

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 100502 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНЫЙ ПРОЕКТ

на тему

МЕТОДИКА ВЫЯВЛЕНИЯ ПОТЕНЦИАЛЬНЫХ КАНАЛОВ УТЕЧКИ
ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ, ВОЗНИКАЮЩИХ В РЕЗУЛЬТАТЕ
СБОЕВ И НЕИСПРАВНОСТЕЙ ТЕХНИЧЕСКИХ СРЕДСТВ

Студент Попова Марина Сергеевна

Руководитель Боровиков А.Ю.

Нормоконтролёр Фатеев А.Г.

Рецензент Давыдов Д.В.

Работа допущена к защите (протокол заседания кафедры от 12.01.17 № 6)

Заведующий кафедрой С.Л. Зефирова

Работа защищена с отметкой _____ (протокол заседания ГЭК

от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2017

Проверено Ю.Г. Галлов
С.Л. Зефирова

РЕФЕРАТ

Отчет 78 с., 14 рис., 23 табл., 17 источников, 1 прил.

КАНАЛ УТЕЧКИ ИНФОРМАЦИИ, НАДЁЖНОСТЬ, СХЕМА ИНФОРМАЦИОННЫХ ПОТОКОВ, ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ, ТРАКТЫ ПРОХОЖДЕНИЯ ИНФОРМАЦИИ

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

Целью дипломного проекта является разработка методики выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств.

В процессе работы была разработана модель угроз безопасности информации ТКС СН и определена актуальность угрозы утечки информации в результате сбоев и неисправностей технических средств. Для чего была рассмотрена архитектура и принципы работы ТКС СН, разработана и проанализирована схема информационных потоков ТКС СН, по результатам чего были выявлены каналы утечки информации, возникающие за счёт неисправностей (сбоев) технических средств, а также получены значения вероятности их возникновения.

В результате работы была разработана методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих за счёт сбоев и неисправностей технических средств.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
УДК 004.056
Политехнический институт

УТВЕРЖДАЮ

Факультет приборостроения,
информационных технологий и
электроники
Выпускающая кафедра:
Информационная безопасность систем
и технологий
Учебная группа 11ПТ1

Зав. кафедрой ИБСТ
к.т.н., доцент С.Л. Зефилов
«13» 10 2016 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ
РАБОТУ**

студента группы 11ПТ1 Поповой Марины Сергеевны

Специальность 100502 – Информационная безопасность
телекоммуникационных систем

Тема дипломного проекта:

Методика выявления потенциальных каналов утечки информации в
телекоммуникационных системах специального назначения, возникающих
в результате сбоев и неисправностей технических средств

Руководитель ВКР

начальник группы 1АО ПФ ФГУП «НТЦ «Атлас» А.Ю. Боровиков

Нормоконтролер

к.т.н., доцент кафедры ИБСТ

А.Г. Фатеев

1 Цели и задачи ВКР

Цель работы – разработать методику выявления потенциальных каналов утечки информации в телекоммуникационных системах специального назначения (ТКС СН), возникающих в результате сбоев и неисправностей технических средств.

Методика предназначена для выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, и может быть применена при анализе ТКС СН на соответствие требованиям информационной безопасности.

2 Тактико – технические требования к выполнению ВКР

Методика включает в себя:

- порядок описания архитектуры ТКС СН;
- порядок описания принципов работы ТКС СН;
- порядок выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств.

Технические требования:

- должна быть разработана типовая архитектура ТКС СН, включающая в себя структуру ТКС СН и описание технических средств (ТС), входящих в состав ТКС СН;
- должны быть описаны принципы работы ТКС СН и алгоритмы функционирования технических средств из ее состава;
- должна быть разработана схема информационных потоков ТКС СН и определен перечень категорий информационных потоков ТКС СН;
- должны быть выявлены потенциальные каналы утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств с применением графов (матриц) представления схемы информационных потоков.

В ВКР должны быть рассмотрены следующие вопросы:

- модель угроз и модель нарушителя ТКС СН;



- типовая архитектура ТКС СН;
- принципы и алгоритмы работы ТКС СН;
- потенциальные каналы утечки информации в ТКС СН, возникающие в результате сбоев и неисправностей технических средств;
- анализ технических средств на предмет возникновения в них сбоев и неисправностей, приводящих к утечке информации;
- методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- структура ТКС СН – 1 л., ф. А1 (плакат);
- схема информационных потоков ТКС СН – 1 л., ф. А1 (плакат);
- матричное представление схемы информационных потоков – 1 л., ф. А1 (плакат);
- дерево событий, отображающее возможные каналы передачи защищаемой информации – 1 л., ф. А1 (плакат);
- UML – диаграмма последовательности действий выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств – 1 л., ф. А1 (плакат);
- UML – диаграмма последовательности действий расчета вероятности возникновения каналов утечки защищаемой информации, возникающих в результате сбоев и неисправностей технических средств – 1 л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № ____ от «__» ____ 2016 г.

Дата выдачи задания « 26 » августа 2016 г.



Время дипломного проектирования с 10 октября 2016 г. по 15 января
2017 г.

Задание к исполнению принял « 26 » августа 2016 г.

Исполнитель ВКР _____ Попова М.С.



СОДЕРЖАНИЕ

Введение.....	11
1 Описание объекта исследования	13
2 Модель угроз безопасности информации и нарушителей ТКС СН	16
2.1 Общие сведения о модели угроз безопасности информации и нарушителей ТКС СН.....	16
2.2 Описание ТКС СН и особенностей её функционирования	16
2.3 Идентификация источников угроз безопасности информации.....	19
2.3.1 Классификация источников угроз безопасности информации	19
2.3.2 Антропогенные источники угроз безопасности информации	19
2.3.3 Техногенные источники угроз безопасности информации	21
2.3.4 Стихийные источники угроз безопасности информации	21
2.4 Идентификация угроз безопасности информации	22
2.5 Оценка возможности реализации угроз безопасности информации	24
3 Описание архитектуры и принципов работы ТКС СН	30
4 Разработка и описание схемы информационных потоков.....	35
5 Выявление потенциальных каналов утечки информации в ТКС СН	40
6 Оценка вероятности возникновения потенциальных каналов утечки информации в ТКС СН	49
7 Методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств	68
Заключение	74
Список использованных источников	75
Приложение А Протокол проверки ВКР на оригинальность	Ошибка! Закладка не оп

ОПРЕДЕЛЕНИЯ

Информационная безопасность – состояние защищенности национальных интересов государства в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1].

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

Модель угроз безопасности информации - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [2].

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС [5].

Надёжность – 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 [9].

Безотказность – свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки [9].

Вероятность безотказной работы – вероятность того, что в пределах заданного времени отказ объекта не возникнет.

Интенсивность отказов – условная плотность вероятности возникновения отказа, которая соответствует номинальному электрическому режиму и нормальным (лабораторным) условиям эксплуатации [9].

Спецнадёжность — это способность объекта или средства выполнять задачи передачи, обработки и хранения информации в определённых условиях

функционирования без возникновения отказов, приводящих к утечке информации (спецотказов) [11].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
ЗИ	–	защита информации
ИБ	–	информационная безопасность
ИС	–	информационная система
ИТ	–	информационная технология
КИ	–	конфиденциальная информация
МСЭ	–	межсетевой экран
ОИ	–	общедоступная информация
ПО	–	программное обеспечение
ТКС	–	телекоммуникационная система
ТС	–	техническое средство
ТСК СН	–	телекоммуникационная система специального назначения
УБИ	–	угроза безопасности информации

ВВЕДЕНИЕ

Интенсивное развитие современных информационных ресурсов и технологий в различных сферах жизни общества оказывает активное влияние на состояние безопасности государства, одной из составляющих которой является обеспечение информационной безопасности.

В доктрине информационной безопасности Российской Федерации под информационной безопасностью понимается состояние защищенности национальных интересов государства в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1].

Основной составляющей информационной безопасности является защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [2].

Другими словами, защита информации представляет собой комплекс мероприятий, направленных на обеспечение целостности, доступности и конфиденциальности информационных ресурсов, который включает в себя анализ возможных угроз безопасности информации и их источников.

В национальном стандарте РФ ГОСТ Р ИСО/МЭК 27005-2010 [3] определено три вида происхождения угроз информационной безопасности:

- умышленное (все умышленные действия, направленные на информационные активы);
- случайное (действия персонала, которые могут случайно нанести ущерб информационным активам);
- природное (угрозы, не основанные на действиях персонала или злоумышленника).

При анализе возможных угроз безопасности информации и их источников большое внимание уделяется угрозам умышленного и случайного происхождения (антропогенные источники угроз), а угрозы природного происхождения, связанные со сбоями и неисправностями технических средств,

чаще всего рассматриваются только с точки зрения обеспечения целостности и доступности обрабатываемой информации. Однако технические сбои и неисправности могут приводить не только к нарушению целостности и доступности информации, но и к нарушению её конфиденциальности. В связи с этим, при анализе информационной системы необходимо уделять особое внимание выявлению угроз нарушения конфиденциальности информации, возникающих в результате сбоев и неисправностей технических средств.

В рамках дипломного проекта была разработана методика выявления потенциальных каналов утечки информации в телекоммуникационных системах специального назначения, возникающих в результате сбоев и неисправностей технических средств, основанная на анализе схем информационных потоков.

1 Описание объекта исследования

Телекоммуникационные системы специального назначения (ТКС СН) представляют собой комплекс технических средств (ТС), обеспечивающих передачу информации на любые расстояния. Термин «специальное назначение» означает предназначение телекоммуникационной системы (ТКС) исключительно для выделенной группы должностных лиц с использованием гарантированных мер обеспечения информационной безопасности.

К ТКС СН предъявляется множество требований по защите информации (ЗИ), одним из которых является конфиденциальность хранимой, принимаемой, обрабатываемой и передаваемой информации, обеспечиваемая с использованием средств защиты информации, а также комплекса организационных мер защиты информации.

В качестве объекта исследования в рамках дипломного проекта была выбрана ТКС СН, предназначенная для обработки информации различных уровней конфиденциальности и её обмена между сегментами сети с использованием межсетевого экрана.

Условно данную ТКС СН можно рассматривать как систему, состоящую из трёх уровней:

- объекты, обрабатывающие конфиденциальную информацию (объекты высокого уровня);
- средства защиты информации (МСЭ);
- объекты, обрабатывающие общедоступную информацию (объекты низкого уровня).

Условная схема рассматриваемой ТКС СН представлена на рисунке 1.

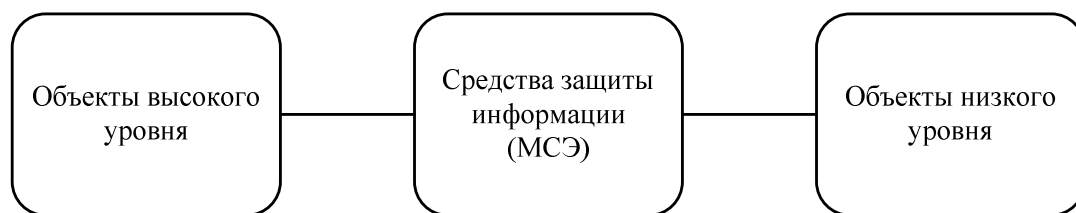


Рисунок 1 – Условная схема ТКС СН

В соответствии с правилами информационной безопасности (мандатной политикой безопасности) любые информационные потоки от объектов низкого уровня к объектам высокого уровня разрешены, а информационные потоки от объектов высокого уровня к объектам низкого уровня запрещены.

ФСТЭК для реализации данных правил разрешает в качестве средства защиты информации использовать межсетевой экран, который располагается между объектами высокого и низкого уровня и в соответствии со списком правил фильтрации разрешает или запрещает передачу информации от одних объектов к другим. При этом в ТКС СН должны быть выполнены требования руководящих документов в соответствии с классом защищённости технических средств [5, 13, 14].

Однако определенные в руководящих документах классы защищённости определяют только набор механизмов защиты, которые должны быть реализованы, но не оценивают качество исполнения аппаратного обеспечения самих технических средств и возможные изменения условий их функционирования.

Например, межсетевой экран, обеспечивающий фильтрацию информационных потоков в ТКС СН, выполнен в виде аппаратно-программного комплекса, надёжное функционирование которого оказывает непосредственное влияние на процесс фильтрации информационных потоков, и любой его кратковременный сбой может привести к нарушению штатного алгоритма работы межсетевого экрана, и, как следствие, к утечке защищаемой информации.

В связи с этим, при построении ТКС СН важно уделять внимание не только выполнению требований руководящих документов, но и оценке качества исполнения и надёжности технических средств ТКС СН.

Именно поэтому в качестве объекта исследования была выбрана данная архитектура построения ТКС СН, на примере которой продемонстрирована возможность влияния сбоев (неисправностей) технических средств на возникновение угроз безопасности информации в ТКС СН и разработана

методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств.

2 Модель угроз безопасности информации и нарушителей ТКС СН

2.1 Общие сведения о модели угроз безопасности информации и нарушителей ТКС СН

Для оценки уровня защищенности системы и грамотного построения её системы защиты необходимо разработать модель угроз безопасности информации, которая является физическим, математическим, описательным представлением характеристик (свойств) угроз безопасности информации [2].

Модель угроз безопасности информации рассматриваемой ТКС СН была разработана на основе проекта методического документа ФСТЭК «Методика определения угроз безопасности в информационных системах», который определяет единый подход к разработке моделей угроз безопасности информации в государственных информационных системах. В соответствии с данным документом разработка модели угроз безопасности информации информационной системы включает в себя описание информационной системы, идентификацию угроз безопасности информации и их источников, а также оценку вероятности (возможности) реализации угроз безопасности информации [4].

2.2 Описание ТКС СН и особенностей её функционирования

Телекоммуникационная система специального назначения, структура которой представлена на рисунке 2, представляет собой комплекс технических средств, обеспечивающих обработку информации различного уровня конфиденциальности и её обмена между выделенными группами должностных лиц.

В состав ТКС СН входят следующие технические средства:

- автоматизированное рабочее место (АРМ) (8 шт.);
- управляемый коммутатор Ethernet HP2530-24G (3 шт.);
- аппаратно-программный МСЭ ALTELL NEO 200 (1 шт.).

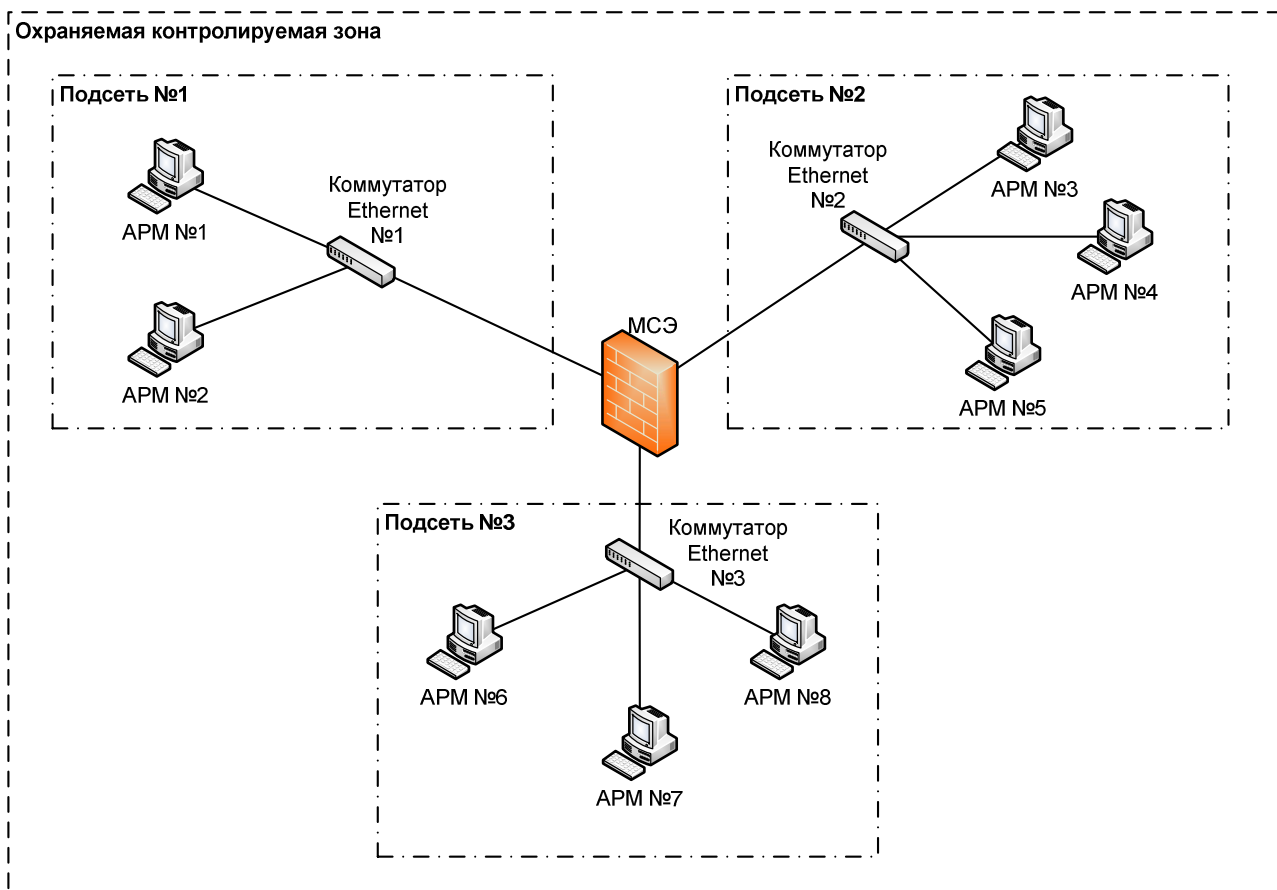


Рисунок 2 – Структура ТКС СН

АРМ реализовано на базе IBM-совместимого компьютера, в состав которого входят системный блок ЭВМ Р-III-2, клавиатура InduKey KG14237 и видеомонитор Advantech FPM-3151.

Управляемый коммутатор Ethernet HP2530-24G второго уровня имеет двадцать четыре сетевых интерфейса Ethernet 10/100/1000 Мбит/сек и обеспечивает коммутацию сетей ТКС СН.

Межсетевой экран ALTELL NEO 200 имеет семь сетевых интерфейсов Ethernet и обеспечивает фильтрацию информационных пакетов между подсетями, их идентификацию и аутентификацию при установлении соединения и регистрацию событий.

ТКС СН состоит из трёх подсетей, обрабатывающих информацию различного уровня конфиденциальности:

- подсеть №1 состоит из двух АРМ и предназначена для обработки конфиденциальной и общедоступной информации;

- подсеть №2 состоит из трёх АРМ и предназначена для обработки конфиденциальной информации;

- подсеть №3 состоит из трёх АРМ и принтера и предназначена для обработки общедоступной информации.

Взаимодействие подсетей ТКС СН осуществляется с помощью межсетевого экрана, который располагается между подсетями и в соответствии со списком правил фильтрации разрешает или запрещает передачу информации из одной части сети в другую. Взаимодействие подсетей в обход МСЭ запрещено.

Для разграничения доступа на АРМ №1 и №2, входящих в состав подсети №1, используются средства разграничения доступа, которые позволяют обеспечить защиту файлов, содержащих конфиденциальную информацию, от несанкционированных действий нарушителя.

Конфиденциальная информация может передаваться от пользователей АРМ №1 и №2 подсети №1 пользователям АРМ №3-№5 подсети №2 и обратно. Передача конфиденциальной информации пользователям АРМ №6-№8 подсети №3 запрещена.

Общедоступная информация может передаваться от пользователей АРМ №1 и №2 подсети №1 пользователям АРМ №6-№8 подсети №3 и обратно. Передача общедоступной информации пользователям АРМ №3-№5 подсети №2 запрещена.

Все технические средства из состава ТКС СН располагаются в одном здании в пределах контролируемой зоны, доступ в которую обеспечивается в соответствии с контрольно-пропускным режимом.

Доступ в помещения, где осуществляется обработка конфиденциальной информации, в рабочее и нерабочее время, а также в нештатных ситуациях осуществляется в соответствии с разработанным перечнем лиц. При этом осуществляется контроль за работой сотрудников, не допущенных к обработке конфиденциальной информации. В помещениях используются входные двери,

оснащенные замком и системой «ключ-карта». По окончании рабочего дня данные помещения опечатываются.

Доступ в помещение, где обрабатывается общедоступная информация, не ограничен.

ТКС СН не имеет подключений к другим информационным системам, сетям общего пользования и международного обмена.

2.3 Идентификация источников угроз безопасности информации

2.3.1 Классификация источников угроз безопасности информации

Источником угрозы безопасности информации является субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации [2].

Условно источники угроз безопасности информации можно разделить на три группы:

- антропогенные источники;
- техногенные источники;
- стихийные источники.

Далее рассмотрены все группы источников угроз безопасности информации с целью формирования предположений о типах источников угроз безопасности информации, актуальных в анализируемой ТКС СН.

2.3.2 Антропогенные источники угроз безопасности информации

К антропогенным источникам угроз безопасности информации относятся субъекты, который имеют санкционированный или несанкционированный доступ к ТКС СН.

Условно антропогенные источники угроз безопасности информации можно разделить на два типа:

- внешние нарушители – лица, не имеющие права доступа к ТКС СН, её техническим средствам и реализующие угрозы безопасности информации из-за границ ТКС СН;

– внутренние нарушители – лица, имеющие право постоянного или разового доступа к ТКС СН, ее отдельным техническим средствам.

Угрозы безопасности информации, реализуемые внешним нарушителем, были исключены из списка возможных угроз безопасности информации в связи с отсутствием подключений ТКС СН к внешним информационно-телекоммуникационным сетям.

Виды возможных внутренних нарушителей анализируемой ТКС СН были определены исходя из списка нарушителей, представленного в проекте методического документа ФСТЭК [4], с учетом структурно-функциональных характеристик ТКС СН и особенностей функционирования.

Возможности реализации угроз безопасности информации каждого вида нарушителя характеризуется его потенциалом, который определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования [4].

Список возможных для данной ТКС СН внутренних нарушителей с указанием их потенциала приведен в таблице 1.

Таблица 1 – Виды внутренних нарушителей

№ п/п	Вид внутреннего нарушителя	Потенциал внутреннего нарушителя
1	Лица, привлекаемые для установки, монтажа и иных видов работы	Базовый (низкий) потенциал
2	Лица, обеспечивающие функционирование и обслуживание ИС	Базовый (низкий) потенциал
3	Пользователи информационной системы	Повышенный (средний) потенциал
4	Администраторы ТКС СН и безопасности	Повышенный (средний) потенциал

Нарушители с базовым потенциалом имеют возможность получить из общедоступных источников информацию об уязвимостях ИС, а также о методах реализации угроз безопасности информации.

Нарушитель с повышенным потенциалом обладает возможностями нарушителей с базовым потенциалом, а также осведомлён о структурно-функциональных характеристиках ИС, её отдельных компонентах и применяемых мерах защиты информации.

С учетом решаемых ТКС СН целей и задач, видов обрабатываемой информации, а также степени возможных последствий (ущерба) от реализации угроз безопасности информации были определены возможные цели (мотивация) реализации внутренними нарушителями угроз безопасности информации в ТКС СН, к которым относятся:

- причинение ущерба путем злоупотребления полномочиями;
- причинение ущерба путем обмана;
- желание самореализации и подтверждение статуса;
- любопытство или месть;
- неквалифицированные или неосторожные действия;
- выявление уязвимостей с целью получения финансовой выгоды.

2.3.3 Техногенные источники угроз безопасности информации

Техногенные источники угроз безопасности информации связаны со сбоями и неисправностями технических средств и программного обеспечения.

Данные источники угроз обусловлены низким качеством технических и программных средств, отсутствием их резервирования, а также низким качеством обслуживания.

Техногенные источники угроз безопасности информации являются наименее прогнозируемыми и поэтому требуют особого внимания.

2.3.4 Стихийные источники угроз безопасности информации

К стихийным источникам угроз безопасности информации относятся природные явления, например, пожар, землетрясение, наводнение и др.

Предсказать и предотвратить данные события практически невозможно, не смотря на применении защитных мер. В связи с этим, стихийные источники угроз безопасности информации в рамках дипломного проекта не рассматриваются.

2.4 Идентификация угроз безопасности информации

Основой при идентификации угроз безопасности информации в ТКС СН являются следующие сведения:

- сведения об актуальных для ТКС СН источниках угроз безопасности информации;
- сведения о наличии уязвимостей, которые могут быть использованы при реализации угроз безопасности информации;
- способы реализации угроз безопасности информации;
- объекты информационной системы, на которые может быть направлена угроза безопасности информации;
- результат реализации угроз безопасности информации.

Таким образом, любая угроза безопасности информации должна описываться следующими параметрами: источник угрозы, уязвимость, способ реализации угрозы, объект воздействия и результат (последствия) от реализации угрозы [4].

Исходя из описания структурно-функциональных характеристик ТКС СН, особенностей её функционирования и идентифицированных источников угроз безопасности информации был составлен список наиболее вероятных угроз безопасности информации, который представлен в таблице 2.

В качестве исходных данных об угрозах безопасности информации был использован банк данных угроз безопасности информации, сформированный ФСТЭК России [6].

Таблица 2 – Перечень угроз безопасности информации ТКС СН

Идентификатор угрозы	Наименование угрозы	Описание угрозы	Источники угрозы	Уязвимость	Способ реализации угрозы	Объекты воздействия	Последствия от реализации угрозы
УБИ.067	Угроза неправомерного ознакомления с защищаемой информацией	Угроза заключается в возможности неправомерного случайного или преднамеренного ознакомления пользователя с информацией, которая для него не предназначена, и дальнейшего её использования для достижения своих целей.	Внутренний нарушитель с низким потенциалом (1) Сбои и неисправность ТС (2)	Отсутствие или уязвимости средств контроля доступа Ошибки в параметрах конфигурации средств контроля доступа Низкое качество ТС	Ознакомление с защищаемой информацией может быть осуществлено: - путём просмотра информации с экранов мониторов и отпечатанных документов; - путём подслушивания разговоров; - путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена.	Защищаемая информация Носители информации Объекты файловой системы	Нарушение конфиденциальности
УБИ.179	Угроза несанкционированной модификации защищаемой информации	Угроза заключается в возможности осуществления нарушителем несанкционированного изменения защищаемой информации	Внутренний нарушитель с низким потенциалом	Отсутствие или уязвимости средств проверки целостности Ошибки в параметрах конфигурации средств проверки целостности Низкое качество ТС	Модификация защищаемой информации может быть осуществлена путём осуществления деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём	Защищаемая информация Носители информации Объекты файловой системы	Нарушение целостности
УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного изменения параметров настройки средства защиты информации.	Внутренний нарушитель с низким потенциалом	Уязвимости мер разграничения доступа к конфигурационным файлам средств защиты информации	Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации	Средство защиты информации	Нарушение конфиденциальности, целостности и доступности

2.5 Оценка возможности реализации угроз безопасности информации

Вероятность реализации угрозы безопасности информации характеризует возможность реализации той или иной угрозы безопасности информации в данной ТКС СН.

Оценка вероятности (возможности) реализации угрозы безопасности информации определяется исходя из уровня проектной защищенности (Y_1) и потенциала нарушителя (Y_2).

Уровень проектной защищенности (Y_1) определяется проектными структурно-функциональными характеристиками ТКС СН, приведёнными в таблице 3.

Таблица 3 – Проектные структурно-функциональные характеристики ТКС СН

Структурно-функциональные характеристики ТКС СН, условия её эксплуатации	Уровень проектной защищенности (Y_1)		
	Высокий	Средний	Низкий
По структуре ТКС СН: локальная ИС		+	
По используемым информационным технологиям: суперкомпьютерные системы		+	
По архитектуре ТКС СН: системы на основе «тонкого клиента»	+		
По наличию взаимосвязей с иными ИС: невзаимодействующая с системами		+	
По наличию подключений к сетям связи общего пользования: неподключенная	+		
По размещению ТС: расположенные в пределах одной контролируемой зоны	+		
По режимам обработки информации: многопользовательская			+
По режимам разграничения прав доступа: с разграничением		+	

Продолжение таблицы 3

Структурно-функциональные характеристики ТКС СН, условия её эксплуатации	Уровень проектной защищенности (Y_1)		
	Высокий	Средний	Низкий
По режимам разделений функций по управлению ТКС СН: выделение рабочих мест для администрирования в отдельный домен		+	
По подходам к сегментированию ТКС СН: с сегментированием		+	

По результатам анализа проектных структурно-функциональных характеристик ТКС СН определено, что 30% характеристик ТКС СН соответствуют высокому уровню, 60% – среднему и 10% – низкому. В соответствии с проектом методического документа ФСТЭК [4] ТКС СН имеет средний уровень проектной защищённости, так как количество её характеристик, соответствующих низкому и среднему уровням, составляет не менее 90%. Таким образом, показатель уровня проектной защищённости (Y_1) соответствует среднему уровню.

Возможность реализации каждой угрозы безопасности информации определяется исходя из определенного ранее уровня проектной защищенности ТКС СН и потенциала нарушителя в соответствии с таблицей 4.

Таблица 4 – Правило определения возможности реализации УБИ

Потенциал нарушителя (Y_2)	Уровень проектной защищённости (Y_1)		
	Высокий	Средний	Низкий
Базовый (низкий)	Низкая	Средняя	Высокая
Базовый (повышенный)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

Возможность реализации угрозы неправомерного ознакомления с защищаемой информацией путём её просмотра с экранов мониторов и

отпечатанных документов и подслушивания разговоров (УБИ.067(1)) в соответствии со средним уровнем проектной защищенности и низким потенциалом нарушителя является средней. Однако для предотвращения реализации данной угрозы применяются следующие меры защиты:

- доступ в контролируемую зону ТКС СН обеспечивается в соответствии с контрольно-пропускным режимом;
- доступ в помещения в рабочее и нерабочее время, а также в нештатных ситуациях осуществляется в соответствии с разработанным перечнем лиц;
- для разграничения доступа в помещения, где осуществляется обработка конфиденциальной информации, используются входные двери, оснащенные замком и системой «ключ-карта» для обеспечения санкционированного прохода в помещения и закрытия дверей на замок;
- помещения, где осуществляется обработка конфиденциальной информации, опечатываются по окончании рабочего дня;
- осуществляется контроль за работой сотрудников, не допущенных к обработке КИ.

В связи с этим, возможность реализации данной угрозы ($Y_{\text{УБИ.067(1)}}$) снижена до низкого уровня.

Возможность реализации угрозы неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей технических средств (УБИ.067(2)) в соответствии с не может быть определена, так как данная методика ориентирована на определение и оценку антропогенных угроз безопасности информации. В связи с этим, возможность реализации данной угрозы ($Y_{\text{УБИ.067(2)}}$) условно принята высокой.

Возможность реализации угрозы несанкционированной модификации защищаемой информации (УБИ.179) в соответствии со средним уровнем проектной защищенности и низким потенциалом нарушителя является средней. Однако в ТКС СН применяются средства разграничения доступа пользователей

к информации, а также осуществляется ежесуточная проверка целостности носителей информации и объектов файловой системы, что позволяет снизить возможность реализации данной угрозы ($Y_{УБИ.179}$) до низкого уровня.

Возможность реализации угрозы несанкционированного изменения параметров настройки средств защиты информации (УБИ.185) в соответствии со средним уровнем проектной защищенности и низким потенциалом нарушителя является средней. Однако в ТКС СН управление средствами защиты информации предусмотрено с выделенного рабочего места, доступ к которому разрешён только администратору безопасности ТКС СН. Также в ТКС СН используются средства контроля целостности средств защиты информации. В связи с этим, возможность реализации данной угрозы ($Y_{УБИ.185}$) снижена до низкого уровня.

Затем было принято об актуальности угроз безопасности информации в рассматриваемой ТКС СН исходя из возможности её реализации ($Y_{УБИ.№}$) и степени возможного ущерба ($X_{УБИ.№}$) в соответствии с таблицей 5.

Таблица 5 – Правило определения актуальности УБИ

Возможность реализации УБИ ($Y_{УБИ.№}$)	Степень возможного ущерба ($X_{УБИ.№}$)		
	Высокий	Средний	Низкий
Низкая	Неактуальная	Неактуальная	Актуальная
Средняя	Неактуальная	Актуальная	Актуальная
Высокая	Актуальная	Актуальная	Актуальная

В связи с тем, что в результате реализации всех угроз безопасности информации возможны умеренные негативные последствия, степень возможного ущерба от реализации данных угроз равен среднему уровню.

В таблице 6 приведено обоснование актуальности всех рассматриваемых для ТКС СН угроз безопасности информации исходя из возможности их реализации и степени возможного ущерба.

Таблица 6 – Актуальность угроз безопасности информации ТКС СН

Угроза	Возможность реализации УБИ (Y _{УБИ.№})	Степень ущерба (X _{УБИ.№})	Актуальность угрозы
Угроза неправомерного ознакомления с защищаемой информацией путём её просмотра с экранов мониторов и отпечатанных документов и подслушивания разговоров (УБИ.067(1))	Низкая	Средняя	Неактуальная
Угроза неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена (УБИ.067(2))	Высокая	Средняя	Актуальная
Угроза несанкционированной модификации защищаемой информации (УБИ.179)	Низкая	Средняя	Неактуальная
Угроза несанкционированного изменения параметров настройки средств защиты информации (УБИ.185)	Низкая	Средняя	Неактуальная

Таким образом, в ТКС СН к актуальным угрозам безопасности информации относится угроза неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей ТС (УБИ.067(2)).

Актуальность данной угрозы может быть также определена с помощью анализа структуры и принципов работы ТКС СН с целью выявления всех каналов утечки информации, возникающих в результате сбоев и неисправностей ТС, и получения вероятностей их возникновения.

Далее рассмотрен, один из подходов выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей ТС, который состоит из четырёх этапов:

- а) описание архитектуры и принципов работы ТКС СН;
- б) разработка и описание схемы информационных потоков;
- в) выявление потенциальных каналов утечки информации в ТКС СН;
- г) оценка вероятности возникновения потенциальных каналов утечки информации в ТКС СН.

3 Описание архитектуры и принципов работы ТКС СН

На первом этапе выявления каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей ТС, необходимо рассмотреть структуру и принципы работы ТКС СН, а именно тракты прохождения информации.

Описание структуры ТКС СН и трактов прохождения информации производится на основе технической документации ТКС СН, к которой относятся руководство по эксплуатации, электрические схемы различных типов (структурная, функциональная, принципиальная и др.) и другие документы. Руководство по эксплуатации позволяет определить назначение (область применения), условия эксплуатации и технические характеристики ТКС СН, а также описывает состав и описание работы ТКС СН [7]. С помощью различных типов схем электрических определяется перечень технических средств ТКС СН, их назначение и взаимосвязи между ними, а также описываются протекающие в ТКС СН процессы [8].

Структура анализируемой ТКС СН и её описание приведены в модели угроз безопасности информации и нарушителей (см. подраздел 2.2).

На этапе описания архитектуры и принципов работы ТКС СН также необходимо привести краткое описание ТС, входящих в состав ТКС СН, для чего удобно использовать таблицу атрибутов ТС. Таблица атрибутов представляет собой матрицу, в которой столбец соответствует одному из ТС, строка – атрибуту ТС, а каждая клетка таблицы отражает значение определенного атрибута для определенного ТС.

Атрибут – свойство объекта, предназначенное для его идентификации, классификации или количественной характеристики. Другими словами, атрибут представляет собой характеристику (свойство) объекта. Выделяют ключевые и описательные атрибуты.

Ключевой атрибут – атрибут, который является уникальным и предназначен для идентификации каждого экземпляра сущности. Ключевые атрибуты обозначаются символом «#».

Описательные атрибуты – атрибуты, которые предназначены для описания и характеристики каждого экземпляра сущности. Выделяют обязательные и необязательные для заполнения описательные атрибуты, которые обозначаются символами «*» и «°» соответственно.

Список стандартных атрибутов ТС приведен в таблице 7.

Таблица 7 – Список стандартных атрибутов ТС

Атрибут	Описание атрибута
#Децимальный (идентификационный) номер	Децимальный (идентификационный) номер ТС является уникальным признаком ТС, который указывается в соответствии с технической документацией.
*Наименование	Полное наименование ТС является обязательным описательным атрибутом и указывается в соответствии с технической документацией.
*Условное обозначение	Условное обозначение ТС является обязательным описательным атрибутом и указывается для обозначения ТС в дальнейшем.
*Тип	Тип изделия является обязательным описательным атрибутом и может принимать определенные значения: - «каналообразующие средства»; - «коммутационные средства»; - «средства защиты информации»; - «оконечная аппаратура».
°Функции	Описание функций ТС является необязательным описательным атрибутом. Данный атрибут предназначен для описания назначения (роли) ТС в рамках анализируемой системы.
°Реализация	Реализация ТС является необязательным описательным атрибутом и может принимать определенные значения: - «аппаратная»; - «аппаратно-программная». Данный атрибут определяет перечень работ, необходимых для оценки возможности возникновения каналов утечки информации.
°Состав	Описание состава ТС является необязательным описательным атрибутом. Данный атрибут может быть использован в дальнейшем при оценке возможности возникновения каналов утечки информации.

В таблице 8 приведено описание ТС, входящих в состав анализируемой ТКС СН.

Таблица 8 – Описание ТС, входящих в состав ТКС СН

Атрибут	Технические средства											
	АРМ №1	АРМ №2	АРМ №3	АРМ №4	АРМ №5	АРМ №6	АРМ №7	АРМ №8	Коммутатор Ethernet №1	Коммутатор Ethernet №2	Коммутатор Ethernet №3	МСЭ
#Децимальный (идентификационный) номер	АБВГ.112345.001								КМТР.111111.112			ALTELL NEO 200
*Наименование	Автоматизированное рабочее место											ALTELL NEO 200
*Условное обозначение	АРМ №1	АРМ №2	АРМ №3	АРМ №4	АРМ №5	АРМ №6	АРМ №7	АРМ №8	Eth№1	Eth№2	Eth№3	МСЭ
*Тип	Оконечная аппаратура								Коммутационные средства			Средства защиты информации
°Функции	1. ТС предназначено для обработки конфиденциальной и общедоступной информации; 2. ТС осуществляет обмен конфиденциальной информацией с подсетью №2. 3. ТС осуществляет обмен общедоступной информацией с подсетью №3.	1. ТС предназначено для обработки конфиденциальной информации; 2. ТС осуществляет обмен конфиденциальной информацией с подсетью №1.		1. ТС предназначено для обработки общедоступной информации; 2. ТС осуществляет обмен общедоступной информацией с подсетью №1.				Коммутатор Ethernet №1 предназначен для объединения АРМ №1 и №2 в локальную вычислительную сеть.	Коммутатор Ethernet №2 предназначен для объединения АРМ №3-№5 в локальную вычислительную сеть.	Коммутатор Ethernet №3 предназначен для объединения АРМ №6-№8 в локальную вычислительную сеть.	1. МСЭ осуществляет фильтрацию информационных пакетов между подсетями. 2. МСЭ осуществляет идентификацию и аутентификацию фильтруемых пакетов при установлении соединения. 3. МСЭ осуществляет проверку целостности системы. 5. МСЭ осуществляет восстановление системы при нарушении работы её компонентов или нарушении целостности. 6. МСЭ осуществляет регистрацию событий.	
°Реализация	Аппаратно-программная								Аппаратно-программная			Аппаратная

Также для понимания принципов работы ТКС СН необходимо описать тракты прохождения информации, которые представляют собой совокупность технического оборудования и линий связи, предназначенных для формирования каналов передачи информации.

При описании трактов прохождения информации необходимо последовательно указать источник информации, промежуточную аппаратуру и получателя информации, а также вид передаваемой информации.

Как отмечено в модели угроз безопасности информации (см. раздел 2), в рассматриваемой ТКС СН обрабатывается информация двух видов: конфиденциальная (КИ) и общедоступная (ОИ).

Конфиденциальная информация может передаваться от пользователей АРМ №1 и №2 подсети №1 пользователям АРМ №3 - №5 подсети №2 и обратно. Передача конфиденциальной информации пользователям АРМ №6 - №8 подсети №3 запрещена.

Таким образом, источниками КИ в ТКС СН являются АРМ №1 – АРМ №5, принадлежавшие подсетям №1 и №2. Передача КИ осуществляется через коммутаторы Ethernet и МСЭ.

Тракты прохождения КИ в ТКС СН приведены ниже:

- АРМ №1 ↔ Eth №1 ↔ МСЭ ↔ Eth №2 ↔ АРМ №3;
- АРМ №2 ↔ Eth №1 ↔ МСЭ ↔ Eth №2 ↔ АРМ №3;
- АРМ №1 ↔ Eth №1 ↔ МСЭ ↔ Eth №2 ↔ АРМ №4;
- АРМ №2 ↔ Eth №1 ↔ МСЭ ↔ Eth №2 ↔ АРМ №4;
- АРМ №1 ↔ Eth №1 ↔ МСЭ ↔ Eth №2 ↔ АРМ №5;
- АРМ №2 ↔ Eth №1 ↔ МСЭ ↔ Eth №2 ↔ АРМ №5.

В свою очередь, общедоступная информация может передаваться от пользователей АРМ №1 и №2 подсети №1 пользователям АРМ №6 - №8 подсети №3 и обратно. Передача общедоступной информации пользователям АРМ №3 - №5 подсети №2 запрещена.

Таким образом, источниками ОИ в ТКС СН являются АРМ №1, АРМ №2, АРМ 6 – АРМ №8, принадлежавшие подсетям №1 и №3. Передача ОИ также осуществляется через коммутаторы Ethernet и МСЭ.

Тракты прохождения ОИ в ТКС СН приведены ниже:

- АРМ №1 ↔ Eth №1 ↔ МСЭ ↔ Eth №3 ↔ АРМ №6;
- АРМ №2 ↔ Eth №1 ↔ МСЭ ↔ Eth №3 ↔ АРМ №6;
- АРМ №1 ↔ Eth №1 ↔ МСЭ ↔ Eth №3 ↔ АРМ №7;
- АРМ №2 ↔ Eth №1 ↔ МСЭ ↔ Eth №3 ↔ АРМ №7;
- АРМ №1 ↔ Eth №1 ↔ МСЭ ↔ Eth №3 ↔ АРМ №8;
- АРМ №2 ↔ Eth №1 ↔ МСЭ ↔ Eth №3 ↔ АРМ №8.

По результатам выполнения первого этапа выявления каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей ТС, была описана архитектура ТСК СН, входящие в её состав ТС, а также тракты прохождения информации. Данная информация является основой для разработки схемы информационных потоков и выявления потенциальных каналов утечки, возникающих в результате сбоев и неисправностей ТС.

4 Разработка и описание схемы информационных потоков

На втором этапе выявления каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей ТС, должна быть разработана схема информационных потоков и приведено описание трактов прохождения информации на её основе.

Схема информационных потоков представляет собой схему, на которой отображаются ТС, входящие в состав ТКС СН и осуществляющие обработку информации, а также потоки информации между ними. При этом любой информационный поток схемы характеризуется следующими параметрами: источник и получатель информации, уровень конфиденциальности передаваемой информации, а также направление движения информационного потока.

Для разработки схемы информационных потоков и её описания удобно использовать теорию графов. Практическая ценность применения теории графов при описании и анализе схем информационных потоков информационной системы с целью выявления потенциальных угроз безопасности информации и построения эффективной системы защиты отмечена в статье «Применение теории графов при выявлении потенциальных угроз безопасности информации» научно-методического журнала «Проблемы современной науки и образования» [15].

Итак, ТКС СН представляет собой ориентированный граф, который состоит из конечного множества вершин, соответствующих ТС системы, и рёбер, отражающих информационные потоки между ними. При этом рёбра должны быть пронумерованы и окрашены в разные цвета в зависимости от вида передаваемой информации. Маршруты графа (чередующаяся последовательность вершин и рёбер) представляют собой тракты прохождения информации, описанные ранее.

Схема информационных потоков анализируемой ТКС СН приведена на рисунке 3.

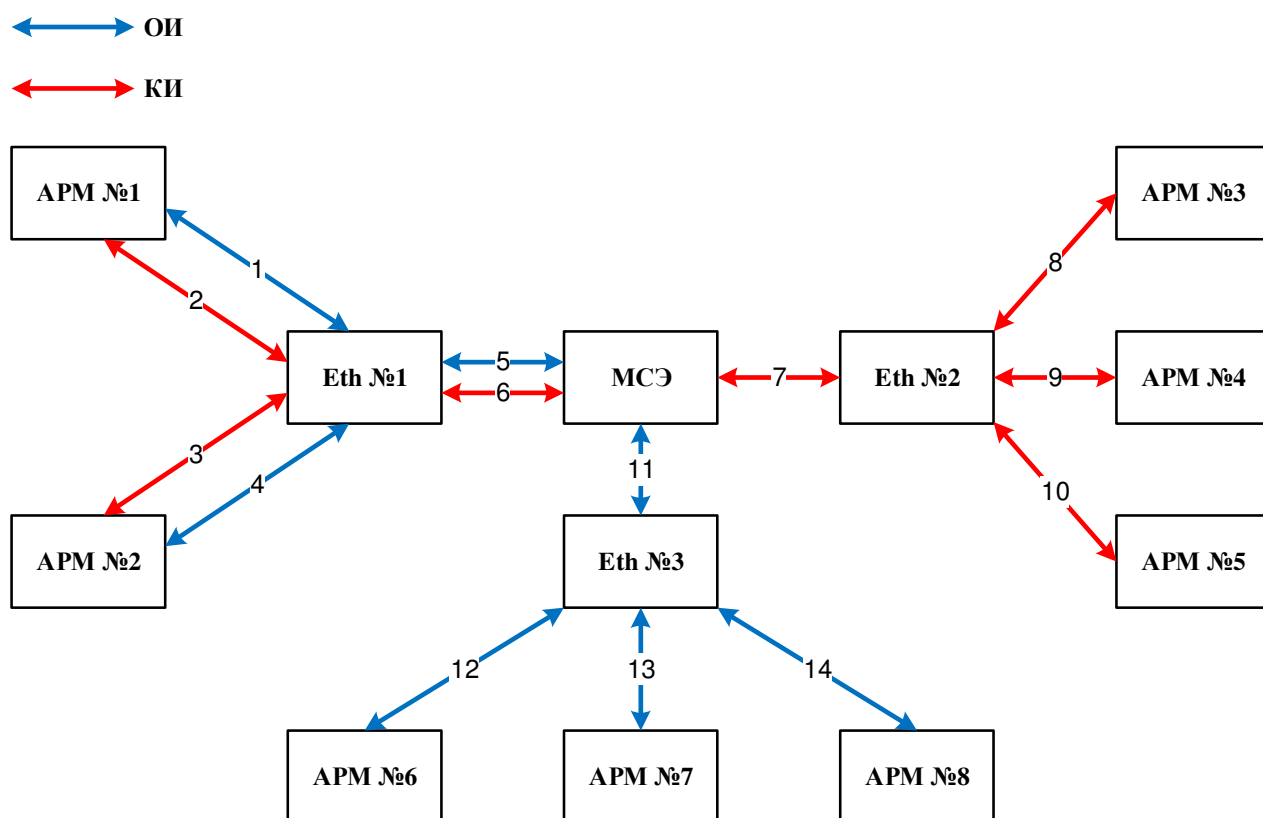


Рисунок 3 – Схема информационных потоков ТКС СН

Штатные тракты прохождения информации, описанные в разделе 3, в соответствии со схемой информационных потоков примут следующий вид:

а) штатные тракты прохождения КИ:

- 1) $APM\ №1 \xleftarrow{2} Eth\ №1 \xleftarrow{6} MCЭ \xleftarrow{7} Eth\ №2 \xleftarrow{8} APM\ №3$;
- 2) $APM\ №2 \xleftarrow{3} Eth\ №1 \xleftarrow{6} MCЭ \xleftarrow{7} Eth\ №2 \xleftarrow{8} APM\ №3$;
- 3) $APM\ №1 \xleftarrow{2} Eth\ №1 \xleftarrow{6} MCЭ \xleftarrow{7} Eth\ №2 \xleftarrow{9} APM\ №4$;
- 4) $APM\ №2 \xleftarrow{3} Eth\ №1 \xleftarrow{6} MCЭ \xleftarrow{7} Eth\ №2 \xleftarrow{9} APM\ №4$;
- 5) $APM\ №1 \xleftarrow{2} Eth\ №1 \xleftarrow{6} MCЭ \xleftarrow{7} Eth\ №2 \xleftarrow{10} APM\ №5$;
- 6) $APM\ №2 \xleftarrow{3} Eth\ №1 \xleftarrow{6} MCЭ \xleftarrow{7} Eth\ №2 \xleftarrow{10} APM\ №5$;

б) штатные тракты прохождения ОИ:

- 1) $APM\ №1 \xleftarrow{1} Eth\ №1 \xleftarrow{5} MCЭ \xleftarrow{11} Eth\ №3 \xleftarrow{12} APM\ №6$;
- 2) $APM\ №2 \xleftarrow{4} Eth\ №1 \xleftarrow{5} MCЭ \xleftarrow{11} Eth\ №3 \xleftarrow{12} APM\ №6$;
- 3) $APM\ №1 \xleftarrow{1} Eth\ №1 \xleftarrow{5} MCЭ \xleftarrow{11} Eth\ №3 \xleftarrow{13} APM\ №7$;
- 4) $APM\ №2 \xleftarrow{4} Eth\ №1 \xleftarrow{5} MCЭ \xleftarrow{11} Eth\ №3 \xleftarrow{13} APM\ №7$;
- 5) $APM\ №1 \xleftarrow{1} Eth\ №1 \xleftarrow{5} MCЭ \xleftarrow{11} Eth\ №3 \xleftarrow{14} APM\ №8$;
- 6) $APM\ №2 \xleftarrow{4} Eth\ №1 \xleftarrow{5} MCЭ \xleftarrow{11} Eth\ №3 \xleftarrow{14} APM\ №8$.

Также описание схемы информационных потоков, как и любого графа, может быть оформлено в виде матриц. Данное представление схемы информационных потоков удобно в случае программной реализации данного алгоритма.

Для выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей ТС, достаточно использовать два вида матриц:

- матрица смежности ТС;
- матрица обрабатываемой информации в ТС.

Матрица смежности ТС A является разновидностью стандартной матрицы смежности графа, в которой столбцы и строки соответствуют вершинам графа, а значение каждой клетки матрицы отражает наличие или отсутствие связи между вершинами. Однако в разрабатываемой матрице смежности ТС каждый столбец матрицы, соответствующий одному ТС, дополнительно разбивается на K столбцов, характеризующих виды обрабатываемой информации (например, в анализируемой ТКС СН количество столбцов для каждого технического средства равно 2, так как в ней ТКС СН обрабатывается конфиденциальная и общедоступная информации), а в клетке матрицы указывается номер ребра, связывающий данные ТС. Использование данного вида матрицы позволяет отразить не только смежные ТС в системе, но и определить вид передаваемой между ними информации.

Таким образом, матрица смежности ТС A имеет размер $N \times KN$, где N – количество ТС, входящих в состав анализируемой ТКС СН, а K – количество видов обрабатываемой информации.

Правила заполнения матрицы смежности ТС A представлены в формуле (1).

$$A[i][(j-1) \times 2 + k] = \begin{cases} 0, & \text{если между ТС } i \text{ и } j \text{ не передается инф. вида } k, \\ \text{номер ребра, который передает инф. вида } k \text{ между ТС } i \text{ и } j. \end{cases} \quad (1)$$

Матрица смежности ТС A рассматриваемой ТКС СН приведена в таблице 9.

Таблица 9 – Матрица смежности ТС

ТС/вид инф.	АРМ №1		АРМ №2		АРМ №3		АРМ №4		АРМ №5		АРМ №6		АРМ №7		АРМ №8		Eth №1		Eth №2		Eth №3		МСЭ	
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ
АРМ №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0
АРМ №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0
АРМ №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0
АРМ №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0
АРМ №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0
АРМ №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0
АРМ №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0
АРМ №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0
Eth №3	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	0	0	11
МСЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0

Матрица обрабатываемой информации в ТС B , столбцы которой соответствуют ТС, строки – видам обрабатываемой информации, а значение каждой клетки матрицы отражает наличие или отсутствие данного вида информации в ТС, позволяет отразить виды информации, обрабатываемые в ТС, и сделать вывод о возможности их «пересечения».

Таким образом, матрица обрабатываемой информации в ТС B имеет размер $K \times N$, где N – количество ТС, входящих в состав ТКС СН, а K – количество видов обрабатываемой информации.

Правила заполнения матрицы обрабатываемой информации в ТС B представлены в формуле (2).

$$B[i][j] = \begin{cases} 0, & \text{если ТС } j \text{ не обрабатывает вид информации } i \\ 1, & \text{если ТС } j \text{ обрабатывает вид информации } i \end{cases} \quad (2)$$

Матрица обрабатываемой информации в ТС B рассматриваемой ТКС СН приведена в таблице 10.

Таблица 10 – Матрица обрабатываемой информации в ТС

ТС/вид инф.	АРМ №1	АРМ №2	АРМ №3	АРМ №4	АРМ №5	АРМ №6	АРМ №7	АРМ №8	Eth №1	Eth №2	Eth №3	МСЭ
КИ	1	1	1	1	1	0	0	0	1	1	0	1
ОИ	1	1	0	0	0	1	1	1	1	0	1	1

Для удобства проведения анализа матрица смежности ТС и матрица обрабатываемой информации в ТС могут быть объединены в матрицу смежности ТС и обрабатываемой в них информацией (см. таблицу 11).

Таблица 11 – Матрица смежности ТС и обрабатываемой в них информацией

ТС/вид инф.	APM №1		APM №2		APM №3		APM №4		APM №5		APM №6		APM №7		APM №8		Eth №1		Eth №2		Eth №3		МСЭ		КИ	ОИ
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ		
APM №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	1	1
APM №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	1	1
APM №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0
APM №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	1	0
APM №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	1	0
APM №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	1
APM №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	1
APM №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	1
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	1	1
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	1	0
Eth №3	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	0	11	0	1	1
МСЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0	1	1

По результатам второго этапа была разработана схема информационных потоков, в соответствии с которой было приведено описание трактов прохождения информации, а также получены два вида матриц, которые будут использованы на следующем этапе при выявлении потенциальных каналов утечки информации.

5 Выявление потенциальных каналов утечки информации в ТКС СН

На данном этапе должен быть проведен анализ разработанной схемы информационных потоков и матриц смежности ТС и обрабатываемой в них информацией с целью выявления всех возможных каналов утечки информации и идентификации ТС, сбоев и неисправности которых могут привести к их возникновению.

На первом этапе выявления потенциальных каналов утечки информации в ТКС СН должны быть определены все технические средства, которые являются источниками подлежащей защите информации. Это необходимо, чтобы исключить из списка потенциальных каналов утечки попадание защищаемой информации в данные технические средства. В рассматриваемой ТКС СН к информации, подлежащей защите, относится конфиденциальная информация, а её источниками являются АРМ №1 - №5, которые в матрице смежности ТС и обрабатываемой в них информацией отмечены звёздочкой («*») (см. таблицу 12).

Таблица 12 – Матрица смежности ТС и обрабатываемой в них информации с отмеченными источниками КИ

ТС/вид инф.	АРМ №1		АРМ №2		АРМ №3		АРМ №4		АРМ №5		АРМ №6		АРМ №7		АРМ №8		Eth №1		Eth №2		Eth №3		МСЭ		КИ	ОИ
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ		
* АРМ №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	1	1
* АРМ №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	1	1
* АРМ №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0
* АРМ №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	1	0
* АРМ №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	1	0
АРМ №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	1
АРМ №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	1
АРМ №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	1
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	1	1
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	1	0
Eth №3	0	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	0	11	0	1
МСЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0	1	1

Затем необходимо для каждого источника защищаемой информации определить возможные каналы её передачи.

В качестве примера рассмотрены возможные каналы передачи конфиденциальной информации от источника АРМ №1.

В соответствии с матрицей смежности ТС и обрабатываемой в них информацией (см. таблицу 13) АРМ №1 взаимодействует только с коммутатором Ethernet №1 в части передачи конфиденциальной и общедоступной информации. Таким образом, конфиденциальная информация может быть передана в коммутатор Ethernet №1 штатно (ребро №2) или в результате нарушения штатных алгоритмов работы АРМ №1 (ребро №1). В таблице красная стрелка отражает штатный канал передачи информации, синяя стрелка – нештатный канал передачи информации, а черная штриховая стрелка означает возможный сбой или неисправность технического средства, приводящие к возникновению нештатного канала передачи информации.

Таблица 13 – Возможные каналы передачи КИ из ТС АРМ №1

ТС/вид инф.	АРМ №1		АРМ №2		АРМ №3		АРМ №4		АРМ №5		АРМ №6		АРМ №7		АРМ №8		Eth №1		Eth №2		Eth №3		МСЭ		КИ	ОИ
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ		
* АРМ №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	1	→ 1
* АРМ №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	1	1
* АРМ №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0
* АРМ №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	1	0
* АРМ №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	1	0
АРМ №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	1
АРМ №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	0	1
АРМ №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	0	1
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	↓ 1	1
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	1	0
Eth №3	0	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	11	0	0	1
МСЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0	1	1

Для наглядного представления возможных каналов передачи конфиденциальной информации из ТС АРМ №1 было использовано дерево событий.

На дереве событий, как и в матрице смежности ТС и обрабатываемой в них информацией, приняты следующие обозначения:

- красная стрелка отражает штатный канал передачи информации;
- синяя стрелка отражает нештатный канал передачи информации;
- курсивом выделены технические средства, входящие в тракты передачи конфиденциальной информации, не являющиеся каналами утечки.

Для возможности сопоставления схемы информационных потоков с полученным деревом событий каждому каналу передачи информации

приписывается номер ребра в соответствии со схемой информационных потоков.

На рисунке 4 в виде дерева событий представлены возможные каналы передачи конфиденциальной информации из ТС АРМ №1, которые были выявлены в результате анализа матрицы смежности ТС и обрабатываемой в них информацией.

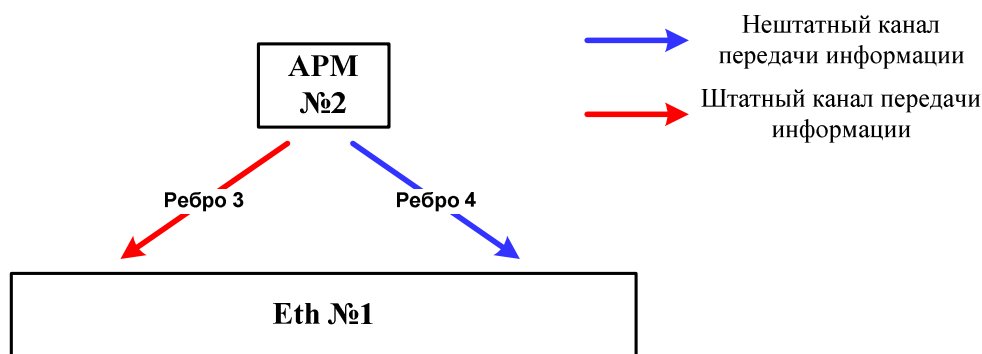


Рисунок 4 – Дерево событий

«Возможные каналы передачи КИ из ТС АРМ №1»

В соответствии с матрицей смежности ТС и обрабатываемой в них информацией (см. таблицу 14) коммутатор Ethernet может передать конфиденциальную информацию либо в АРМ №2 (ребра №3 и №4), либо в другие подсети через МСЭ (ребра №5 и №6). В связи с тем, что АРМ №2 также как и АРМ №1, является источником конфиденциальной информации, то её передача в данное техническое средство не является опасным событием.

Таблица 14 – Возможные каналы передачи КИ из коммутатора Ethernet №1

ТС/вид инф.	АРМ №1		АРМ №2		АРМ №3		АРМ №4		АРМ №5		АРМ №6		АРМ №7		АРМ №8		Eth №1		Eth №2		Eth №3		МСЭ		КИ	ОИ
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ		
* АРМ №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	1	1
* АРМ №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	1	1
* АРМ №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0
* АРМ №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	1	0
* АРМ №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	1	0
АРМ №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	1
АРМ №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	0	1
АРМ №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	0	1
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	1	→	1
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	1	0
Eth №3	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	11	0	0	0	1
МСЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0	1	1

Возможные каналы передачи конфиденциальной информации из коммутатора Ethernet №1 отражены на рисунке 5.

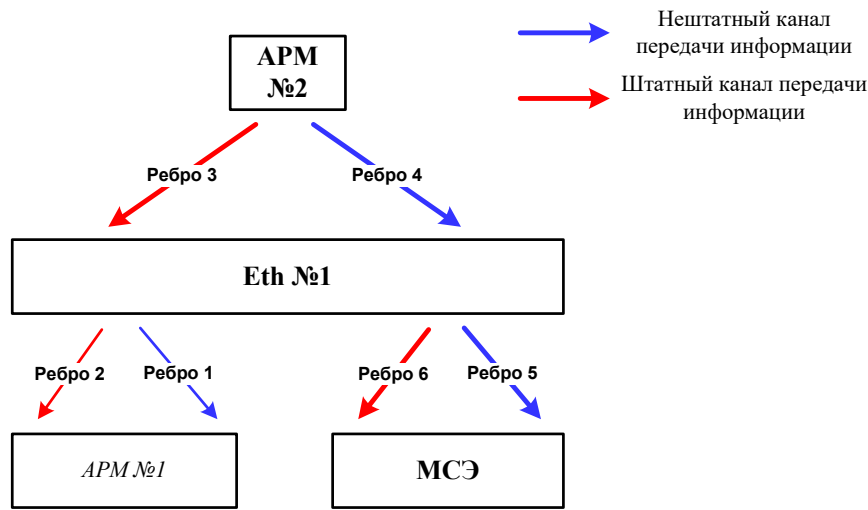


Рисунок 5 – Дерево событий

«Возможные каналы передачи КИ из коммутатора Ethernet №1»

В соответствии с матрицей смежности ТС и обрабатываемой в них информацией (см. таблицу 15) межсетевой экран, осуществляющий фильтрацию передаваемой информации, должен либо штатно передать конфиденциальную информацию в коммутатор Ethernet №2 подсети №2 (ребро №7), либо отбраковать конфиденциальную информацию, поступившую в MCЭ в качестве общедоступной информации (ребро №5). Однако в результате сбоев и неисправностей межсетевого экрана конфиденциальная информация может быть передана в коммутатор Ethernet №3 подсети №3, не предназначенной для её обработки (ребро №11).

Таблица 15 – Возможные каналы передачи КИ из MCЭ

ТС/вид инф.	APM №1		APM №2		APM №3		APM №4		APM №5		APM №6		APM №7		APM №8		Eth №1		Eth №2		Eth №3		MCЭ		КИ	ОИ
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ		
* APM №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	1	1
* APM №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	1	1
* APM №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0
* APM №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	1	0
* APM №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	1	0
APM №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	1
APM №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	1
APM №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	1
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	1	1
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	1	0
Eth №3	0	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	0	11	0	1
MCЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0	1	1

Возможные каналы передачи конфиденциальной информации из межсетевого экрана представлены на рисунке 6.

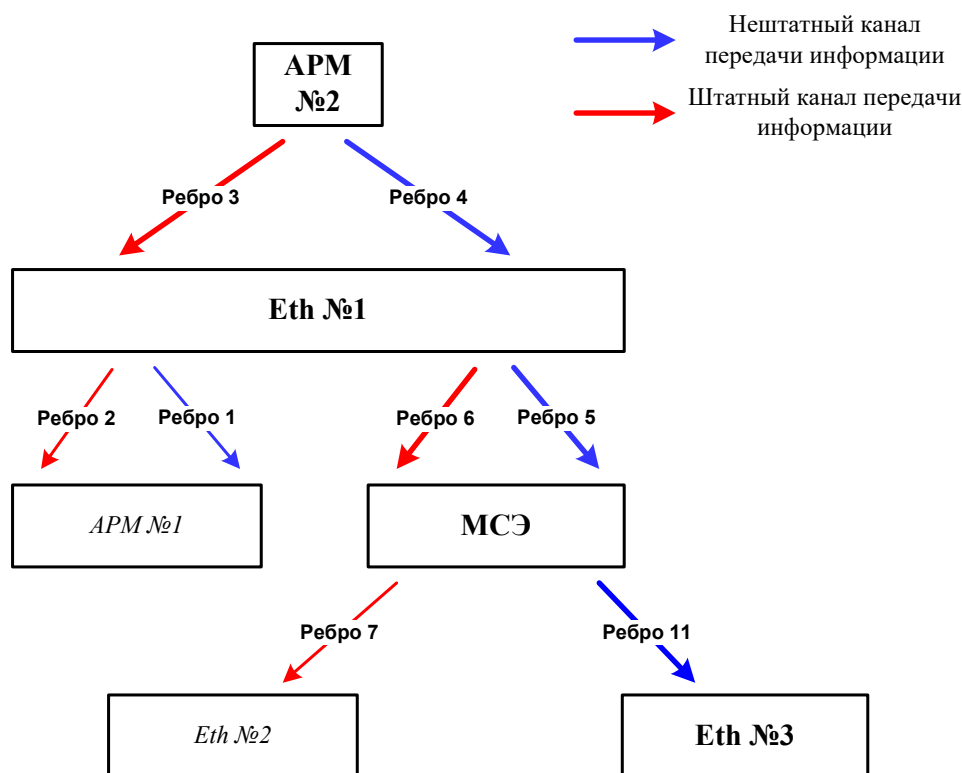


Рисунок 6 – Дерево событий «Возможные каналы передачи КИ из МСЭ»

В соответствии с матрицей смежности ТС и обрабатываемой в них информацией (см. таблицу 16) передача конфиденциальной информации через коммутатор Ethernet №2 в АРМ №3 – №5 (ребра №8 - 10) не является опасным событием, так как они являются её источниками, а передача конфиденциальной информации через коммутатор Ethernet №3 в АРМ №6 – 8 (ребра №12 - 14) является опасным событием.

Таблица 16 – Возможные каналы передачи КИ из ТС Eth №2 и №3

ТС/вид инф.	АРМ №1		АРМ №2		АРМ №3		АРМ №4		АРМ №5		АРМ №6		АРМ №7		АРМ №8		Eth №1		Eth №2		Eth №3		МСЭ		КИ	ОИ
	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ	КИ	ОИ		
* АРМ №1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	1	1
* АРМ №2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	1	1
* АРМ №3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0
* АРМ №4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	1	0
* АРМ №5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	1	0
АРМ №6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	1
АРМ №7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	1
АРМ №8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	0	0	0	1
Eth №1	2	1	3	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	1	1
Eth №2	0	0	0	0	8	0	9	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	1	0
Eth №3	0	0	0	0	0	0	0	0	0	0	0	12	0	13	0	14	0	0	0	0	0	0	0	11	0	1
МСЭ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	5	7	0	0	11	0	0	1	1

Возможные каналы передачи конфиденциальной информации из коммутаторов Ethernet №2 и №3 представлены на рисунке 7.

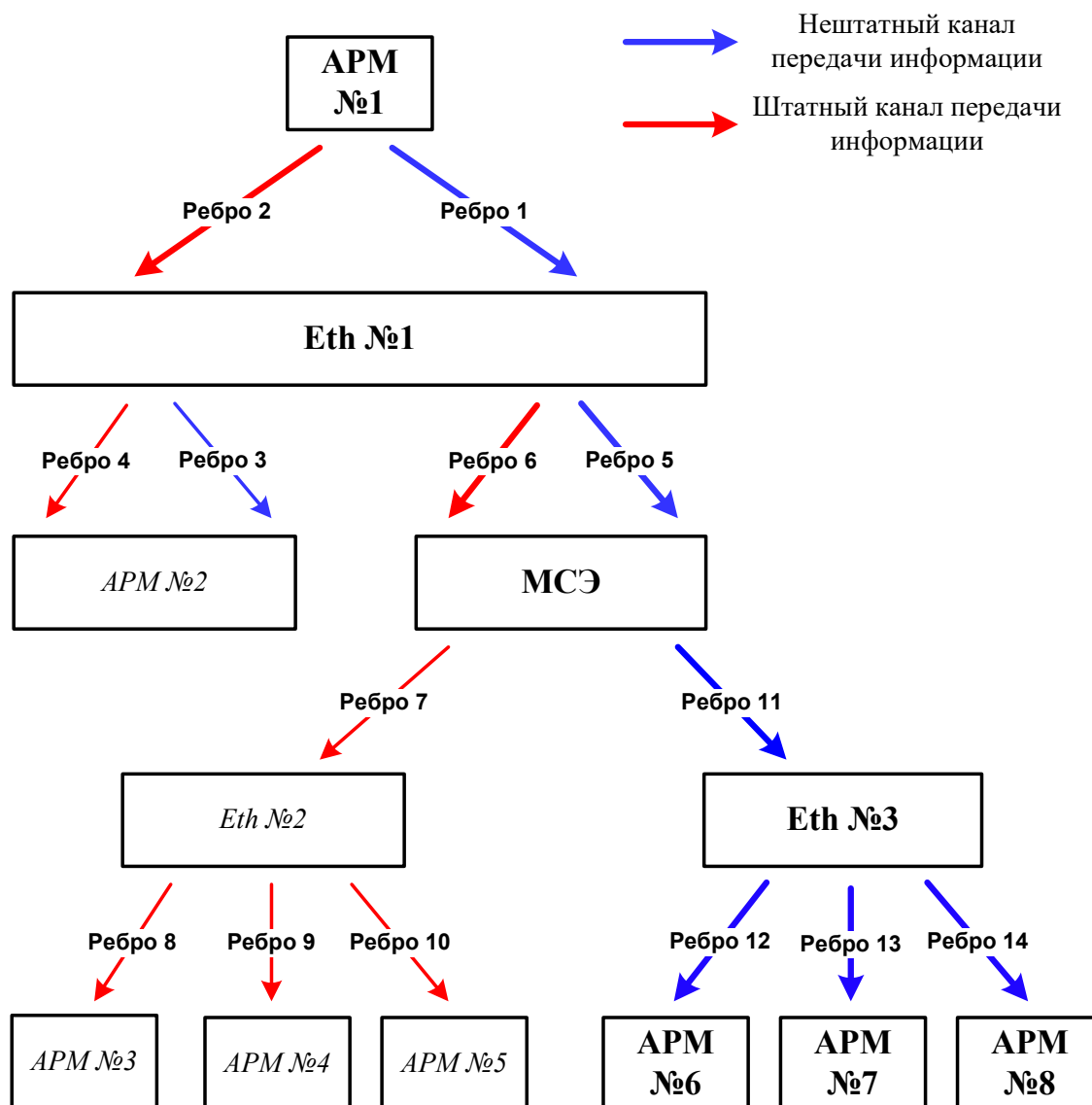


Рисунок 7 – Дерево событий

«Возможные каналы передачи КИ от ТС АРМ №1»

Таким образом, были определены все возможные каналы передачи конфиденциальной информации от АРМ №1 (см. рисунок 7).

На основании построенного дерева событий (см. рисунок 7) выявлены следующие каналы утечки конфиденциальной информации, к возникновению которых могут привести сбои (неисправности) АРМ №1, МСЭ и коммутаторов Ethernet №1 и 3:

- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№1);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№2);

- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№3);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№4);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№5);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№6);
- АРМ №1 $\xrightarrow{1}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№7);
- АРМ №1 $\xrightarrow{1}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№8);
- АРМ №1 $\xrightarrow{1}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№9).

Аналогично проводится анализ в случаях, когда источниками конфиденциальной информации являются ТС АРМ №2-5 (см. рисунки 8 и 9).

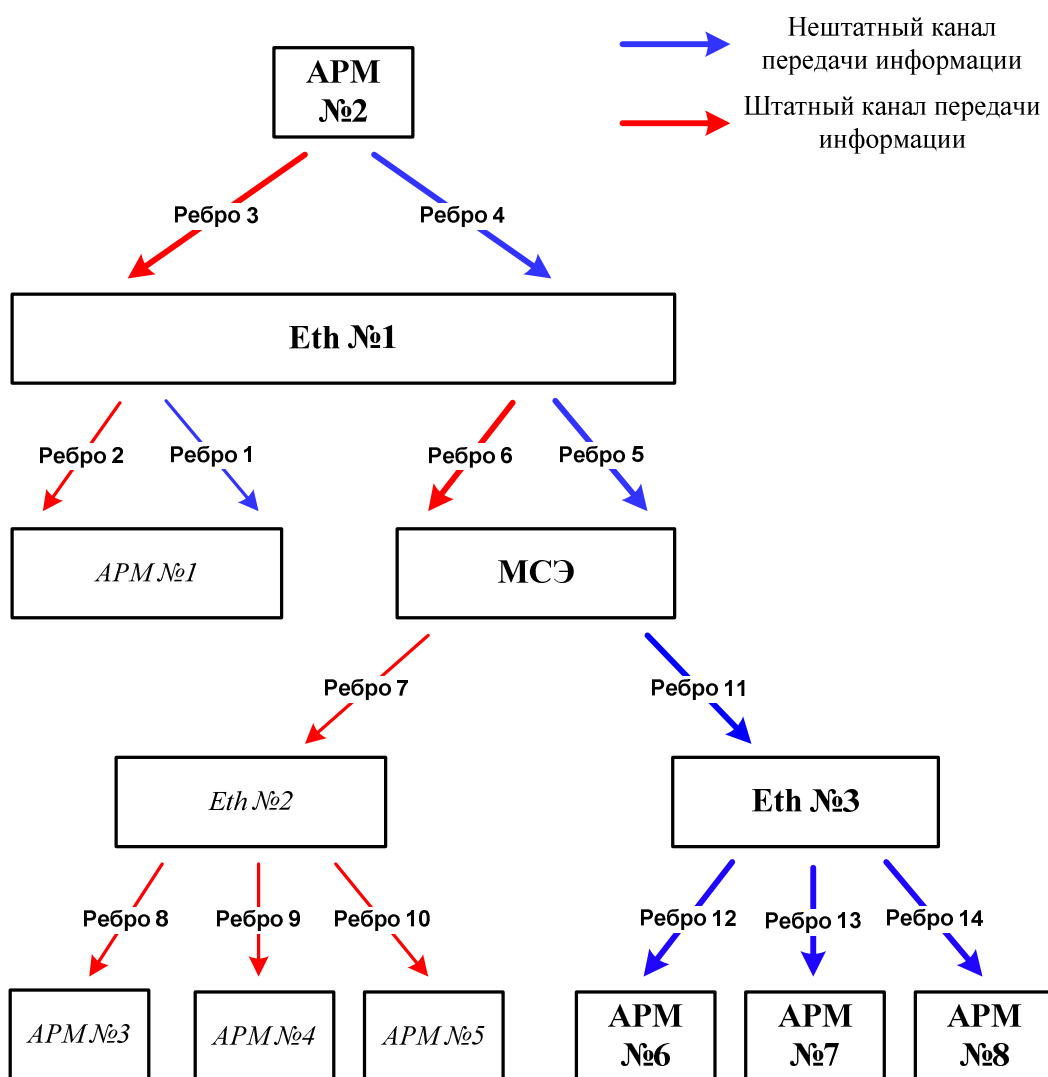


Рисунок 8 – Дерево событий «Возможные каналы передачи КИ от ТС АРМ №2»

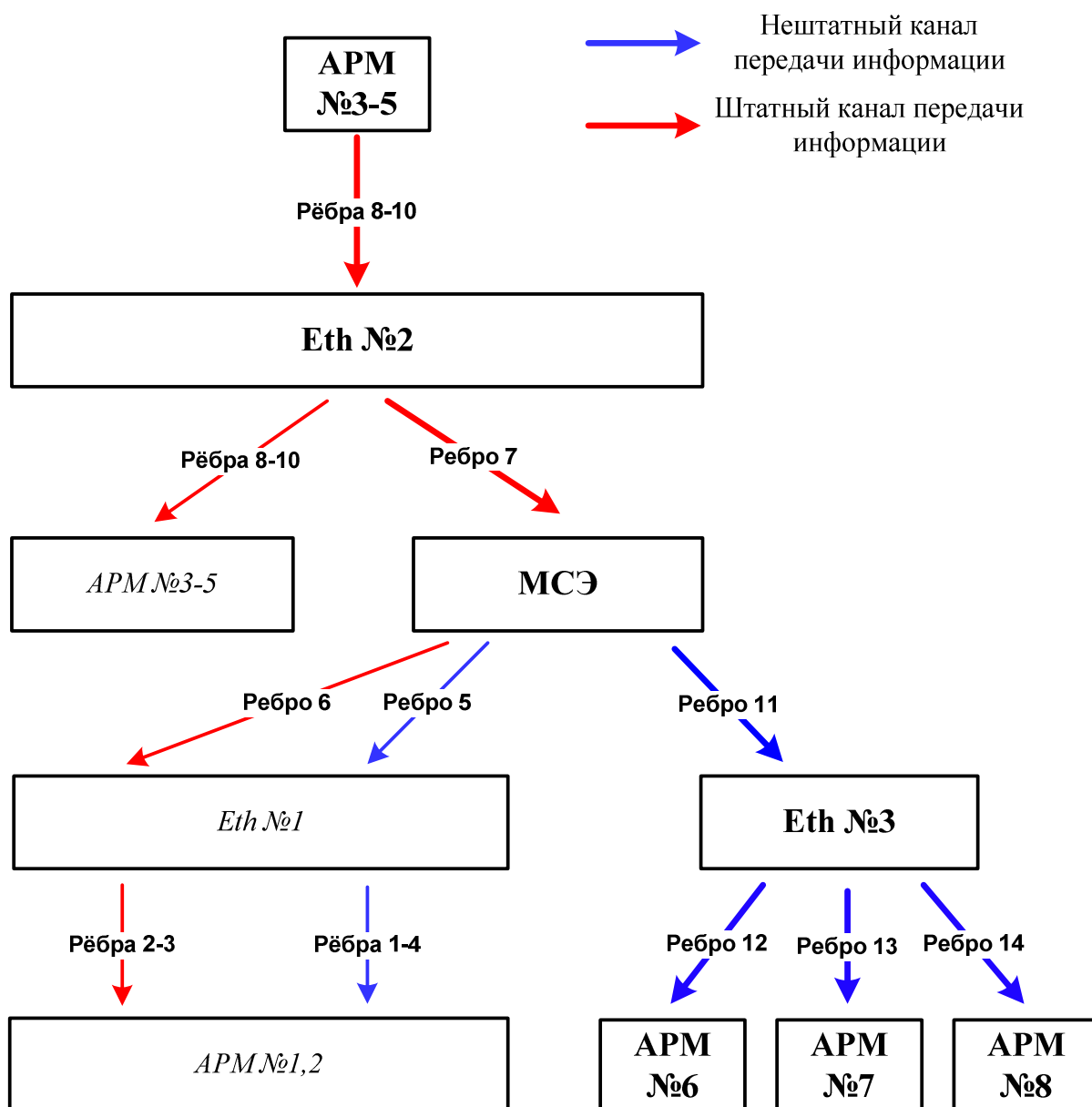


Рисунок 9 – Дерево событий «Возможные каналы передачи КИ от ТС АРМ №3-5»

На основании построенных деревьев событий (см. рисунки 8 и 9) выявлены следующие каналы утечки конфиденциальной информации, к возникновению которых могут привести сбои (неисправности) АРМ №2-5, МСЭ и коммутаторов Ethernet №1 и 3:

- АРМ №2 $\xrightarrow{3}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№10);
- АРМ №2 $\xrightarrow{3}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№11);
- АРМ №2 $\xrightarrow{3}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№12);
- АРМ №2 $\xrightarrow{3}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№13);
- АРМ №2 $\xrightarrow{3}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№14);

- АРМ №2 $\xrightarrow{3}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№15);
- АРМ №2 $\xrightarrow{4}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№16);
- АРМ №2 $\xrightarrow{4}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№17);
- АРМ №2 $\xrightarrow{4}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№18);
- АРМ №3 $\xrightarrow{8}$ Eth №2 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№19);
- АРМ №3 $\xrightarrow{8}$ Eth №1 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№20);
- АРМ №3 $\xrightarrow{8}$ Eth №1 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№21);
- АРМ №4 $\xrightarrow{9}$ Eth №2 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№22);
- АРМ №4 $\xrightarrow{9}$ Eth №1 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№23);
- АРМ №4 $\xrightarrow{9}$ Eth №1 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№24);
- АРМ №5 $\xrightarrow{10}$ Eth №2 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№25);
- АРМ №5 $\xrightarrow{10}$ Eth №1 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№26);
- АРМ №5 $\xrightarrow{10}$ Eth №1 $\xrightarrow{7}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№27).

Таким образом, по результатам анализа матрицы смежности ТС и обрабатываемой в них информацией, а также построенного на его основе дерева событий были выявлены потенциальные каналы утечки конфиденциальной информации в ТКС СН и определены технические средства, сбои и неисправности которых могут привести к их возникновению.

6 Оценка вероятности возникновения потенциальных каналов утечки информации в ТКС СН

Четвертым этапом выявления каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей ТС, является оценка вероятности возникновения потенциальных каналов утечки информации в ТКС СН. На основе полученного значения вероятности может быть сделан вывод об актуальности (неактуальности) угрозы неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей ТС.

Основной причиной возникновения данной угрозы является низкое качество ТС, входящих в состав ТКС СН. Основной характеристикой качества ТС является его надёжность. В соответствии с национальным стандартом ГОСТ 27.002-89 надёжность – это 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 [9].

Надёжность ТС является количественной характеристикой одного или нескольких свойств: долговечность, ремонтпригодность, безотказность и сохраняемость. Способность технического средства сохранять работоспособное состояние относится к свойству безотказности, которое характеризуется следующими показателями: вероятность безотказной работы, вероятность отказа, средняя наработка до отказа, интенсивность отказов и др. В связи с тем, что причиной утечки защищаемой информации являются отказы и сбои ТС, в качестве показателей исправности и неисправности ТС были выбраны вероятность безотказной работы и вероятность отказа.

Вероятность безотказной работы ТС $P(t)$ определяет вероятность того, что в пределах заданного времени (например, времени наработки) отказ ТС не возникнет.

При экспоненциальном распределении времени до отказа вероятность безотказной работы определяется выражением (3).

$$P(t) = e^{-\lambda t} \quad (3)$$

где λ – интенсивность отказов ТС.

Вероятность отказа $Q(t)$ является обратной величиной вероятности безотказной работы ТС $P(t)$ и определяется выражением (4).

$$Q(t) = 1 - P(t) = 1 - e^{-\lambda t} \quad (4)$$

Под интенсивностью отказов ТС (λ , [1/ч]) понимается условная плотность вероятности возникновения отказа, которая соответствует номинальному электрическому режиму и нормальным (лабораторным) условиям эксплуатации [9]. Однако условия работы ТС на практике, как правило, оказываются более жесткими, нежели нормальные. В связи с этим введено понятие эксплуатационной интенсивности отказов ($\lambda_{\text{э}}$, [1/ч]), при расчете которой учитываются факторы эксплуатации ТС (например, температурный режим эксплуатации).

Интенсивность отказов (эксплуатационная интенсивность отказов) сложного изделия складывается из независимых отказов его составных частей (компонентов) и определяется выражением (5).

$$\lambda_{\text{изделия}} = \sum_{i=1}^N \lambda_i \quad (5)$$

где N – число компонентов изделия.

Однако, не все компоненты, входящие в состав ТС, могут привести к ошибочной передаче информации. Поэтому в рамках оценки вероятности возникновения потенциальных каналов утечки информации в ТКС СН целесообразней использовать понятия «спецнадёжности» и «спецотказов».

Спецнадёжность — это способность объекта или средства выполнять задачи передачи, обработки и хранения информации в определённых условиях функционирования без возникновения отказов, приводящих к утечке информации [11]. Соответственно, к спецотказам относятся отказы, приводящие к утечке информации.

Таким образом, при расчёте интенсивности спецотказов ТС будут учитываться не все компоненты из его состава, а лишь те, которые могут привести к возникновению потенциальных каналов утечки КИ в ТКС СН.

Для оценки вероятности возникновения потенциальных каналов утечки КИ в ТКС СН могут быть использованы деревья событий, разработанные на предыдущем этапе (см. рисунки с 7 по 9). Для этого каждой ветке дерева событий может быть присвоена вероятность её возникновения (вероятность безотказной работы или вероятность отказа), а вероятность возникновения канала утечки информации определяется путём их перемножения.

Далее приведена оценка вероятности возникновения потенциальных каналов утечки на примере первого дерева событий (см. рисунок 10).

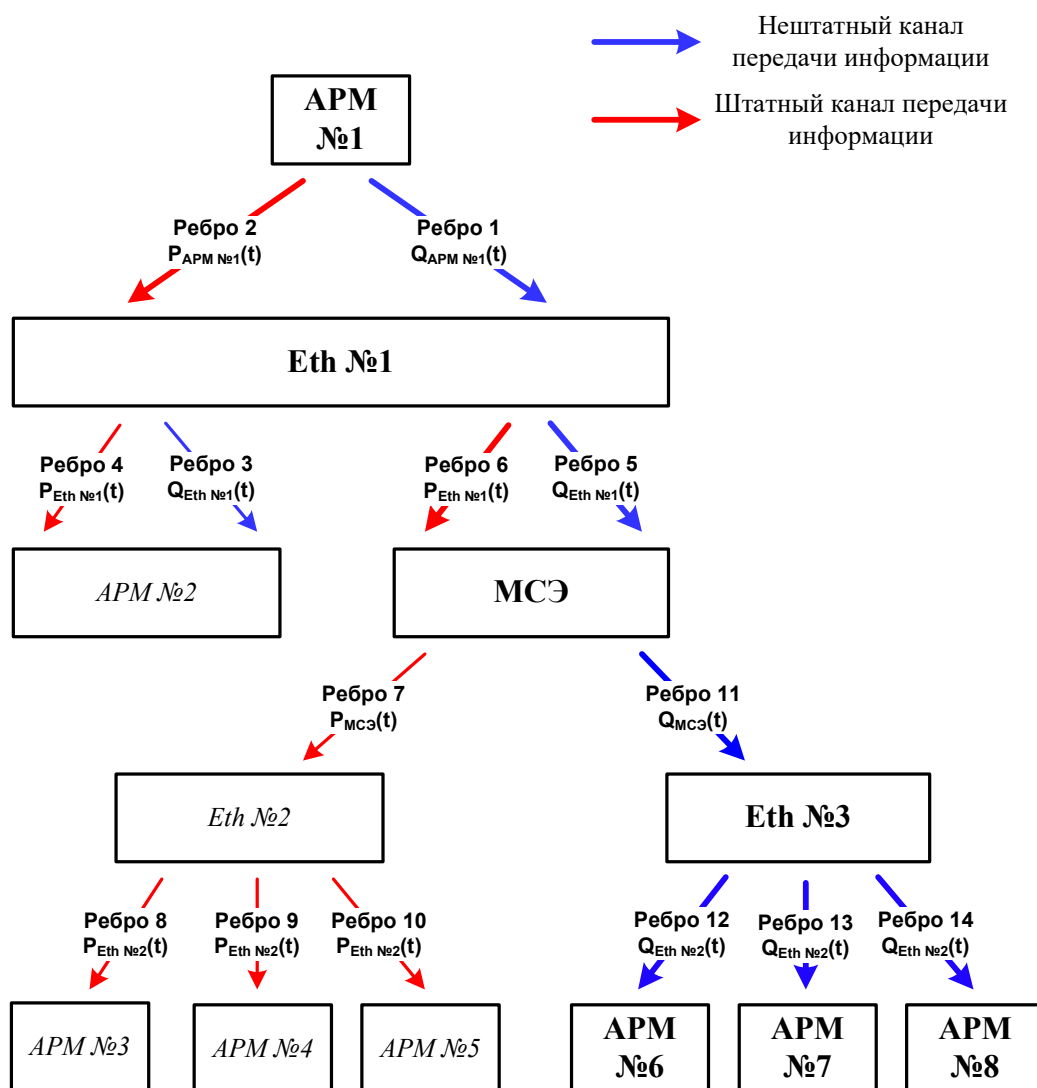


Рисунок 10 – Дерево событий «Возможные каналы передачи КИ от ТС APM №1»

Для дерева событий, представленного на рисунке 10, определены следующие каналы утечки КИ:

- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№1);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№2);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{6}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№3);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№4);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№5);
- АРМ №1 $\xrightarrow{2}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№6);
- АРМ №1 $\xrightarrow{1}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{12}$ АРМ №6 (№7);
- АРМ №1 $\xrightarrow{1}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{13}$ АРМ №7 (№8);
- АРМ №1 $\xrightarrow{1}$ Eth №1 $\xrightarrow{5}$ МСЭ $\xrightarrow{11}$ Eth №3 $\xrightarrow{14}$ АРМ №8 (№9).

К возникновению данных каналов утечки КИ могут привести сбои (неисправности) АРМ №1, МСЭ и коммутаторов Ethernet №1 и 3. Таким образом, для получения значений вероятности безотказной работы и вероятности отказов необходимо провести анализ данных ТС.

Далее в качестве примера был выполнен анализ ТС АРМ №1.

ТС АРМ представляет собой автоматизированное рабочее место и объединяет программно-аппаратные средства, обеспечивающие взаимодействие оператора с компьютером, предоставляет возможность ввода информации с клавиатуры и её вывод на экран монитора. Аппаратно ТС АРМ реализовано на базе IBM-совместимого компьютера и представляет собой промышленный персональный компьютер, предназначенный для работы в неблагоприятных условиях (повышенная вибрация, загрязненная атмосфера, повышенная влажность, повышенная и пониженная температуры). Питание терминала дежурного по связи осуществляется от сети напряжением (220 плюс-минус 22) В и частотой (50 плюс-минус 1-2) Гц.

Взаимодействие оператора с ТС АРМ в процессе работы происходит в диалоговом режиме, который поддерживается набором меню, справочной системой и многооконным интерфейсом оператора. Решение задач оператора осуществляется через окна на экране видеомонитора, через которые

производится вывод информации, необходимой для ведения диалога с терминалом.

Архитектура аппаратного обеспечения АРМ представлена на рисунке 11.

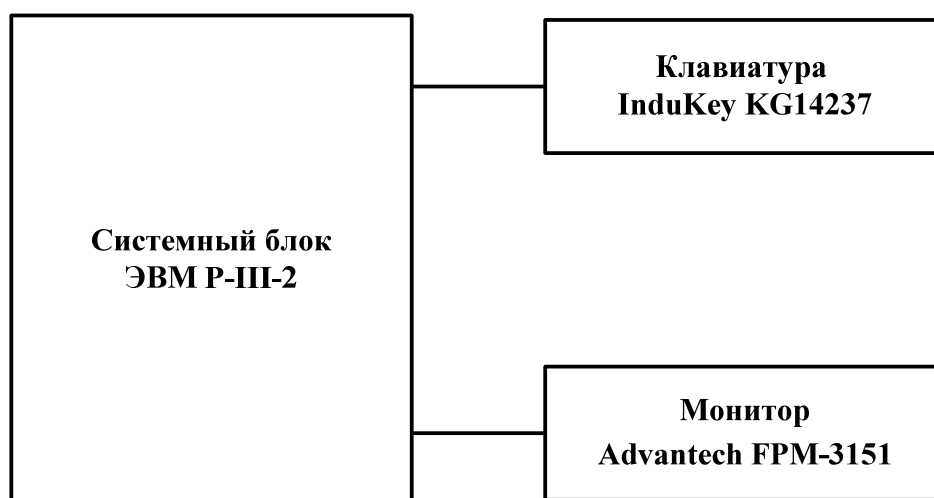


Рисунок 11 – Архитектура аппаратного обеспечения АРМ

Основным аппаратно-программным компонентом изделия является системный блок ЭВМ Р-III-2. К средствам ведения диалога с оператором (пользователем) относятся: клавиатура InduKey KG14237, имеющая в своем составе сенсорное устройство, и видеомонитор Advantech FPM-3151.

Профессиональный сенсорный монитор Advantech FPM-3151 предназначен для решения широкого спектра промышленных задач и использования в жестких условиях эксплуатации. Монитор оборудован в жесткий, нержавеющий корпус и предназначен для настенного и настольного креплений, также предусмотрен монтаж в панель. На мониторе расположен ряд кнопок для настройки параметров экрана пользователем (яркость, контраст и т.д.). При необходимости монитор может быть заблокирован.

Основные характеристики монитора Advantech FPM-315 представлены в таблице 17.

Таблица 17 – Основные характеристики монитора Advantech FPM-315

Параметр	Значение параметра
Диагональ экрана монитора	15"
Максимальное разрешение монитора	1024 × 768

Продолжение таблицы 17

Параметр	Значение параметра
Тип дисплея	ЖК
Соотношение сторон	4:3
Сенсорный экран	Да
Яркость	350 кд/м ²
Контрастность	700:1
Горизонтальная область обзора	160°
Максимальное количество цветов	16,2 млн.
Интерфейсы	VGA и DVI-D
Диапазон рабочих температур	-20°C ... +60°C
Ширина×высота×глубина	422 мм×311 мм×70 мм
Вес	7,8 кг

Клавиатура InduKey KG14237 предназначена для применения в промышленной автоматизации. Клавиатура упакована в алюминиевый корпус и предназначена для монтажа в панель. На клавиатуре расположены 83 силиконовые клавиши с углеродным контактом. В качестве указательного устройства используется емкостная сенсорная панель (TouchPad). Клавиатура поддерживает два языка: русский и английский.

Основные характеристики клавиатуры InduKey KG14237 представлены в таблице 18.

Таблица 18 – Основные характеристики клавиатуры InduKey KG14237

Параметр	Значение параметра
Количество клавиш	83
Вид контактов	Силиконовые клавиши с углеродным контактом
Ход клавиш	1,2 мм
Сила нажатия	1,2 ньютона
Срок эксплуатации	1 миллион нажатий

Продолжение таблицы 18

Параметр	Значение параметра
Языки	Английский и русский
Тип указательного устройства	Сенсорная панель (TouchPad) емкостная
Материал корпуса	Алюминий
Уровень защиты корпуса	IP65
Интерфейс (клавиатура)	PS/2
Интерфейс (указательное устройство)	PS/2
Диапазон рабочих температур	0°C ... +70°C
Диапазон температуры хранения	-25°C ... +80°C
Ширина×высота×глубина	405 мм×135 мм×19,5 мм
Вес	0,55 кг

Системный блок ЭВМ Р-III-2 представляет собой корпус, в котором находятся основные функциональные компоненты автоматизированного рабочего места.

Корпусом системного блока ЭВМ Р-III-2 является шасси IPC-6806SB-15ZBE компании Advantech с двумя отсеками для дисководов (НГМД и НЖМД), двумя интерфейсами ввода-вывода (USB) и со встроенным блоком питания стандарта ATX мощностью 150 Вт, время безотказной работы которого составляет 50000 часов.

Внутри корпуса системного блока установлена пассивная объединительная плата PCA-6105P5-0B2E компании Advantech с пятью слотами расширения PCI, не содержащая электронных компонент, кроме разъемов шины, нескольких буферов и драйверных систем.

Вся системная логика реализована на системной плате PCI-7031D-S6A1E компании Advantech, установленной в пятый слот расширения PCI объединительной платы.

Структурная схема системной платы Advantech PCI-7031D-S6A1E представлена на рисунке 12.

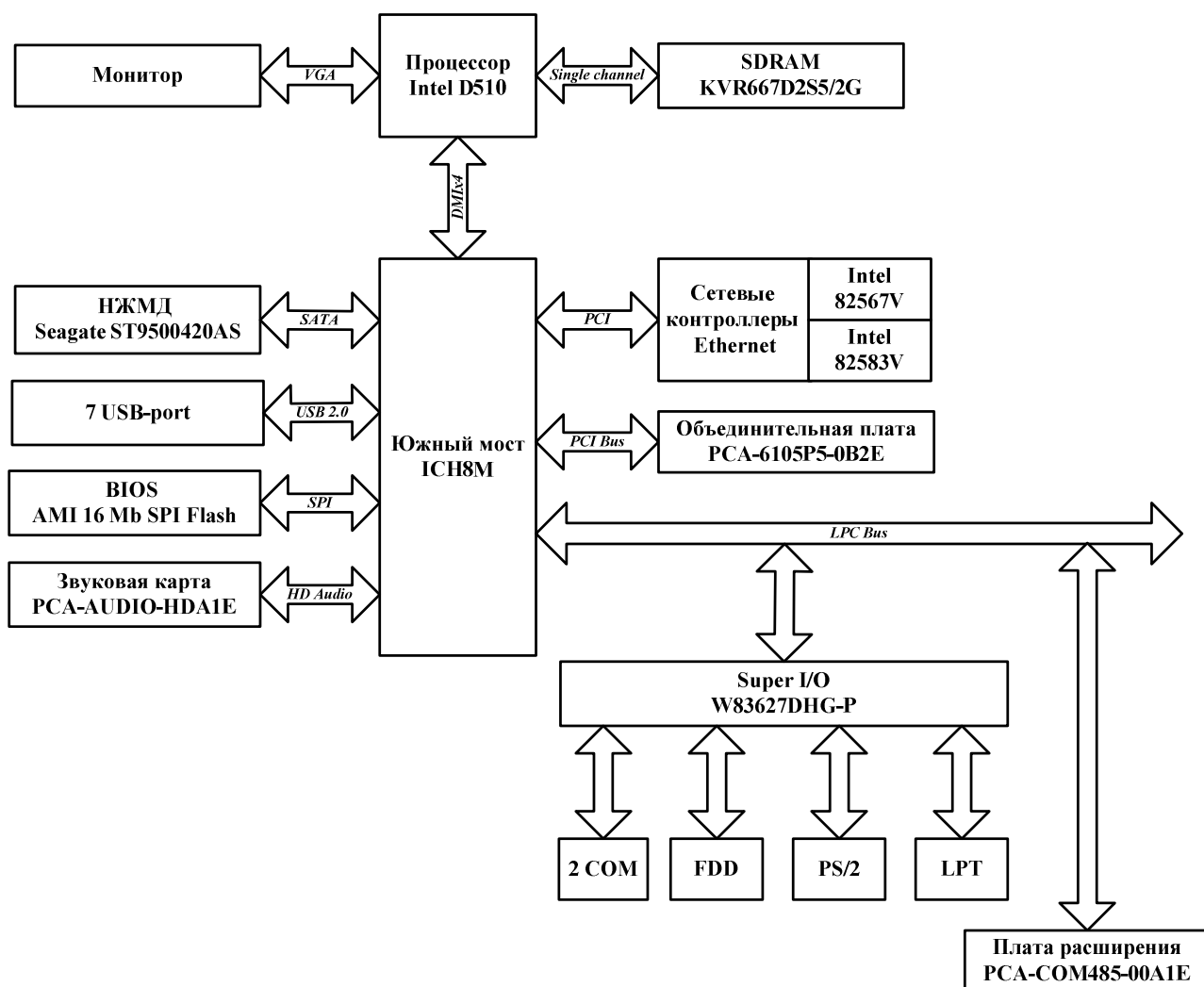


Рисунок 12 – Структурная схема системной платы

Advantech PCI-7031D-S6A1E

В состав системной платы Advantech PCI-7031D-S6A1E входят следующие аппаратные компоненты:

- процессор Intel Atom D510, который обеспечивает выполнение процедур обработки данных и взаимодействие всех устройств. Микропроцессоры Intel Atom предназначены для применения в нетбуках, неттопах, коммуникаторах и других портативных устройствах, для которых важно малое потребление энергии;

- контроллер-концентратор ввода-вывода (южный мост, SB) Intel ICH8M, обеспечивающий взаимодействие центрального процессора с жестким диском, PCI-картами (PCI-Express), интерфейсами SATA, USB и др.

Для соединения южного моста и процессора используется последовательная шина DMI, разработанная компанией Intel;

- оперативная память (SDRAM) Kingston KVR667D2S5/2G, которая предназначена для оперативного обмена информацией между процессором, внешней памятью и периферийными подсистемами;

- накопитель на жестком магнитном диске (НЖМД) Seagate ST9500420AS, который позволяет автономно сохранять информацию для последующего ее использования независимо от состояния компьютера;

- микросхема BIOS (базовая система ввода-вывода) AMI 16 Mb SPI Flash, которая является ключевым элементом системной платы и содержит программу начального загрузчика, предназначенную для загрузки ОС с диска, драйвера низкого уровня, предназначенных для обслуживания основных устройств ввода-вывода, и программу POST, предназначенную для тестирования устройств ПК при включении питания;

- звуковая карта PCA-AUDIO-HDA1E, которая является одной из составляющих аудиосистемы компьютера и предназначена для работы со звуком на компьютере;

- сетевые контроллеры локальной сети Ethernet Intel 82567V и 82583V, которые интегрированы в чипсет «Южный мост» и предназначены для взаимодействия с другими изделиями, находящимися в локальной сети;

- сопроцессор Super I/O W83627DHG-P, который отвечает за низкоскоростные порты и подключается к южному мосту с помощью шины LPC, разработанной компанией Intel в качестве низкоскоростного соединения. Super I/O сочетает функции контроллера дисководов гибких дисков (FDD), контроллера параллельного порта (LPT-порт), контроллера последовательного порта (COM-порт) и контроллера интерфейса PS/2;

- плата расширения PCA-COM485-001A1E 4xRS-458/422 с функцией автоматического управления, которая обеспечивает подключение устройств по шине RS-458/422.

После анализа состава ТС необходимо рассмотреть принципы работы и взаимодействие аппаратных компонент в ТС с целью определения аппаратных компонент, сбоев и неисправности которых могут приводить к ошибочной передаче КИ.

При включении изделия АРМ выполняется самотестирование напряжений блоком питания. Если значения напряжений соответствует норме, на процессор подается напряжение и сигнал сброса. Процессор осуществляет сброс памяти и переходит в режим работы.

Работа процессора начинается с получения из BIOS POST-программы (*Power-On Self-Test* – самотестирование при включении). В соответствии с POST-программой производится тестирование и проверка составляющих изделия АРМ: регистров процессора, оперативной памяти, устройств ввода-вывода, системного таймера, порта звуковой сигнализации, функциональных подсистем BIOS др. Если в результате POST-процедуры произойдет какой-либо сбой или будут выявлены ошибки аппаратных компонентов, то изделие выдаст диагностические сообщения в виде последовательности коротких и длинных сигналов или краткие текстовые сообщения, по которым можно определить причину неисправности. Кроме проведения начальной диагностики BIOS занимается инициализацией устройств компьютера, загружая в их регистры определенные значения.

После успешного прохождения POST-процедуры происходит передача управления загрузчику операционной системы, который загружает операционную систему в изделие АРМ. После загрузки операционной системы выполняется проверка целостности файловой системы. В случае если целостность не нарушена, оператору предоставляется возможность пройти аутентификацию при помощи ввода имени пользователя и пароля. После чего изделие АРМ переходит в рабочий режим и готово к использованию.

Источником данных (информация ограниченного доступа и команды управления) является оператор, который путем взаимодействия с графическим интерфейсом рабочей программы и (или) путем ввода данных с клавиатуры,

инициирует формирование сообщения данных. Передачу данных с клавиатуры в южный мост осуществляет сопроцессор Super I/O W83627DHG-P.

Для обработки полученных данных южный мост осуществляет их передачу в процессор, который формирует пакеты для дальнейшей передачи по интерфейсу Ethernet. При этом необходимые данные считываются из НЖМД. После обработки данных южный мост передает сформированные пакеты в драйвер Ethernet, который управляет дальнейшей передачей информации по интерфейсу Ethernet.

В процессе работы результаты обработки данных выводятся на экран монитора. Выход из строя видеоадаптера проявляется в отсутствии или искажении изображения на экране монитора, что не приводит к возникновению опасных событий.

Таким образом, по результатам рассмотрения принципов работы и взаимодействия аппаратных компонент в изделии АРМ было определено, что отказ изделия АРМ может быть вызван сбоями и неисправностями системного блока, который в свою очередь определяется отказами его пяти составляющих:

- центральный процессор (CPU), сбои и неисправности которого 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 передаче КИ в технические средства, не предназначенные для её обработки;

- чипсет «Южный мост» (SB), сбои и неисправности которого могут приводить к искажению команд и данных, передаваемых/принимаемых от устройств, подключенных по низкоскоростным шинам PCI, IDE, SATA, в результате чего возможны отклонения алгоритма работы от штатных правил обработки информации, приводящие к передаче КИ в технические средства, не предназначенные для её обработки;

- оперативная память (SDRAM), сбои и неисправности которой 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 передаче КИ в технические средства, не предназначенные для её обработки;

– накопитель на жестком магнитном диске (НЖМД), сбои и неисправности которого 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 передаче КИ в технические средства, не предназначенные для её обработки.

Таким образом, к возникновению опасных событий могут привести сбои и неисправности следующих аппаратных компонент: центральный процессор (CPU), южный мост (SB), оперативная память (SDRAM) и накопитель НЖМД.

Расчет эксплуатационной интенсивности отказа был выполнен в автоматизированной системе расчета надежности (АСРН), которая позволяет рассчитывать суммарную интенсивность отказов аппаратуры, укомплектованной ЭРИ отечественного и иностранного производства (ИП).

Разработчиком АСРН является ОАО «Российский научно-исследовательский институт «Электронстандарт», которое является головной организацией Российского агентства по системам управления в области надежности, сертификации, метрологии, стандартизации качества электронных приборов.

Автоматизированная система расчета надежности (АСРН) разработана на базе двух справочников «Надёжность электрорадиоизделий» и «Надёжность электрорадиоизделий иностранного производства» редакции 2006 г., и позволяет рассчитывать суммарную интенсивность отказов аппаратуры вплоть до 3 уровня детализации без учета резервирования, а также вероятность безотказной работы. Автоматизированная система расчета надежности позволяет производить расчет интенсивности отказов как в режиме эксплуатации, так и в режиме хранения в составе подвижных и неподвижных объектов. Также к возможностям программы относятся формирование и расчет

изделий, не входящих в номенклатуру справочника, формирование базы данных электрорадиоизделий, а также экспорт результатов расчета в форматы HTML и RTF.

При расчете эксплуатационной интенсивности отказов пользователю необходимо выбрать класс и группу электрорадиоизделия, указать необходимые для данной группы параметры, температуру окружающей среды и электрорадиоизделия, а также условия эксплуатации.

При расчете эксплуатационной интенсивности отказов были использованы технические характеристики выбранных аппаратных компонент (см. таблицы с 19 по 22).

Таблица 19 – Технические характеристики процессора Intel Atom D510

Параметр	Значение параметра
Тактовая частота	1,66 ГГц
Кеш второго уровня	1 Мбайт
Топологический размер	45 нм
Размер корпуса	22 мм × 22 мм
Размер кристалла	87 мм ²
Расчетная TDP	13 Вт
Форм-фактор	FCBGA
Число контактов	599
DMI	2,5 GT/s
Температура перехода	100°C
Количество транзисторов в ядре процессора	176 млн.
Набор команд	64-bit
Диапазон напряжения	0.8 В – 1,175 В
Количество ядер	2

Таблица 20 – Технические характеристики 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 мкм
Площадь кристалла	1,18 см ²
Температура корпуса	105°C
Поддержка PCI	4 (32 бит/33 МГц)
Версия USB	USB 2.0
Количество портов SATA	3
Интегрированный сетевой адаптер	10/100/1000
Интегрированный адаптер IDE	1 Channel

Таблица 21 – Технические характеристики оперативной памяти Kingston KVR667D2S5/2G

Параметр	Значение параметра
Стандарт	DDR2
Форм-фактор	SODIMM
Количество контактов	200
Объем памяти	2 ГБ
Эффективная частота	667 МГц
Пропускная способность	5300 Мб/с
Поддержка ECC	Нет
Количество чипов на модуле	16
Напряжение питания	1,8 В
Максимальная выделяемая мощность	1,944 Вт

Продолжение таблицы 21

Параметр	Значение параметра
Операционная температура	55°C – 65°C
Компоновка чипов на модуле	Двусторонняя
Габариты	67,6 мм × 30 мм

Таблица 22 – Технические характеристики НЖМД Seagate ST9500420AS

Параметр	Значение параметра
Форм-фактор	2,5"
Тип интерфейса	SATA, SATAII
Емкость	500 Гбайт
Среднее время поиска	14 мс
Объем буфера обмена	16 Мбайт
Частота вращения шпинделя	7200 об/мин
Среднее время наработки на отказ	600 000 ч
Уровень шума при чтении	25 дБ
Потребляемая мощность при работе	1,55 Вт

Результаты расчета эксплуатационных интенсивностей отказов выбранных аппаратных компонент и изделия АРМ №1 в целом представлены в таблице 23.

Таблица 23 – Эксплуатационная интенсивность отказов ЭРИ ТС АРМ №1

Обозначение компонента	Наименование компонента	Интенсивность отказа компонента ($\lambda_{\text{э}}$), 1/ч	Общая эксплуатационная интенсивность отказов ТС АРМ ($\lambda_{\text{АРМ №1}}$), 1/ч
CPU	Центральный процессор	$7,15 \times 10^{-4}$	$\lambda_{\text{АРМ №1}} = \lambda_{\text{CPU}} + \lambda_{\text{SB}} + \lambda_{\text{SDRAM}} + \lambda_{\text{HDD}} = 7,17 \times 10^{-4} \text{ 1/ч}$
SB	Чипсет «Южный мост»	$4,35 \times 10^{-7}$	
SDRAM	Оперативная память	$4,68 \times 10^{-7}$	
HDD	Накопитель НЖМД	$1,67 \times 10^{-6}$	

На основе полученной эксплуатационной интенсивности отказов по формуле (3) была рассчитана вероятность безотказной работы ТС АРМ №1 в течение суток (t равно 24 часам):

$$P_{\text{АРМ}\text{№1}}(t) = e^{-\lambda_{\text{АРМ}\text{№1}}t} = 9,83 \times 10^{-1}$$

Тогда вероятность отказа ТС АРМ №1 в соответствии с выражением (4) составляет:

$$Q_{\text{АРМ}\text{№1}}(t) = 1 - P(t) = 1,71 \times 10^{-2}$$

В случае отсутствия исходных данных об аппаратном обеспечении технического средства 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 [9].

Параметр «Наработка на отказ» определяется по формуле (6).

$$MTBF = \frac{1}{\lambda} \text{ часов} \quad (6)$$

Например, для коммутатора Ethernet Cisco Catalyst WS-C2960-8TC-L наработка на отказ $MTBF$ равна 615549 часам [15], соответственно интенсивность отказов коммутатора Ethernet, рассчитанная по формуле (6), равна:

$$\lambda_{\text{Eth}\text{№1}} = \frac{1}{MTBF} = 1,62 \times 10^{-6} \text{ 1/ч}$$

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

$$P_{\text{Eth}\text{№1}}(t) = e^{-\lambda_{\text{Eth}\text{№1}}t} = 0,999961011$$

$$Q_{\text{Eth}\text{№1}}(t) = 1 - P(t) = 3,9 \times 10^{-5}$$

Аналогично была рассчитана вероятность безотказной работы и вероятность отказа МСЭ:

$$\lambda_{\text{МСЭ}} = \frac{1}{MTBF} = \frac{1}{40000 \text{ ч}} = 1,62 \times 10^{-6} \text{ 1/ч}$$

$$P_{MC3}(t) = e^{-\lambda_{Eth \text{ №1}} t} = 0,99940018$$

$$Q_{MC3}(t) = 1 - P(t) = 0,00059982$$

Однако при расчёте вероятностей безотказной работы и вероятностей отказов технических средств может быть проведён анализ не только аппаратного обеспечения, но и анализ специального программного обеспечения, по результатам которого данные вероятности могут быть скорректированы [17]. Например, в случае некорректно реализованного алгоритма информационного взаимодействия технических средств, а также в случае наличия в программном обеспечении опасных программных конструкций может приводить к увеличению вероятности возникновения опасных событий, а использование в специальном программном обеспечении технического средства механизмов защиты информации от угроз техногенного характера способствует снижению данных вероятностей. Таким образом, совместно с анализом аппаратного обеспечения технических средств рекомендуется проводить анализ программного обеспечения, реализующего основные алгоритмы информационного взаимодействия технических средств, с целью получения уточнённых вероятностей возникновения опасных событий. Однако в рамках дипломного проекта вопросы, связанные с анализом программного обеспечения технических средств, не рассматривались, и вероятности безотказной работы и вероятностей отказов технических средств не были изменены.

На основе полученных значений вероятностей безотказной работы и вероятностей отказов технических средств были рассчитаны вероятности возникновения потенциальных каналов утечки конфиденциальной информации №1 - №9:

$$P_1(t) = P_2(t) = P_3(t) = P_{APMN\text{№1}}(t) \times P_{Eth\text{№1}}(t) \times Q_{MC3}(t) \times Q_{Eth\text{№2}}(t) = 2,3 \times 10^{-8}$$

$$P_4(t) = P_5(t) = P_6(t) = P_{APMN\text{№1}}(t) \times Q_{Eth\text{№1}}(t) \times Q_{MC3}(t) \times Q_{Eth\text{№2}}(t) = 8,96 \times 10^{-13}$$

$$P_7(t) = P_8(t) = P_9(t) = Q_{APMN\text{№}1}(t) \times Q_{Eth\text{№}1}(t) \times Q_{MCЭ}(t) \times Q_{Eth\text{№}2}(t) = \\ = 1,56 \times 10^{-14}$$

Расчёт потенциальных каналов утечки конфиденциальной информации №10 - №27 выполняется аналогичным образом.

$$P_{10}(t) = \dots = P_{12}(t) = P_{APMN\text{№}2}(t) \times P_{Eth\text{№}1}(t) \times Q_{MCЭ}(t) \times Q_{Eth\text{№}3}(t) = \\ = 2,3 \times 10^{-8}$$

$$P_{13}(t) = \dots = P_{15}(t) = P_{APMN\text{№}2}(t) \times Q_{Eth\text{№}1}(t) \times Q_{MCЭ}(t) \times Q_{Eth\text{№}3}(t) = \\ = 8,96 \times 10^{-13}$$

$$P_7(t) = \dots = P_9(t) = Q_{APM\text{ №}2}(t) \times Q_{Eth\text{ №}1}(t) \times Q_{MCЭ}(t) \times Q_{Eth\text{ №}3}(t) = \\ = 1,56 \times 10^{-14}$$

$$P_{19}(t) = \dots = P_{27}(t) = P_{APMN\text{№}3-5}(t) \times P_{Eth\text{№}2}(t) \times Q_{MCЭ}(t) \times Q_{Eth\text{№}3}(t) = \\ = 2,3 \times 10^{-8}$$

Для того, чтобы сделать вывод о выполнении требований конфиденциальности обрабатываемой в ТКС СН информации, необходимо сравнить полученные значения вероятностей с допустимым значением утечки защищаемой информации P_∂ . Допустимое значение утечки защищаемой информации P_∂ должно быть определено на этапе проектирования ТКС СН в соответствии с требованиями нормативных документов.

Угроза неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей ТС, можно считать неактуальной в случае, если полученные значения вероятности возникновения потенциальных каналов утечки конфиденциальной информации не превышает допустимое значение утечки защищаемой информации:

$$\begin{cases} P_1(t) < P_\partial \\ \dots \\ P_{27}(t) < P_\partial \end{cases}$$

В обратном случае, угроза признается актуальной, в связи с чем, необходимо предусмотреть доработку архитектуры ТКС СН или реализацию механизмов защиты от утечки конфиденциальной информации.

Если для анализируемой ТКС СН допустимое значение утечки защищаемой информации P_0 равно 10^{-5} , то вероятности возникновения потенциальных каналов утечки КИ №1 – №27 ($P_1(t), \dots, P_{27}(t)$) не превышают допустимое значение. Соответственно, для ТКС СН данной архитектуры угроза неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей технических средств, является неактуальной.

7 Методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств

В рамках дипломного проекта был разработан методический подход к выявлению потенциальных каналов утечки информации, возникающих в результате сбоев и неисправностей технических средств.

Целью данной методики является выявление потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, а также определение возможности их возникновения.

Методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, включает в себя четыре этапа:

- а) описание архитектуры и принципов работы ТКС СН;
- б) разработка и описание схемы информационных потоков;
- в) выявление потенциальных каналов утечки информации в ТКС СН;
- г) оценка вероятности возникновения потенциальных каналов утечки информации в ТКС СН.

На первом этапе «Описание архитектуры и принципов работы ТКС СН» должна быть рассмотрена структура ТКС СН, описан её состав, а также принципы работы ТКС СН. Для этого необходимо изучить техническую документацию на ТКС СН, в состав которой входят руководство по эксплуатации, электрические схемы различных типов (структурная, функциональная, принципиальная и др.) и другие документы. Результатом выполнения данного этапа является общее описание анализируемого объекта.

На втором этапе «Разработка и описание схемы информационных потоков» должна быть разработана схема информационных потоков ТКС СН в виде ориентированного графа, на основе которой должны быть описаны тракты прохождения информации. При описании схемы информационных потоков

необходимо использовать матрицы смежности ТС и обрабатываемой в них информацией, которые являются результатом выполнения данного этапа.

На третьем этапе «Выявление потенциальных каналов утечки информации в ТКС СН» должен быть проведен анализ матриц смежности ТС и обрабатываемой в них информацией с целью выявления всех возможных каналов утечки информации. Результатом выполнения данного этапа являются деревья событий, отражающие возможные каналы передачи информации, и список потенциальных каналов утечки информации, составленный на их основе.

На четвертом этапе «Оценка вероятности возникновения потенциальных каналов утечки информации в ТКС СН» должен быть определены технические средства, сбои и неисправности которых могут привести к возникновению потенциальных каналов утечки информации, а также проведен их анализ. Результатом выполнения данного этапа являются значения вероятности возникновения каждого потенциального канала утечки информации, которые позволяют сделать вывод об актуальности (неактуальности) угрозы неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей ТС.

Для наглядного представления последовательности действий выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, была использована UML-диаграмма деятельности, которая показывает поток переходов от одной деятельности к другой [12].

UML-диаграмма деятельности в общем случае состоит из состояний деятельности и действия, а также переходов между ними.

Состояние действия изображается прямоугольником с закругленными краями, внутри которого записывается выражение (действие). Состояние действия не детализируется и не может быть прервано.

Состояние деятельности имеет такое же обозначение, однако оно может быть детализировано и прервано.

Потоки обозначаются стрелками и представляют собой простой переход из одного состояния действия (деятельности) в другое. Помимо простых переходов, в UML-диаграммах деятельности выделяют параллельные и ветвящиеся переходы. Параллельные переходы позволяют отображать параллельно выполняемые действия (деятельности), для чего используется выделенная черта, служащая для разделения и объединения потоков. Ветвящиеся переходы отражают несколько вариантов действий (деятельностей) в зависимости от выполнения условия, для обозначения которого используется ромб.

UML-диаграмма последовательности действий выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, представлена на рисунке 13.

Также в виде UML-диаграммы деятельности была отображена последовательность действий при анализе ТС, сбои и неисправности которых могут привести к возникновению потенциальных каналов утечки информации в ТКС СН (см. рисунок 14).

Разработанная методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, позволяет выявлять все возможные каналы передачи защищаемой информации, а также исключает влияние человеческого фактора при разработке и анализе схемы информационных потоков ТКС СН.

Также стоит отметить возможность программной реализации алгоритма анализа схемы информационных потоков, и соответственно сокращение времени, необходимого для выявления всех потенциальных каналов утечки и расчёта вероятности их возникновения.

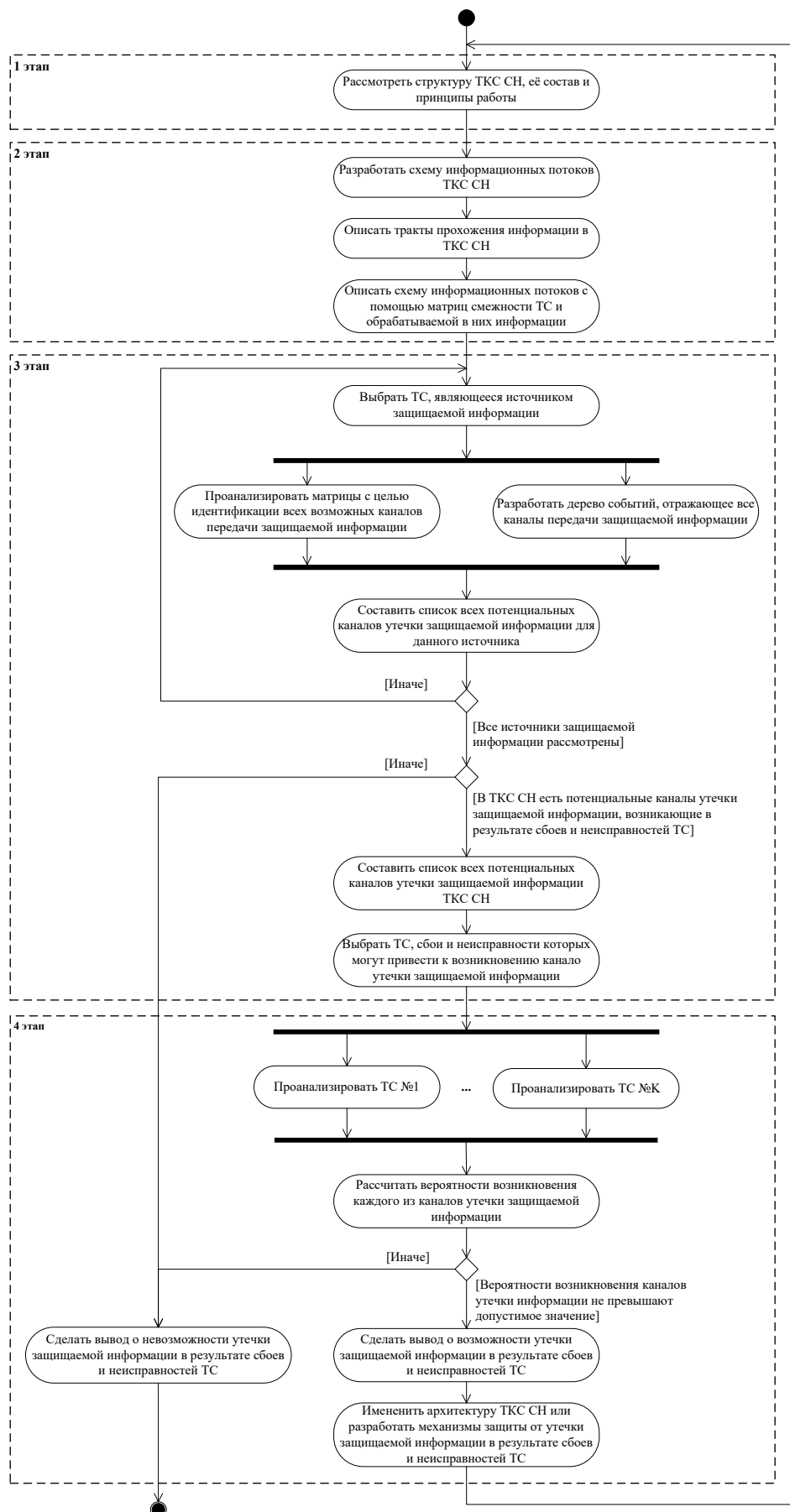


Рисунок 13 - UML – диаграмма последовательности действий выявления потенциальных каналов утечки информации в ТКС СН

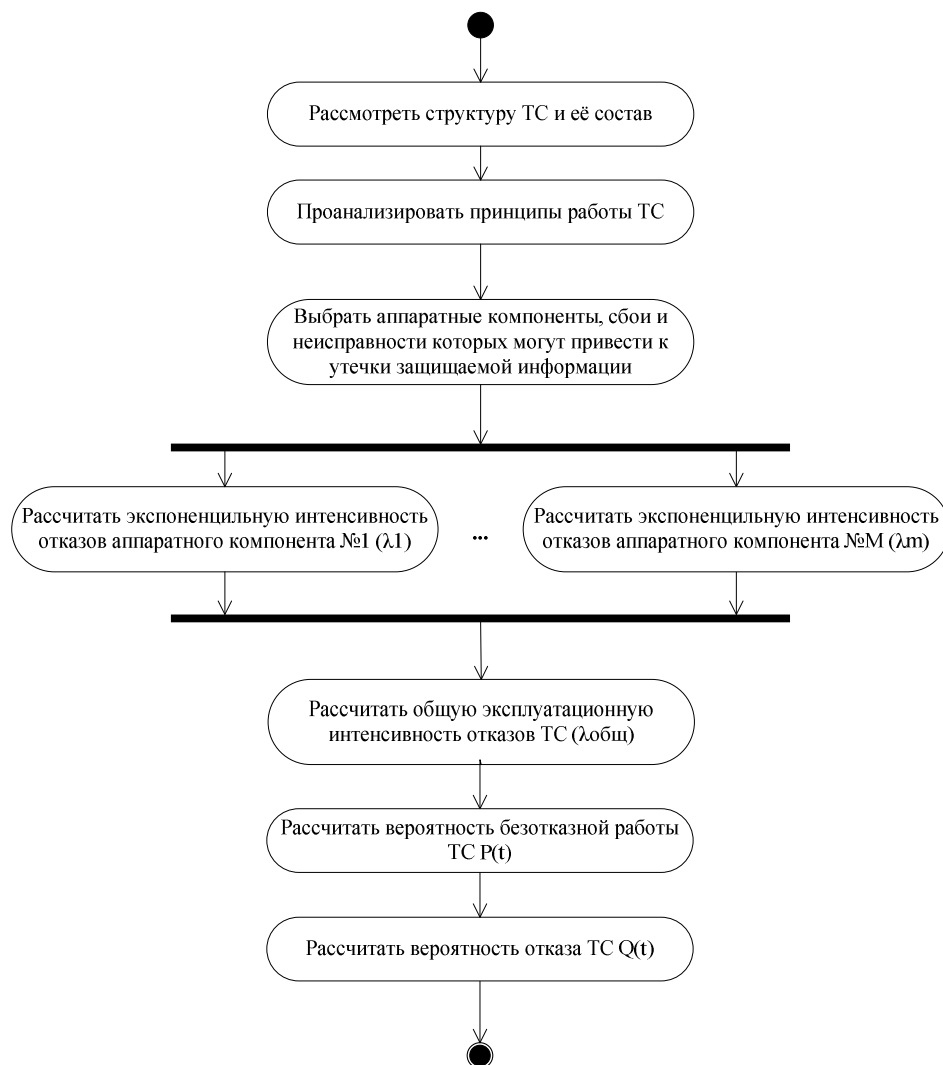


Рисунок 14 – UML – диаграмма последовательности действий анализа технических средств

Разработанная в рамках дипломного проекта методика позволяет выявить потенциальные каналы утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, а также оценить вероятность их возникновения. Сравнение заданного допустимого значения утечки защищаемой информации и полученных в результате анализа ТКС СН вероятностей позволяют сделать вывод об актуальности (неактуальности) угрозы неправомерного ознакомления с защищаемой информацией путём ошибочной передачи защищаемой информации пользователю, которому она не предназначена, в результате сбоев и неисправностей технических средств.

Таким образом, методика выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей

технических средств, может применяться при анализе ТКС СН на соответствие требованиям информационной безопасности.

ЗАКЛЮЧЕНИЕ

В рамках дипломного проекта был разработан методический подход к выявлению потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств.

Данный методический подход основан на разработке схемы информационных потоков ТКС СН, по результатам анализа которой выполняется построение деревьев событий возможных каналов передачи информации и выявление потенциальных каналов утечки информации в ТКС СН.

Оценка возможности возникновения потенциальных каналов утечки информации выполняется путём анализа технических средств, сбоев (неисправностей) которых могут привести к утечке защищаемой информации, и последующим расчётом их надёжности.

Таким образом, можно сделать вывод о возможном применении разработанной методики выявления потенциальных каналов утечки информации в ТКС СН, возникающих в результате сбоев и неисправностей технических средств, при анализе ТКС СН на соответствие требованиям информационной безопасности.

Техническое задание на выпускную квалификационную работу выполнено в полном объёме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. URL: <http://base.garant.ru/182535/> (дата обращения: 15.09.2016 г.).

2 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]. URL: <http://docs.cntd.ru/document/1200058320> (дата обращения: 15.09.2016 г.).

3 ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс]. URL: <http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010> (дата обращения: 15.09.2016 г.).

4 Проект методического документа ФСТЭК «Методика определения угроз безопасности в информационных системах». [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/812> (дата обращения: 13.10.2016 г.).

5 Руководящий документ ФСТЭК. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/295> (дата обращения: 03.09.2016 г.).

6 Банк данных угроз безопасности информации. ФСТЭК. [Электронный ресурс]. URL: <http://bdu.fstec.ru/> (дата обращения: 03.09.2016 г.).

7 ГОСТ 2.610-2006. Единая система конструкторской документации. Правила выполнения эксплуатационных документов. [Электронный ресурс]. URL: <http://docs.cntd.ru/document/1200045483> (дата обращения: 17.09.2016 г.).

8 ГОСТ 2.701-2008. Единая система конструкторской документации. Схемы. Виды и типы. Общие требования к выполнению. [Электронный ресурс]. URL: <http://docs.cntd.ru/document/gost-2-701-2008> (дата обращения: 17.09.2016 г.).

9 ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения. [Электронный ресурс]. URL: <http://docs.cntd.ru/document/gost-27-002-89> (дата обращения: 19.09.2016 г.).

10 Боровиков С.М. Расчёт показателей надёжности радиоэлектронных средств [Текст] : учеб.-метод. пособие / С. М. Боровиков, И. Н. Цырельчук, Ф. Д. Троян. – Минск : БГУИР, 2010. – 68 с.

11 Демидов А. А.. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Текст] : учебное пособие. — СПб : Университет ИТМО, 2015. – 70 с.

12 Буч Г. Язык UML. Руководство для пользователя [Текст] / Буч Г., Рамбо Д., Джекобсон А.: Пер с англ. – М. : ДМК, 2000 – 432 с.

13 Руководящий документ ФСТЭК. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/296> (дата обращения: 03.09.2016 г.).

14 Руководящий документ ФСТЭК. Средства вычислительной техники. Защита от несанкционированного доступа к информации. [Электронный ресурс]. URL: <http://fstec.ru/component/attachments/download/297> (дата обращения: 03.09.2016 г.).

15 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.

16 Catalyst 2960. [Электронный ресурс]. URL: http://www.solyar.ru/products_and_services/production/catalyst-2960/ws-c2960-8tc-1/ (дата обращения: 16.12.2016 г.).

17 Карпов А.П., Попова М.С. Влияние программного обеспечения на надежность информационной системы. [Электронный ресурс]. URL: http://alley-science.ru/domains_data/files/Journal_December_16/VLIYaNIE%20PROGRAMMN

[OGO%20OBESPEChENIYa%20NA%20NADEZhNOST%20INFORMACIONNOY%20SISTEMY.pdf](#) (дата обращения: 28.12.2016 г.)

Протокол проверки ВКР на оригинальность

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Методика выявления потенциальных каналов утечки информации в телекоммуникационных системах специального назначения, возникающих в результате сбоев и неисправностей технических средств» студента 6 курса М.С. Поповой специальности 100502 Информационная безопасность телекоммуникационных систем.

Руководитель ВКР Боровиков Алексей Юрьевич

Информация о документе:

Имя исходного файла: ВКР_Попова.docx

Имя компании: Пензенский гос. Университет

Тип документа: Прочее

Имя документа: Группа 11ПТ1 ВКР Попова М.С.

Модули поиска: Университетская библиотека онлайн, Модуль поиска ЭБС "Лань", Диссертации и авторефераты РГБ, Модуль поиска ЭБС БиблиоРоссика, Кольцо вузов, Пензенский гос. Университет. Цитирования

Текстовые

СТАТИСТИКИ:

Индекс читаемости: сложный

Неизвестные слова: в пределах нормы

Макс. длина слова: в пределах нормы

Большие слова: в пределах нормы

Оригинальные блоки: 93,76%

Заимствованные блоки: 5,95%

Заимствование из "белых" источников: 0,29%

Итоговая оценка оригинальности: **94,05%**



А.Ю. Боровиков