадров и отчетных документов;

– ведение базы данных.

Временные характеристики выполнения основных функций системы приведены в таблице Г.3.

Таблица Г.3 – Временные характеристики выполнения основных функций системы

Наименование	Периодичность
1. Сбор информации с аналоговых и дискретных датчиков.	Не более 1с
2. Ручной ввод информации	По мере необходимости
3. Обработка информации и определение значений параметров по измеренным сигналам	С периодичностью опроса
4. Интегрирование расходов продуктов	Смена, сутки, месяц
5. Предупредительная и аварийная сигнализация отклонений параметров от регламентных норм	С периодичностью опроса при отклонениях от регламентных норм
6. Представление информации о ходе технологического процесса и состоянии оборудования	По запросу, с периодом обновления не более 2 с.
7. Формирование и вывод оперативных и отчетных документов	По запросу либо в заданное время
8. Регулирование	Непрерывно, выдача управляющих сигналов определяется периодом опроса
9. Дистанционное управление	По мере необходимости
10. Защита технологического оборудования	При отклонениях параметров от регламентных норм. Реакция системы защиты на аварийное состояние не более 0,1с.

В системе предусмотрены сводки событий и активных тревог, в системе предусмотрены следующие рабочие панели:

- панели общего обзора - предназначены для контроля за работой всего производства и для получения быстрого доступа к более подробным панелям;

- мнемосхемы - представляют собой графические изображения технологических блоков и оборудования, средств КИП, отображают структуру алгоритмов управления и их состояние;

- панели настройки – предоставляют доступ для контроля и изменения настроечных параметров конкретной позиции;

- панели сигналов тревоги - отражают в хронологическом порядке срабатывания технологической сигнализации в ходе процесса;

- панели трендов - предусмотрены 2 вида отображения трендов: панель списка трендов системы, панель одиночного тренда.

Оператору-технологу предоставлены простые и естественные способы вызова и ввода данных для различных панелей:

- вызов из мнемосхемы по условному изображению;

- выбор из меню;

- ввод данных через соответствующую зону на экране.

Приложение Д

(рекомендуемое)

Фотоматериал исследования

Рисунок Д.1 – Фото колеи от грузовых машин на месте прокладки ВОЛС АСУ ТП

Рисунок Д.2 – Фото траншеи по завершении прокладки ВОЛС АСУ ТП

Рисунок Д.3 – Фото выступающего из-под земли оптического кабеля АСУ ТП: глубина прокладки кабеля менее 10 см (требуемая глубина 1.2 м)

Рисунок Д.4 – Фото соединительной муфты ВОЛС на поверхности земли

Рисунок Д.5 - Фото ВОЛС, выступающей над землёй на высоту более 1 м

Рисунок Д.6 – Фото ввода ЛЭП, питающих БКЭС

Рисунок Д.7 – Фото опоры ЛЭП при подводе к БКЭС

Рисунок Д.8 – Фото опор ЛЭП, питающих БКЭС

Рисунок Д.9 – Фото мобильного средства видеомониторинга угроз ИБ промышленных объектов (квадрокоптер Parrot Bebop Drone 2)

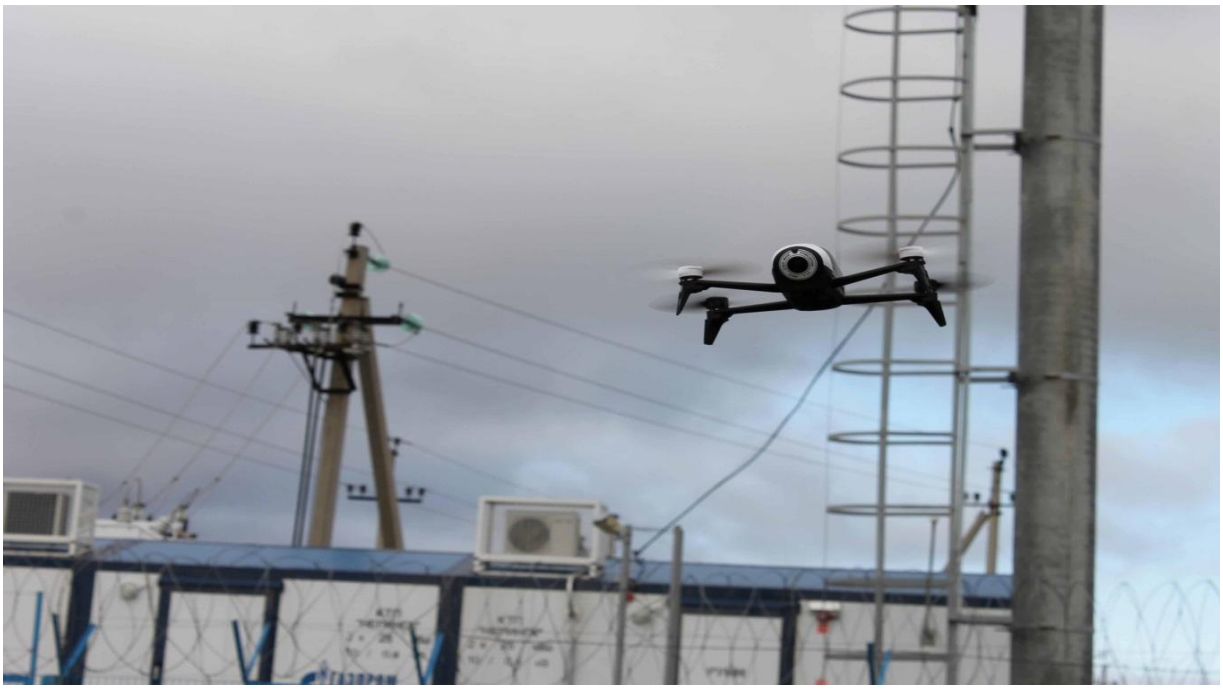


Рисунок Д.10 – Фото процесса видеомониторинга угроз ИБ на БКЭС

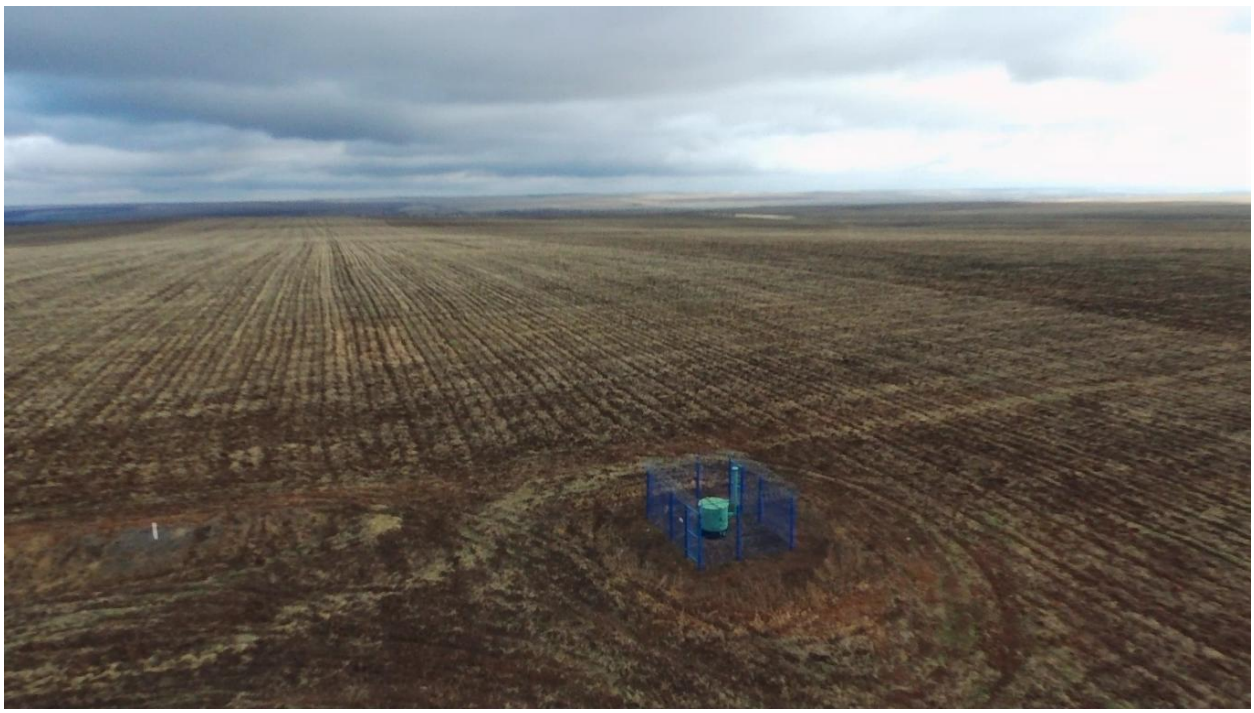


Рисунок Д.11 – Экранная форма аэросъемки объектов АСУ ТП (кабельного колодца)

Рисунок Д.12 – Экранная форма аэросъемки объектов АСУ ТП (БКЭС)