

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 10.05.02 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ
ОПРЕДЕЛЕНИЯ ВОЗМОЖНОСТИ ВОЗНИКНОВЕНИЯ ОПАСНЫХ
СОБЫТИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Студент _____ Карпов Артем Павлович

Руководитель _____ Боровиков А.Ю.

Нормоконтролёр _____ Иванов А.П.

Рецензент _____ Давыдов Д.В.

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефилов

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2017

РЕФЕРАТ

Отчет 80 с., 10 рис., 18 табл., 15 источников, 1 прил.

ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ, МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОТКАЗ, УТЕЧКА ИНФОРМАЦИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Объектом дипломного проекта является телекоммуникационная система специального назначения (ТКС СН).

Целью дипломного проекта является разработка методики анализа программного обеспечения для определения возможности возникновения опасных событий в ТКС СН.

В процессе работы была описана типовая структура, принципы и алгоритмы функционирования ТКС СН, разработана модель угроз безопасности информации для этой ТКС СН, определены технические средства из состава ТКС СН, для которых необходимо провести анализ аппаратно-программного обеспечения с целью определения возможности возникновения опасных событий. Рассмотрен порядок анализа аппаратно-программного обеспечения для выбранных изделий, в результате которого определена возможность (вероятность) возникновения опасных событий для рассматриваемой ТКС СН.

В результате работы была разработана методика анализа программного обеспечения для определения возможности возникновения опасных событий в ТКС СН.

СОДЕРЖАНИЕ

Введение.....	7
1 Описание архитектуры и принципов работы ТКС СН	10
2 Модель угроз и модель нарушителя ТКС СН.....	16
2.1 Обоснование выбора методики разработки модели угроз и модели нарушителя для ТКС СН.....	16
2.2 Процесс определения угроз безопасности информации в информационной системе	18
2.3 Оценка возможностей нарушителей по реализации угроз безопасности информации (разработка модели нарушителя).....	21
2.4 Оценка актуальности угроз безопасности информации.....	23
3 Принципы и алгоритмы работы ТКС СН	32
4 Анализ технических средств из состава ТКС СН на предмет возникновения в них неисправностей (сбоев), приводящих к возникновению опасных событий.....	36
5 Анализ программного обеспечения технических средств из состава ТКС СН с целью определения возможности возникновения опасных событий в результате неисправностей (сбоев) технических средств	50
5.1 Состав программного обеспечения.....	52
5.2 Описание процесса сборки (развертывания) специального программного обеспечения.....	53
5.3 Описание протокола взаимодействия.....	56
5.4 Выбор модулей для анализа.....	58
5.5 Восстановление алгоритма работы модулей	62
5.6 Анализ восстановленного алгоритма работы	65
5.7 Схема восстановленного алгоритма работы	66
5.8 Выводы по результатам анализа программного обеспечения	68
6 Методика анализа программного обеспечения для определения возможности возникновения опасных событий в ТКС СН.....	70

Заключение	78
Список использованных источников	79
Приложение А Протокол проверки ВКР на оригинальность	81

ОПРЕДЕЛЕНИЯ

В настоящем отчете применяют следующие термины с соответствующими определениями.

Автоматизированная система – организационно-техническая система, обеспечивающая выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство и тому подобное) или их сочетаниях [1].

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [2].

Сеть специального назначения – сеть электросвязи, создаваемая для производственных и специальных потребностей органов государственной власти [3].

Контролируемая зона – это территория или пространство, на которых исключено неконтролируемое пребывание лиц или транспортных средств без постоянного или разового доступа [4].

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем [5].

Межсетевой экран – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами [6].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
БИ	–	безопасность информации
ВПО	–	встроенное программное обеспечение
ГИС	–	государственная информационная система
ЗИ	–	защита информации
ИСПДн	–	информационная система персональных данных
КЗ	–	контролируемая зона
КИ	–	конфиденциальная информация
ИБ	–	информационная безопасность
ИС	–	информационная система
МСЭ	–	межсетевой экран
НКИ	–	не конфиденциальная информация
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПЗУ	–	постоянное запоминающее устройство
ПО	–	программное обеспечение
СПО	–	специальное программное обеспечение
ТСК СН	–	телекоммуникационная система специального назначения
ТС	–	техническое средство
УБИ	–	угроза безопасности информации

ВВЕДЕНИЕ

Одно из важнейших направлений обеспечения информационной безопасности Российской Федерации – решение широкого круга вопросов, связанных с защитой информации при внедрении современных информационных технологий в государственные системы связи и обработки информации. Последние объединяются под общим названием информационно-телекоммуникационных систем специального назначения, которые создаются в интересах органов государственной власти и управления.

Защита информации, обрабатываемой в таких системах, является важнейшей задачей, которая решается на всех этапах жизненного цикла ТКС СН. Оценка состояния информационной безопасности базируется на анализе угроз информационной безопасности, а также источников угроз (потенциальной возможности нарушения защиты). В связи с этим, основным этапом в процессе обеспечения информационной безопасности является разработка модели угроз и модели нарушителя ТКС СН.

По способам реализации угрозы безопасности информации можно классифицировать на угрозы несанкционированного доступа, угрозы утечки информации по техническим каналам, угрозы стихийного характера и угрозы техногенного характера.

При обеспечении информационной безопасности ТКС СН, как правило, проблемным вопросом является совместная обработка данных различных уровней конфиденциальности.

По требованиям действующих нормативных документов, подобные ТКС СН необходимо сегментировать и подключать сети с различными уровнями конфиденциальности посредством МЭ соответствующего класса. Подобные защитные меры направлены на парирование угроз несанкционированного доступа.

Организационно-техническими защитными мерами (введение КЗ, создание пропускной системы и т.д.) обеспечивается снижение

возможности реализации угроз утечки информации по техническим каналам.

Угрозы стихийного характера являются трудно прогнозируемыми, в связи с этим защитные меры, направленные на снижение ущерба от реализации подобных угроз применяются всегда.

Угрозы техногенного характера – это угрозы информационной системе, источниками которых являются технические средства системы, неисправности и сбои которых, могут приводить к возможности возникновения опасных событий. В отношении данного типа угроз информационной безопасности для ТКС СН действующая нормативная база не предусматривает защитных мер. Это связано с тем, что в период разработки нормативных документов проблема обеспечения надежности аппаратного обеспечения технических средств являлась неактуальной – технические средства разрабатывались на элементной базе, обеспечивающей высокие показатели безотказной работы и эксплуатировались в основном в лабораторных условиях.

Однако, современный уровень развития радиоэлектроники характеризуется расширением круга задач, возложенных на технические средства, повышением требований к точности и быстродействию вычислений, ростом сложности электронной аппаратуры, сложностью условий, в которых осуществляется эксплуатация технических средств. Описанные факторы резко снижают надежность аппаратного обеспечения технических средств. Одновременно усложняется и программное обеспечение, под управлением которых функционируют технические средства – функционал современного программного обеспечения может предусматривать как защиту от отказов аппаратного обеспечения, так и устранение возникающих отказов. В этих условиях, задача получения обоснованных показателей надежности технических средств не может быть решена без анализа программного обеспечения этих ТС.

Таким образом, на современном этапе развития электроники, угрозы техногенного характера являются актуальными. Для определения возможности возникновения опасных событий, в результате реализации этих угроз, необходимо проводить анализ как аппаратного, так и программного обеспечения технических средств.

В данной работе определена типовая структура, принципы и алгоритмы функционирования ТКС СН, разработана модель угроз безопасности информации для этой ТКС СН, определены технические средства, неисправности (сбои) в аппаратно-программном обеспечении которых могут приводить к реализации угроз безопасности информации техногенного характера. На примере ПЭВМ, проведен анализ аппаратного обеспечения, получена вероятность возникновения отказа ТС в период эксплуатации, обоснована необходимость проведения анализа программного обеспечения для определения возможности реализации угроз безопасности техногенного характера, разработана методика анализа программного обеспечения для определения возможности возникновения опасных событий, в результате применения которой, могут быть получены обоснованные показатели надежности ТС.

1 Описание архитектуры и принципов работы ТКС СН

В данном дипломном проекте рассмотрены проблемы обеспечения информационной безопасности телекоммуникационной системы специального назначения (далее – ТКС СН). ТКС СН является одним из видов сетей связи специального назначения.

Сеть связи специального назначения – сеть электросвязи, создаваемая для производственных и специальных потребностей органов государственной власти [3]. Данная сеть может выполнять задачи среды передачи данных (ЛВС) и организации внутренней телефонной связи. В данной работе рассмотрена ТКС СН, которая представляет собой ЛВС, предназначенную для решения задач органов государственной власти.

Очевидно, что важнейшим условием функционирования ТКС СН является обеспечение безопасности информации, обрабатываемой в подобных сетях. Безопасностью информации определяется состояние защищённости информации, при котором обеспечены её основные свойства: конфиденциальность, доступность и целостность.

В данном дипломном проекте рассмотрена типовая архитектура ТКС СН, которая может функционировать в различных учреждениях, организациях и предприятиях, обеспечивающих работу органов государственной власти. Как правило, в рассматриваемых ТКС СН осуществляется обработка конфиденциальной информации различного уровня конфиденциальности.

Подобные ТКС СН должны соответствовать требованиям по безопасности информации, которые декларированы в нормативных документах ФСТЭК [7-11]. Типовым решением задачи обработки информации различного уровня конфиденциальности является разделение ТКС СН на несколько локальных вычислительных сетей (далее ЛВС).

Рассматриваемые ЛВС взаимодействуют посредством межсетевого экрана, который выполняет функцию фильтрации потоков информации при обмене между ЛВС с различным уровнем конфиденциальности

обрабатываемых данных. При этом рассматриваемые локальные вычислительные сети не имеют подключения к сетям общего пользования (таким как Internet).

В связи с этим, была разработана типовая структура ТКС СН, приведенная на рисунке 1.

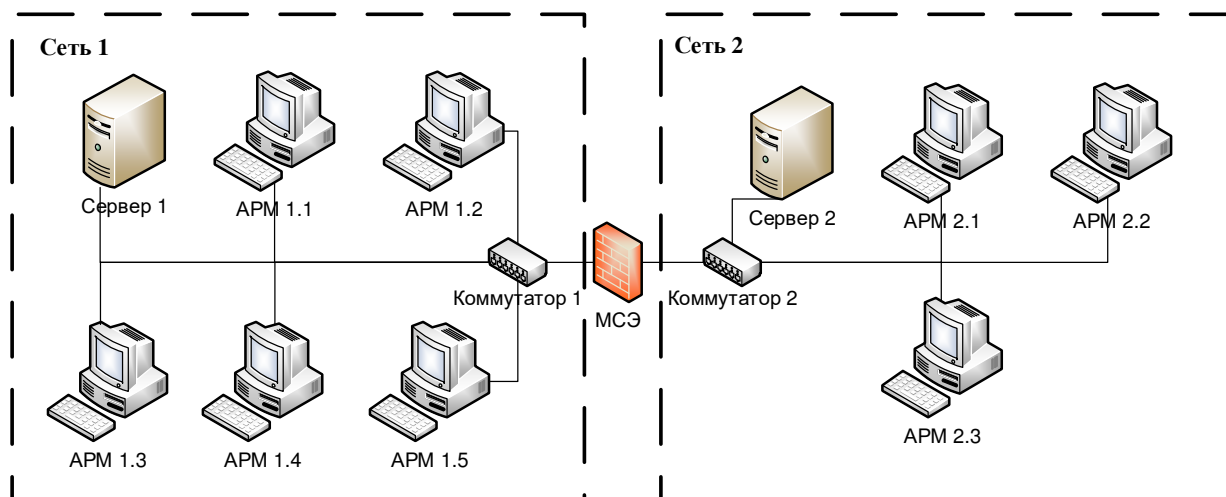


Рисунок 1 – Структура телекоммуникационной системы специального назначения

Рассматриваемая ТКС СН находится в одном здании, в пределах контролируемой зоны. Сеть 1 обрабатывает информацию ограниченного доступа (конфиденциальную) и открытую (не конфиденциальную) информацию. Сеть 2 обрабатывает только не конфиденциальную информацию.

Согласно приказу ФСТЭК №17 [10], взаимодействие подобных сетей должно осуществляться с использованием МЭ. Требования к межсетевому экрану определены в руководящем документе Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» [7].

Приведем некоторые исходные данные, характеризующие рассматриваемую ТКС СН и необходимые для разработки модели угроз и модели нарушителя ТКС СН:

– уровни конфиденциальности информационных ресурсов, обрабатываемых ТКС СН: конфиденциально, несекретно;

– перечень должностных лиц, которые имеют доступ к штатным средствам ТКС СН с указанием уровня их полномочий представлен в таблице 1;

Таблица 1 – Перечень лиц, имеющих доступ к штатным средствам ТКС СН, с указанием их полномочий

Роль	Рабочее место	Доступные информационные ресурсы (высший гриф конфиденциальности)
<i>Сеть 1</i>		
Руководитель учреждения	АРМ 1.1	Информация, обрабатываемая на АРМ 1.1(КИ), сервере 1(КИ), 2(НИ)
Заместитель руководителя учреждения	АРМ 1.2	Информация, обрабатываемая на АРМ 1.2(КИ), сервере 1(КИ), 2(НИ)
Руководитель работ	АРМ 1.3	Информация, обрабатываемая на АРМ 1.3(КИ), сервере 1(КИ)
Исполнитель работ №1	АРМ 1.4	Информация, обрабатываемая на АРМ 1.4(КИ), сервере 1(КИ)
Исполнитель работ №2	АРМ 1.5	Информация, обрабатываемая на АРМ 1.5(КИ), сервере 1(КИ)
<i>Сеть 2</i>		
Руководитель экономического отдела	АРМ 2.1	Информация, обрабатываемая на АРМ 2.1(НИ), сервере 2 (НИ)
Сотрудник экономического отдела	АРМ 2.2	Информация, обрабатываемая на АРМ 2.2(НИ), сервере 2 (НИ)
Сотрудник экономического отдела	АРМ 2.3	Информация, обрабатываемая на АРМ 2.2(НИ), сервере 2 (НИ)

– режим обработки данных в АС: коллективный;

– размещение ТКС СН: в пределах контролируемой зоны (далее КЗ);

– перечень аппаратно-программного обеспечения ТКС СН приведен в таблице 2;

Таблица 2 – Перечень аппаратно-программного обеспечения ТКС СН

Техническое средство	Аппаратное обеспечение	Программное обеспечение
АРМ 1.1, АРМ 1.2, ... АРМ 1.5	Процессор: Intel Core 2 Duo-Mobile	Встроенное программное обеспечение:

Продолжение таблицы 2

Техническое средство	Аппаратное обеспечение	Программное обеспечение
	<p>T7500</p> <p>ОЗУ: SDRAM Kingston KVR 667 D2 S5/2G, 4Gb</p> <p>Видео: Intel Graphics Media Accelerator (GMA) X3100</p> <p>SDD: Intel SSD SA2CW 120 G310, 500GB</p> <p>Корпус, БП: 450BT</p> <p>Звуковая карта: Realtec</p> <p>Сетевая карта: 1Gbit</p> <p>Электронный замок: Соболь-PCI</p> <p>Монитор: Samsung C27F 390 FHI VGA</p> <p>Клавиатура: Microsoft 700x-KeyBoard USB</p> <p>Мышь: Logitech 710N USB</p>	<p>Intel v.1.07, 11.05.2012;</p> <p>Системное программное обеспечение:</p> <p>ОС «Astra Linux Special Edition»</p> <p>Специальное программное обеспечение:</p> <p>Специально разработанные средства (приложения) для проведения работ в зависимости от вида деятельности учреждения (клиентская часть).</p> <p>Secret Net 7.</p>
<p>APM 2.1, APM 2.2, APM 2.3</p>	<p>Процессор: Intel Xeon 3520</p> <p>ОЗУ: 4Gb</p> <p>Видео: onboard</p> <p>HDD: 500GB</p> <p>Корпус, БП: 450BT</p> <p>Звуковая карта: Realtec</p> <p>Сетевая карта: 1Gbit</p> <p>Монитор: Samsung C27 F390 FHI VGA</p> <p>Клавиатура: Microsoft 700x-KeyBoard USB</p> <p>Мышь: Logitech 710N USB</p>	<p>Встроенное программное обеспечение:</p> <p>Intel v.1.07, 11.05.2012;</p> <p>Системное программное обеспечение:</p> <p>ОС «Astra Linux Special Edition»</p> <p>Специальное программное обеспечение:</p> <p>Microsoft Office 2013;</p> <p>1С-предприятие (клиентская часть)</p>
<p>Сервер 1</p>	<p>Производитель: Intel</p> <p>Тип процессора: E5, Xeon</p> <p>Код процессора: intel xeon e5-2609 v3</p> <p>Частота процессора: 1 ГГц</p> <p>Количество процессоров: 1</p>	<p>Встроенное программное обеспечение:</p> <p>Intel v.1.07, 11.05.2012;</p> <p>Системное программное обеспечение:</p>

Продолжение таблицы 2

Техническое средство	Аппаратное обеспечение	Программное обеспечение
	Тип оперативной памяти: DDR4 Объем памяти: 1 Гб Количество слотов памяти: 16 Интерфейс жесткого диска: SATA	ОС «Microsoft Windows Server 2012 Standart» Специальное программное обеспечение: Специально разработанные средства (приложения) для проведения работ в зависимости от вида деятельности учреждения (серверная часть) СУБД Oracle Database 11g SecretNet 7.
Сервер 2	Производитель: Intel Тип процессора: E5, Xeon Код процессора: intel xeon e5-2609 v3 Частота процессора: 1 ГГц Количество процессоров: 1 Тип оперативной памяти: DDR4 Объем памяти: 1 Гб Количество слотов памяти: 16 Интерфейс жесткого диска: SATA	Встроенное программное обеспечение: Intel v.1.07, 11.05.2012; Системное программное обеспечение: ОС «Microsoft Windows Server 2012 Standart» Специальное программное обеспечение: 1С: Предприятие (серверная часть)
Коммутатор 1, 2	Коммутатор Cisco Catalyst 4900	ОС: «Cisco Input output system v.12.2(53)SG1»
МСЭ	Межсетевой экран Cisco PIX Firewall PIX-506E ver. 6.3 – по 3 классу для МЭ	ОС: Программное обеспечение Cisco IOS ADVANCED ENTERPRISE SERVICES версия 12.4(5b)

– информационные потоки, возникающие при взаимодействии объектов ТКС СН, приведены на рисунке 2;

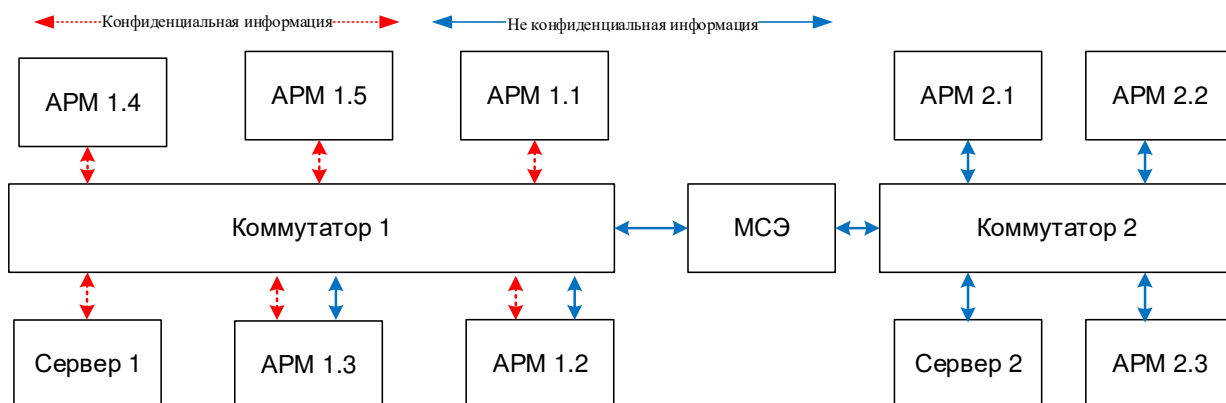


Рисунок 2 – Схема информационных потоков ТКС СН

Таким образом, на первом этапе дипломного проектирования была разработана структура типовой ТКС СН, определены основные исходные данные для разработки модели угроз и модели нарушителя для данной ТКС СН.

2 Модель угроз и модель нарушителя ТКС СН

2.1 Обоснование выбора методики разработки модели угроз и модели нарушителя для ТКС СН

Для определения требований по обеспечению безопасности информации, обрабатываемой в ТКС СН, предъявляемых как к системе защиты ТКС СН, так и к самой телекоммуникационной системе, а также в целях определения необходимости анализа аппаратно-программного обеспечения технических средств из состава ТКС СН, необходимо разработать модель угроз и модель нарушителя для данной ТКС СН.

Модель угроз представляет собой физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации для объекта обеспечения безопасности, и является отправной точкой при разработке адекватных мер защиты для ТКС СН.

В зависимости от типа телекоммуникационной системы, модель угроз может разрабатываться в соответствии с требованиями и методическими документами ФСТЭК (ИСПДн, ГИС, и др.), ФСБ (ТКС, обрабатывающие сведения, содержащие государственную тайну и имеющие в своем составе оборудование шифрованной связи) и (или) МО (ТКС, разработанные и решающие задачи оборонно-промышленного комплекса).

Рассматриваемая ТКС СН не обрабатывает сведения, содержащие государственную тайну, не имеет в своем составе аппаратуры шифрованной связи и в общем случае должна соответствовать требованиям ФСТЭК о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Данные требования декларированы в приказе ФСТЭК №17 от 11 февраля 2013г. [10].

Для разработки модели угроз и модели нарушителя, адекватной требованиям приказа ФСТЭК №17 в данном дипломном проекте был использован проект методического документа ФСТЭК «Методика

определения угроз безопасности информации в информационных системах» [12].

Необходимо отметить некоторые характеристики выбранной методики:

- методика не распространяется на идентификацию угроз безопасности информации, для ТКС СН, обрабатывающих сведения, составляющие государственную тайну;

- методика предназначена для ИС, функционирующих в целях реализации задач органов государственной власти, органов местного самоуправления, и организациям, являющимся в соответствии с законодательством РФ делегатами отдельных функций данных органов;

- данная методика применяется на этапах создания и эксплуатации ИС;

- методика применяется совместно с банком данных УБИ, сформированных ФСТЭК;

- методика ориентирована на определение и оценку антропогенных и техногенных угроз безопасности информации.

Согласно данному документу, процесс разработки модели угроз и модели нарушителя состоит из следующих этапов:

- процесс определения угроз безопасности информации в информационной системе;

- оценка возможностей нарушителя при реализации угроз безопасности информации (разработка модели нарушителя);

- определение актуальных угроз безопасности информации в информационных системах.

Результатом выполнения данных этапов, является разработанная для ТКС СН модель угроз и модель нарушителя.

2.2 Процесс определения угроз безопасности информации в информационной системе

Цель определение угроз безопасности информации – установление возможности нарушения конфиденциальности, целостности, доступности информации, содержащейся в ТКС СН. Определение угроз носит систематический характер, и осуществляется как на этапе создания телекоммуникационной системы, так и в ходе ее эксплуатации.

Согласно рассматриваемому методическому документу, систематический подход определения УИБ предусматривает:

- определение области применения процесса определения УИБ;
- идентификацию источников и угроз безопасности информации;
- оценка возможности реализации угроз и степени возможного ущерба в случае такой реализации.

Систематический подход к определению угроз безопасности информации необходим для определения потребности в конкретных требованиях к защите информации и создания адекватной эффективной системы защиты информации в ТКС СН.

Необходимо отметить, что сформированная в рамках дипломного проекта модель угроз и модель нарушителя не является исчерпывающей. Это, прежде всего, связано с тем, что разработанная ТКС СН является абстрактной типовой моделью ИС, обрабатывающей информацию ограниченного доступа различного уровня. В связи с этим, модель угроз для рассматриваемой ТКС СН содержит наиболее характерные угрозы для подобной системы.

Далее рассмотрено применение систематического подхода определения угроз информационной безопасности в информационных системах согласно вышеупомянутой методике для разработанной ТКС СН.

2.2.1 Определение области применения процесса определения угроз безопасности информации

В рамках выполнения данного этапа определения угроз ИБ в ИС были определены как физические (периметр контролируемой зоны, места размещения оборудования ТКС СН), так и логические (сегменты сети) границы ИС, в которых принимаются и контролируются меры по защите информации, определены сегменты ИС.

Информационная система размещена в двух помещениях здания, строительные конструкции которого являются границами КЗ. ИС состоит из двух подсетей, каждая из которых обрабатывает информацию, различного уровня конфиденциальности. Сеть 1 обрабатывает информацию с высшим уровнем конфиденциальности «Конфиденциально». Сеть 2 обрабатывает информацию с высшим уровнем конфиденциальности «Не конфиденциально». Сети физически взаимодействуют посредством коммутаторов, и логически разделены посредством межсетевого экрана, обеспечивающего фильтрацию пакетов различного уровня конфиденциальности.

2.2.2 Идентификация источников угроз и угроз безопасности информации

В обобщенном виде угрозы безопасности информации характеризуется:

- источниками угроз;
- факторами, обуславливающими возможность реализации угроз;
- способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации.

Угрозами безопасности информации могут являться как субъекты, в том числе физические лица, организации, так и явления: стихийные бедствия, техногенные аварии, иные природные катастрофы.

В целях идентификации угроз безопасности информации в рассматриваемой телекоммуникационной системе специального назначения были определены следующие факторы модели угроз:

- возможности (тип, вид, потенциал) нарушителей, а именно: тип нарушителя (внутренний или внешний), вид нарушителя (согласно классификации ФСТЭК) и потенциал (согласно классификации ФСТЭК), необходимые нарушителям для реализации угроз безопасности информации;

- уязвимости, использующиеся при реализации угроз безопасности информации (например, внедренные на этапе проектирования или эксплуатации программные закладки);

- способы и методы реализации УИБ;

- объекты воздействия информационной системы (автоматизированные рабочие места, коммуникационное оборудование и др.), на которые может быть направлена угроза безопасности информации;

- результат, а также возможные последствия (рассматривается худший случай) возникающие вследствие реализации угроз безопасности информации.

Результаты идентификации источников угроз для рассматриваемой ТКС СН сведены в таблицу 3

2.2.3 Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба

По результатам идентификации источников угроз, определим наиболее характерные угрозы, для этих источников:

- внутренний нарушитель: УБИ. 067. Угроза неправомерного ознакомления с защищаемой информацией;

- внешний нарушитель: УБИ. 139. Угроза преодоления физической защиты;

– техногенный источник угрозы: угроза утечки конфиденциальной информации в сеть, не предназначенную для обработки КИ, в результате неисправностей (сбоев) программно-аппаратных средств ТКС СН. Данный вид угрозы также может рассматриваться как угроза неправомерного ознакомления с защищаемой информацией (УБИ 067), которая может быть реализована внутренним нарушителем, за счет неисправностей (сбоев) ТС из состава ТКС СН; стихийный источник угрозы: угроза уничтожения конфиденциальной информации в результате стихийных бедствий (пожара).

Вероятность реализации угрозы оценивается сочетанием вероятности (возможности) реализации угрозы и степени ущерба, причиняемого в результате реализации угрозы.

Данная оценка будет приведена ниже, при определении актуальных для рассматриваемой ТКС СН угроз ИБ.

2.3 Оценка возможностей нарушителей по реализации угроз безопасности информации (разработка модели нарушителя)

На данном этапе разработки модели угроз, оцениваются возможности нарушителей по реализации угроз безопасности информации. Целью такой оценки является формирование предположения о возможностях (тип, вид, потенциал) нарушителей, которые могут реализовать угрозы безопасности информации в телекоммуникационной системе специального назначения с известными структурно-функциональными свойствами и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

В процессе разработки модели нарушителя ТКС СН были определены:

- . возможности (тип, вид, потенциал) нарушителей, обеспечивающие реализацию угроз безопасности информации;
- возможные цели нарушителей каждого вида при реализации УИБ;

Таблица 3 – Источники угроз для рассматриваемой ТКС СН

Источник угрозы	Тип источника угрозы	Потенциал нарушителя	Используемые уязвимости	Способы реализации угроз БИ	Объект ИС на который направлена угроза	Результат от реализации угроз ИБ
Внутренний нарушитель	Антропогенный	Средний	Уязвимости в СЗИ от НСД, недостаток организационно-технических мер и др.	Уничтожение, хищение КИ, и др.	Объекты Сети 1	Нарушение К,Ц,Д
Внешний нарушитель		Средний	Недостаток организационно-технических мер и др.	Утечка информации по каналам ПЭМИН	Объекты Сети 1	Нарушение К
Неисправность (сбой) аппаратно-программного обеспечения	Техногенный	—	Низкое качество технических, программных или программно-технических средств; низкое качество систем жизнеобеспечения (кондиционирования, электроснабжения, охранных систем и т.д.); низкое качество технического обслуживания ТКС СН со стороны организаций и лиц, выполняющих такое обслуживание.	Утечка информации в результате неисправностей (сбоев) коммутационного оборудования ТС, являющихся источниками КИ, нарушение целостности, доступности КИ	Объекты Сети 1	Нарушение К,Ц,Д
Стихийное бедствие	Стихийный	—	—	Пожар в помещении, где расположена ТКС СН	—	Нарушение К, Ц, Д

– способы и методы, посредством которых может быть реализованы угрозы безопасности информации.

При оценке типа, вида и потенциала нарушителей не рассматривалась угроза стихийного характера по объективным причинам.

Результаты оценки возможностей нарушителей приведены в таблице 4.

2.4 Оценка актуальности угроз безопасности информации

Актуальность угроз безопасности информации определяется в отношении угроз, для которых экспертным методом определено, что:

– возможности (потенциал) нарушителя достаточны для реализации угрозы безопасности информации;

– в информационной системе могут иметься потенциальные уязвимости, которые могут быть использованы при реализации угрозы безопасности информации;

– структурно-функциональные характеристики и особенности функционирования информационной системы не исключают возможности применения способов, необходимых для реализации угрозы безопасности информации (существует сценарий реализации угрозы безопасности);

– реализация угрозы безопасности информации приведет к нарушению конфиденциальности, целостности или доступности информации, в результате которого возможно возникновение неприемлемых негативных последствий (ущерба).

– Актуальность угрозы оценивается сочетанием таких характеристик как возможность реализации угрозы и степень возможного ущерба.

– Возможность реализации угрозы оценивается сочетанием потенциала нарушителя и уровнем проектной защищенности ИС. Потенциал нарушителя приведен в таблице 3.

– Уровень проектной защищенности рассматриваемой ТКС СН приведен в таблице 5.

Таблица 4 – Модель нарушителя ТКС СН

Угроза	Тип нарушителя	Вид нарушителя	Цели нарушителя	Возможный способ реализации угроз ИБ
Угроза преодоления физической защиты	Внешний нарушитель	Внешние субъекты: Организации, разрабатывающие, производящие, поставляющие программные, технические средства Физические лица	Причинение имущественного ущерба Внедрение дополнительных функциональных возможностей в программное обеспечение на этапе разработки.	Реализация угрозы преодоления физической защиты возможна при условии успешного применения нарушителем любого из методов проникновения на объект
Угроза неправомерного ознакомление с защищаемой информацией	Внутренний нарушитель	Пользователи информационной системы	Причинение имущественного ущерба Непреднамеренные, неосторожные или неквалифицированные действия	При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.
Угроза утечки защищаемой информации (угроза неправомерного ознакомление с защищаемой информацией в результате неисправностей (сбоев аппаратно-программного обеспечения ТС из состава ТКС СН))	Внутренний нарушитель	Пользователи информационной системы	Причинение имущественного ущерба Непреднамеренные, неосторожные или неквалифицированные действия	В результате неисправностей программно-аппаратного обеспечения, возможно попадание КИ в Сеть 2, как следствие - реализация угрозы неправомерного ознакомления с защищаемой информацией

Таблица 5 – Уровень проектной защищенности ТКС СН

Технические и эксплуатационные характеристики	Уровень Защищенности
По территориальному размещению	Средний
По используемым информационным технологиям	Высокий
По архитектуре информационной Системы	Высокий
По наличию соединения с сетями общего пользования	Высокий
По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования	Высокий
По размещению технических средств:	Высокий
По режимам обработки информации в информационной системе	Низкий
По режимам разграничения прав доступа:	Высокий
По режимам разделения функций по управлению информационной системой	Высокий
По подходам к сегментированию информационной системы	Высокая

Так как 80% показателей проектной защищенности ТКС СН имеют уровень «Высокий», уровень проектной защищенности так же имеет значение «Высокий».

Таким образом, возможности реализации идентифицированных угроз для ТКС СН определены следующим образом:

- возможность реализации угрозы неправомерного ознакомления с защищаемой информацией: «Средняя»;
- возможность реализации угрозы преодоления физической защиты: «Средняя»;
- возможность реализации угрозы утечки информации в результате неисправностей (сбоев) программно-аппаратного обеспечения ИС в рамках данной методики определить невозможно. Вопрос оценки возможности реализации данной угрозы будет рассмотрен далее. Для оценки актуальности угрозы примем значение возможности реализации угрозы как «Средняя»;
- возможность реализации угрозы стихийного бедствия: «Низкая».

Для оценки актуальности угроз ИБ для рассматриваемой ТКС СН необходимо оценить степень возможного ущерба владельцу защищаемой информации при реализации каждой угрозы. Однако степень возможного ущерба напрямую зависит от деятельности учреждения, в котором развернута ТКС СН. Так как в данной работе рассмотрена абстрактная модель ТКС СН, степень ущерба для каждой угрозы принимается равной значению «Средняя».

Таким образом, были определены следующие актуальные угрозы для разработанной ТКС СН:

- угроза неправомерного ознакомления с защищаемой информацией;
- угрозы преодоления физической защиты;
- угроза утечки защищаемой информации в результате неисправностей (сбоев) программно-аппаратного обеспечения.

Для ТКС СН конкретного учреждения (организации) данный перечень расширяется (уточняется) в соответствии со спецификой деятельности конкретной организации.

В общем случае, все идентифицированные в процессе разработки модели угроз актуальные угрозы ИБ можно отнести к одному из следующих видов угроз:

- угрозы несанкционированного доступа, реализуются в результате осуществления несанкционированного (в том числе случайного) доступа, в результате которого осуществляется нарушение следующих свойств защищаемой информации: конфиденциальность, целостность и доступность, и включают в себя:

- угрозы несанкционированного доступа в операционную систему АРМ с использованием штатного программного обеспечения;
- угрозы создания режимов работы, выходящих за рамки штатного функционирования программных средств в результате умышленных изменений служебных данных, игнорирования предусмотренных в штатных

условиях ограничений на состав и характеристики обрабатываемой информации, искажения (модификации) самих данных и т.п.;

- угрозы внедрения вредоносных программ (программно-математического воздействия);

- угрозы утечки по техническим каналам реализуются посредством регистрирования распространяемого ТКС СН информативного сигнала, в среде передачи и включают в себя:

- угрозы утечки акустической (речевой) информации;
 - угрозы утечки видовой информации;
 - угрозы утечки информации по каналам побочных электромагнитных излучений и наводок;

- угрозы стихийного характера реализуются в результате непреодолимого воздействия природных катаклизмов;

- угрозы техногенного характера реализуются в результате нештатной работы аппаратно-программного обеспечения ТКС СН.

Для каждого вида угроз (актуальных для ТКС СН) необходимо предусмотреть меры защиты, снижающие возможность их возникновения для приемлемого уровня.

Угрозы стихийного характера не поддаются прогнозированию, в связи с этим защитные меры для этих угроз применяются всегда. К таким мерам относится: резервирования оборудования, применение источников бесперебойного питания и др. В связи с этим, угрозы стихийного характера не представляют интереса в данной работе.

Угрозы НСД и угрозы утечки информации по техническим каналам идентифицируются в процессе разработки модели угроз. После этого в соответствии с разработанной моделью угроз и руководящими документами по защите информации для данного класса информационной системы, выполняется формирование перечня мер по защите информации.

В соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [8] рассматриваемая ТКС СН относится к классу защищенности 1Г, так как является многопользовательской, с высшим уровнем конфиденциальности обрабатываемой информации «Конфиденциально». Для данной ТКС СН руководящими документами, декларирующими требования к системе защиты информации, являются следующие документы:

– РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [8];

– РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [7];

– РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [9];

– приказ ФСТЭК № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [10].

После применения мер по защите информации для класса защищенности 1Г, возможность реализации угроз НСД и утечки по техническим каналам, как правило, снижается до приемлемого уровня.

Для примера, в таблице 6 приведено соответствие идентифицированных в процессе данной работы угроз безопасности информации некоторому количеству применяемых в СЗИ ТКС СН защитным мерам по требованиям рассмотренных нормативных документов.

Таблица 6 – Соответствие угроз ИБ защитным мерам СЗИ ТКС СН

Угроза ИБ	ЗМ	Руководящий документ
Угроза	Взаимодействие сегмента сети, в котором	Приказ ФСТЭК 11 февраля

Продолжение таблицы 6

Угроза ИБ	ЗМ	Руководящий документ
неправомерного ознакомления с защищаемой информацией	обрабатывается информация ограниченного доступа с другими сегментами ТКС СН необходимо осуществлять в соответствии с требованиями информационной безопасности. Коммуникационное оборудование (коммутаторы, концентраторы, маршрутизаторы) должно быть расположено в пределах контролируемой зоны.	2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
	При настройке коммуникационного оборудования и монтаже кабельной системы ТКС СН необходимо учитывать распределение трафика по сегментам сети в соответствии с видами деятельности организации.	Приказ ФСТЭК 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
	Подключение ЛВС, осуществляющей обработку информацию ограниченного доступа к автоматизированной системе иного класса защищенности должно осуществляться посредством МЭ. Для защиты КИ при ее передаче по каналам связи между сегментами ТКС СН, обрабатывающими информацию, различного уровня конфиденциальности необходимо использовать МЭ. В случае рассматриваемой ТКС СН (класс 1Г) - МЭ не ниже четвертого класса	РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
	Необходимо осуществлять идентификацию и проверку подлинности субъектов доступа при входе в систему (операционную систему АРМ) с использованием идентификатора (кода) и пароля условно-постоянного действия, который имеет длину не менее шести символов (использование минимум двух алфавитов, например - буквенный и циферный)	Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
	Требование по обеспечению доверенной загрузки средств вычислительной техники	Приказ ФСТЭК 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей

Продолжение таблицы 6

Угроза ИБ	ЗМ	Руководящий документ
		государственную тайну, содержащейся в государственных информационных системах».
Угроза преодоления физической защиты	Для обеспечения защиты информации в процессе эксплуатации ТКС СН должны выполняться следующие основные положения и требования: допуск к защищаемой информации лиц, работающих в ТКС СН, необходимо осуществлять в соответствии с установленной разрешительной системой допуска; во время обработки КИ в помещениях, где размещаются средства, осуществляющие ее обработку, могут находиться только лица, допущенные к обрабатываемой информации в соответствии с разрешительной системой допуска; допуск прочих лиц, доступ к системе которым необходим в соответствии со служебной необходимостью (ремонтные, профилактические работы) возможен только с разрешения руководителя организации	Приказ ФСТЭК 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
	Необходимо организовать контролируемую зону, в пределах которой размещены стационарные ТС, обрабатывающие конфиденциальную информацию, и средства защиты такой информации, а также средства обеспечения функционирования ТКС СН.	Приказ ФСТЭК 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей
	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключают несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены	государственную тайну, содержащейся в государственных информационных».
	Необходимо обеспечить физическую охрану ТКС СН (устройств и носителей информации), предусматривающую постоянное наличие охраны территории КЗ. Несение охранной службы должно осуществляться с использованием технических средств охраны и персонала. При этом обязательным является использование пропускного режима и	Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и

Продолжение таблицы 6

Угроза ИБ	ЗМ	Руководящий документ
	специальное оборудование помещений где расположена ТКС СН;	требования по защите информации».

В рассмотренной выше таблице приведена только часть защитных мер, направленных на снижение вероятностей реализации идентифицированных угроз. При этом, рассмотренные защитные меры значительно снижают вероятность реализации угроз безопасности информации.

Таким образом, можно говорить о том, что угрозы НСД и угрозы утечки информации по техническим каналам парируются в результате применения защитных мер согласно требованиям руководящих документов для рассматриваемой ТКС СН.

Однако в результате реализации защитных мер по требованиям рассмотренных нормативных документов не снижается вероятность реализации техногенных видов угроз, в частности - утечки защищаемой информации за счет неисправностей (сбоев) аппаратно-программных средств из состава ТКС СН.

Таким образом, по результатам разработки модели угроз и модели нарушителей для рассматриваемой ТКС СН была идентифицирована актуальная угроза безопасности информации техногенного характера: угроза утечки защищаемой информации за счет неисправностей (сбоев) аппаратно-программных средств из состава ТКС СН.

3 Принципы и алгоритмы работы ТКС СН

В данном разделе описаны принципы и алгоритмы работы рассматриваемой ТКС СН в режиме штатного функционирования с целью определения технических средств из состава телекоммуникационной системы, неисправности (сбои) в аппаратно-программном обеспечении которых могут приводить к реализации актуальной угрозы утечки информации, рассмотренной в предыдущем разделе.

На схеме информационных потоков (см.рисунок 2) обобщенно отражены процессы обмена конфиденциальной и не конфиденциальной информации. Источниками КИ при информационном обмене в ТКС СН являются следующие технические средства: АРМ 1.1, ..., АРМ 1.5, сервер 1.

В штатном режиме функционирования, сотрудники, работающие на автоматизированных рабочих местах из состава Сети 1 посредством специального программного обеспечения, выполняют следующие операции: прием с сервера, создание, изменение, обработку, хранение, удаление документации, содержащей конфиденциальные сведения локально, на своих рабочих местах. В конце каждого рабочего дня (возможно чаще) каждый сотрудник выполняет синхронизацию (передачу) подготовленной документации на локальном АРМ с сервером Сети 1.

Помимо этого, в конце каждой рабочей недели, каждый сотрудник выполняет подготовку и передачу отчетности о проделанной работе к АРМ руководителя отдела (АРМ 1.2 (АРМ 1.1)). Руководитель отдела, заместитель руководителя отдела, в числе прочего выполняют подготовку и передачу документации о выполненной работе (приведенной к типу не конфиденциально) в экономический отдел (бухгалтерия, отдел кадров). Передача информации внутри Сети 1 реализуется посредством Ethernet-коммутатора. Межсетевое взаимодействие обеспечивается с использованием МСЭ.

Источниками НКИ являются следующие ТС: АРМ 2.1, АРМ 2.2, АРМ 2.3, сервер 2. В штатном режиме функционирования, сотрудники, работающие на

автоматизированных рабочих местах из состава Сети 2 посредством специального программного обеспечения, выполняют следующие операции: прием с сервера 2, создание, изменение, обработку, хранение, удаление документации, содержащей не конфиденциальные сведения локально, на своих рабочих местах. В конце каждого рабочего дня (возможно чаще) каждый сотрудник выполняет синхронизацию подготовленной документации на локальном АРМ с сервером Сети 2.

Таким образом, по результатам рассмотрения штатного алгоритма взаимодействия технических средств из состава ТКС СН, были определены технические средства, одновременно обрабатывающие КИ и НКИ, к таким ТС относятся: АРМ 1.1, АРМ 1.2, Коммутатор 1. Сбои (неисправности в аппаратно-программном обеспечении данных технических средств могут привести к пересечению потоков НКИ и КИ).

Необходимо отметить, что анализ структурной схемы, а также схемы информационных потоков ТКС СН в данном случае является тривиальной задачей. Для анализа схемы информационных потоков ТКС СН, имеющей более сложную структуру и топологию, удобно использовать теорию графов. Практическая ценность применения теории графов при описании и анализе схем информационных потоков информационной системы с целью определения возможности возникновения опасных событий для ТКС СН за счет неисправностей и сбоев ТС из состава подобной системы, отмечена в статье «Применение теории графов при выявлении потенциальных угроз безопасности информации» научно-методического журнала «Проблемы современной науки и образования» [13].

Опасным событием (S) является реализация актуальной для ТКС СН угрозы: утечка КИ из Сети 1, предназначенной для обработки информации ограниченного доступа, в Сеть 2, не предназначенную для обработки информации ограниченного доступа. Рассмотрим возможные элементарные события в ТКС СН, ведущие к реализации актуальной угрозы для ТКС СН.

В процессе штатной передачи несекретной информации на сервер 1, за счет неисправностей (сбоев) в аппаратно-программном обеспечении АРМ 1.1 (АРМ 1.2) возможно ошибочное формирования пакета данных к передаче, содержащего конфиденциальную информацию (в поля данных пакета записывается КИ вместо НИ). Коммутаторы 1, 2 штатно передадут пакет посредством МСЭ (штатно) на сервер 1, непредназначенный для обработки информации ограниченного доступа.

Данное событие (S_I) так же возможно за счет неисправностей (сбоев) в аппаратно-программном обеспечении АРМ 1.3 (АРМ 1.4, АРМ 1.5, сервер 1): при формировании пакета к передаче, содержащего КИ, искажается поле адреса, в результате чего, коммутатор, посредством МСЭ (штатно) направляет пакет в сеть, не предназначенную для обработки информации ограниченного доступа.

Таким образом, неисправности (сбои) технических средств АРМ 1.1 ..., АРМ 1.5, сервера 1 являются опасными событиями и могут быть представлены следующим выражением (знак «+» в данном случае является логической дизъюнкцией)

$$S_I = (S_{ARM1} + S_{ARM2} + S_{ARM3} + S_{SARM4} + S_{ARM5} + S_{Server}). \quad (1)$$

В процессе сетевого взаимодействия технических средств Сети 1, за счет неисправностей (сбоев) в аппаратно-программном обеспечении коммутатора 1 возможно искажение адресных полей пакетов, в результате чего, пакеты посредством МСЭ (штатно) ошибочно отправляются в Сеть 2, не предназначенную для обработки информации ограниченного доступа. Таким образом, неисправность (сбой) ТС коммутатор 1, является опасным событием (S_2) и может быть представлено следующим выражением

$$S_2 = S_{comm}, \quad (2)$$

тогда событие утечки КИ из сети, предназначенной для обработки информации ограниченного доступа, в сеть, не предназначенную для обработки информации ограниченного доступа, можно представить следующим выражением

$$S=S_1+S_2. \quad (3)$$

При оценке возможности утечки КИ из сети, предназначенной для обработки информации ограниченного доступа, в сеть, не предназначенную для обработки информации ограниченного доступа, в первую очередь необходимо проанализировать МСЭ. Как правило, при межсетевом взаимодействии, в случаях, рассмотренных выше (при искажении адресной части пакета, а также при искажении полей данных пакета) МСЭ не обеспечивает отбраковку ошибочно сформированных пакетов. В связи с этим, в данном дипломном проекте рассмотрен только этот случай использования МСЭ, как наиболее характерный.

Таким образом, по результатам анализа принципов и алгоритмов функционирования, а также схемы информационных потоков ТКС СН можно сделать вывод о том, что в результате неисправностей (сбоев) аппаратно-программного обеспечения изделий АРМ 1.1...АРМ 1.5, сервер 1, коммутатор 1 из состава ТКС СН возможно возникновение опасных событий. Для определения показателей надежности данных технических средств, необходимо провести анализ аппаратно-программного обеспечения данных изделий.

4 Анализ технических средств из состава ТКС СН на предмет возникновения в них неисправностей (сбоев), приводящих к возникновению опасных событий

4.1 Анализ аппаратного обеспечения технических средств из состава ТКС СН

В данном разделе проведен анализ технических средств из состава ТКС СН, аппаратного обеспечения данных ТС, с целью определения вероятностей неисправностей (сбоев), приводящих к возникновению опасных событий для ТКС СН.

По результатам рассмотрения принципов и алгоритмов функционирования ТКС СН были выбраны ТС для анализа: АРМ 1.1...АРМ 1.5, сервер 1, коммутатор Ethernet. Анализ аппаратного обеспечения ТС был приведен на примере АРМ 1.1.

Изделие АРМ 1.1 представляет собой автоматизированное рабочее место руководителя отдела и предназначено для автоматизации задач, входящих в полномочия данного сотрудника.

Аппаратная часть АРМ 1.1 реализован на базе персональной электронно-вычислительной машины, в состав которой включаются жидкокристаллический монитор клавиатура и координатный манипулятор типа «мышь». Состав аппаратного обеспечения АРМ 1.1 приведен на рисунке 3.

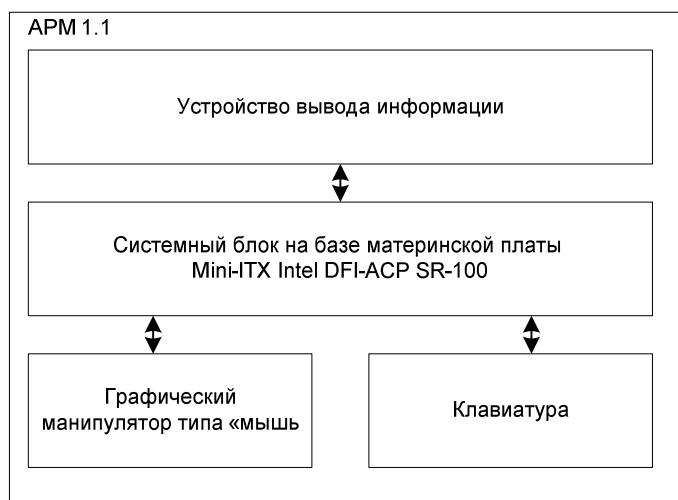


Рисунок 3 – Состав изделия АРМ 1.1

Рассматриваемая ЭВМ предназначена для использования в качестве рабочих станций в составе локальных вычислительных сетей, в качестве автономных персональных ЭВМ. ЭВМ характеризуется малым энергопотреблением, низким уровнем шума и малыми габаритами. Оригинальная конструкция позволяет крепить системный блок на горизонтальных и вертикальных поверхностях.

Основным аппаратно-программным блоком изделия АРМ 1.1 является системный блок, который изготавливается на базе системной платы форм-фактора mini-ITX (базовый вариант Mini-ITX Intel DFI-ACP SR100). К средствам ведения диалога с оператором (пользователем) относятся: клавиатура, графический манипулятор с прокруткой ГМ-П, и жидкокристаллический монитор.

Структурная схема материнской платы Mini-ITX Intel DFI ACP SR100, которая реализует основные функциональные задачи, приведена на рисунке 4.

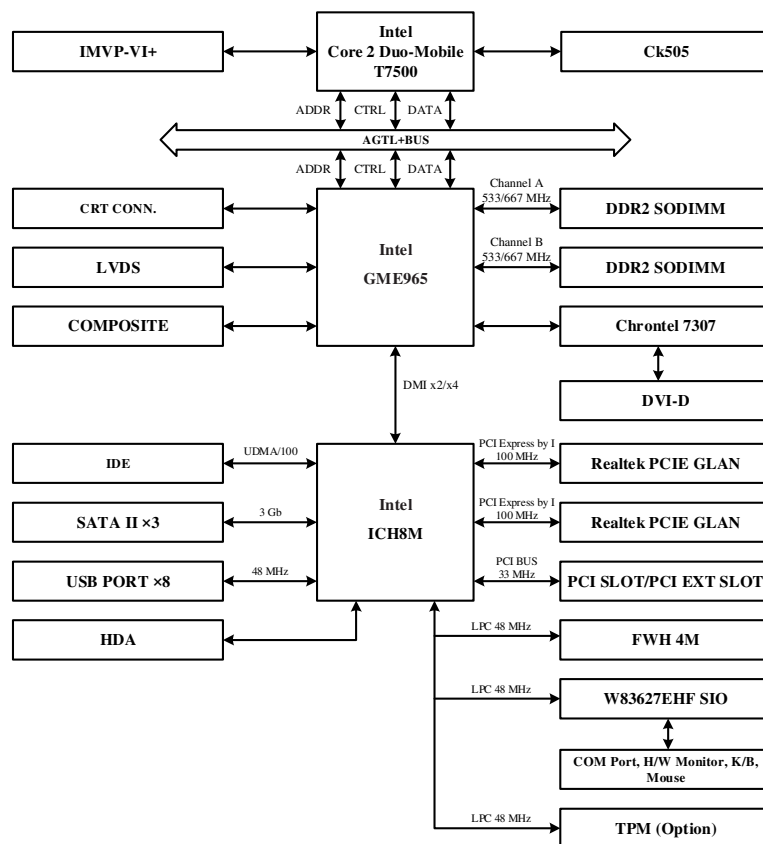


Рисунок 4 – Структурная схема материнской платы Intel DFI-ACP SR100

Далее рассмотрим назначение и основные характеристики используемых в работе аппаратных компонент из состава системного блока и материнской платы Intel DFI-ACP SR100.

Процессор Intel Core 2 Duo-Mobile T7500 (семейство 86-разрядных микропроцессоров) предназначен для клиентских систем и основан на микроархитектуре Core, разработанной и производимой корпорацией Intel.

Основные параметры процессора Intel Core 2 Duo-Mobile T7500 представлены в таблице 7.

Таблица 7 – Основные параметры процессора Intel Core 2 Duo-Mobile T7500

Параметр	Значение параметра
Базовая тактовая частота	2200 МГц
Кэш первого уровня	64 Кб
Кэш второго уровня	4096 Кб
Топологический размер	65 нм
Размер корпуса	35 мм × 35 мм
Расчетная TDP	35 Вт
Форм-фактор	FPGA
Число контактов	478
Площадь кристалла	143 мм ²
Максимальная рабочая температура	100°C
Набор команд	64-bit
Диапазон напряжения	1.075 В – 1.250 В
Количество ядер	2

Чипсет «Северный мост» Mobile Intel GME965 Express Chipset отвечает за работу процессора Intel Core 2 Duo с оперативной памятью и видеоадаптером.

Основные параметры чипсета Intel GME965 представлены в таблице 8.

Таблица 8 – Основные параметры чипсета Intel GME965

Параметр	Значение параметра
Расчетная TDP	13,5 Вт
Форм-фактор	FCBGA
Число контактов	1299
Температура корпуса	105°C
Поддерживаемая частота системной шины	800 МГц
Максимальный объем памяти	4 Гбайт
Типы памяти	DDR2 533/667 МГц
Максимальное число каналов памяти	2
Интегрированная графическая система	Да
Вывод графической системы	VGA, SDVO, LVDS

Южный мост Intel ICH8M поддерживает шину PCI, контроллер SATA, контроллер USB, контроллер Ethernet, контроллер LPC и контроллер SPI. Для соединения южного моста и северного моста используется последовательная шина DMI, разработанная компанией Intel.

Основные параметры южного моста Intel ICH8M представлены в таблице 9.

Таблица 9 – Основные параметры южного моста Intel ICH8M

Параметр	Значение параметра
Рабочее напряжение	1,05 В
Размер корпуса	31 мм × 31 мм
Расчетная TDP	2,4 Вт
Форм-фактор	mBGA
Число контактов	676
Топологический размер	250 нм
Площадь кристалла	1,18 см ²
Температура корпуса	105°C
Поддержка PCI	4 (32 бит/33 МГц)
Версия USB	USB 2.0
Общее количество интерфейсов SATA	3
Сетевой адаптер (onBoard)	10/100/1000
Интегрированный адаптер IDE	1 Channel

Оперативная память используется для оперативного обмена информацией между процессором, внешней памятью и периферийными подсистемами.

Основные параметры оперативной памяти Kingston KVR 667 D2 S5/2G представлены в таблице 10.

Таблица 10 – Основные параметры SDRAM Kingston KVR667D2S5/2G

Параметр	Значение параметра
Стандарт	DDR2
Форм-фактор	SODIMM
Количество контактов	200
Объем памяти	2 ГБ
Тактовая частота	667 МГц
Пропускная способность	5300 Мб/с
Поддержка ECC	Нет
Количество чипов на модуле	16
Компоновка чипов на модуле	Двусторонняя
Напряжение питания	1,8 В

Накопитель SSD предназначен для энергонезависимого долговременного хранения всего программного обеспечения, констант и исходных данных, необходимых для функционирования изделия.

Основные параметры SSD Intel SSD SA2 CW 120G 310 представлены в таблице 11.

Таблица 11 – Основные параметры накопителя SSD Intel SSD SA2 CW 120G310

Параметр	Значение параметра
Тип	Твердотельный накопитель
Объем	120 Гбайт
Форм-фактор	2,5"
Скорость чтения данных	270 Мбайт/с
Скорость записи данных	130 Мбайт/с
Интерфейс	SATA II
Среднее время наработки на отказ	1 200 000 ч
Потребляемая мощность при работе	2,5 Вт

BIOS содержит драйвера низкого уровня для обслуживания основных устройств ввода-вывода, программу начального загрузчика, выполняющую функцию загрузки ОС с диска, и программу POST, осуществляющую тестирование устройств ПК при включении питания.

Внешняя видеокарта Intel Graphics Media Accelerator (GMA) X3100 предназначена для обработки и отображения компьютерной графики на экране изделия.

Основные параметры видеокарты Intel GMA X3100 представлены в таблице 12.

Таблица 12 – Основные параметры видеокарты Intel GMA X3100

Параметр	Значение параметра
Тактовая частота	500 МГц
Тип памяти	mit Hauptspeicher geteilt (shared)
Максимум памяти	384 Мбайт
Технология	90 нм
DirectX	DirectX 10, Shader 3.0
Потребляемая мощность при работе	13.5 Вт

Звуковая карта Realtek ALC262 является одной из составляющих аудиосистемы компьютера и позволяет работать со звуком на компьютере.

Основные параметры звуковой карты Realtek ALC262 представлены в таблице 13.

Таблица 13 – Основные параметры звуковой карты Realtek ALC262

Параметр	Значение параметра
Количество ЦАП	2
Разрядность ЦАП	24 бит
Количество АЦП	3
Разрядность АЦП	20 бит

Внешний сетевой адаптер Realtek RTL8111B позволяет организовать сеть Gigabit Ethernet с высокой пропускной способностью, максимальной надежностью и стабильностью канала связи.

Основные параметры сетевого адаптера Realtek RTL8111B представлены в таблице 14.

Таблица 14 – Основные параметры сетевого адаптера Realtek RTL8111B

Параметр	Значение параметра
Интерфейс	PCI
Форм-фактор	FCBGA
Число контактов	1299
Скорость передачи данных	10 Мбит/с, 100 Мбит/с, 1000 Мбит/с

Далее были определены компоненты из состава процессорного модуля изделия АРМ 1.1, сбои и неисправности которых могут приводить к возникновению опасных событий, рассмотренных в разделе 2.

Сбои и неисправности микросхемы CPU могут приводить к ошибочному выполнению команд или искажению команд и данных СПО в процессе его выполнения, в результате чего возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к возникновению опасных событий.

Причинами неустойчивой работы центрального процессора могут быть сбои в блоке управления при считывании команд (данных) из оперативной памяти, сбои в арифметико-логическом устройстве (АЛУ) при считывании команд (данных) из регистров и при непосредственном выполнении команд, а также сбои при записи/чтении команд (данных) в ассоциативную память.

Сбои и неисправности чипсета «Северный мост» могут приводить к искажению команд и данных, в результате чего возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к возникновению опасных событий.

Причинами неустойчивой работы чипсета могут быть сбои в блоках управления, сбои в регистрах управления и данных, предназначенных для пересылки информации.

Сбои и неисправности чипсета могут приводить к искажению команд и данных, передаваемых/принимаемых от устройств, подключенных по низкоскоростным шинам, в результате чего возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к возникновению опасных событий.

Причинами неустойчивой работы чипсета могут быть сбои в блоках управления, сбои в регистрах управления периферийными устройствами, а также сбои в регистрах данных, предназначенных для пересылки информации.

Сбои и неисправности микросхемы SDRAM могут приводить к искажению команд и данных СПО в процессе его выполнения, в результате чего возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к возникновению опасных событий.

Причинами неустойчивой работы оперативной памяти могут быть сбои в любой ячейке памяти, вызванные, например, некачественной фильтрацией питающего напряжения или «плавающей» формой управляющих импульсов.

Сбои и неисправности накопителя SSD могут приводить к искажению команд и данных СПО во время их записи, чтения или хранения, в результате чего в процессе выполнения СПО возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к возникновению опасных событий.

Причинами неустойчивой работы накопителя SSD могут быть сбои в работе импульсных блоков питания накопителя SSD, сбои одной или

нескольких микросхем NAND Flash-памяти, а также программные сбои в микроконтроллере накопителя SSD.

Сбои и неисправности микросхемы BIOS могут приводить к искажению команд встроенного программного обеспечения (ВПО), используемых СПО в процессе его выполнения, в результате чего возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к возникновению опасных событий.

Сбои и неисправности видеоадаптера могут приводить к искажению (пропаданию) данных, выводимых на экран дисплея. Однако данное событие приведет к невозможности восприятия оператором отображаемой на экране дисплея информации, что не является опасным последствием и не приведет к возникновению опасных событий.

Сбои и неисправности звуковой карты могут приводить к искажению (пропаданию) звуковой информации, воспроизводимой в наушниках и колонках. Однако данное событие приведет к невозможности восприятия звуковой информации оператором, что не является опасным последствием и не приведет к возникновению опасных событий.

Сбои и неисправности сетевых адаптеров могут приводить к искажению (пропаданию) данных, принимаемых/передаваемых по локальной сети Ethernet. Однако данное событие приведет к невозможности обмена данными между сопрягаемыми изделиями по сети Ethernet, что не является опасным последствием и не приведет к возникновению опасных событий.

Таким образом, к возникновению опасных событий могут привести неисправности (сбои) следующих аппаратных компонент – центральный процессор (CPU), чипсет «Северный мост» (NB), чипсет «Южный мост» (SB), оперативная память (SDRAM), накопитель SSD (SSD) и базовая система ввода-вывода (BIOS).

Для определения возможности возникновения неисправностей (сбоев) выбранных компонентов, и как следствие, реализации актуальной угрозы информационной безопасности для рассматриваемой ТКС СН необходимо

рассчитать надежность выбранных элементов. Надежность – свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования

Для расчета вероятности возникновения опасных событий за счет неисправностей (сбоев) в аппаратно-программном обеспечении ТС, будем использовать следующие показатели надежности:

- вероятность безотказной работы компонента $P(t)$ – вероятность того, что в пределах заданного времени отказ компонента ТС не возникнет;
- вероятность отказа компонента $Q(t)$ определяет вероятность, с которой в пределах заданного времени возникнет отказ компонента ТС;
- эксплуатационная интенсивность отказов λ – условная плотность вероятности возникновения отказа компонента в условиях эксплуатации.

При экспоненциальном распределении времени до отказа вероятность безотказной работы технического средства определяется выражением

$$P(t) = e^{-\lambda t}. \quad (4)$$

Вероятность отказа является обратной величиной, относительно значения вероятности безотказной работы, данное соотношение можно представить выражением

$$Q(t) = 1 - P(t) = 1 - e^{-\lambda t}. \quad (5)$$

Таким образом, зная эксплуатационную интенсивность отказов изделия АРМ 1.1 можно рассчитать вероятность безотказной работы (вероятность отказа) в течении заданного промежутка времени.

Эксплуатационная интенсивность отказов АРМ 1.1 складывается из независимых отказов его компонентов: центральный процессор (CPU), чипсет «Северный мост» (NB), чипсет «Южный мост» (SB), оперативная память (SDRAM), накопитель SSD (SSD) и базовая система ввода-вывода (BIOS) и определяется выражением

$$\lambda_{\text{АРМ 1.1}} = \lambda_{\text{CPU}} + \lambda_{\text{NB}} + \lambda_{\text{SB}} + \lambda_{\text{SDRAM}} + \lambda_{\text{SSD}} + \lambda_{\text{BIOS}}. \quad (6)$$

Расчет эксплуатационной интенсивности отказа был выполнен с использованием автоматизированной системы расчета надежности (АСРН), которая позволяет рассчитывать суммарную интенсивность отказов аппаратуры, укомплектованной ЭРИ отечественного и иностранного производства (ИП). При расчете эксплуатационной интенсивности отказов для каждого компонента изделия АРМ 1.1 были указаны технические характеристики, согласно спецификациям, выбраны класс и группа электрорадиоизделия, указаны необходимые для данной группы параметры, температуру окружающей среды и электрорадиоизделия, а также условия эксплуатации.

Полученные значения эксплуатационных интенсивностей отказов ЭРИ, используемых в изделии АРМ 1.1, приведены в таблице 15.

Таблица 15 – Эксплуатационная интенсивность отказов ЭРИ АРМ 1.1

Наименование элемента	Типономинал элемента	Часовая эксплуатационная интенсивность отказа элемента	Суточная вероятность неисправности элемента	Обозначение вероятности
CPU	Центральный процессор Intel Core 2 Duo-Mobile T7500	$3,71 \times 10^{-5}$	$8,90 \times 10^{-4}$	P_{CPU}
NB	Чипсет «Северный мост» Intel GME965	$7,29 \times 10^{-6}$	$1,75 \times 10^{-4}$	P_{NB}
SB	Чипсет «Южный мост» Intel ICH8M	$2,87 \times 10^{-6}$	$6,88 \times 10^{-5}$	P_{SB}
SDRAM	Оперативная память	$4,20 \times 10^{-6}$	$1,01 \times 10^{-4}$	P_{SDRAM}

Продолжение таблицы 15

Наименование элемента	Типономинал элемента	Часовая эксплуатационная интенсивность отказа элемента	Суточная вероятность неисправности элемента	Обозначение вероятности
	Kingston KVR 667 D2 S5/2G			
SSD	Накопитель SSD Intel SSD SA2 CW 120G 310	$8,33 \times 10^{-7}$	$2,00 \times 10^{-5}$	P_{SSD}
BIOS	Базовая система ввода-вывода BIOS	$2,50 \times 10^{-8}$	$6,00 \times 10^{-7}$	P_{BIOS}

На основе полученной эксплуатационной интенсивности отказов по формуле (4) была рассчитана вероятность безотказной работы ТС АРМ 1.1 (параметр t равен 24 часам, так как ЭВМ перезагружается не реже чем один раз в сутки)

$$P_{APM1.1}(t) = e^{-\lambda_{APM1.1}t} = 0,9987446.$$

Тогда вероятность отказа ТС АРМ 1.1 в соответствии с выражением (5) составляет

$$Q_{APM1.1}(t) = 1 - P_{APM1.1}(t) = 0,126 \times 10^{-2}.$$

В случае отсутствия исходных данных об аппаратном обеспечении технического средства (например, ТС является изделием иностранного производства) для расчета вероятности безотказной работы можно использовать параметр «Наработка на отказ (MTBF)», который характеризует отношение суммарной наработки восстанавливаемого объекта к математическому ожиданию числа его отказов в течение этой наработки. Данное соотношение может быть представлено выражением

$$MTBF = \frac{1}{\lambda} \text{ часов.} \quad (7)$$

Например, для коммутаторов из состава рассматриваемой ТКС СН Ethernet Cisco Catalyst 4900 наработка на отказ (*MTBF*) равна 145 422 часам [14], соответственно интенсивность отказов коммутатора Ethernet, рассчитанная по формуле (7), равна

$$\lambda_{Eth} = \frac{1}{MTBF} = 6,87 \times 10^{-6} \text{ 1/ч.}$$

На основе полученной интенсивности отказов коммутатора Ethernet рассчитана вероятность его безотказной работы и вероятность его отказа в течение суток (t равно 24 часам)

$$P_{Eth}(t) = e^{-\lambda_{Eth} N_{\text{Э1}} t} = 1,65 \times 10^{-4},$$

$$Q_{Eth}(t) = 1 - P(t) = 0,999835134.$$

В результате анализа аппаратного обеспечения технических средств из состава рассматриваемой ТКС СН были получены вероятности неисправностей (сбоев) этих ТС. Полученные вероятности можно использовать в качестве интегральных вероятностей возникновения опасных событий для технических средств их состава ТКС СН. Подставляя значения полученных вероятностей в выражение (3) можно вычислить интегральную вероятность реализации актуальной для ТКС СН угрозы информационной безопасности – угрозы утечки КИ из Сети 1 в Сеть 2.

Однако, интегральные значения вероятностей, полученные с использованием современных автоматизированных систем расчета надежности, не являются обоснованной оценкой возникновения опасных событий за счет неисправностей (сбоев) технических средств. В качестве примера, рассчитанная вероятность неисправностей (сбоев) для АРМ 1.1, в несколько раз превышает статистические значения вероятности отказов аппаратного обеспечения для ПЭВМ, разработанных несколько лет назад. В связи с этим, разработчики

внедряют в программное обеспечение, под управлением которого работает техническое средство механизмы защиты от отказов аппаратного обеспечения, а также механизмы восстановления работоспособности после отказа. В связи с этим, становится актуальной проблема обоснования полученных вероятностей отказов аппаратного обеспечения, за счет анализа программного обеспечения технического средства.

4.2 Обоснование необходимости анализа программного обеспечения технических средств из состава ТКС СН

Так как современные технические средства из состава ТКС СН работают под управлением программного обеспечения, рассчитанные в результате анализа аппаратного обеспечения технических средств интегральные вероятности возникновения опасных событий могут быть обоснованы только в том случае, когда проведен анализ программного обеспечения включающий в себя:

- восстановление алгоритма работы с целью подтверждения его корректного функционирования и обеспечения выполнения предъявленных к обработке информации требований;
- определение алгоритмических особенностей применения механизмов защиты информации, реализованных в программном обеспечении, с целью уменьшения значения вероятности возникновения опасных событий ТС;
- определение отсутствия (наличия) опасных программных конструкций с целью обоснования влияния на возникновение опасных событий только неисправностей (сбоев) аппаратного обеспечения.

Следует отметить, что программное обеспечение с точки зрения надежности имеет свою специфику относительно аппаратного обеспечения. Если характеристики аппаратного обеспечения с течением времени эксплуатации меняются, накапливаются изменения, которые могут привести к отказам, то программные средства с течением времени остаются неизменными. Однако, допущенные при разработке, отладке и загрузке программ в целевую

информационную систему ошибки могут приводить в процессе эксплуатации к ошибкам или сбоям [15].

Таким образом, необходимо помимо анализа аппаратного обеспечения указанных технических средств, необходимо провести анализ программного обеспечения, реализующего основные алгоритмы взаимодействия ТС в составе ТКС СН в целях получения обоснованных вероятностей возникновения опасных событий.

5 Анализ программного обеспечения технических средств из состава ТКС СН с целью определения возможности возникновения опасных событий в результате неисправностей (сбоев) технических средств

В данном разделе проведен анализ программного обеспечения технических средств из состава ТКС СН, с целью определения возможности возникновения опасных событий для ТКС СН рассмотренных в разделе 2 данного дипломного проекта.

По результатам рассмотрения принципов и алгоритмов функционирования ТКС СН были выбраны ТС для анализа: АРМ 1.1...АРМ 1.5, сервер 1, коммутатор Ethernet.

Анализ программного обеспечения технического средства, позволяющий определить возможность возникновения опасных событий для ТКС СН за счет отказов ПО ТС, в общем случае должен отражать следующие сведения:

- информацию о составе программного обеспечения – необходимо определить перечень программного обеспечения (встроенного, системного и специального), функционал, сведения об типе программного обеспечения, реализующего протоколы взаимодействия ТС в составе ТКС СН для дальнейшего анализа (как правило – специальное программное обеспечение);

- сведения о аппаратных и программных средствах, необходимых для сборки программного обеспечения, информацию об условиях, процессе и результатах сборки программного обеспечения, реализующего протоколы взаимодействия ТС в составе ТКС СН;

- описание и анализ протоколов взаимодействия ТС в составе ТКС СН, которые реализует анализируемое программное обеспечения;

- информацию о программной инициализации технического средства и переходе в штатный режим функционирования, описание трактов прохождения КИ и НИ в процессе обработки информации, на основании которого выбираются программные модули для восстановления алгоритма работы;

- сведения о точке входа в программное обеспечение, реализующее протоколы взаимодействия ТС в составе ТКС СН;
- информацию об основных функциональных задачах ПО, с описанием алгоритмов ключевых функций, осуществляющих обработку КИ;
- схему восстановленного алгоритма работы, отражающую основные функциональные задачи, а также функции программы (при наличии), в процессе выполнения которых, возможно возникновение опасных событий;
- информацию (при наличии) об опасных программных конструкциях, ошибочно реализованных протоколах информационно-логического взаимодействия, об ошибках совместимости ПО и др. ошибок ПО, обнаруженных при пооператорном анализе, а также при анализе с использованием средств статического анализа исходного кода;
- выводы о возможности возникновения опасных событий в ТС.

Основываясь на сведениях, которые должны быть получены по результатам анализа программного обеспечения определим исходные данные для анализа программного обеспечения в соответствии с разрабатываемой методикой:

- сведения о языке и среде программирования СПО ТС;
- тексты программ СПО (модули исходного кода);
- рабочая программа СПО (модули исполняемого кода, файлы статических или динамических библиотек);
- сведения о назначении программы, области применения, применяемых методах, классе решаемых задач, минимальной конфигурации технических средств;
- сведения описывающие процедуры сборки и развертывания СПО;
- протоколы взаимодействия ТС.

Рассмотрим анализ программного обеспечения на примере технического средства АРМ 1.1.

5.1 Состав программного обеспечения

Все программное обеспечение изделия АРМ 1.1 разделено на встроенное, системное и специальное. Состав ПО АРМ 1.1 с указанием десятичных номеров и данных о сертификатах соответствия приведен в таблице 16.

Таблица 16 – Состав программного обеспечения изделия АРМ 1.1

Наименование программного изделия	Децимальный номер	Данные о сертификате соответствия
<i>Встроенное программное обеспечение</i>		
Встроенное программное обеспечение (BIOS Intel v.1.07, 11.05.2012)	–	–
<i>Системное программное обеспечение</i>		
ОС «Astra Linux Special Edition»	РУСБ.10015	Сертификат МО РФ № 1339 от 24.09.2010 (действителен до 15.09.2018)
СЗИ «SecretNet 7.6»	RU.88338853.501410	Сертификат ФСТЭК №2143 (действителен до 12.04.2021)
<i>Специальное программное обеспечение</i>		
СПО (клиентская часть) реализующее основные протоколы взаимодействия ТС в составе ТКС СН	–	–

СПО АРМ 1.1 устанавливается на нескольких компьютерах, входящих в состав Сети 1, объединенных в локальную вычислительную сеть (ЛВС). Функционирование Сети 1 обеспечивается согласованной работой всех компьютеров (АРМ 1.2, АРМ 1.3, АРМ 1.4, АРМ 1.5), выполняющих различные задачи.

Основными задачами СПО изделия АРМ 1.1 являются:

- распределение функциональных задач между компьютерами из состава Сети 1;
- управление, отображение текущего состояния и контроль рабочего процесса выполняемого компьютерами из состава Сети 1;
- сбор и хранение информации о проделанной работе, распределение и учет трудозатрат в процессе выполнения функциональных задач;

- информационный обмен с компьютерами и сервером в составе Сети 1 в части передачи КИ;
- информационный обмен с Сетью 2 в части передачи сведений о сотрудниках, о проделанной работе, иных сведений (НКИ);
- предоставление оператору программного комплекса справочной информации.

Состав СПО изделия АРМ 1.1 приведен в таблице 17.

Таблица 17 – Состав СПО изделия АРМ 1.1

Название модуля	Описание модуля
main.cpp	Модуль, содержащий точку входа в программу.
init.cpp	Модуль, реализующий инициализацию программных компонент СПО.
...	...

Таким образом, по результатам рассмотрения состава ПО АРМ 1.1, был сделан вывод, что СПО изделия АРМ 1.1 осуществляет обработку КИ, а также участвует в процессе обмена НКИ с Сетью 2. В связи с этим, далее проведен анализ СПО АРМ 1.1 с целью определения возможности возникновения опасных событий в процессе его функционирования.

5.2 Описание процесса сборки (развертывания) специального программного обеспечения

СПО изделия АРМ 1.1 является сложносоставным программным обеспечением, включающим в себя как внутренние модули, представленные файлами исходных кодов, так и внешние модули, представленные загружаемыми динамическими библиотеками. СПО изделия разработано на языке программирования C++ с использованием библиотек QT 4.8.5, среды разработки *QtCreator*, *QtDesigner* и компилятора *GCC*.

Для каждого файла исходного кода проекта СПО изделия была рассчитана контрольная сумма по алгоритму CRC-32 и зафиксированы размеры файлов. Перечень файлов исходного кода проекта программы, данные о контрольных суммах и размерах файлов приведены в таблице 18.

Таблица 18 – Перечень программных модулей СПО изделия

Имя файла	Размер файла (байт)	CRC
main.cpp	3 626	7311CB90
utils.h	1 317	1EEE706D
const.h	25 279	377869AE
...	...	...

Для сборки проекта программы изделия необходимо установить среду разработки и отладки QT Creator, комплект библиотек QT 4.8.5, а также компилятор MinGW 4.4. Все указанные средства разработки относятся к категории свободно-распространяемого программного обеспечения.

После установки среды разработки, средства компиляции и комплекта библиотек, выполняется настройка QT Creator. Для этого в параметрах среды разработки, необходимо указать путь к исполняемому файлу средства компиляции MinGW, а также к папке библиотеки QT 4.8.5. После этого создать новый комплект сборки и запуска QT-проектов, включив в него вышеуказанный компилятор и библиотеку.

После настройки среды QT Creator выполняется загрузка проекта «ARM1.1», посредством запуска файла arm.pro. При загрузке проекта в среду разработки, необходимо указать созданный ранее комплект сборки, после чего запустится обозреватель проекта, где можно проверить наличие всех файлов проекта.

Посредством команды «Собрать проект», осуществляется запуск компонента qmake, формирующего конфигурационный файл Makefile и далее, компонента gcc, непосредственно выполняющего сборку программы. После выполнения указанной команды, было получено сообщение об успешной сборке проекта.

В результате сборки программы был сформирован deb-пакет arm.deb, который имеет размер 28 983 Кб и контрольную сумму 0x86481B51, рассчитанную по алгоритму CRC-32.

СПО устанавливается на АРМ 1.1, АРМ 1.2. Перед установкой ПО должна быть проведена установка операционной системы специального

назначения «Astra Linux Special Edition» в соответствии с руководством администратора РУСБ.10015-01 95 01.

Установка СПО АРМ 1.1 производится из deb-пакетов, сформированных из конфигурационных, исполняемых файлов, а также файлов библиотек, полученных в результате компиляции проектов СПО. Для установки СПО необходимо выполнить последовательность команд в терминале:

- *su*, ввести пароль администратора для получения прав;
- *cp <исходный_файл> <целевая_директория>*, <целевая_директория> – директория, из которой будет производиться установка;
- *cd <целевая_директория>*;
- *dpkg -i *.deb*, дождаться окончания процесса установки пакетов;
- *apt-get install -f -y*, данная команда позволяет убедиться, что все пакеты корректно установились.

После установки пакетов необходимо выполнить перезагрузку. Настройка СПО производится в автоматическом режиме при установке СПО АРМ 1.1 устанавливается IP-адрес, выполняется тестирование системы на соответствие минимальным требованиям установки, редактируются конфигурационные файлы программы, выполняется контроль зависимостей ПО.

Результатом установки СПО АРМ 1.1 является распакованная, сконфигурированная, протестированная программа, функционирующая под управлением ОС «Astra Linux Special Edition».

При перезагрузке (включении) изделия АРМ 1.1 происходит загрузка операционной системы специального назначения «Astra Linux Special Edition». По окончании загрузки ОС автоматически загружается СПО АРМ 1.1.

Таким образом, по результатам сборки и развертывания специального программного обеспечения АРМ 1.1 были сделаны следующие выводы:

- сборка проекта осуществляется с помощью свободно распространяемых средств разработки, отладки и компиляции;

- сборка выполняется автоматически, возможность вмешаться в процесс сборки отсутствует;
- ошибок ПО в процессе сборки не обнаружено;
- развертывание программного обеспечения выполняется средствами операционной системы «Astra Linux Special Edition»;
- собранное и развернутое программное обеспечение функционирует под управлением операционной системы «Astra Linux Special Edition».

5.3 Описание протокола взаимодействия

В процессе штатного функционирования, изделие АРМ 1.1 взаимодействует с изделиями АРМ 1.2, АРМ 1.3, АРМ 1.4, АРМ 1.5, сервер 1 из состава Сети 1 в части обмена КИ, а также с ТС АРМ 2.1, сервер 2 из состава Сети 2 в части обмена НКИ.

Взаимодействие АРМ 1.1 с указанными изделиями осуществляется по интерфейсу Fast Ethernet 10/100 BaseTX с использованием принципов сетевого взаимодействия на основе стека протоколов TCP/IP. Для обеспечения обмена используются следующие протоколы сетевой модели OSI:

- на физическом и канальном уровне – протокол Ethernet;
- на сетевом уровне – протокол IP;
- на транспортном уровне – протокол UDP.

АРМ 1.1 осуществляет взаимодействие с изделиями из Сети 1 и Сети 2 по однотипным алгоритмам, с использованием одинаковых способов сопряжения, сообщениями единого формата переменной длины.

Основные данные от ТС сервер 1 (сервер 2) поступают по запросу (команде) от АРМ 1.1. Также существуют несанкционированные (служебные) сообщения, формируемые и передаваемые изделием сервер 1 (сервер 2) без запроса от АРМ 1.1. В состав таких сообщений могут входить: статусные сообщения, сообщения о загрузке. Данные между АРМ 1.1 и АРМ 1.2 (АРМ 1.3, ..., АРМ 1.5, АРМ 2.1) передаются в свободном режиме при возникновении необходимости обмена.

Сообщения взаимодействия передаются пакетами переменной длины. Порядок передачи полей – слева направо. Порядок байтов в числовых полях – младшим байтом вперед. Пакеты сообщения обмена имеют общую структуру, представленную на рисунке 5.

Заголовок Ethernet	Заголовок IP	Заголовок UDP	Заголовок прикладного уровня					Полезные данные (DATA)
			ID	Addr	N	COM	G	
18 В	20 В	8 В	1 В	1 В	1 В	1 В	1 В	

Рисунок 5. Структура пакета управляющего сообщения

Таким образом, пакет сообщения включает стандартные заголовки Ethernet, IP, UDP и непосредственно данные, состоящие из заголовка прикладного уровня и полезных данных. Описание структуры заголовка управления:

- ID – идентификатор начала сообщения, принимает значение 0x7E;
- ADDR – уникальный адрес получателя пакета, равен 0x1 для АРМ 1.1;
- N – длина поля DATA сообщения в байтах (максимальный размер сообщения не может превышать 255 байт);
- COM – номер сообщения;
- G – уровень конфиденциальности информации 0x00 для НКИ, 0x01 для КИ.

В полезных данных (поле DATA) сообщения содержатся фрагменты документации НИ (НКИ). Структура поля DATA сообщений может изменяться в зависимости от передаваемого сообщения или поле DATA может вообще отсутствовать.

Таким образом, по результатам рассмотрения протокола информационно-логического взаимодействия изделия АРМ 1.1 и изделий АРМ 1.2, ..., АРМ 1.5, АРМ 2.1, сервер 1, сервер 2 сделаны следующие выводы:

- в процессе взаимодействия изделие АРМ 1.1 осуществляет обмен сообщениями КИ и НКИ. Принцип обмена данными сообщениями идентичен, в

структуре передаваемых пакетов различаются лишь поля заголовков (Ethernet, IP, UDP, прикладной заголовок);

- в сообщениях обмена имеются поля, которые могут содержать данные из большого множества значений, в том числе формирующиеся динамически в зависимости от входных параметров;

- в результате искажения полей заголовков пакета, возможно возникновение опасных для ТКС СН событий.

5.4 Выбор модулей для анализа

В данном разделе рассмотрены принципы работы, тракты прохождения информации и взаимодействие программных модулей СПО изделия АРМ 1.1 с целью определения программных модулей для дальнейшего восстановления алгоритма работы путем пооператорного анализа их исходных текстов.

При включении ТС блок питания системного блока АРМ выполняет самотестирование напряжений. Если значения напряжений соответствует норме, то на процессор подается напряжение и сигнал сброса. Процессор сбрасывает свою память и начинает работу. Работа процессора начинается с получения из BIOS программы POST (Power-On Self-Test – самотестирование при включении), которая осуществляет начальную инициализацию и тестирование аппаратного обеспечения ТС:

- тестирование регистров процессора;
- копирование BIOS в оперативную память, и проверка контрольных сумм BIOS;
- проверка контрольной суммы ПЗУ;
- проверка системного таймера и порта звуковой сигнализации;
- тест контроллера прямого доступа к памяти;
- проверка регенерации памяти и тестирование 64Кбайт нижней памяти;
- настройка чипсета;
- поиск и настройка;
- полное тестирование оперативной памяти;

- тестирование клавиатуры и других устройств ввода-вывода;
- проверка контрольной суммы CMOS и состояния батареек;
- инициализация COM и LPT-портов;
- инициализация дисководов и IDE-устройств;
- распределение системных ресурсов;
- поиск других устройств, содержащих свой BIOS (самодиагностика функциональных подсистем BIOS);
- вызов программного прерывания BIOS, по которому ищется загрузочный сектор.

Если в результате выполнения процедуры POST произойдет какой-либо сбой или будут выявлены ошибки аппаратных компонентов, то ТС выдаст определённую комбинацию звуковых сигналов и на экран монитора выведется сообщение об ошибке.

После успешного выполнения процедур POST происходит дальнейшая передача управления загрузчику операционной системы, который загружает ОС «Astra Linux Special Edition». По окончании загрузки ОС автоматически загружается СПО АРМ 1.1, изделие переходит в режим работы.

В режиме работы СПО АРМ 1.1 решает следующие задачи:

- распределение функциональных задач между компьютерами из состава Сети 1;
- управление, отображение текущего состояния и контроль рабочего процесса, выполняемого компьютерами из состава Сети 1;
- сбор и хранение информации о проделанной работе, распределение и учет трудозатрат в процессе выполнения функциональных задач;
- информационный обмен с компьютерами и сервером в составе Сети 1 в части передачи КИ;
- информационный обмен с Сетью 2 в части передачи сведений о сотрудниках, о проделанной работе, иных сведений (НКИ);

– предоставление оператору программного комплекса справочной информации.

Схема взаимодействия программ изделия АРМ 1.1 представлена на рисунке 6.

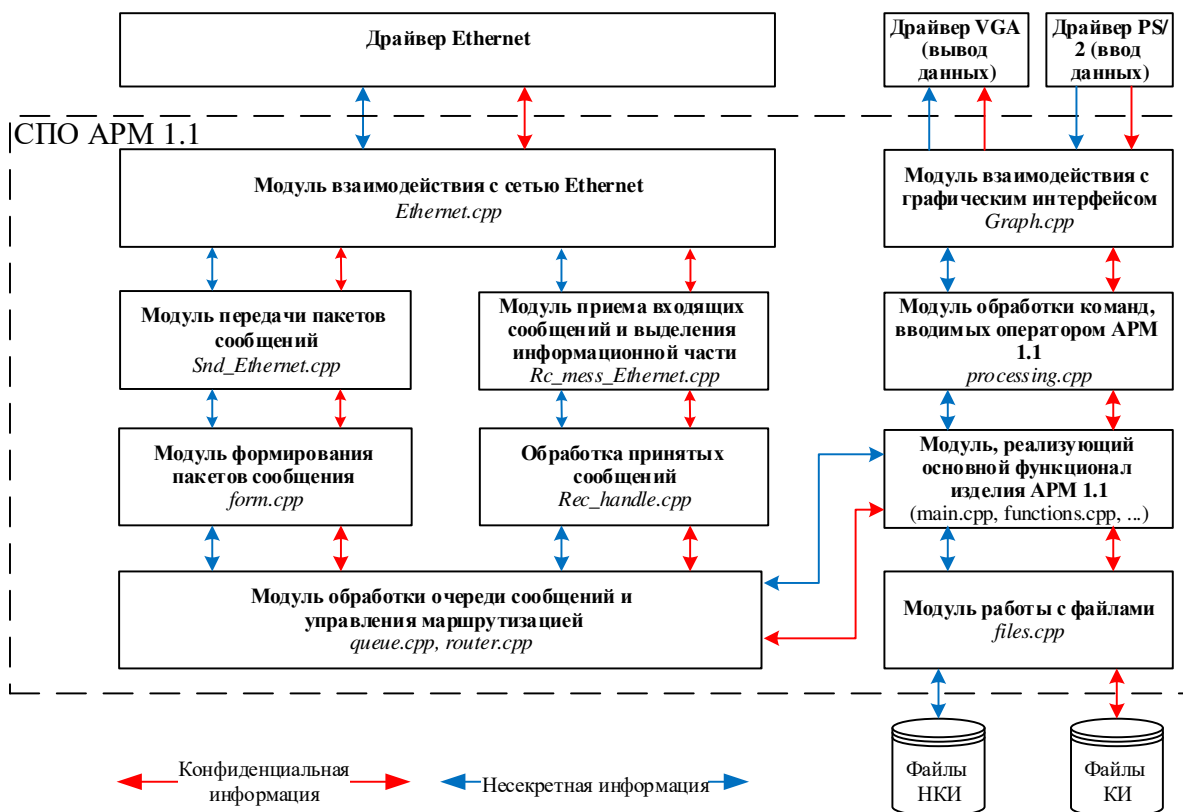


Рисунок 6 – Схема взаимодействия программ изделия АРМ 1.1

На схеме взаимодействия программ показаны потоки прохождения НКИ и КИ и обработка данных видов информации в модулях из состава СПО изделия. Описание трактов прохождения информации проведено на примере приема сообщений (КИ, НКИ) от изделий из состава ТКС СН и передачи сообщений (КИ, НКИ) к абонентам из состава ТКС СН.

Рассмотрим прием сообщений (КИ, НКИ) от изделий из состава ТКС СН:

– при поступлении сообщения драйвер Ethernet обрабатывает полученное сообщение и передает его в модуль взаимодействия с сетью Ethernet (*Ethernet.cpp*), где пакет помещается в очередь на обработку в модуле приема входящих сообщений *Rc_mess_Ethernet.cpp*;

– модуль приема входящих сообщений *Rc_mess_Ethernet.cpp* принимает сообщение. В случае успешного приёма в модуле *Rc_mess_Ethernet.cpp* производится выделение из сообщения данных с КИ (НКИ) и передача этих данных в модуль обработки принятых сообщений (*rec_handle.cpp*);

– в процессе обработки принятых сообщений, проверяются поля заголовков пакетов, в случае успешной проверки, полученное сообщение помещается в очередь обработки сообщений (модуль *queue.cpp*);

– модуль обработки очереди сообщений выполняет передачу принятого пакета в модуль, реализующий основной функционал изделия АРМ 1.1, где данные пакетов объединяются в принятый документ (файл), который сохраняется на жестком диске АРМ 1.1 с помощью модуля *files.cpp* и при необходимости, выводится на экран с помощью модуля взаимодействия с графическим интерфейсом (*graph.cpp*).

Рассмотрим передачу сообщений к изделиям из состава ТКС СН:

– в случае поступления команд оператора, модуль обработки команд оператора (*processing.cpp*) и модуль взаимодействия с графическим интерфейсом (*graph.cpp*) выполняют формирование и передачу соответствующего команде управляющего сообщения к модулю, реализующему основной функционал изделия АРМ 1.1 (*main.cpp*, *functions.cpp*);

– модуль, реализующий основной функционал изделия, в зависимости от типа управляющего сообщения, запускает процесс локальной работы с файлами (модуль *files.cpp*), либо посредством модуля работы с файлами запускает процесс передачи того или иного файла к абонентам ТКС СН;

– в процессе передачи файла к абонентам ТКС СН, файл разбивается на информационные пакеты, которые помещаются в очередь обработки сообщений (модуль *queue.cpp*);

– модуль обработки очереди сообщений передает очередное сообщение к модулю формирования пакетов сообщения (*form.cpp*), а затем к модулю

передачи пакетов сообщений (*snd_Ethernet.cpp*), где для каждого пакета формируются заголовки прикладного и сетевого уровня, после чего пакет передается к модулю взаимодействия с сетью Ethernet (*Ethernet.cpp*), где к пакету средствами ОС добавляется Ethernet-заголовок, после чего, пакет передается в ЛВС.

Таким образом, по результатам рассмотрения состава, назначения и алгоритма взаимодействия программ изделия определены модули, участвующие в процессе обработки и обмена КИ, НКИ: *processing.cpp*, *Ethernet.cpp*, *snd_Ethernet.cpp*, *form.cpp*, *queue.cpp*, *files.cpp*, *main.cpp*, *functions.cpp*, *graph.cpp*, *Rc_mess_Ethernet.cpp*, *rec_handle.cpp*.

Функциональные отклонения в работе данных модулей могут привести к нарушению штатных правил обработки информации, передаваемой в Сеть 2, в результате чего возможно появление опасных событий.

В связи с этим рассмотрим алгоритм функционирования вышеперечисленных модулей, полученный по результатам пооператорного анализа исходного кода.

5.5 Восстановление алгоритма работы модулей

В данном разделе представлен алгоритм работы программы, восстановленный по результатам пооператорного анализа исходного кода программных модулей, выбранных для анализа в разделе 5.4.

СПО АРМ 1.1 представляет собой клиент-серверное приложение, разработанное с применением следующих основных механизмов взаимодействия программных компонент (подпрограмм):

- механизм обработки сетевых событий с помощью сокетов протокола UDP/IP;
- механизм интерактивного взаимодействия с оператором;
- механизм работы с файлами с использованием библиотеки QT;
- механизм сигналов/слотов, реализующий межпроцессорное взаимодействие внутри СПО;

Точкой входа в СПО АРМ 1.1 является функция *int main(...)* модуля *main.cpp*. В данной функции осуществляется чтение конфигурационного файла и настройка параметров для дальнейшего обмена данными программного роутера с устройствами, с которыми подразумевается взаимодействие, и запуск программы. Псевдокод основной функции программы представлен ниже:

```
int main (int argc, char *argv[])
{
    инициализация объекта класса, управляющего графикой      (QApplication a(argc, argv))
    чтение номера ПК      (pathFileForNumPk = "./xml_config/comanderhmi_sw_router.xml")
    чтение типа абонента      (abonent = readTypeAbonent(pathFileForNumPk))
    чтение пароля абонента      (secur = readPasswordSecurity(pathFileForNumPk))
    если (secur)
    {
        установка защиты паролем      (CsrPlexMQ::getInstance()->setPasswordSecurity())
    }
    установка типа сети      (readTypeLAN(pathFileForNumPk))
    конфигурация роутера      (configCsrProgramModulesRouter(...))
    запуск роутера (сетевых      (CsrPlexMQ::getInstance()->beginWork(...))
соединений)
    запуск программы      (a.exec())
}
```

СПО АРМ 1.1 реализует следующие основные функциональные задачи (алгоритмы):

- настройка и установление сетевых соединений;
- формирование и передача КИ, НКИ;
- прием НКИ, КИ, инициативных сообщений и вывод принятой информации на графический интерфейс.

Далее рассмотрены результаты пооператорного анализа исходного кода программы для каждой из реализованных СПО АРМ 1.1 функциональных задач. Восстановление алгоритма работы функциональной задачи приведено на примере процесса настройки и установления сетевых соединений.

Настройка и установление сетевых соединений АРМ 1.1 выполняется в два этапа в основной функции *int main(...)*, модуля *main.cpp*.

На первом этапе вызывается функция *configCsrProgramModulesRouter(typelan, this_abonent, default_pk_type)* осуществляющая чтение конфигурационного файла для модуля обмена данными (роутера) и запись в роутер имен устройств, с которыми подразумевается взаимодействие.

На втором этапе осуществляется запуск роутера (настройка и установление сетевых соединений) с помощью вызова функции *CsrPlexMQ::beginWork(...)*.

Определение:

bool CsrPlexMQ::beginWork(QList<QString> listDevice).

Входной параметр:

QList<QString> listDevice – список устройств, подключаемых к роутеру.

Возвращаемое значение:

- true – успешно;
- false – не успешно.

Алгоритм работы:

Данная функция получает в качестве параметра список зарегистрированных устройств в роутере, после чего каждому устройству из списка в соответствии с его номером создается список *listInterfaceForHub*, связывающий адрес (код) устройства и настройки интерфейса на прием и передачу. Если в результате работы список пуст, то функция возвращает значение *False*, а иначе вызывает функцию *QSoftwareHub::beginWork(listInterfaceForHub)* модуля *qsoftwarehub.cpp* и возвращает значение *True*.

Определение:

bool QSoftwareHub::beginWork(QList<QString> listInterface).

Входной параметр:

QList<QString> listInterface – список настроек интерфейсов для устройств.

Возвращаемое значение:

- true – успешно;
- false – не успешно.

Алгоритм работы.

Данная функция отвечает за настройку и установление сетевых соединений для устройств из списка (в том числе обеспечивает взаимодействие по UDP с абонентами из сети 1 и сети 2) и выполняет следующие действия:

- создает объекты классов работы с UDP сокетами;
- создает объекты классов работы с RAW сокетами;
- создает объекты классов работы с TCP сокетами.

5.6 Анализ восстановленного алгоритма работы

В данном разделе рассмотрены возможные последствия нештатного функционирования СПО АРМ 1.1 в процессе реализации основных функциональных задач.

Ниже приведены основные функциональные задачи СПО изделия АРМ 1.1, а также возможные последствия нештатного функционирования СПО при реализации данных функциональных задач.

По результатам восстановления алгоритма работы функциональной задачи «Инициализация ресурсов СПО и установление сетевых соединений» был сделан вывод о том, что нештатное функционирование СПО АРМ 1.1 при выполнении данной функциональной задачи может привести к невозможности корректной загрузки СПО или организации сетевого взаимодействия по сети «Ethernet», что не является опасным событием.

По результатам восстановления алгоритма работы функциональной задачи «Формирование и передача КИ, НКИ» были сделаны следующие выводы:

- нештатное функционирование СПО АРМ 1.1 при обмене НКИ с абонентами из Сети 2 привести к ошибочному формированию сообщения,

содержащего КИ, в результате чего возможно попадание КИ на ТС из состава Сети 2, что является опасным последствием (S_{KI});

– нештатное функционирование СПО АРМ 1.1 при обмене КИ с абонентами из Сети 1 привести к ошибочному формированию сообщения, содержащего НКИ, в результате чего возможно попадание НКИ на ТС из состава Сети 1, что не является опасным последствием.

По результатам восстановления алгоритма работы функциональной задачи «Прием НКИ, КИ и вывод принятой информации на графический интерфейс» был сделан вывод о том, что нештатное функционирование СПО АРМ 1.1 при выполнении данной функциональной задачи может привести к невозможности корректного приема НКИ (КИ), что не является опасным последствием.

5.7 Схема восстановленного алгоритма работы

В результате пооператорного анализа исходных текстов модулей СПО изделия АРМ 1.1 восстановлен алгоритм их функционирования и определены основные функции программы, отклонения функционирования которых от штатного алгоритма могут привести к возникновению опасных последствий:

CsrPlexMQ::sendDataToDevice(), CsrPlexMQ::sendData(),
QsoftwareHub::sendData(), UDPReadThread::writeBlock(), ...,
QUdpSocket::writeDatagram().

Схема восстановленного алгоритма программы, описывающая инициализацию, прием, обработку, формирование и отправку команд управления приведена на рисунке 7.

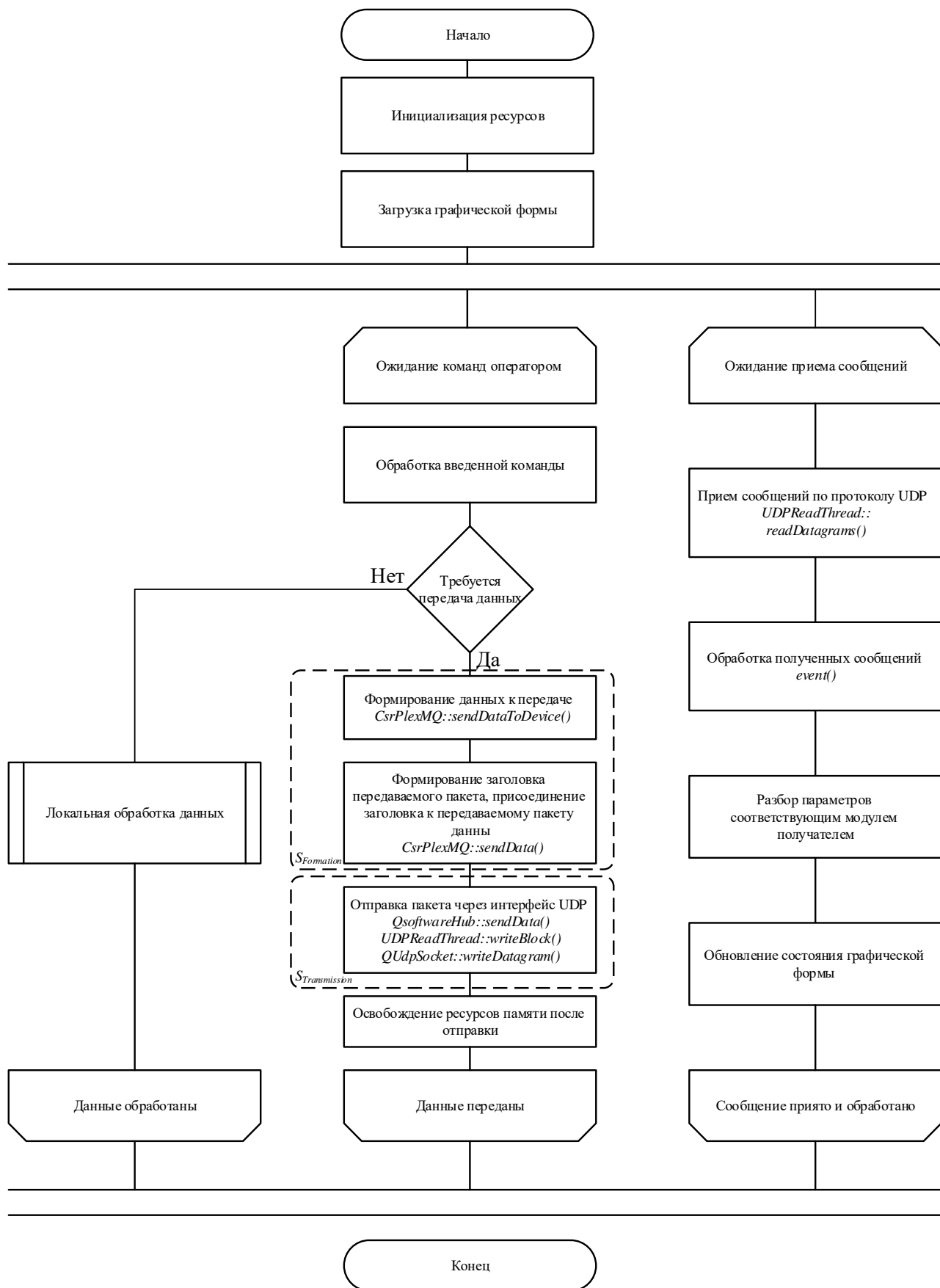


Рисунок 7 – Схема восстановленного алгоритма работы АРМ 1.1

5.8 Выводы по результатам анализа программного обеспечения

По результатам рассмотрения назначения, состава программного обеспечения изделия АРМ 1.1, принципов взаимодействия программ и их алгоритма работы, восстановленного по исходным текстам программы, сделаны следующие выводы:

- средств передачи управления программы в обход штатного алгоритма ее функционирования, отладочных программных компонентов, а также опасных программных конструкций языка программирования «C++» в СПО изделия АРМ 1.1 не обнаружено;

- при включении питания изделия АРМ 1.1 производится предпусковой контроль аппаратного обеспечения с помощью процедуры самотестирования POST и выполняется проверка целостности файловой системы средствами ОС СН «Astra Linux Special Edition»;

- СПО изделия АРМ 1.1 осуществляет обмен конфиденциальной и не конфиденциальной информацией, а также участвует в формировании, обработке и хранении данных видов информации;

- при взаимодействии с изделиями из ТКС СН обмен данными осуществляется формализованными сообщениями в соответствии с рассмотренными протоколами взаимодействия, а сообщения, несоответствующие формату протоколов, отбраковываются СПО;

- в СПО изделия АРМ 1.1 в результате нарушения штатного алгоритма функционирования возможно попадание КИ в Сеть 2 по каналу обмена информацией НКИ.

- Таким образом, установлено, что в изделии АРМ 1.1 возможно возникновение опасного события S_{KI} , в результате несовместного возникновения следующих факторов:

- отклонений от штатного алгоритма работы СПО при формировании пакетов с НКИ к ТС из состава Сети 2, в следующих функциях: *CsrPlexMQ::sendDataToDevice()* модуля *router.cpp*,...,

CsrPlexMQ::FormDataToSend модуля *router.cpp*. В результате чего, возможно формирование и дальнейшая штатная передача пакета данных к абонентам из Сети 2, содержащих КИ (S_{Form});

– отклонений от штатного алгоритма работы СПО при передаче пакетов с НКИ к ТС из состава Сети 2, в следующих функциях: *CsrPlexMQ::sendData()* модуля *router.cpp*, ..., *QsoftwareHub::sendData()* модуля *form.cpp*, *UDPReadThread::writeBlock()* модуля *Snd_Ethernet.cpp*, *QUdpSocket::writeDatagram()* модуля *Snd_Ethernet.cpp*. В результате чего, возможна передача пакета данных к абонентам из Сети 2, содержащих КИ (S_{Send}).

Опасное событие S_{KI} в этом случае может быть представлено выражением

$$S_{KI} = S_{Send} + S_{Form}. \quad (8)$$

6 Методика анализа программного обеспечения для определения возможности возникновения опасных событий в ТКС СН

В ходе данного дипломного проекта была разработана методика анализа программного обеспечения технических средств из состава ТКС СН. Целью данной методики является определение возможности возникновения опасных событий для телекоммуникационной системы за счет отклонений от штатного алгоритма функционирования технических средств из состава ТКС СН.

Как показано в разделе 5, методику анализа программного обеспечения ТС из состава ТКС СН можно условно разделить на восемь этапов:

- описание состава программного обеспечения ТС;
- описание процесса сборки и развертывания программного обеспечения;
- описание и анализ протоколов взаимодействия ТС в составе ТКС СН;
- выбор модулей из состава ПО для анализа;
- восстановление алгоритма программы;
- разработка схемы восстановленного алгоритма программы;
- формирование выводов по результатам анализа программного обеспечения.

В процессе выполнения первого этапа анализа ПО, согласно разработанной методике, необходимо составить перечень всего программного обеспечения, входящего в состав исследуемого ТС, а также описать функциональные задачи специального программного обеспечения и перечня его программных модулей. Результатами выполнения данного этапа являются следующие сведения:

- сформирован перечень программного обеспечения – встроенного, системного, функционального, специального входящего в состав ТС, с указанием десятичных номеров и сведений о сертификатах соответствия;
- краткое описание функциональных задач программного обеспечения, отражающее взаимодействие технического средства в составе ТКС СН;

- сформирован перечень программных модулей СПО с кратким описанием назначения этих модулей.

В процессе выполнения второго этапа анализа ПО, согласно разработанной методике, необходимо выполнить фиксацию версии исследуемого программного обеспечения, провести сборку и развертывание программного обеспечения. Для выполнения данного этапа анализа можно воспользоваться UML-диаграммой последовательности действий, выполняемых в процессе сборки и развертывания программного обеспечения ТКС СН (см.рисунок 8). Результатами выполнения данного этапа являются следующие сведения:

- сведения о версии СПО, языке программирования, среде разработки и выполнения СПО;
- сведения о программных и аппаратно-программных средствах, необходимых для сборки СПО;
- информацию о результатах сборки, а также о соответствии собранного СПО функционирующей в составе ТКС СН программе;
- сведения о средствах, методах, процедурах, используемых при развертывании СПО;
- сведения об ошибках компиляции (при наличии).

В процессе выполнения третьего этапа анализа ПО, согласно разработанной методике, необходимо описать и проанализировать протоколы взаимодействия ТС в составе телекоммуникационной системы. Результатами выполнения данного этапа являются следующие сведения:

- перечень ТС с которыми взаимодействует исследуемое техническое средство, с описанием физической среды сопряжения и механизмов обмена данными;
- описание формата информационных сообщений, с указанием назначения каждого поля и перечня значений, которые могут содержаться в этих полях;

– информацию о наличии (отсутствии) в полях сообщений обмена значений, которые могут приводить к возникновению опасных событий, определенных для ТКС СН.

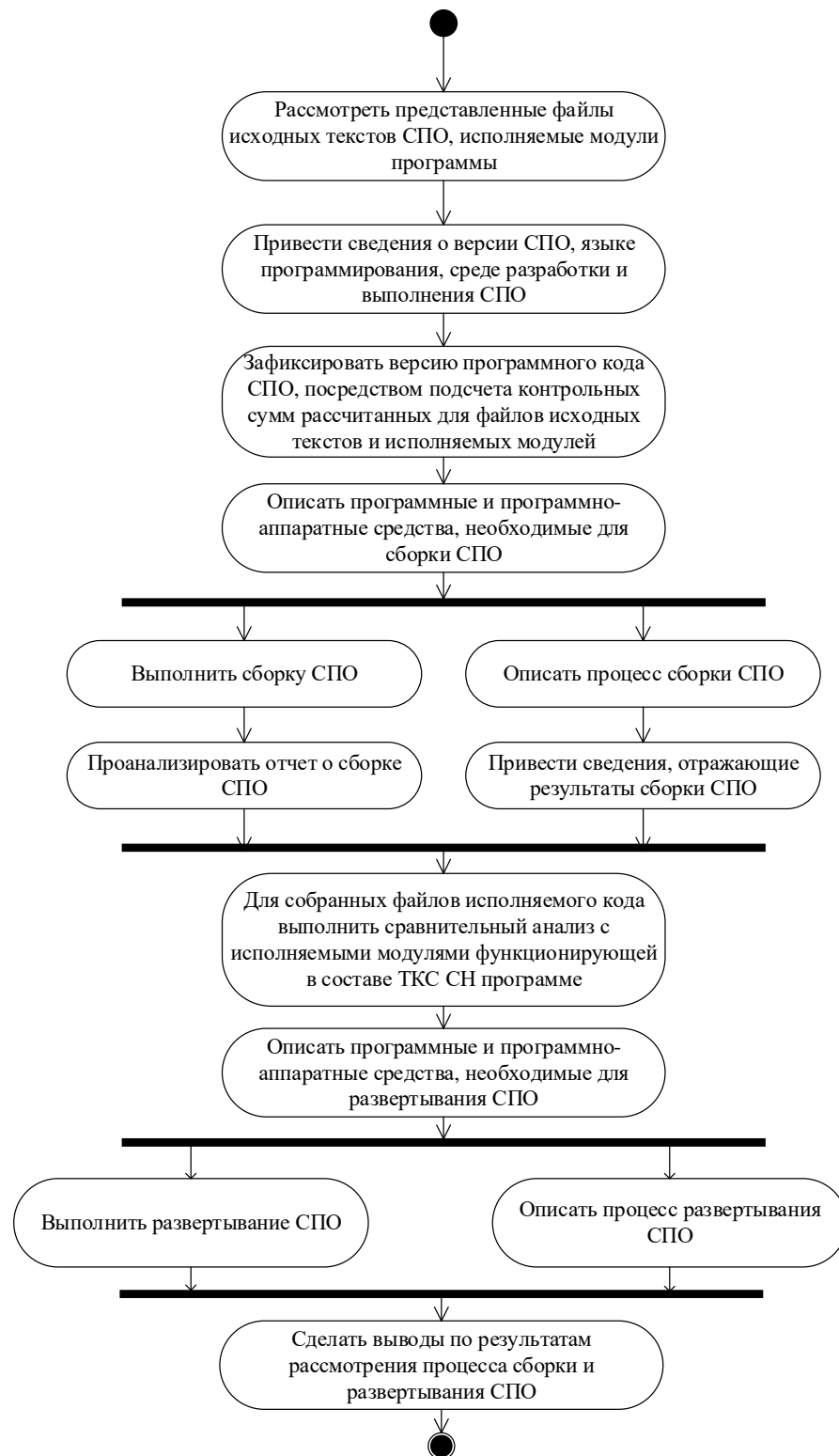


Рисунок 8 – UML-диаграмма последовательности действий, выполняемых в процессе сборки и развертывания программного обеспечения

В процессе выполнения четвертого этапа анализа ПО, согласно разработанной методике, необходимо описать принципы работы, тракты прохождения информации, и провести анализ взаимодействия функциональных компонент (подпрограмм) в ТС. Результатами выполнения данного этапа являются следующие сведения:

- описание принципа работы исследуемого ТС, начиная с включения питания и заканчивая переходом в штатный режим работы;
- описание принципов работы исследуемого ТС в режиме работы СПО с указанием перечня ТС, с которыми оно взаимодействует;
- разработанная схема взаимодействия программ СПО. Схема взаимодействия программ должна содержать все основные программные компоненты и их взаимосвязи, отражающие прохождение информации различного типа (конфиденциальной, не конфиденциальной, служебной) в исследуемом ТС.
- описание схемы взаимодействия программ с указанием используемых модулей и основных функциональных задач (прием, обработка, формирование и передача сообщений);
- перечень модулей, выбранных по результатам анализа схемы взаимодействия подпрограмм для восстановления алгоритма работы программы, путем пооператорного анализа этих модулей.

На пятом этапе анализа программного обеспечения, согласно разработанной методике, необходимо восстановить алгоритм работы программы путем пооператорного анализа текстов (исходного кода) программных модулей, выбранных в результате выполнения предыдущего этапа анализа. Для выполнения данного этапа анализа можно воспользоваться UML-диаграммой последовательности действий, восстановления алгоритма программы (см. рисунок 9). Результатами выполнения данного этапа являются следующие сведения:

- перечень основных механизмов взаимодействия программных компонент;

- описание программного модуля, содержащего точку входа в программу, описание основной функции программы и разработанный псевдокод этой функции;

- перечень основных функциональных задач, реализованных в СПО ТС;

- описание восстановленного алгоритма работы основных функциональных задач СПО, с указанием функций, участвующих в процессе выполнения основной ветки алгоритма и их описания. Разработанная схема (граф) вызовов функций подзадачи;

На шестом этапе анализа программного обеспечения, согласно разработанной методике, необходимо провести анализ восстановленного алгоритма работы на предмет определения возможных последствий в результате отклонений от штатного алгоритма в процессе выполнения функциональных задач СПО. Результатом выполнения данного этапа является перечень основных функциональных задач с указанием худших последствий отклонения от штатного алгоритма в процессе решения этих задач

На седьмом этапе анализа программного обеспечения, согласно разработанной методике, необходимо разработать схему восстановленного на предыдущем этапе алгоритма работы программы ТС. Результатом выполнения данного этапа является схема восстановленного алгоритма работы выбранных модулей программы, с указанием на ней критичных, приводящих к возникновению опасных событий подпрограмм.

На восьмом этапе анализа программного обеспечения, согласно разработанной методике, необходимо сделать выводы по результатам анализа программного обеспечения. В выводах необходимо отразить информацию (при наличии) о выявленных в процессе анализа ПО опасных программных конструкциях, ошибочно реализованных протоколах информационно-логического взаимодействия, об ошибках совместимости ПО и др. ошибок ПО,

обнаруженных при пооператорном анализе, а также при анализе с использованием средств статического анализа исходного кода. В результате выполнения данного этапа необходимо определить возможность (невозможность) возникновения опасных для ТКС СН событий, в результате отклонения ТС от штатного режима функционирования.

Для наглядного представления описанной методики была разработана диаграмма последовательности действий анализа программного обеспечения ТС из состава ТКС СН (см.рисунок 10).

Результатом анализа программного обеспечения по разработанной методике является перечень опасных событий для ТКС СН, которые могут возникнуть в результате отклонения от штатного алгоритма функционирования исследуемого технического средства.

Результаты анализа программного обеспечения по разработанной методике можно использовать для уточнения вероятности возникновения опасных событий для ТКС СН за счет неисправностей (сбоев) исследуемого ТС. На основании результатов анализа программного обеспечения, могут быть сформулированы рекомендации по доработке программно-аппаратного обеспечения ТС в целях снижения вероятности возникновения опасных событий для ТКС СН.

Таким образом, можно сделать вывод о том, что результаты разработанной методики анализа программного обеспечения для определения возможности возникновения опасных событий могут быть применены при анализе ТКС СН на соответствие требованиям информационной безопасности.

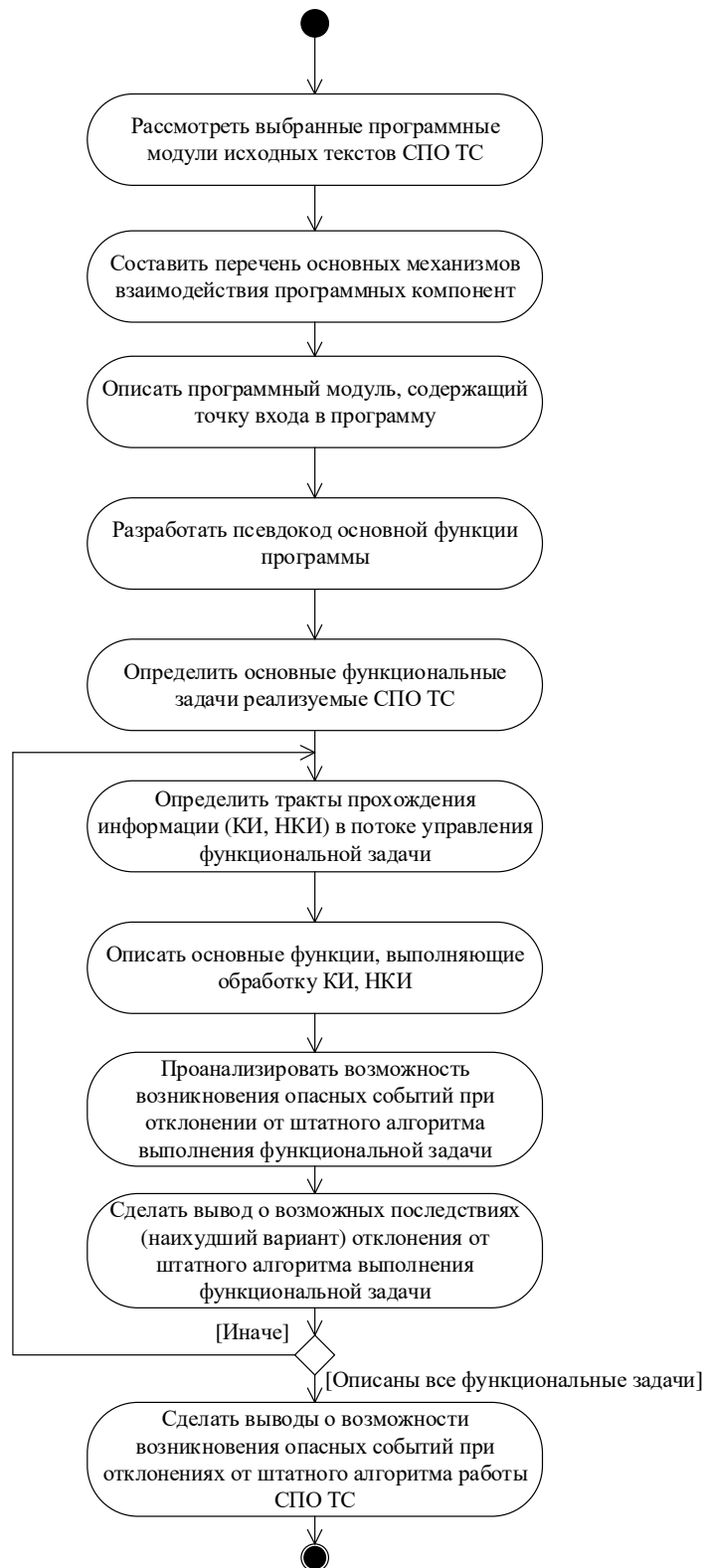


Рисунок 9 – UML-диаграмма последовательности действий при восстановлении алгоритма ПО

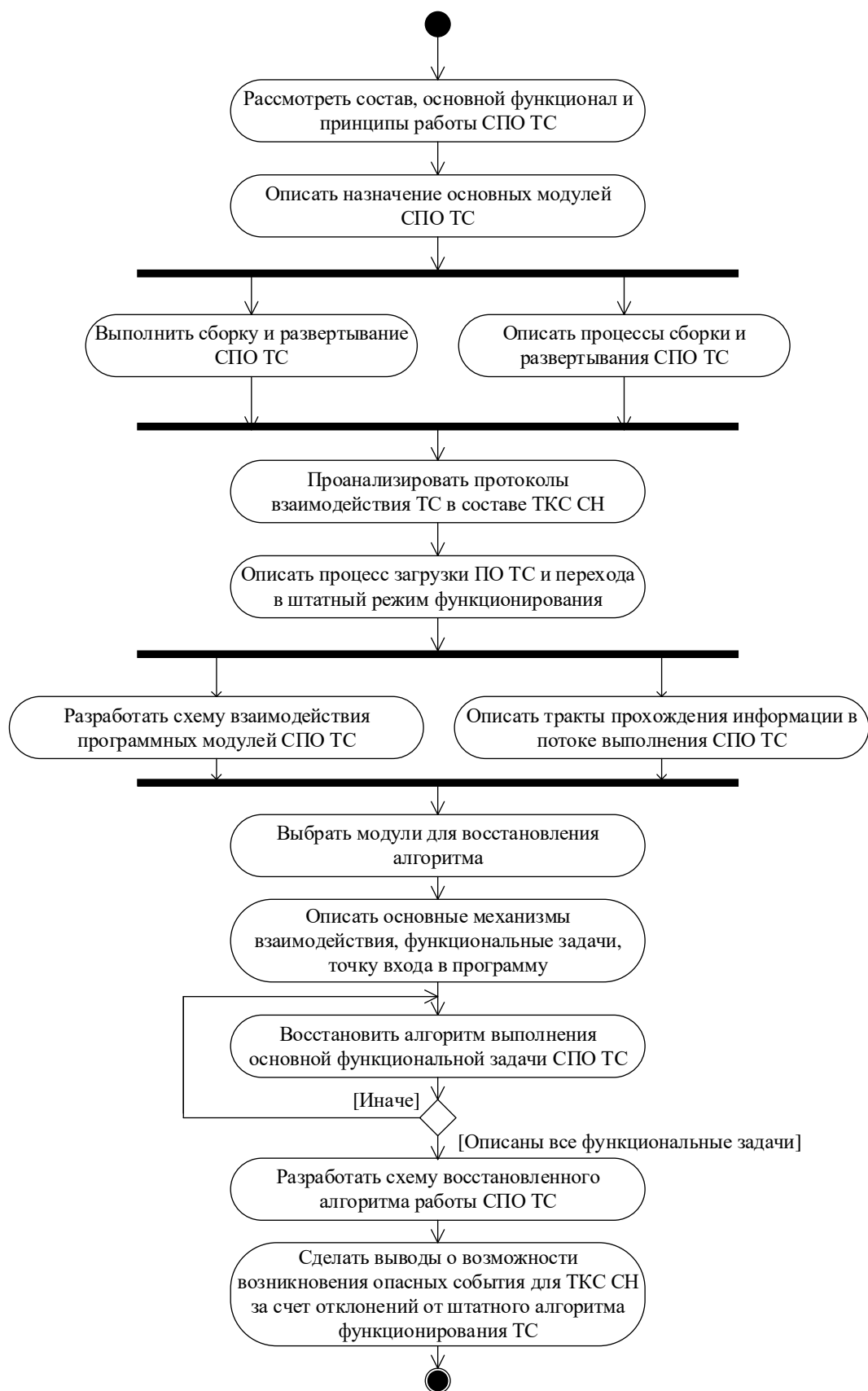


Рисунок 10 – UML-диаграмма последовательности действий при анализе программного обеспечения

ЗАКЛЮЧЕНИЕ

В ходе выполнения дипломного проекта была определена необходимость анализа программного обеспечения для определения возможности возникновения опасных событий в ТКС СН за счет неисправностей (сбоев) в аппаратно-программном обеспечении ТС из ее состава.

В процессе работы была разработана типовая структура, принципы и алгоритмы функционирования ТКС СН, разработана модель угроз безопасности информации для этой ТКС СН, определены технические средства из состава ТКС СН, для которых необходимо провести анализ аппаратно-программного обеспечения с целью определения возможности возникновения опасных событий. Рассмотрен порядок анализа аппаратно-программного обеспечения для выбранных изделий, в результате которого определена возможность возникновения опасных событий для рассматриваемой ТКС СН.

В результате работы была разработана методика анализа программного обеспечения для определения возможности возникновения опасных событий в ТКС СН.

Техническое задание на выпускную квалификационную работу выполнено в полном объеме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 РД-680-88. Методические указания. Автоматизированные системы. Основные положения. – Москва, 1989.
- 2 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Москва: Стандартинформ, 2008.
- 3 Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ.
- 4 РД 21-02-2006. Типовая инструкция о защите информации в автоматизированных средствах центрального аппарата, территориальных органов и организаций федеральной службы по экологическому, технологическому и атомному надзору. – Москва, 2006.
- 5 Указ Президента РФ от 6 марта 1997 г. N 188. Об утверждении перечня сведений конфиденциального характера. – Москва, 1997.
- 6 Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. — МГТУ им. Н. Э. Баумана, 2002. — 306 с.
- 7 Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» ФСТЭК 1997 г.
- 8 Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» ФСТЭК 1992 г.
- 9 Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» ФСТЭК 1992 г.
- 10 Приказ ФСТЭК № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» 2013 г.
- 11 Руководящий документ «Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации.

Классификация по уровню контроля отсутствия недекларированных возможностей» Гостехкомиссия, 1999 г.

12 Методический документ «Методика определения угроз безопасности информации в информационных системах» ФСТЭК 2015 г.

13 Попова М.С., Карпов А.П. Применение теории графов при выявлении потенциальных угроз безопасности информации // Проблемы современной науки и образования 2016. № 35 (77) С. 50-52.

14 Cisco Catalyst 4948E and 4948E-F Ethernet Switches Data Sheet. [Электронный ресурс]. URL: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4948e-ethernet-switch/data_sheet_c78-598933.html (дата обращения: 28.12.2016 г.).

15 Карпов А.П., Попова М.С. Влияние программного обеспечения на надежность информационной системы // Научно-практический электронный журнал Аллея Науки 2016. № 4 (401) С. 312-318.

Приложение А

Протокол проверки ВКР на оригинальность