Акционерное общество

«Концерн воздушно-космической обороны «Алмаз-Антей»

АКЦИОНЕРНОЕ ОБЩЕСТВО «НАЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ПРИБОРОСТРОЕНИЯ ИМЕНИ В.В. ТИХОМИРОВА»

(АО «НИИП ИМЕНИ В.В. ТИХОМИРОВА»)

УТВЕРЖДАЮ

Генеральный директор

АО «НИИП имени В.В. Тихомирова»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ю.И. Белый

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

по эскизному проекту СЧ ОКР

«Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М»

Шифр «ЕКУТС-Б-СОЦ-ПО»

Начальник НИО-1 – Главный конструктор

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.А. Поисов

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020г.

г. Жуковский 2020

**РЕФЕРАТ**

Пояснительная записка по эскизному проекту СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М» выполнена на 116 страницах, содержит 9 таблиц, 15рисунков, 33 приложения.

В пояснительной записке изложены результаты исследования проведенного на этапе эскизного проектирования аппаратно-программного комплекса для модуля СОЦ из состава комплексного тренажера. Приводятся:

- назначение и область применения аппаратно-программного комплекса;

- описание и обоснование конструкции аппаратно-программного комплекса приведение перечня составных частей и структурной схемы;

- описана организация работы тренажера с применением аппаратно-программного комплекса, приведен перечень основных задач с их описанием.

Так же приводятся сквозной план-график работ по СЧ ОКР и технико-экономическое обоснование стоимости проведения СЧ ОКР и стоимости серийного производства аппаратно-программного комплекса.

СОДЕРЖАНИЕ

Введение 9

1 Назначение и область применения 11

1.1 Назначение единого комплекса учебно-тренировочных средств ЗРК 9К317М 11

1.2 Основные задачи, выполняемые единым комплексом учебно-тренировочных средств ЗРК 9К317М 12

1.3 Состав единого комплекса учебно-тренировочных средств ЗРК 9К317М 13

1.4 Состав и структурная схема комплексного тренажера 13

1.5 Назначение и основные задачи решаемые, на АРМО модуля тренажера СОЦ ПО 15

1.6 Назначение и основные задачи решаемые, на РМИ модуля тренажера СОЦ ПО 16

1.7 Состав и структура АРМО реального СОЦ 9С18М1-3

2. Описание и обоснование выбранной конструкции. 18

2.1 Состав аппаратуры модуля СОЦ ПО 18

2.1.1 Состав и структура аппаратуры АРМО 18

2.1.2 Состав и структура аппаратно-программного комплекса АРМ инструктора комплексного тренажера 21

2.2 Описание составных частей СОЦ ПО 22

2.2.1 Описание ЭВМ АРМО 22

2.2.2 Описание ЭВМ РМИ 25

2.2.3 Описание ЭВМ имитатора аппаратуры СОЦ 26

2.2.4 Описание УЭВМ типа РАМЭК-113 24

2.2.5 Сетевой коммутатор 26

2.3 Обоснование выбора и описание операционной системы. 27

2.4 Обоснование выбора и описание среды программирования 33

2.5 Обоснование выбора и описание средств защиты от несанкционированного доступа 38

2.5.1 Перечень требуемых средств защиты от несанкционированного доступа 38

2.5.2 Описание средств защиты от несанкционированного доступа 42

2.5.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа 43

2.5.2.2 Меры по управление доступом субъектов доступа к объектам доступа 45

2.5.2.3 Меры по ограничению программной среды 48

2.5.2.4 Меры по защите машинных носителей информации 49

2.5.2.5 Меры по регистрации событий безопасности 50

2.5.2.6 Меры по антивирусной защиты. 52

2.5.2.7 Меры по обнаружению вторжений 52

2.5.2.8 Меры по контролю (анализу) защищенности информации 52

2.5.2.9 Меры по обеспечению целостности информационной системы и информации 53

2.5.2.10 Меры по обеспечению доступности информации 55

2.5.2.11 Меры по защите среды виртуализации 56

2.5.2.12 Меры по защите технических средств 58

2.5.2.13 Меры по защите информационной системы, ее средств, систем связи и передачи данных 58

2.5.3 Перечень защищаемых ресурсов АРМ ИКТ 64

3. Основные технические характеристики АРМ ИКТ 66

3.1 Основные ТТХ АРМ ИКТ 66

3.2 Основные задачи, решаемые в АРМ ИКТ, с кратким описанием 66

4. Описание организации работы с применением АРМ ИКТ 79

4.1 Описание общего процесса функционирования 79

4.1.1 Взаимодействие и принцип работы составных частей АРМ ИКТ при подготовке комплексного тренажера к тренировке 79

4.1.2 Взаимодействие и принцип работы составных частей АРМ ИКТ в режиме комплексной тренировки 80

4.1.3 Взаимодействие и принцип работы составных частей АПК в режиме комплексной тренировки 80

4.1.4 Работа администратора безопасности информации 82

4.2 Описание типовых сценариев тренировки 84

4.2.1 Общие предложения по вариантам налета СВН 84

4.2.2 Предлагаемые варианты налетов средств воздушного нападения противника 86

4.2.2.1 Сценарий 1 удар по ЗРК одиночным самолетом F-35A 89

4.2.2.2 Сценарий 2 удар по ЗРК одиночным самолетом F-35A совершающим маневр змейка 89

4.2.2.3 Сценарий 3 удар по ЗРК одиночным самолетом F-35A совершающим маневр кабрирование (пикирование) 90

4.2.2.4 Сценарий 4 удар по ЗРК группой самолетом F-35A построением ромб (квадрат). 90

4.2.2.5 Сценарий 5 удар по ЗРК группой самолетом F-35A построением клин 90

4.2.2.6 Сценарий 6 удар по ЗРК группой самолетом F-35A построением фронт 91

4.2.2.7 Сценарий 7 удар по ЗРК зависающим вертолетом 91

4.2.2.8 Сценарий 8 удар по ЗРК имитацией авианалета 91

4.2.2.9 Сценарий 9 удар по ЗРК имитацией авианалета 95

4.2.2.10 Сценарий 10 осуществление доразведки средств ЗРК с помощью БПЛА с последующим нанесением удара самолетами F-35A, вооруженными планирующими бомбами 98

5 Расчеты, подтверждающие работоспособность и надежность АРМ ИКТ 102

6 Ожидаемые технико-экономические показатели 104

6.1 Технико-экономическое обоснование стоимости 104

6.1.1 Ожидаемые стоимостные показатели этапов СЧ ОКР 104

6.1.2 Ожидаемые стоимостные показатели серийного образца 114

7 Уровень стандартизации и унификации 115

7.1 Унификация аппаратурного состава АРМ ИКТ с аппаратурным составом ПБУ ПО, РПН ПО, СОУ ПО, ЦВС ПУ, ЦВС ПЗУ 115

Заключение 116

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АПМДЗ – аппаратно-программный модуль доверенной загрузки;

АРМ – автоматизированное рабочее место;

АРМ АБИ – автоматическое рабочее место администратора безопасности информации;

АРМ-ИКТ – аппаратно-программный комплекс для модуля АРМ инструктора комплексного тренажера;

АРМО – автоматизированное рабочее место оператора;

АФК – автоматизированный функциональный контроль;

БЛА – беспилотный летательный аппарат;

БПЛА – беспилотный летательный аппарат

ВКП – вышестоящий командный пункт

ВМЦ – видеомонитор цветной

ЗРК – зенитный ракетный комплекс

ЗРС – зенитная ракетная система

ЗУР – зенитная управляемая ракета

КУСПП – Комбинированное устройство стабилизированного питания и преобразования

ЛВС – локальная вычислительная сеть

ЛЦ – ложная цель

ОС – операционная система

ОС СН – операционная система специального назначения

ПАБ – планирующая авиационная бомба

ПБУ – пункт боевого управления;

ПВО – противовоздушная оборона

ПЗУ – пуско-заряжающая установка;

ПКИ – покупные комплектующие изделия

ПО – программное обеспечение

ПС – программное средство

ПУ – пусковая установка;

РКД – расчетно-калькуляционные материалы

РЛС – радиолокационная станция

РПН – радиолокатор подсвета и наведения;

РТР – радиотехническая разведка

РЭБ – ПРР противорадиолокационными ракетами

САВЗ – средства антивирусной защиты

СВН – средства воздушного нападения

СЗИ НСД – средства защиты информации от несанкционированного доступа

СОУ – самоходная огневая установка;

СОЦ – станция обнаружения целей;

СПО – системное программное обеспечение

СЧ – составная часть;

ТП – технический проект

ТТХ – тактико-технические характеристики

УВМ – универсальная вычислительная машина

ФИО – фамилия, имя, отчество.

ФПО – функциональное программное обеспечение

ЦКМ – цифровая карта местности

ЭВМ – электронная вычислительная машина

ЭПР – эффективная площадь рассеивания

**Введение**

Эскизный проект на аппаратно-программный комплекс для модуля тренажера оператора СОЦ, входящего в состав комплексного тренажера ЗРК 9К317М, выполняется в соответствии с техническим заданием на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплексного учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» (Приложение 1).

Единый комплексный тренажер предназначен для подготовки подразделений противовоздушной обороны с целью приобретения и совершенствования навыков боевой работы личного состава подразделений, вооруженных зенитными ракетными комплексами средней дальности 9К317М «Бук-М3».

Модуль СОЦ ПО из состава единого комплексного тренажера предназначен для:

- для обучения, тренировки и совершенствования навыков боевой работы старшего оператора и оператора изделия 9С18М1-3 в части взаимодействия с АРМО;

- обеспечения работы как в составе единого тренажерного комплекса, так и в автономном режиме, с возможностью самостоятельно выбирать сценарии для тренировки и создавать новые;

- обеспечения возможности наблюдения, записи и протоколирования действий обучаемых для дальнейшей оценки и воспроизведения;

- автоматического формирования оценки знаний, умений, действий и навыков обучаемых расчетов;

- ведения занятий по специальной и технической подготовке с расчетами боевых средств;

- подготовки справочных, учебных и учебно-методических материалов, компьютерных лекций, презентаций, тестов для обеспечения проведения основных видов занятий.

**1 Назначение и область применения**

**1.1 Назначение единого комплекса учебно-тренировочных средств ЗРК 9К317М**

Единый комплекс учебно-тренировочных средств ЗРК 9К317М предназначен для проведения эффективной подготовки и обучения расчетов станции обнаружения целей (СОЦ) 9С18М1-3, пункта боевого управления (ПБУ) 9С510М, самоходной огневой установки (СОУ) 9А317М, радиолокатора подсвета и наведения (РПН) 9С36М, пусковой установки (ПУ) 9А316М, пуско-заряжающей установки (ПЗУ) 9А316, как в высших военных учебных заведениях ПВО, так и в действующих войсковых частях, на полигонах, в учебных центрах с целью формирования и поддержания у операторов навыков ведения боевой работы по отражению ударов средств воздушного нападения (СВН) в различных условиях воздушной и помеховой обстановки, проведения погрузочно-разгрузочных работ, тренировки механиков-водителей гусеничных машин, а также для моделирования результатов боевых действий расчетов и тренировки с целью поддержания и совершенствования приобретенных навыков как в составе всех боевых средств ЗРК, так и автономно.

Особенности использования – отсутствие расхода моторесурса боевых машин, больших материальных затрат, требуемых при проведении тренировочных работ на боевых машинах, а также полная имитация пуска ракет и уничтожения имитируемых целей, возможность создания налета любой сложности.

Изделие разрабатывается на современной элементной базе с применением компьютеров в качестве основных вычислительных средств. Подобное техническое решение позволяет значительно сократить расходы на ПКИ, номенклатуру ПКИ, а также уменьшить трудоемкость изготовления и обслуживания единого комплекса учебно-тренировочных средств ЗРК 9К317М.

**1.2 Основные задачи, выполняемые единым комплексом учебно-тренировочных средств ЗРК 9К317М**

Единый комплекс учебно-тренировочных средств ЗРК 9К317М обеспечивает:

* обучение и индивидуальную тренировку расчетов боевых средств ЗРК 9К317М;
* выполнение расчетами СОУ, ПУ, ПЗУ всех операций при проведении заряжания и разряжания изделий;
* выполнение расчетами ЗРК 9К317М всех операций боевой работы во всех режимах обзора воздушного пространства, обнаружения, сопровождения воздушных целей и стрельбы ЗУР;
* имитацию радиолокационных сигналов отражаемых от имитируемых целей, метеообразований и местных предметов с учетом рельефа местности, заданных погодных условий, заданной помеховой обстановки, типов и параметров имитируемых целей, режимов работы средств единого комплекса учебно-тренировочных средств ЗРК 9К317М;
* имитацию появления одиночных и групповых воздушных целей всех типов (бомбардировщик, истребитель, штурмовик, вертолет, беспилотный летательный аппарат, крылатая ракета и т.д.) поступающих с произвольных направлений в зоне обнаружения радиолокационных средств ЗРК, в том числе постановщиков помех;
* моделирование визуальной обстановки, соответствующей имитируемым условиям стрельбы на средствах отображения информации рабочих мест боевых средств ЗРК, в том числе визуального образа целей и метеообразований ОЭС-БУК;
* имитационную стрельбу ЗУР в диапазоне боевых возможностей по имитированным воздушным целям и имитацию их поражения с вероятностью, соответствующей конкретному типу цели и условиям ее обстрела.

Интерфейсы рабочих мест инструктора комплексного тренажера и инструкторов тренажеров ПБУ, СОЦ, СОУ, РПН, ПУ (ПЗУ) должны использовать готовые сценарии налета, а также иметь возможность создавать свои сценарии.

Таким образом, обучение на тренажере максимально приближено к боевой и учебной обстановке.

**1.3 Состав единого комплекса учебно-тренировочных средств ЗРК 9К317М**

В состав единого комплекса учебно-тренировочных средств ЗРК 9К317М входят:

1. Комплексный тренажер
2. Тренажер механиков-водителей гусеничных машин;
3. Учебно-тренировочный комплект по отработке навыков заряжания/разряжания изделий в составе:

* модуль заряжания/разряжания самоходной огневой установки 9А317М;
* модуль заряжания/разряжания пусковой установки 9А316М;
* модуль заряжания/разряжания пуско-заряжающей установки 9А316;
* габаритный массовый макет ЗУР 9М317М;
* габаритный массовый макет ЗУР 9М317.

1. Комплект учебных плакатов.

**1.4 Состав и структурная схема комплексного тренажера**

В состав комплексного тренажера входят:

- модуль автоматизированного рабочего места инструктора единого комплекса учебно-тренировочных средств ЗРК 9К317М;

- модуль ПБУ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М с рабочим местом инструктора;

- модуль СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М с рабочим местом инструктора;

- до 6 модулей СОУ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М с рабочим местом инструктора;

- до 6 модулей РПН из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М с рабочим местом инструктора;

- до 8 модулей ПУ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М;

- до 8 модулей ПЗУ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М.

Примечания:

1 Общее количество модулей СОУ и РПН в едином комплексе учебно-тренировочных средств ЗРК 9К317М не более 6.

2 Общее количество модулей ПУ и ПЗУ в едином комплексе учебно-тренировочных средств ЗРК 9К317М не более 8.

Техническая связь между модулями единого комплекса учебно-тренировочных средств ЗРК 9К317М обеспечивается проводной линией связи Ethernet 100/1000 BASE-T.

Речевая связь между модулями единого комплекса учебно-тренировочных средств ЗРК 9К317М обеспечивается изделием 1В133, которое обеспечивает внутреннюю телефонную связь между всеми абонентами модулей (количество абонентов зависит от исполнения) и внешнюю телефонную дуплексную связь по двухпроводным линиям связи длиной до 15 км.

Структурная схема тренажера ЗРК показана на рисунке 1.



Рисунок 1 - структурная схема комплексного тренажера ЗРК

**1.5 Назначение и основные задачи решаемые, на АРМО модуля тренажера СОЦ ПО**

Основное назначении, это имитация работы реальной аппаратуры СОЦ 9С18М1-3 во всех штатных режимах как при автономной работе, так и при работе в составе комплекса учебно-тренировочных средств ЗРК 9К317М ЕКУТС-Б по единой воздушной обстановке.

Модуль СОЦ ПО представляет собой совокупность программных средств, ЭВМ и аппаратных средств управления и коммутации и предназначен для:

- максимального приближения работы тренажера к работе реального СОЦ;

- проведения автоматизированного функционального контроля модуля СОЦ, отображения результатов на автоматизированном рабочем месте инструктора СОЦ и их передачу на рабочее место инструктора комплексного тренажера;

- обеспечения автоматического учета и протоколирования действий обучаемых расчетов, подготовку отчета о тренировке и оценку знаний и умений обучаемых расчетов, выдачу результатов проверки на рабочее место инструктора СОЦ и комплексного тренажера;

- обеспечения индикации идентичной индикации на рабочих местах реальной СОЦ;

- имитации и отображения радиолокационной воздушной обстановки посредством ряда типовых задач, количество и содержание которых определяется посредством оперативного изменения воздушной обстановки инструктором в следующем объеме:

- начало движения цели;

- исключение цели из налета;

- ввод новых целей;

- начало (окончание) маневра;

- начало (окончание) постановки помехи;

- корректировка отдельных параметров целей.

- имитацию и отображение радиолокационной обстановки на основе исходных параметров тренировки и воздушной обстановки, принятой от рабочего места инструктора комплексного тренажера, с привязкой к карте местности и с учетом:

- рельефа местности;

- заданных погодных условий;

- захвата метеообразований;

- заданной помеховой обстановки;

- дальности положения, ракурса и типа цели;

- режима работы СОЦ;

- пропадания низколетящих целей за местными предметами;

- изменения уровня отраженного сигнала в зависимости от дальности;

- амплитудной флуктуации сигналов цели по случайному закону;

- появления ложных целей и местных предметов с привязкой к карте местности;

- различных построений одиночных и групповых целей;

- признаков госопознавания аэродинамических целей.

**1.6 Назначение и основные задачи решаемые, на РМИ модуля тренажера СОЦ ПО**

Рабочее место инструктора СОЦ ПО представляет собой совокупность программных средств, ЭВМ и аппаратных средств управления и коммутации и предназначен для:

- приема и отображения исходных параметров воздушной обстановки от рабочего места инструктора комплексного тренажера по согласованному протоколу информационного сопряжения;

- выдачи параметров и режимов работы тренажера, этапов боевой работы на рабочее место инструктора комплексного тренажера по согласованному протоколу информационного сопряжения;

- задания исходных параметров тренировки при автономной рабочее тренажера СОЦ, выбор и отображение цифровой карты местности из заданного набора, установку координат точки стояния, установку параметров фоновой обстановки;

- обеспечения задания воздушной обстановки посредством ряда типовых задач с установкой необходимых параметров;

- обеспечения защиты от изменения параметров базового набора типовых заданий на тренаж;

- имитацию воздушной обстановки с максимальным количеством одновременно имитируемых целей до 80 штук, с учетом типов целей и государственной принадлежности и обеспечением имитации сброса целей с сопровождения, маневров целей, задания и изменения в процессе тренировки помеховых и погодных условий, а так же имитации ложных целей;

- создание, сохранение и последующую загрузку инструктором новых заданий на тренаж;

- загрузку, сохранение и удаление наборов цифровых карт местности для тренировки боевого расчета СОЦ.

**1.7 Состав и структура АРМО изделия 9С18М1-3**

В состав автоматизированного рабочего места оператора изделия 9С18М1-3 входят:

- видеомонитор цветной, ВМЦ-51 ЖКМ с диагональю экрана 51 см, для отображения одного и растров обзора РЛС, отображения табло «меню» позволяющего оперативно управлять режимами работы РЛС и отображением получаемой от не информации;

- видеомонитор цветной малогабаритный ВМЦМ-21.2.1 с диагональю экрана 25 см., для опционального вывода растров обзора РЛС и дополнительной информации для оператора;

- клавиатура малогабаритная КЛ-85, для ввода данных и переключения режимов;

- манипулятор графической информации МГ1, для навигации по командам «меню» и управления графическим курсором.

Структурная схема представлена на рисунке 2.



Рисунок 2. Структурная схема АРМО изделия 9С18М1-3.

На ЭВМ «БАГЕТ-23В» функционирует программное обеспечение, которое содержит алгоритмы управления обзором, первичной и вторичной обработки, обмена и выдачи информации на АПД для передачи на КП и видеомониторы, организации работы и контроля РЛС, тренировки оператора, расчета коэффициентов горизонтирования.

**2. Описание и обоснование выбранной структуры модуля СОЦ**

В данном разделе приведены состав и структурная схема модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М. Дополнительно приведены предложения по составным частям изделия, в т.ч. взаимодействующим с АПК для АРМ инструктора комплексного тренажера. Структурная схема, состав аппаратуры и выбор ее исполнения может изменяться и дополняться на этапе ТП с согласованием с головным исполнителем ОКР.

**2.1 Состав аппаратуры модуля СОЦ ПО**

Основными требованиями ТЗ на разработку является использование для реализации одной или нескольких унифицированных ЭВМ, в целях уменьшения стоимости аппаратуры и простоты ее обслуживания, ограничения по электропитанию, а так же физическое повторение органов управления и средств индикации реального СОЦ. В связи с этим предлагается использование следующей структурной схемы, представленной на рисунке 3.



Рисунок 3. Структурная схема модуля тренажера СОЦ.

Реализация и линии связи подключения имитатора блока 07.26.02 определяется на этапе ТП и согласуется с головным исполнителем ОКР.

**2.1.1 Состав аппаратуры АРМО**

В целях максимального приближения облика тренажера к реальному АРМО используется штатная система индикации и органы управления, состав которой представлен в разделе 1.7 данного документа. В состав АРМО добавляется УВМ РАМЭК 113, на котором будет функционировать адаптированное программное обеспечение, используемое на реальной ЭВМ «БАГЕТ 23В». При разработке и отладке вместо штатных мониторов, клавиатуры и графического манипулятора могут быть использованы любые другие мониторы и средства взаимодействия с оператором имеющие те же линии связи или адаптированные аналоги.

**2.1.2 Состав аппаратуры РМИ**

Рабочее место инструктора является максимально унифицированным с РМИ других модулей входящих в состав комплексного тренажера. В состав входят следующие составные части:

- ЭВМ РМИ на базе УВМ РАМЭК 113;

- специальное и системное программное обеспечение, поставляемое в составе ЭВМ;

- монитор жидкокристаллический не менее 25 дюймов соединяемый с ЭВМ по цифровому кабелю DVI-D или HDMI, 2 шт.;

- USB-клавиатура;

- USB-манипулятор, мышка, трекбол или любой другой графический манипулятор.

**2.1.3 Состав прочей аппаратуры СОЦ ПО**

Так же в состав аппаратуры СОЦ ПО входит ЭВМ на базе УВМ РАМЭК 113 с специальным и системным программным обеспечением, обеспечивающим имитацию реальной аппаратуры, используемой при работе СОЦ. А так же сетевой коммутатор для обеспечения обмена информации между РМИ, АРМО и РМИ КТ по лини связи Ethernet 10/100/1000 Base-T.

На блоке 07.26.02 из состава СОЦ содержатся кнопки включения РЛС и управления режимами ее работы, а так же табло с индикаторами функционирующих режимов. Необходимость и вариант исполнения имитатора данного блока в итоговом тренажере определяется на этапе ТП и согласуется с головным исполнителем ОКР. На этапе разработки и отладки программного обеспечения СОЦ ПО используется программный имитатор данного блока, функционирующий на УВМ АРМО.

Полный состав используемой в модуле СОЦ ПО аппаратуры приведен в таблице 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № пп | Наименование, индекс | Обозначение | Кол-во | Примечания |
| 1 | Видеомонитор цветной  ВМЦ-51ЖКМ | НВИТ.467846.136 | 1 | Серийное |
| 2 | Видеомонитор цветной  ВМЦ-21.2.1 | НВИТ.467846.136 | 1 | Серийное |
| 3 | Видеомонитор цветной | - | 2 | Тип согласуется с Заказчиком на этапе ТП |
| 3 | ЭВМ на базе УВМ  типа РАМЭК 113 | - | 3 |  |
| 4 | Клавиатура малогабаритная КЛ-85 | ТЕЦА.468312.028-08.05 | 1 | Серийное |
| 5 | Манипулятор графической информации МГ1 | ТЕЦА.468312.028-08.05 |  | Серийное |
| 6 | USB-клавиатура | - |  | Тип согласуется с Заказчиком на этапе ТП |
| 7 | USB-графический манипулятор | - |  | Тип согласуется с Заказчиком на этапе ТП |
| 8 | Коммутатор/экран локальной вычислительной сети | ТЕЦА.468367.026-02.03 | 1 | Тип уточняется и согласуется с Заказчиком на этапе ТП |
| 9 | Имитатор блока 07.26.02 | - |  | Наличие и тип уточняется и согласуется с Заказчиком на этапе ТП |

Таблица 1. Состав аппаратуры модуля СОЦ ПО.

**2.2 Описание составных частей СОЦ ПО**

**2.2.1 Описание ЭВМ АРМО**

ЭВМ АРМО предназначена для решения информационных задач, задач управления аппаратурой модуля, сопряжения с внешними абонентами, сбора и обработки информации с последующим выводом данных на два видеомонитора.

ЭВМ АРМО

– Содержит штатное ПО Багет-23В комплекса СОЦ, адаптированное для работы на УВМ РАМЭК 113.

- В качестве линий связи используется Ethernet, штатные линии связи Багет-23В эмулируются через протоколы UDP и TCP/IP.

- Обеспечивает взаимодействие с обучаемым посредством штатной клавиатуры КЛ-85 и штатного графического манипулятора МГ1.

- Отображает на мониторах штатное изображение процессов, проходящих в комплексе СОЦ.

ЭВМ АРМО будет разрабатываться на базе УВМ РАМЭК 113 путем дополнения ЭВМ требуемыми платами расширения для дооснащения УВМ РАМЭК 113 нужным количеством каналов связи Ethernet, Manchester, USB, средствами доверенной загрузки и установки СПО для обеспечения выполнения функций АРМ АБИ. ЭВМ для РМИ по аппаратному составу будет полностью унифицирована с ЭВМ для изготовления АРМ-ИКТ.

Общее описание ЭВМ типа РАМЭК-113 приведено в 2.2.4.

**2.2.2 Описание ЭВМ РМИ**

ЭВМ РМИ предназначена для выполнения задач управления процессом тренажа, протоколирования и наблюдения за действиями операторов модулей тренажера СОЦ ПО с последующим отображением данных на двух ЖК-мониторах.

ЭВМ РМИ в том числе обеспечивает:

- сбор и обработку данных о процессе работы, состоянии и действиях обучаемого.

- сохранение, загрузку, поиск требуемых данных, отображение ранее зарегистрированных данных и процесса работы тренажера в режиме реального времени на двух ЖК-мониторах.

- передачу данных на ЭВМ имитатора аппаратуры СОЦ, в том числе параметры ВО, координаты ТС, курс, крен, тангаж, данные по рельефу и метеоусловиям, помеховую обстановку

- прием и регистрацию действия обучаемого, а также трассы целей.

ЭВМ РМИ будет разрабатываться на базе УВМ РАМЭК 113 путем дополнения ЭВМ требуемыми платами расширения для дооснащения УВМ РАМЭК 113 нужным количеством каналов связи Ethernet, Manchester, USB, средствами доверенной загрузки и установки СПО для обеспечения выполнения функций АРМ АБИ. ЭВМ для РМИ по аппаратному составу будет полностью унифицирована с ЭВМ для изготовления АРМ-ИКТ.

Общее описание ЭВМ типа РАМЭК-113 приведено в 2.2.4.

**2.2.3 Описание ЭВМ имитатора аппаратуры СОЦ**

ЭВМ Имитатор аппаратуры СОЦ предназначен для имитации данных, которые поступают на вход ЭВМ АРМО на основании данных, которые поступают от ЭВМ РМИ и выбранных режимах, которые приходят с РМИ АРМО.

ЭВМ Имитатор аппаратуры СОЦ

- Получает информацию от ЭВМ РМИ о текущей ВО, координатах ТС, курсе, крене, тангаже, помеховой обстановке, рельефе, метеоусловиях, отказах аппаратуры и режимах тренажа.

- На основании данных, полученных от ЭВМ РМИ, ЭВМ имитатора аппаратуры СОЦ формирует пакеты данных для ЭВМ АРМО.

- Получает информацию от ЭВМ АРМО о действиях оператора и соответствующих командах управления, в соответствии с которыми меняет имитируемые данные.

ЭВМ Имитатор аппаратуры СОЦ будет разрабатываться на базе УВМ РАМЭК 113 путем дополнения ЭВМ требуемыми платами расширения для дооснащения УВМ РАМЭК 113 нужным количеством каналов связи Ethernet, Manchester, USB, средствами доверенной загрузки и установки СПО для обеспечения выполнения функций АРМ АБИ. ЭВМ для РМИ по аппаратному составу будет полностью унифицирована с ЭВМ для изготовления АРМ-ИКТ.

Общее описание ЭВМ типа РАМЭК-113 приведено в 2.2.4.

**2.2.4 Описание УЭВМ типа РАМЭК-113**

УВМ РАМЭК-113 предназначена для эксплуатации в качестве самостоятельного изделия или в составе комплексов аппаратуры, размещенных на колесных и гусеничных шасси, не имеющих противопульного бронирования и артиллерийскоминометного вооружения при автономном или централизованном обслуживании в условиях круглосуточной или сменной работы, с перерывами на техническое обслуживание в соответствии с руководством по эксплуатации.

По устойчивости к воздействию климатических и механических факторов УВМ относится к группе 1.3 ГОСТ РВ 20.39.304–98 (без работы на ходу).

Внешний вид ЭВМ приведен на рисунке 4.



Рисунок 4 – внешний вид ЭВМ типа РАМЭК-113

Общие функциональные характеристики базовой ЭВМ типа РАМЭК-113 приведены в таблице 2.

Таблица 2 – основные ТТХ базовой ЭВМ типа РАМЭК-113

|  |  |
| --- | --- |
| **Характеристика** | **Значение** |
| Процессор | Intel Core i7-4770S 3.1 ГГц, 8 MБ |
| Память | 16 Гб |
| Видео контроллер | Дискретный, объём видеопамяти от 1Gb |
| Накопитель | SSD, 2х512 Гб |
| Внешние интерфейсы | 3хRS-232, 1хRS-232/422/485, 8xUSB 2.0, 1xVGA, 1xDVI-D, 2х10/100/1000 Base-T/TX, 1xMic In, 1xSpk Out |
| Возможность установки средств НСД | Есть |
| Совместимость с операционными системами | Astra Linux SE 1.4, 1.5, 1,6 Microsoft Windows® 7, 10 |
| Габариты ШхВхГ, мм | 420х88х380 |
| Способ монтажа | 19” стойка |
| Питание | Постоянный ток, 27В |
| Время наработки на отказ | 4000 часов |

**2.2.5 Сетевой коммутатор**

Коммутатор Ethernet предназначен для информационного обмена между электронными блоками в стандартах Ethernet 10/100/1000 Base-T, Ethernet 1000 Base-BX и обеспечивает:

- объединение в единую информационную сеть устройств, комплексов и систем с помощью каналов передачи информации через физическую среду «Витая пара»;

- возможность управления процессом коммутации с задачей конкретного маршрута коммутации для потока данных;

- вывод на лицевую панель индикации состояния работы сети признаков наличие связи, установления скорости обмена 10/100/1000 Мбит/с, признака передачи данных.

Коммутатор Ethernet содержит:

- 16 каналов передачи данных типа Ethernet 10/100/1000 BASE-TX;

- процессор управления;

- соединители;

- индикаторы;

Электропитание коммутатора обеспечивается от источника постоянного тока напряжением от 11 В до 36 В. Потребляемая мощность не более 50 Вт. Время готовности не более 1 минуты. Время непрерывной работы не менее 24 часов. Средняя наработка на отказ 10000 часов. Масса не более 3 кг.

**2.3 Обоснование выбора и описание операционной системы.**

В соответствии с ТЗ на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля АРМ инструктора комплексного тренажера из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М» в качестве типа операционной системы указано использовать операционную систему типа «Astra Linux»

Операционная система создается группой компаний Astra Linux — одним из лидеров российского рынка информационных технологий в области разработки программного обеспечения и средств защиты информации, в том числе операционных систем семейства Astra Linux и платформ виртуализации. На рынке — с 2008 года. В команде Astra Linux сегодня трудится более 250 высокопрофессиональных разработчиков и сотрудников техподдержки.

Astra Linux — операционная система специального назначения на базе ядра Linux, созданная для комплексной защиты информации и построения защищённых автоматизированных систем. Востребована в первую очередь в российских силовых ведомствах, спецслужбах и государственных органах. Обеспечивает степень защиты обрабатываемой информации до уровня государственной тайны «особой важности» включительно. Сертифицирована в системах сертификации средств защиты информации Минобороны, ФСТЭК и ФСБ России. Включена в Единый реестр российских программ Минкомсвязи России.

Производителем разрабатывается базовая версии Astra Linux — Common Edition (общего назначения) и её модификация Special Edition (специального назначения):

- издание общего назначения — Common Edition — предназначено для среднего и малого бизнеса, образовательных учреждений;

- издание специального назначения — Special Edition — предназначено для автоматизированных систем в защищённом исполнении, обрабатывающих информацию со степенью секретности «совершенно секретно» включительно.

Особенности версии Astra Linux Special Edition:

а) Идентификация и аутентификация

Функция идентификации и аутентификации пользователей в Astra Linux основывается на использовании механизма PAM. Кроме того, в состав операционной системы включены средства поддержки двухфакторной аутентификации

б) Дискреционное разграничение доступа

В Astra Linux реализован механизм избирательного управления доступом, который заключается в том, что на защищаемые именованные объекты устанавливаются (автоматически при их создании) базовые правила разграничения доступа в виде идентификаторов номинальных субъектов (UID и GID), которые вправе распоряжаться доступом к данному объекту и прав доступа к объекту. Определяются три вида доступа: чтение (read, r), запись (write, w) и исполнение (execution, x).

Кроме общей схемы разграничения доступа, Astra Linux поддерживает также список контроля доступа — ACL, с помощью которого можно для каждого объекта задавать права всех субъектов на доступ к нему.

в) Мандатное разграничение доступа

В операционной системе реализован механизм мандатного разграничения доступа. Принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение/запись/исполнение), мандатного контекста безопасности, связанного с каждым субъектом, и мандатной метки, связанной с объектом.

Механизм мандатного разграничения доступа затрагивает следующие подсистемы:

- механизмы IPC;

- стек TCP/IP (IPv4);

- файловые системы Ext2/Ext3/Ext4;

- сетевую файловую систему CIFS;

- файловые системы proc, tmpfs.

В Astra Linux Special Edition существует 256 мандатных уровней доступа (от 0 до 255) и 64 мандатных категории доступа

При работе на разных мандатных уровнях и категориях операционная система формально рассматривает одного и того же пользователя, но с различными мандатными уровнями, как разных пользователей и создаёт для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается.

г) Модель контроля и управления доступом

Вместо системы принудительного контроля доступа SELinux, в Astra Linux Special Edition используется запатентованная мандатная сущностно-ролевая ДП-модель управления доступом и информационными потокам (МРОСЛ ДП-модель), которая лишена недостатков модели Белла — Лападулы (деклассификация, нарушение логики доступа к данным при обработке потока информации в распределённой среде) и содержит дополнительные способы разграничения доступа, например, два уровня целостности системы.

В отличие от классической модели мандатного управления доступом, в МРОСЛ ДП-модели дополнительно к мандатному управлению доступом реализован мандатный контроль целостности дистрибутива и файловой системы (препятствующий доступу к защищаемой информации скомпрометированными субъектами после перехвата управления и повышения привилегий (получения административных прав), предусмотрено ролевое управление доступом, наличие иерархии сущностей и применено противодействие запрещённым потокам по памяти и по времени.

Указанная математическая модель реализована в программном коде специалистами АО «НПО „РусБИТех“» и Академии ФСБ России и верифицирована Институтом системного программирования Российской академии наук. В результате дедуктивной верификации модель была полностью формализована и верифицирована.

В настоящее время используемая в Astra Linux Special Edition модель разграничения доступа является единственной практически реализованной моделью, не основанной на SELinux, в российских реализациях операционных систем на базе Linux.

д) Защита от эксплуатации уязвимостей

В состав ядра операционной системы Astra Linux включён набор изменений PaX, обеспечивающий работу программного обеспечения в режиме наименьших привилегий и защиту от эксплуатации различных уязвимостей в программном обеспечении:

- запрет записи в область памяти, помеченную как исполняемая;

- запрет создания исполняемых областей памяти;

- запрет перемещения сегмента кода;

- запрет создания исполняемого стека;

- случайное распределение адресного пространства процесса.

е) Другие функции:

- Очистка оперативной и внешней памяти и гарантированное удаление файлов: операционная система выполняет очистку неиспользуемых блоков файловой системы непосредственно при их освобождении, используя маскирующие последовательности.

- Маркировка документов: разработанный механизм маркировки позволяет серверу печати (CUPS) проставлять необходимые учётные данные в выводимых на печать документах. Мандатные атрибуты автоматически связываются с заданием для печати на основе мандатного контекста получаемого сетевого соединения. Вывод на печать документов без маркировки субъектами доступа, работающими в мандатном контексте с грифом выше «несекретно», невозможен.

- Регистрация событий: расширенная подсистема протоколирования, интегрированная во все компоненты операционной системы и осуществляющая надёжную регистрацию событий с использованием специального сервиса parlogd.

- Механизмы защиты информации в графической подсистеме: графическая подсистема включает в себя Х-сервер Xorg, пользовательский рабочий стол Fly, а также ряд программных средств, предназначенных как для пользователей, так и для администраторов системы. Проведена работа по созданию и встраиванию в графическую подсистему необходимых механизмов защиты информации, обеспечивающих выполнение мандатного разграничения доступа в графических приложениях, запущенных в собственном изолированном окружении.

- Механизм контроля замкнутости программной среды: реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов в формате ELF. Проверка производится на основе проверки векторов аутентичности, рассчитанных в соответствии с ГОСТ Р 34.10-2012 и внедряемых в исполняемые файлы в процессе сборки.

- Контроль целостности: для решения задач контроля целостности применяется функция хеширования в соответствии с ГОСТ Р 34.11-94.1.

Последняя версия специального издания операционной системы Astra Linux - Astra Linux 1.6 «Смоленск».

Astra Linux 1.6 «Смоленск» относительно предыдущей версии имеет следующие новшества:

1) Существенно переработано рабочее окружение Fly. Fly — собственная разработка РусБИТеха на базе библиотеки Qt. Имеет в своем составе стандартный набор средств. Освежена стандартная тема оформления в соответствии с современными тенденциями. В новой версии пользователь может адаптировать цветовую палитру по своему желанию. Из любопытных особенностей следует отметить изменение оформления рабочего стола в зависимости от прав пользователя.

2) В отличие от предыдущих версий Astra Linux, в новой версии за основу рабочей среды взято свободное ПО «KDE Framework». KDE Framewor — это программный инструментарий, лежащий в основе популярной рабочей среды KDE. Тем самым разработчики повысили качество и функциональность Fly, попутно улучшив совместимость с приложениями, разработанными для среды KDE.

3) Добавлен новейший комплект офисных программ LibreOffice 6.0. Данное нововведение предлагает лучшую функциональность.

4) Включен Blender — профессиональное свободное программное обеспечение для создания трёхмерной компьютерной графики, включающее в себя средства моделирования, анимации, рендеринга, постобработки и монтажа видео.

5) Включены в состав многие приложения KDE: запись компакт-дисков (k3b), редактор Kate, терминал Konsole и д.р.

6) В дополнение к традиционным средствам построения сетевых доменов Astra Linux Directory добавлена домен FreeIPA. FreeIPA — открытый проект для создания централизованной системы управления пользователями, компьютерами с интеграцией зон DNS, доменами Samba и системой Kerberos 5. FreeIPA дает возможность централизации многих функциональных аспектов инфраструктуры.

7) Для удобства администрирования добавлены графические утилиты для работы с доменами. Включен графический интерфейс к брандмауэру UFW.

8) Добавлен прокси-сервер HAProxy в дистрибутив ОС.

9) Для настройки сети внедрен iproute2 вместо iproute.

10) PostgreSQL обновлен до версии 9.6.

11) Включены многие дополнительные пакеты Ruby, а сам Ruby обновлен до версии 2.3.

12) Дистрибутив QEMU пополнился средой виртуализации и кластеризации с возможностью построения высоконадежных отказоустойчивых систем.

13) Дистрибутив Hardened пополнился ядром с усиленной самозащитой. Hardened Linux — это несколько изменений в компиляторе и ядре, которые увеличивают общую защищенность системы от взлома. Hardened-ядро умеет блокировать массу потенциально опасных операций. Hardened ядро пришло на замену защите PaX.

14) Расширены возможности мандатного контроля целостности (МКЦ). Вместо двух уровней целостности (версия 1.5) теперь доступно 8 уровней. Некоторые уровни распределены между системными средствами. Контроль целостности влияет на возможность изменения объектов операционной системы пользователем.

15) Расширены механизмы блокировки выполнения недоверенного кода, в том числе и на интерпретируемых языках программирования (python, perl, ruby,.).

16) Данные на дисках и компьютерной сети теперь могут быть защищены маскирующим преобразованием.

17) В состав дистрибутива включены утилиты обновления микрокода процессоров Intel и AMD.

19) Подверглись изменениям функции подсистемы мандатной защиты данных (PARSEC). Сервер графического интерфейса теперь работает под пользовательской учетной записью. Протокол SSH переведен на использование российских алгоритмов ГОСТ. Отключение входа через консоль и многое другое.

**2.4 Обоснование выбора и описание среды программирования**

Разработчиками операционной системы Astra Linux в качестве основной среды разработки рекомендован кроссплатформенный фреймворк для разработки программного обеспечения на языке программирования C++ - Qt.

Qt является кроссплатформенным фреймворком для разработки приложений от компании Trolltech, а на данный момент владельцем кода является компания Digia. Фреймворк предоставляет API на языке C++. Qt часто используется разработчиками для разработки кроссплатформенных приложений.

Библиотека Qt задумывалась и начиналась как кросс-платформенный тулкит (toolkit) для быстрой разработки графических интерфейсов (GUI) приложений на языке C++, с целью упростить жизнь программистов, пишущих на C++ кросс-платформенные, переносимые GUI-приложения, которые должны работать и в среде Windows, Symbian, и в среде Unix/Linux под X11, и на компьютерах Macintosh.

В настоящее время Qt значительно переросла рамки тулкита для разработки графических интерфейсов приложений. Она предоставляет использующему её программисту целостный фреймворк (framework), позволяющий при написании большей части приложения использовать только «родные» классы Qt и практически полностью отказаться от написания системно-зависимого кода, использования системных вызовов (будь то Win32 API или Unix system calls) или от изобретения собственных кросс-платформенных обёрток и «велосипедов». Классы Qt покрывают почти все потребности программиста. В Qt предусмотрены классы и для работы со строками, и для работы с файлами, сетью, базами данных, XML, и для обеспечения многопоточности в приложении, и многое-многое другое. По своим возможностям и богатству библиотека Qt сравнима с .NET Framework или с системой классов Java 2 EE.

Qt предоставляет программисту не только удобный набор библиотек классов, но и определённую модель разработки приложений, определённый каркас их структуры. Следование принципам и правилам «хорошего стиля программирования на C++/Qt» существенно снижает частоту таких трудно отлавливаемых ошибок в приложениях, как утечки памяти (memory leaks), необработанные исключения, незакрытые файлы или неосвобождённые дескрипторы ресурсных объектов, чем нередко страдают программы, написанные «на голом C++» без использования библиотеки Qt.

Важным преимуществом Qt является хорошо продуманный, логичный и стройный набор классов, предоставляющий программисту очень высокий уровень абстракции. Благодаря этому программистам, использующим Qt, приходится писать значительно меньше кода, чем это имеет место при использовании, например, библиотеки классов MFC. Сам же код выглядит стройнее и проще, логичнее и понятнее, чем аналогичный по функциональности код MFC или код, написанный с использованием «родного» для X11 тулкита Xt. Его легче поддерживать и развивать.

Кроме того, даже если программисту в данный конкретный момент не нужна кроссплатформенность для его конкретного приложения (например, планируется версия только для Windows или только для Macintosh), никто не может знать, что понадобится завтра. Бизнес-планы могут поменяться, и может оказаться и нужным, и выгодным выпустить версию для другой операционной системы или другой аппаратной платформы. В случае использования Qt для этого понадобится всего лишь перекомпиляция исходного кода. В случае же использования, например, MFC или «родных» системных API понадобится много тяжёлой работы по портированию, адаптации и отладке, а то и переписыванию с нуля существующего исходного кода для другой ОС или аппаратной платформы.

Многие компании-разработчики приложений Windows используют Qt ещё по одной причине: даже если код пишется и в обозримом будущем будет писаться только для платформы Windows и тестируется только на ней, возможность откомпилировать один и тот же исходный код на одной и той же платформе Windows двумя разными компиляторами (Microsoft Visual C++ и GCC/Win32) гарантирует лучшее качество исходного кода и лучшую его совместимость со стандартом C++. Что немаловажно для кода, который планируется длительно поддерживать и развивать.

При помощи Qt можно разрабатывать приложения с графическим интерфейсом, приложения, работающие с сетью, приложения, работающие с базами данных и мультимедийные приложения, работать с XML-структурами и 3D-графикой, осуществлять рисование и доступ к сетевым ресурсам. Поскольку поддерживается ряд платформ, Qt может работать на Linux, Mac OS, Windows, Meego, встраиваемых Linux-системах и Symbian.

Со времени своего появления в 1996 году библиотека легла в основу многих программных проектов. Кроме того, Qt является фундаментом популярной рабочей среды KDE, входящей в состав многих дистрибутивов Linux.

Qt позволяет запускать написанное с его помощью программное обеспечение в большинстве современных операционных систем путём простой компиляции программы для каждой системы без изменения исходного кода. Включает в себя все основные классы, которые могут потребоваться при разработке прикладного программного обеспечения, начиная от элементов графического интерфейса и заканчивая классами для работы с сетью, базами данных и XML. Является полностью объектно-ориентированным, расширяемым и поддерживающим технику компонентного программирования.

Отличительная особенность — использование метаобъектного компилятора — предварительной системы обработки исходного кода. Расширение возможностей обеспечивается системой плагинов, которые возможно размещать непосредственно в панели визуального редактора. Также существует возможность расширения привычной функциональности виджетов, связанной с размещением их на экране, отображением, перерисовкой при изменении размеров окна.

Комплектуется визуальной средой разработки графического интерфейса Qt Designer, позволяющей создавать диалоги и формы в режиме WYSIWYG. В Qt имеется огромный набор виджетов (Widget), таких как: кнопки, прогресс бары, переключатели, checkbox, и другие — они обеспечивают стандартную функциональность GUI (графический интерфейс пользователя). Позволяет использовать весь функционал пользовательского интерфейса — меню, контекстные меню, drag&drop. Визуальное создание интерфейса позволяет легко и просто создавать интерфейс, перетаскивая различные виджеты(выпадающие списки, кнопки, переключатели) на форму.

В поставке Qt есть Qt Linguist — графическая утилита, позволяющая упростить локализацию и перевод программы на многие языки.

Qt Assistant — справочная система Qt, упрощающая работу с документацией по библиотеке, а также позволяющая создавать кроссплатформенную справку для разрабатываемого на основе Qt программного обеспечения.

Начиная с версии 4.5.0 в комплект включена среда разработки Qt Creator, которая включает редактор кода, справку, графические средства Qt Designer и возможность отладки приложений. Qt Creator может использовать GCC или Microsoft VC++ в качестве компилятора и GDB в качестве отладчика. Для Windows-версий библиотека комплектуется компилятором, заголовочными и объектными файлами MinGW.

Существуют версии библиотеки для Microsoft Windows, систем класса UNIX с графической подсистемой X11, Android, iOS, Mac OS X, Microsoft Windows CE, QNX, встраиваемых Linux-систем и платформы S60. Идет портирование на Windows Phone и Windows RT, Haiku и Tizen.

Простейшая схема, демонстрирующая архитектуру Qt, представлена на Рисунке 5.

На верхнем уровне находится код программы на языке C++. Уровнем ниже расположены классы Qt для создания графического интерфейса, взаимодействия с WebKit, работы с базами данных и.т.д., а еще ниже расположен уровень поддержки различных операционных систем. Ранее Qt поддерживал также язык программирования Java; версия для языка Java называлась Jambie. По мере продвижения разработки Qt, становилось все сложнее поддерживать версии для C++ и Java, поэтому и было принято решение поддерживать только версию для C++.

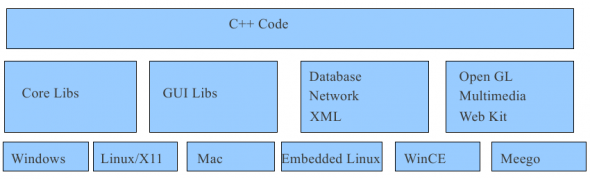


Рисунок 5 - Архитектура Qt

В настоящее время Qt фреймворк активно развивается. Имеет интуитивно понятное API, огромную документацию с большим количеством примеров, мощнейшую среду разработки QtCreator и дополнительный инструментарий.

**2.5 Обоснование выбора и описание средств защиты от несанкционированного доступа**

**2.5.1 Перечень требуемых средств защиты от несанкционированного доступа**

СЗИ НСД изделия представляет собой объединенную единым функциональным предназначением совокупность средств защиты информации от НСД.

СЗИ НСД предназначена для:

- защиты информации от несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этого программного обеспечения;

- автоматического контроля защищаемых программных и информационных ресурсов от деструктивного воздействия компьютерных вирусов;

- управления средствами защиты администратором безопасности;

- периодического контроля состояния средств защиты информации;

- защиты информации от НСД как в рамках изделия, так и при сопряжении (обмене информацией) с другими изделиями.

К программно-техническим, программным и техническим средствам защиты информации относиться:

- автоматизированное рабочее место (далее – АРМ) администратора безопасности информации (далее – АБИ) с комплексом программ АБИ;

- средства защиты информации от НСД операционной системы;

- средства доверенной загрузки;

- средства антивирусной защиты (далее – САВЗ);

- средства межсетевого экранирования;

- средства документирования информации;

- средства сигнализации;

- средства защиты технических средств изделия от несанкционированного доступа к их монтажу, информационным разъемам, носителям информации (защитные кожухи, шкафы-стойки и. т.п.);

- средства резервного копирования информации;

- средства восстановления СЗИ, предусматривающие ведение двух копий программных СЗИ и их оперативное восстановление функций СЗИ при сбоях;

- средства контроля целостности СЗИ, программных и информационных ресурсов, предусматривающие, в том числе, контроль целостности средств ЗИ по контрольным суммам всех компонент СЗИ, как в процессе загрузки, так и динамически в процессе работы изделий.

СЗИ НСД изделия реализовывают требования класса защищенности от НСД к информации «1Г», в соответствии с РД Гостехкомиссии (ФСТЭК) России 1992 г. «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации».

Сопряжение модулей комплексного тренажера между собой, а также с другими изделиями и системами должно осуществляться с использованием межсетевых экранов, имеющие сертификаты соответствия «Требованиям в области…(требования к межсетевым экранам), утвержденным приказом ФСТЭК России 2016 года № 9 для КСА РК ГОЗ-ГТ, не ниже чем по 4 классу типа «А».

СЗИ от НСД изделия так же обеспечивает:

а) световую и акустическую сигнализацию на АРМ АБИ и АРМ нарушителя фактов или попыток НСД к защищаемым ресурсам изделия;

б) акустическую сигнализацию несанкционированного вскрытия технических средств изделия;

в) автоматическое блокирование АРМ изделия после троекратной неверной попытки установления подлинности пользователя, троекратной неверной попытки идентификации пользователя;

г) разблокирование АРМ изделия после автоматической блокировки только администратором безопасности информации;

д) контроль целостности неизменных компонентов программного обеспечения изделия по их контрольным суммам при загрузке системы, а также по команде администратора безопасности;

е) контроль доступа (опечатывание, опломбирование и т.п.) к внутреннему монтажу технических средств изделия, опечатывание незадействованных разъемов съемных носителей информации;

ж) предотвращение несанкционированных подключений к расстыковкам кабельных разъемов технических средств изделия, включая коммутационные средства организации вычислительных сетей;

и) защиту от компьютерных вирусов и восстановление зараженных файлов;

к) генерацию паролей;

л) архивирование журналов регистрации и просмотра архивных журналов с возможностью их печати.

м) АРМ и серверы изделия должны оснащаться средствами доверенной загрузки, имеющими действующие сертификаты соответствия требованиям ФСБ России к аппаратно-программному модулю доверенной загрузки (АПМДЗ) по классу «3Б», либо «Требованиям в области... (требования к средствам доверенной загрузки)», утвержденным приказом ФСТЭК России 2013 года № 119дсп не ниже 4 класса защиты типа «УБ» и/или «ПР».

Комплекс программ АБИ иметь единую визуальную среду администрирования, позволяющему ему в графическом интерфейсе решать функциональные задачи и обеспечивать:

а) удаленную настойку средств защиты информации;

б) блокирование/разблокирование с АРМ АБИ работы пользователя, программ и устройств изделия в случае обнаружения попыток, фактов НСД;

в) просмотр и печать (при необходимости) АБИ журналов подсистемы регистрации и учета;

г) архивацию журналов регистрации за необходимый промежуток времени;

д) ведение журнала учета защищаемых ресурсов (каталогов, файлов, программ);

е) ведение таблицы разграничения доступа (с возможностью документирования) пользователей, их прав и полномочий;

ж) корректировку параметров идентификации и полномочий доступа к защищаемым ресурсам;

и) генерацию, установку и смену паролей доступа пользователям с использованием программы генерации пароля;

к) формирование и печать списка пользователей с соответствующими им заблаговременно-сгенерированными паролями;

л) постановку/снятие на контроль целостности компонента программного обеспечения (каталогов, файлов) изделия с АРМ АБИ;

м) отображение и документирование результатов контроля целости программного обеспечения с указанием элементов, подвергшихся изменению, и характера изменений;

н) проведение антивирусной проверки ПО всех АРМ изделия с АРМ АБИ по команде администратора;

о) отображение и документирование результатов антивирусной проверки ПОс указанием элементов подвергшихся заражению;

п) создание резервных копий машинных носителей информации (CD, DVD, и т.п.);

р) тестирование работоспособности средств защиты.

Операционная система, применяемая в АРМ ИКТ, обеспечивает:

а) защиты от несанкционированного уничтожения, блокирования, копирования информации и обнаружения попытки произвести указанные выше действия;

б) разграничений уровня доступа и генерацией паролей;

в) доверенной загрузки имеющей действующий сертификат соответствия требованиям ФСБ России к аппаратно-программному модулю доверенной загрузки (АПМДЗ) по классу «3Б», либо «Требованиям в области... (требования к средствам доверенной загрузки)», утвержденным приказом ФСТЭК России 2013 года № 119дсп не ниже 4 класса защиты типа «УБ» и/или «ПР».;

- системное программное обеспечение с функционалом:

а) защиты от деструктивного воздействия компьютерных вирусов;

б) межсетевого экранирования не ниже чем по 4 классу типа «А»;

в) контроля целостности данных;

- защиту от несанкционированного подключения к аппаратуре вычислительной системы,

- резервную систему хранения данных.

**2.5.2 Описание средств защиты от несанкционированного доступа**

Средства защиты от несанкционированного доступа ОС Astra Linux 1.6 позволяют реализовать следующие меры:

- идентификация и аутентификация субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;

- ограничение программной среды;

- защита машинных носителей информации;

- регистрация событий безопасности;

- антивирусная защита;

- обнаружение вторжений;

- контроль (анализ) защищенности информации;

- обеспечение целостности информационной системы и информации;

- обеспечение доступности информации;

- защита среды виртуализации;

- защита технических средств;

- защита информационной системы, ее средств, систем связи и передачи данных;

Ниже подробно рассмотрены способы реализации мер защиты.

**2.5.2.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа**

Операционная система Astra Linux обеспечивает следующие меры по идентификации и аутентификации:

1) Идентификация и аутентификация пользователей, являющихся работниками оператора. Аутентификация осуществляется локально или централизованно с помощью организации единого пространства пользователей, в основу которого положен доменный принцип построения сети с использованием сетевого протокола сквозной доверенной аутентификации.

Многофакторная аутентификация обеспечивается совместным применением средств идентификации и аутентификации ОС СН, средств доверенной загрузки и устройств аутентификации (например, USB-токенов).

2) Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных. Идентификация устройств осуществляется по логическим именам, по комбинации имени, логического, физического адресов, по информации об устройстве локально или централизованно с использованием сетевого протокола сквозной доверенной аутентификации

3) Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов пользователя. Управление идентификаторами пользователей (присвоение и блокирование идентификаторов, а также ограничение срока действия идентификаторов (учетных записей) осуществляется администратором локально или централизованно с помощью инструментов управления политикой безопасности

4) Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Управление средствами аутентификации осуществляется администратором, для защиты аутентификационной информации в ОС СН по умолчанию используются отечественные алгоритмы по ГОСТ 28147-89 и ГОСТ Р 34.11-2012

5) Защита обратной связи при вводе аутентификационной информации. Защита обратной связи при вводе аутентификационной информации обеспечивается исключением отображения действительного значения аутентификационной информации при ее вводе пользователем в диалоговом интерфейсе.

6) Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей). Аутентификация осуществляется локально или с помощью организации единого пространства пользователей.

7) Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа. Идентификация всех объектов и устройств и применение результатов идентификации при реализации механизмов управления доступом, контроля целостности, резервного копирования и регистрации событий безопасности, связанных с этими объектами доступа

**2.5.2.2 Меры по управление доступом субъектов доступа к объектам доступа**

Операционная система Astra Linux обеспечивает следующие меры по управлению доступом:

1) Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей. Управление учетными записями пользователей (заведение, активация, блокирование и уничтожение) осуществляется администратором локально или централизованно с помощью инструментов управления политикой безопасности.

2) Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа. Монитор обращений из состава ОС СН предусматривает дискреционное, мандатное и ролевое управление доступом, а также реализацию мандатного контроля целостности. Решение о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности пользователя и классификационной метки объекта. Управление доступом осуществляется применительно ко всем объектам, включая объекты файловой системы, базы данных, процессам и устройствам.

3) Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами. Управление информационными потоками в информационной системе осуществляется средствами ОС СН, реализующими функции контроля и фильтрации проходящих информационных потоков в соответствии с заданными правилами.

Правила (или цепочки) фильтрации выполняются в соответствии с атрибутами отправителя и получателя сетевых пакетов, а также атрибутами передаваемой информации (классификационными метками и контрольными суммами, вычисляемых в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012).

4) Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы. Разделение полномочий (ролей) пользователей осуществляется администратором с помощью инструментов управления политикой безопасности в соответствии с организационно-распорядительной документацией оператора.

5) Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы. Назначение минимально необходимых прав и привилегий, разделение полномочий (ролей) пользователей осуществляется администратором с помощью инструментов управления политикой безопасности в соответствии с организационно-распорядительной документацией оператора

6) Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе). Ограничение количества неуспешных попыток входа и блокирования учетной записи и сеанса доступа пользователя при превышении числа неуспешных попыток аутентификации устанавливается администратором с помощью инструментов управления политикой безопасности

7) Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации.

8) Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему. Сведения о предыдущей аутентификации, количестве успешных и неуспешных попыток входа предоставляются пользователю (в соответствии с его правилами разграничения доступа) и администратору с использованием средств протоколирования

9) Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы. Ограничение числа параллельных сеансов для каждого пользователя (или группы) и мониторинга осуществляется администратором с помощью инструментов управления политикой безопасности и встроенных программных решений организации распределенного мониторинга.

10) Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу. Блокирование сеанса доступа пользователя по истечении заданного администратором интервала времени бездействия осуществляется автоматически или по запросу.

11) Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации. Решение о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение, запись, исполнение), мандатного контекста безопасности пользователя и классификационной метки объекта. Управление доступом осуществляется применительно ко всем объектам, включая объекты файловой системы, базы данных, процессам и устройствам.

12) Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки. В ОС СН реализовано мандатное управление доступом к информации в процессе ее хранения и обработки с учетом атрибутов безопасности (классификационных меток в формате, установленном ГОСТ Р 58256).

13) Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

14) Регламентация и контроль использования в информационной системе технологий беспроводного доступа.

15) Регламентация и контроль использования в информационной системе мобильных технических средств. Реализуется средствами ОС СН, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.

16) Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

17) Обеспечение доверенной загрузки средств вычислительной техники.

**2.5.2.3 Меры по ограничению программной среды**

Операционная система Astra Linux обеспечивает следующие меры по ограничению программной среды:

1) Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения. Задача запуска в информационной системе разрешенного программного обеспечения реализуется средствами ограничения программной среды.

2) Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения. Задача управления установкой в информационную систему разрешенного программного обеспечения реализуется средствами регламентного контроля целостности устанавливаемого программного обеспечения в составе доверенного служебного репозитория с использованием хэш-функции или электронной цифровой подписи

3) Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов. Задача установки в информационную систему разрешенного программного обеспечения реализуется средствами регламентного контроля целостности устанавливаемого программного обеспечения в составе доверенного служебного репозитория с использованием хэш-функции или электронной цифровой подписи.

**2.5.2.4 Меры по защите машинных носителей информации**

Операционная система Astra Linux обеспечивает следующие меры по защите машинных носителей информации:

1) Учет машинных носителей информации. Реализуется средствами ОС СН, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной̆ техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей̆ информации на основе установленных администратором правил разграничения доступа.

2) Управление доступом к машинным носителям информации.

3) Контроль перемещения машинных носителей информации за пределы контролируемой зоны.

4) Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах.

5) Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации. Реализуется средствами ОС СН, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей̆ информации на основе установленных администратором правил разграничения доступа.

6) Контроль ввода (вывода) информации на машинные носители информации. Реализуется средствами ОС СН, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.

7) Контроль подключения машинных носителей информации. Реализуется средствами ОС СН, обеспечивающими контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации на основе установленных администратором правил разграничения доступа.

8) Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания). Задача уничтожения (стирания) информации, исключения возможности восстановления защищаемой информации реализуется с помощью средств защиты памяти, настройки параметров использования машинных носителей

**2.5.2.5 Меры по регистрации событий безопасности**

Операционная система Astra Linux обеспечивает следующие меры по регистрации событий безопасности:

1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения. События безопасности, подлежащие регистрации, и сроки их хранения определяются администратором.

2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются администратором.

3) Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения. Сбор, запись и хранение информации о событиях безопасности осуществляются с помощью средств централизованного протоколирования и ведения журналов аудита событий безопасности, установленных администратором, хранения записей системных журналов и записей о событиях безопасности в обособленном хранилище. Для своевременного выявления инцидентов и реагирования на них в информационной системе используются системы управления событиями безопасности (SIEM).

4) Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти. Реагирование на сбои регистрации и предупреждения администратора при заполнении объема памяти для хранения информации о событиях безопасности осуществляются с помощью средств централизованного протоколирования и аудита событий безопасности.

5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности реализуется с использованием средств организации распределенного мониторинга сети и жизнеспособности и целостности серверов. С целью выявления инцидентов безопасности и реагирования на них и анализа записанных сетевых потоков в информационной системе могут использоваться сертифицированные системы управления событиями безопасности (SIEM) и систем обнаружения вторжений.

6) Генерирование временных меток и (или) синхронизация системного времени в информационной системе. Синхронизация системного времени в информационной системе реализуется с использованием возможностей синхронизации системных часов.

7) Защита информации о событиях безопасности. Защита информации о событиях безопасности реализуется монитором обращений в соответствии с реализованными правилами разграничения доступа к журналам аудита.

8) Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе. Просмотр и анализ информации о действиях пользователей предоставляется администратору (пользователям в соответствии с установленными правилами разграничения доступа) с использованием средств централизованного протоколирования и ведения журналов аудита событий безопасности.

**2.5.2.6 Меры по антивирусной защиты.**

Операционная система Astra Linux обеспечивает следующие меры по антивирусной защите:

1) Реализация антивирусной защиты.

2) Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

**2.5.2.7 Меры по обнаружению вторжений**

Операционная система Astra Linux обеспечивает следующие меры по обнаружению вторжений:

1) Обнаружение вторжений.

2) Обновление базы решающих правил.

**2.5.2.8 Меры по контролю (анализу) защищенности информации**

Операционная система Astra Linux обеспечивает следующие меры по контролю (анализу) защищенности информации:

1) Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. Выявление и оперативное устранение уязвимостей ОС СН производится разработчиком в соответствии с «Требованиями к уровням доверия», утвержденным приказом ФСТЭК России №131, и ГОСТ Р 56939.

2) Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации. Контроль целостности обновлений ОС СН осуществляется проведением динамического контроля целостности файлов с использованием электронной цифровой подписи и регламентного контроля целостности с использованием функции хэширования.

3) Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. Контроль работоспособности встроенного комплекса средств защиты информации ОС СН осуществляется с помощью автоматического и регламентного тестирования функций безопасности.

4) Контроль состава технических средств, программного обеспечения и средств защиты информации.

5) Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

**2.5.2.9 Меры по обеспечению целостности информационной системы и информации**

Операционная система Astra Linux обеспечивает следующие меры по обеспечению целостности информационной системы и информации:

1) Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. Для обеспечения контроля целостности программного обеспечения и средств защиты информации используются средства динамического и регламентного контроля целостности.

2) Контроль целостности информации, содержащейся в базах данных информационной системы. Контроль целостности информации реализуется с использованием функций безопасности системы управления базами данных.

3) Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций. В целях обеспечения возможности восстановления работоспособности системы используется режим восстановления и средства резервного копирования.

4) Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

5) Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы. Контроль содержания информации, основанный на свойствах объектов доступа, осуществляется согласно установленной политики управления доступом.

6) Ограничение прав пользователей по вводу информации в информационную систему. Ввод пользователями информации осуществляется строго с учетом и в соответствии с установленными правилами разграничения доступа.

7) Контроль точности, полноты и правильности данных, вводимых в информационную систему.

8) Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях. Контроль осуществляется средствами протоколирования и аудита событий (в том числе, действий пользователя) в соответствии с установленными правилами разграничения доступа

**2.5.2.10 Меры по обеспечению доступности информации**

Операционная система Astra Linux обеспечивает следующие меры по обеспечению доступности информации:

1) Использование отказоустойчивых технических средств. Возможность работы ОС СН на нескольких технических средствах в отказоустойчивом режиме обеспечивает доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер).

2) Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы.

3) Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование. Контроль за состоянием информационной системы осуществляется путем регистрации событий и анализа содержимого системных журналов

4) Периодическое резервное копирование информации на резервные машинные носители информации. Резервное копирование осуществляется с использованием специальных программ и утилит, позволяющих восстанавливать информацию и объекты файловой системы с сохранением их атрибутов безопасности и аудита.

5) Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала. Резервное копирование осуществляется с использованием программ и утилит, позволяющих восстанавливать информацию и объекты файловой системы, и сервисов планирования выполнения заданий.

6) Кластеризация информационной системы и (или) ее сегментов. Возможность работы ОС СН на нескольких технических средствах в отказоустойчивом режиме обеспечивает доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер).

7) Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации.

**2.5.2.11 Меры по защите среды виртуализации**

Операционная система Astra Linux обеспечивает следующие меры по защите среды виртуализации:

1) Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.

2) Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин. Управление доступом осуществляется с использованием технологии KVM, которая включает специальный модуль ядра и средство создания виртуального аппаратного окружения для изоляции и управления виртуальными гостевыми машинами.

3) Регистрация событий безопасности в виртуальной инфраструктуре. Регистрация событий безопасности в виртуальной инфраструктуре осуществляется с использованием интерфейсов управления средствами виртуализации, штатных средств протоколирования и аудита.

4) Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры. Управление информационными потоками в информационной системе осуществляется средствами ОС СН, реализующими функции контроля и фильтрации проходящих информационных потоков в соответствии с заданными правилами.

Правила (или цепочки) фильтрации выполняются в соответствии с атрибутами отправителя и получателя сетевых пакетов, а также атрибутами передаваемой информации.

5) Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией. Доверенная загрузка виртуальных машин реализуется средствами создания замкнутой программной среды, настройками подсистемы эмуляции аппаратного обеспечения и контроля целостности образов виртуальных машин. Для ЭВМ — защита реализуется с применением средств доверенной загрузки.

6) Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных. Управление перемещением виртуальных машин реализуется с использованием интерфейсов управления средствами виртуализации.

7) Контроль целостности виртуальной инфраструктуры и ее конфигураций. Доверенная загрузка виртуальных машин реализуется средствами создания замкнутой программной среды, настройками подсистемы эмуляции аппаратного обеспечения и контроля целостности образов виртуальных машин.

8) Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры. Резервное копирование реализуется с использованием средств кластеризации и создания распределенных хранилищ информации.

9) Реализация и управление антивирусной защитой в виртуальной инфраструктуре.

10) Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей. Разбиение виртуальной инфраструктуры на сегменты обеспечивается с использованием штатных средств ОС СН, реализующих технологию виртуальных локальных сетей (VLAN) стандарта IEEE 802.1q.

**2.5.2.12 Меры по защите технических средств**

Операционная система Astra Linux обеспечивает следующие меры по защите среды виртуализации:

1) Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам.

2) Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

3) Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

4) Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

5) Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

**2.5.2.13 Меры по защите информационной системы, ее средств, систем связи и передачи данных**

Операционная система Astra Linux обеспечивает следующие меры по защите информационной системы, ее средств, систем связи и передачи данных:

1) Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы. Разделение функций по управлению (администрированию) системой в целом и системой защиты информации, функций по обработке информации реализуется согласно мерам УПД.

2) Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом. Предотвращение задержки или прерывания выполнения процессов осуществляется с использованием утилит управления приоритетами процессов.

3) Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи. Обеспечение защиты информации при ее передаче обеспечивается средствами контроля целостности передаваемой информации и использования защищенных каналов.

4) Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации). Доверенный канал обеспечивается средствами создания защищенных каналов и в соответствии с правилами разграничения доступа и установленными привилегиями.

5) Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств. Запрет реализуется с помощью исключения или блокирования доступа к модулям, отвечающим за работу соответствующих периферийных устройств, в соответствии с установленными правилами разграничения доступа, а также применением механизма фильтрации сетевых пакетов.

6) Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене информацией с иными информационными системами. Защита реализуется с применением сертифицированных средств защиты информации, реализующих функции контроля и фильтрации сетевого потока, поддерживающих управление сетевыми потоками с использованием классификационных меток. Передача и контроль целостности атрибутов информации осуществляется в соответствии с политикой управления доступом с учетом атрибутов передаваемой информации (классификационными метками в формате в соответствии с ГОСТ Р 58256 и контрольными суммами, вычисляемыми в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012). Целостность заголовка IP-пакетов, содержащего классификационную метку, обеспечивается с применением средств защиты канала передачи информации.

7) Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода. Исключение несанкционированного использования технологий (запрета исполнения и несанкционированного использования кода) реализуется средствами создания ограничение программной среды, в частности созданием «замкнутой программной среды». Контроль осуществляется с помощью инструментов регистрации и анализа событий безопасности в системных журналах.

8) Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи.

9) Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации.

10) Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам. Подтверждение происхождения источника получаемой информации осуществляется службой DNS (системой доменных имен).

11) Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов. Осуществляется средствами ОС СН, реализующими функции контроля и фильтрации проходящих информационных потоков в соответствии с заданными правилами. Подлинность сетевых соединений обеспечивается средствами организации сквозной доверенной аутентификации, использования защищенных каналов и проверки целостности передаваемых пакетов.

12) Исключение возможности отрицания пользователем факта отправки информации другому пользователю.

13) Исключение возможности отрицания пользователем факта получения информации от другого пользователя.

14) Использование устройств терминального доступа для обработки информации. Возможность обработки информации с помощью устройств терминального доступа реализуется средствами реализации терминального сервера, технологий «тонкого клиента» в сетях с клиент-серверной или терминальной архитектурой и службы виртуальных рабочих столов.

15) Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации. Защита файлов, не подлежащих изменению, реализуется средствами контроля целостности объектов файловой системы и настройкой правил разграничения доступа.

16) Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов. В ОС СН идентифицированы и приведены условия исключения скрытых каналов передачи информации в соответствии с «Требованиями к уровням доверия», утвержденным приказом ФСТЭК России №131. Условиями исключения скрытых каналов является реализуемая ОС СН политика дискреционного и мандатного управления доступом, мандатного контроля целостности, а также возможность изоляции процессов в совокупности с очисткой областей оперативной памяти и обеспечение запуска процессов в замкнутой относительно остальных процессов среде по памяти.

17) Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.

18) Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения. Обеспечение загрузки и исполнения программного обеспечения и контроль целостности программного обеспечения осуществляется средствами управления доступом к подключаемым устройствам и средствами контроля целостности.

19) Изоляция процессов (выполнение программ) в выделенной области памяти. Изоляция процессов (выполнение программ) в выделенной области памяти реализована в ядре ОС СН.

20) Защита беспроводных соединений, применяемых в информационной системе.

21) Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы. Исключение доступа пользователя к «остаточной» информации реализуется с использованием механизмов очистки оперативной и внешней памяти и изоляции процессов в соответствии с установленными правилами разграничения доступа.

22) Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы. Обеспечение защиты от угроз, направленных на отказ в обслуживании, реализуется ограничением замкнутой программной среды, настройкой режима «киоск», ограничением пользователей по использованию вычислительных ресурсов, интерпретаторов, макросов и консолей.

23) Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

24) Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.

25) Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды). Возможность использования в информационной системе различных типов программного обеспечения реализуется с помощью использования виртуальной инфраструктуры, в составе которой возможно функционирование «недоверенных» гостевых операционных систем в доверенной среде ОС СН.

26) Использование прикладного и специального программного обеспечения, имеющих возможность функционирования в средах различных операционных систем.

27) Создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации.

28) Воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик информационной системы или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы.

29) Перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающую защиту информации, в случае возникновении отказов (сбоев) в системе защиты информации информационной системы. В случае возникновения отказов перевод информационной системы осуществляется с использованием средств восстановления ОС СН и с применением наборов базовых конфигураций.

**2.5.3 Перечень защищаемых ресурсов АРМ ИКТ**

В соответствии со структурой АРМ ИКТ функциональное программное обеспечение и данные, которые необходимо защищать от несанкционированного доступа располагаются только в ЭВМ РМИ-КТ и ЭВМ РМИ-КТВ. Подключение отдельных съемных накопителей к АРМ ИКТ не предусмотрено.

Учитывая, что ЭВМ РМИ-КТ и ЭВМ РМИ-КТВ функционируют под управлением операционной системы Astra Linux, обеспечивающей меры по защите от несанкционированного доступа, перечисленные в 2.5.2, то защита ЭВМ РМИ-КТ и ЭВМ РМИ-КТВ обеспечивается в полном объеме и соответствует требованиям ТЗ за исключением:

- доверенной загрузки операционной системы с физическим ключом;

- защиты ЭВМ РМИ-КТ, ЭВМ РМИ-КТВ, коммутаторов от несанкционированного доступа к их монтажу, информационным разъемам, носителям информации (защитные кожухи, шкафы-стойки и. т.п.);

- акустическую сигнализацию несанкционированного вскрытия технических средств изделия;

- контроль доступа (опечатывание, опломбирование и т.п.) к внутреннему монтажу технических средств изделия, опечатывание незадействованных разъемов съемных носителей информации;

- предотвращение несанкционированных подключений к расстыковкам кабельных разъемов технических средств изделия, включая коммутационные средства организации вычислительных сетей.

Для реализации вышеперечисленных задач при разработке РКД будет реализованы:

- возможность размещения ЭВМ РМИ-КТ, ЭВМ РМИ-КТВ, коммутаторов в серверной стойке обеспечивающей защиту от несанкционированного доступа к их монтажу, информационным разъемам, носителям информации, возможность опечатывания двери доступа к аппаратуре, акустическую сигнализацию при несанкционированном вскрытии;

- возможность на ЭВМ РМИ-КТ, ЭВМ РМИ-КТВ контроля доступа (опечатывание, опломбирование и т.п.) к внутреннему монтажу ЭВМ, опечатывание незадействованных разъемов съемных носителей информации;

- возможность на ЭВМ РМИ-КТ, ЭВМ РМИ-КТВ использования доверенной загрузки операционной системы с физическим ключом.

Таким образом, для АРМ АБИ ресурсами, требующими защиты от несанкционированного доступа, являются ЭВМ РМИ-КТ и ЭВМ РМИ-КТВ. Имеется возможность обеспечения несанкционированного доступа в соответствии и в объеме требований ТЗ за счет встроенных средств в операционную систему Astra Linux 1.6, за счёт конструкции ЭВМ (доверенная загрузка и опечатывание разъемов) и возможности размещения ЭВМ в специализированной серверной стойке.

**3. Основные технические характеристики модуля СОЦ ПО**

**3.1 Основные ТТХ СОЦ ПО**

Основные тактико-технические характеристики СОЦ ПО следующие:

- взаимодействие по каналу Ethernet 10/100/1000 Base-T с РМИ-ИКТ.

- взаимодействие по каналу Ethernet 10/100/1000 Base-T с модулем ПБУ.

- взаимодействие по каналу Ethernet между имитатором аппаратуры СОЦ, адаптированным ПО Багет-23В из состава СОЦ, рабочим местом инструктора.

- отображение информации на двух ЖК-мониторах;

- подключение сенсорного манипулятора по каналу RS232

- подключение пульта управления(клавиатуры) по каналу RS232

- питание всей аппаратуры (ЭВМ и коммутаторов) от сети 27 В;

- выполнение ФПО на трех высокопроизводительных ЭВМ (перечень выполняемых задач (программных модулей) приведен в 3.2).

**3.2 Основные задачи, решаемые в модуле СОЦ ПО**

СОЦ ПО можно разделить на ряд обособленных задач, которые будут реализовываться в виде отдельных программных модулей, взаимодействующих меду собой через программный диспетчер.

Можно выделить следующие модули:

1) Модуль начального пуска и инициализации СОЦ ПО.

*Обеспечивает запуск процессов и потоков, инициализация графической подсистемы, инициализация сетевой подсистемы, подготовка к работе сенсорного манипулятора и пульта управления.*

2) Модули сетевого обмена.

*Обеспечивают прием и передачу информации по каналам Ethernet*

3) Модуль внутреннего обмена

*Обеспечивают прием и передачу по имитируемым линиям связи – МПИ, VME.*

4) Модуль управления прерываниями

*Обеспечивает тактирование потоков и процессов для корректной работы адаптированного ПО Багет-23В*

5) Модуль адаптированного ПО Багет-23В

*Содержит ПО Багет-23В, специально адаптированное для работы на УВМ типа РАМЭК 113 под операционной системой Astra Linux.*

6) Модуль имитации аппаратуры СОЦ

*Обеспечивает прием, трансляцию, пересчет и подготовку информации от РМИ-КТ, далее упаковку данных в формат линии МПИ для передачи в адаптированное ПО Багет-23В.*

7) Модуль подготовки информации о действиях оператора

*Обеспечивает подготовку и упаковку информации о действиях оператора для передачи в РМИ-ИКТ.*

8) Модуль выдачи информации о трассах целей

*Обеспечивает подготовку и упаковку трасс целей от адаптированного ПО для передачи в РМИ-ИКТ.*

9) Модуль имитации рельефа и метеоусловий

*Обеспечивает имитацию снижения амплитуды сигналов от целей в зависимости от условий задачи, поставленной инструктором.*

10) Модуль помеховой обстановки.

*Обеспечивает имитацию постановки пассивной или активной помехи, в зависимости от условий задачи, поставленной инструктором.*

11) Модуль имитации АФК аппаратуры СОЦ

*Обеспечивает имитацию неисправности блоков и узлов СОЦ по командам инструктора СОЦ*

12) Модуль АФК

*Обеспечивает проведение и сбор результатов АФК.*

13) Модуль автономного формирования заданий для тренировки \_\_\_\_ СОЦ

*Обеспечивает запуск готовых сценариев тренировки, их корректировку и создание новых сценариев.*

14) Модуль создания, сохранения, загрузки, поиска сценариев тренировки.

*Обеспечивает возможность создания, сохранения, загрузки, поиска сценариев тренировки, в том числе с использованием типовых заданий на тренаж в качестве шаблона.*

15) Модуль имитации ВО

*Обеспечивает имитацию воздушной обстановки с учетом типов целей и государственной принадлежности.*

16) Модуль регистрации работы обучаемого

*Обеспечивает автоматический учет и протоколирование действий обучаемых.*

17) Модуль автоматического формирования оценки

*Обеспечивает автоматическую подготовку отчета о тренировке и оценку знаний и умений обучаемых, выдачу результатов на рабочие места инструкторов СОЦ и комплексного тренажера.*

18) Модуль взаимодействия с АРМ ИКТ

*Обеспечивает прием и передачу данных с АРМ ИКТ*

19) Модуль взаимодействия с ПБУ ПО

*Обеспечивает прием и передачу данных с ПБУ ПО*

20) Модуль отображения действия обучаемого

*Обеспечивает отображение действий обучаемого на мониторе инструктора*

21) Модуль работы с ЦКМ

*Обеспечивает выбор и отображение цифровой карты местности из заданного набора.*

22) Модуль работы с фоновой обстановкой

*Обеспечивает установку параметров – времени года, времени суток, метеообразований.*

Состав и задачи модулей могут изменяться на этапе ТП.

**4. Описание организации работы с применением СОЦ ПО**

**4.1 Описание общего процесса функционирования**

Аппаратно-программный комплекс для модуля СОЦ ПО из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М обеспечивает выполнение задач в различных режимах работы путем взаимодействия с составными частями тренажера ЗРК и внешними абонентами (изд. 83Т455).

Работа СОЦ ПО может быть изложена в такой последовательности:

а) работа составных частей СОЦ ПО при подготовке комплексного тренажера ЗРК к тренировке;

б) работа составных частей СОЦ ПО при подготовке исходных данных и проведении тренировки.

в) работа администратора безопасности информации.

**4.1.1 Взаимодействие и принцип работы составных частей СОЦ ПО при подготовке комплексного тренажера к тренировке**

При подаче внешнего питания ( +27 В) на ЭВМ РМИ, ЭВМ имитатора аппаратуры СОЦ, ЭВМ с адаптированным ПО Багет-23В и составные части СОЦ ПО производится их самоконтроль, загрузка системного и специального ПО ЭВМ РМИ, идентификация и авторизация пользователя – инструктора тренажера, загрузка функционального программного обеспечения ЭВМ имитатора аппаратуры СОЦ, ЭВМ с адаптированным ПО Багет-23В, включение концентраторов локальных вычислительный сетей.

ФПО ЭВМ РМИ при запуске производит запуск функционального ПО, а также функциональный контроль интерфейсов взаимодействия с составными частями модуля (концентраторы ЛВС) и отображение результатов контроля в виде схем на ЖКИ инструктора.

При исправности концентраторов внешних ЛВС ФПО ЭВМ РМИ производит инициализацию обмена и установку связи с АРМ ИКТ, ПБУ, ЭВМ имитатора аппаратуры СОЦ, ЭВМ с адаптированным ПО Багет-23В по каналу ЛВС, отображение на ЖКИ АРМ инструктора информации о состоянии связи и параметрах работы сопрягаемых внешних абонентов.

ФПО ЭВМ РМИ обеспечивает контроль интерфейса связи с пультом и манипулятором и проверку их функционирования, производит сбор, обработку и отображение состояние и процесса работы всех модулей тренажера.

ФПО ЭВМ АРМО производит тестирование запуск функционального ПО, а также функциональный контроль интерфейсов взаимодействия с составными частями модуля (концентраторы ЛВС, устройства ввода, связь с ЭВМ имитатором аппаратуры СОЦ) и в случае обнаружения проблем – выводит соответствующее сообщение на штатные мониторы.

**4.1.2 Взаимодействие и принцип работы составных частей СОЦ ПО в режиме тренировки.**

Инструктор комплексного тренажера единого комплекса учебно-тренировочных средств ЗРК 9К317М назначает режимы автономной или комплексной тренировки на тренажере СОЦ ПО.

В режиме автономной тренировки с АРМ инструктора комплексного тренажера на ЭВМ РМИ выдается информация о плане тренировки и личных данных обучаемых.

В режиме комплексной тренировки АРМ инструктора комплексного тренажера выдает на РМИ информацию о составе тренажеров, принимающих участие в тренировке, информацию о режимах боевой работы тренажеров, параметрах трасс общей воздушной обстановки, картографической информацией, получая от них информацию о действиях обучаемого расчета, результатах проведенной тренировки с оценками обучающихся.

ЭВМ РМИ передает на ЭВМ имитатора аппаратуры СОЦ параметры ВО, координаты ТС, курс, крен, тангаж, данные по рельефу и метеоусловиям, помеховую обстановку. По этим данным ЭВМ имитатора аппаратуры СОЦ формирует пакеты по целям и меткам и передает их в ЭВМ с адаптированным ПО Багет-23В где они отображаются штатными алгоритмами на мониторах. Действия обучаемого, а также трассы целей отправляются обратно на ЭВМ имитатора аппаратуры СОЦ и ЭВМ РМИ.

**4.1.3 Взаимодействие и принцип работы составных частей АПК в режиме комплексной тренировки**

Для организации комплексной тренировки на АРМ инструктора комплексного тренажера с помощью программных модулей ФПО предает на ЭВМ РМИ по каналу ЛВС команду начала тренировки.

ЭВМ РМИ при получении от АРМ инструктора комплексного тренажера команды начала тренировки на модулях производится подготовка к боевой работе. Действия обучаемых фиксируются на РМИ тренажера СОЦ ПО в формализованном виде (коды нажатых клавиш на клавиатуре, действия оператора на экранах АРМ обучаемых). Данные протоколирования боевой работы расчета могут быть выданы в реальном времени на АРМ инструктора комплексного тренажера (при наличии запроса).

При получении от АРМ инструкторов модулей донесений об окончании подготовки к боевой работе инструктор тренажера ПБУ выдает на РМИ СОЦ ПО команду на запуск задачи воздушного налета.

При этом на РМИ СОЦ ПО выдается по каналам ЛВС параметры трасс единой ВО в реальном времени, а ФПО РМИ предаёт на АРМ инструктора тренажера ЗРК донесения об этапах боевой работы.

По окончании заданного времени воздушного налета или по команде инструктора комплексного тренажера проводится остановка имитации целей единой воздушной обстановки.

По окончании тренировки производится ее автоматизированная оценка с учетом полученной от РМИ СОЦ ПО информации с формированием отчета о тренировке, который выдается на печать на устройство УД-711М, отправляется на изд. 83Т455, выгружается на внешний носитель (при необходимости).

В режиме комплексной тренировки работа ЭВМ имитатора аппаратуры СОЦ и ЭВМ с адаптированным ПО Багет-23В проходит как указано в главе 4.1.2.

**4.1.4 Работа администратора безопасности информации**

Программное средство автоматизированного рабочего места администратора безопасности информации (ПС АРМ АБИ) предназначено для автоматизации повседневной деятельности администраторов безопасности информации при выполнении работ входящих в домен ALD серверах и рабочих станциях, функционирующих под управлением операционной системы специального назначения «Astra Linux Special Edition» (управляемых устройствах).

ПС АРМ АБИ предоставляет администратору безопасности эргономичный графический интерфейс, представляющий собой набор экранных форм для ввода, редактирования и просмотра информации.

ПС АРМ АБИ имеет визуальную среду администрирования, позволяющую администратору безопасности информации в графическом интерфейсе решать функциональные задачи и обеспечивать:

- контроль состояния управляемых устройств;

- контроль целостности неизменных компонент программного обеспечения;

- корректировку параметров идентификации и полномочий доступа к защищаемым ресурсам;

- генерацию, установку и смену паролей доступа пользователей с использованием программы генерации паролей;

- блокировка/разблокировка пользователей (в том числе их текущих сессий на устройствах домена) по команде АБИ;

- отображение состояния антивирусной защиты управляемых устройств;

- тестирование работоспособности средств защиты

Программа АРМ АБИ обеспечивает решение следующих основных задач:

1) построение списка доменов и реестра управляемых устройств, и контроль состояния управляемых устройств;

2) управление разграничением доступа к ресурсам управляемых устройств;

3) управление доступом пользователей к устройствам домена;

4) генерация, установка и смена паролей учетных записей пользователей с использованием программы генерации паролей;

5) проведение регламентного контроля целостности на управляемых устройствах с возможностью отображения и документирования результатов;

6) управление работой и контроль состояния средств антивирусной защиты на управляемых устройствах;

7) тестирование работоспособности средств защиты информации на управляемых устройствах с возможностью отображения и документирования результатов;

8) формирование и просмотр журналов системы централизованного

протоколирования;

9) стирание защищаемой информации на управляемых устройствах по команде администратора безопасности информации;

10) резервное копирование данных (конфигурации) управляемых доменов;

11) возможность передачи на АРМ АБИ экстренного сообщения о возникновении внештатной ситуации («Работа под принуждением») с любого управляемого устройства;

12) оповещение администратора безопасности о фактах, или попытках НСД к защищаемым ресурсам;

13) передачу событий НСД на АРМ АБИ верхнего уровня.

* 1. **Описание типовых сценариев тренировки**

**4.2.1 Общие предложения по вариантам налета СВН**

Перечень ТТХ для каждого типа самолета участвующего в налете, имеет в своем составе следующие компоненты: минимальная и максимальные скорости полета. ЭПР самолета (в зависимости от ракурса); количество точек подвески оружия «воздух-поверхность»; вектор дальностей обнаружения типовых наземных целей системами обнаружения самолета; ракурсность систем обнаружения самолета; канальность системы управления оружием; энергетический потенциал станции активных помех; частотные диапазоны помехопостановки; максимальное количество РЛС в одном частотном диапазоне, которым может быть поставлена прицельная помеха; минимальная ширина полосы постановки прицельной помехи; и др.

Перечень ТТХ для каждого типа управляемых ракет имеет в своем составе следующие компоненты: максимальная/минимальная дальность пуска и ракурсность оружия; параметры, определяющие траекторию ракеты; циклограмму подготовки к пуску; минимальное время между пусками; скорость полета; вероятности поражения типовых наземных целей; ЭПР ракеты; и др.

Перечень ТТХ для каждого типа крылатых ракет имеет в своем составе: ЭПР ракеты в зависимости от ракурса, тип системы наведения, дальности действия головок самонаведения (при наличии);

Перечень ТТХ для каждого типа баллистических ракет имеет в своем составе: ЭПР ракеты, минимальную/максимальную дальность пуска (опорную траекторию полета БР) и др.

Перечень ТТХ для каждого типа БЛА, имеет в своем составе следующие компоненты: ЭПР БЛА; минимальная и максимальная скорости полета; диапазон высот полета; дальности системы обнаружения/целеуказания/разведки; максимальная/минимальная дальность пуска и ракурсность оружия (при наличии); и др.

Вышеуказанные параметры средств СВН могут корректироваться в рамках реальных ТТХ средств СВН в процессе обучения боевых расчетов ЗРК инструкторами единого комплекса учебно-тренировочных средств ЗРК 9К317М со своих рабочих мест для обеспечения возможности изменения имитируемой воздушной обстановки.

Войсковая ПВО будет применяться в следующих основных условиях:

**На первом этапе** боевых действий (пока система ПВО не подавлена) система ПВО будет вести боевые действия в условиях, массированного применения крылатых ракет типа RGM/UGM-109, AGM-158, ракет «воздух-поверхность» большой дальности АGM-154-ER(США), Delilah (Израиль), запускаемых вне зоны действия системы ПВО. На данном этапе боевых действий возможно массированное применение сверхдешевых БЛА, а также возможны удары нестратегическими баллистическими ракетами.

**На втором этапе** боевых действий основные силы пилотируемой и беспилотной авиации будут задействованы для уничтожения системы ПВО. В первую очередь подвергнутся атаке зенитные комплексы средней дальности «Бук-М3».

Общая схема подавления будет следующей:

– поиск зон дислокации ЗРК с использованием всех видов разведки (спутниковой, авиационной, агентурной и т.д.)

– провокация излучения ЗРК с использованием ложных целей или ложных команд оповещения от вышестоящего АСУ ПВО;

– одновременный с провокацией излучения удар противорадиолокационными ракетами по включившимся средствам ПВО; запуск ракет будет осуществляться либо вне зоны действия системы ПВО, либо с кратковременным заходом с малых высот в зону действия системы ПВО; удар может прикрываться помехопостановщиками типа ЕF-18G;

– удар по позициям боевых средств ЗРК ракетами большой и средней дальности (типа AGM-154 JSOW, JSOW-ЕR) со спутниковой системой наведения и/или телевизионной или тепловизионной системами наведения (удар производился через 10-15 минут после обнаружения позиции ЗРК);

– поиск и уничтожение выживших средств ПВО беспилотной авиацией.

**На третьем этапе боевых действий** (когда система ПВО в основном подавлена) ударные самолеты наносят основные удары с помощью корректируемых и неуправляемых бомб, а также оснащаются для самообороны небольшим количеством ложных целей типа MALD и противорадиолокационных ракет типа AARGM. В случае внезапного обнаружения выжившего зенитного ракетного комплекса, действующего «из засады», самолеты противника запускают ложные цели и противорадиолокационные ракеты в направлении ЗРК, отворачивают и уходят из зоны действия ЗРК, а также вызывают дежурную группу подавления. В логике действий авиации противника внезапно обнаруженный ЗРК, как правило, имеет статус непосредственно угрожающей цели, имеет более высокий приоритет, чем назначенная в полетном задании цель и подлежит первоочередному уничтожению. Параллельно с оснащением ударных групп средствами самообороны ведется непрерывный поиск и уничтожение выживших ЗРК, в основном, с использованием специальных самолетов радиотехнической RC‑135 (США) и радиолокационной разведки E-8(США) а также разведывательно-ударных БЛА типа MQ-9А (США).

# 

# 4.2.2 Предлагаемые варианты налетов средств воздушного нападения противника

Тактико-технические характеристики моделируемых СВН принимаются в соответствии с материалами НИР «Грифон».

Предполагается, что разведка противника до начала каждого авиаудара достаточно точно определила дислокацию и примерный состав боевых средств ЗРК «Бук-М3». При этом местоположение конкретных боевых машин и их точное количество противнику неизвестно.

Авианалёты выполняется под прикрытием воздушных комплексов РЭБ и состоит из трёх последовательных этапов. Цель первого этапа – создание общей помеховой обстановки для снижения возможностей радиолокационных средств ПВО по обнаружению средств воздушного нападения противника. Для этого противник применяет специализированные самолёты РЭБ, барражирующие на безопасном расстоянии от предполагаемой дислокации элементов системы ПВО, в режиме постановки заградительных шумовых помех в диапазоне боевой работы радиолокационных средств ПВО. Самолёты РЭБ продолжают работу на втором и третьем этапах. Включение и отключение помех при проведении тренировки боевых расчетов ЗРК производит инструктор единого комплекса учебно-тренировочных средств ЗРК 9К317М со своего рабочего места. При проведении тренировки боевых средств ЗРК автономно Включение и отключение помех производят инструктора с рабочих мест модулей.

Целью второго этапа является вывод из строя радиолокационных средств системы ПВО. Для этого противник производит удар противорадиолокационными ракетами (ПРР) последних модификаций с самолётов тактической авиации. В первую очередь целенаправленно поражаются РЛС обнаружения кругового обзора, затем – станции наведения зенитных ракет. Работа тактической авиации происходит под прикрытием самолётов РЭБ, начавших работу на первом этапе. Кроме того, удар ПРР предваряется пуском ложных целей, способных сымитировать группу самолётов тактической авиации противника. Ложные цели необходимы для обеспечения непрерывной работы станции кругового обзора и включения станций наведения зенитных ракет, а также доразведки мест их дислокации и типов задействованных средств ПВО.

Цель третьего этапа – поражение прикрываемой группировки ракетных войск. Для этого противник применяет с ударных беспилотных летательных аппаратов управляемые ракеты класса «воздух-поверхность» (УР «В‑П»).

Общая схема построения налётов при проведении тренировок боевых расчетов представлена на рисунке 10.

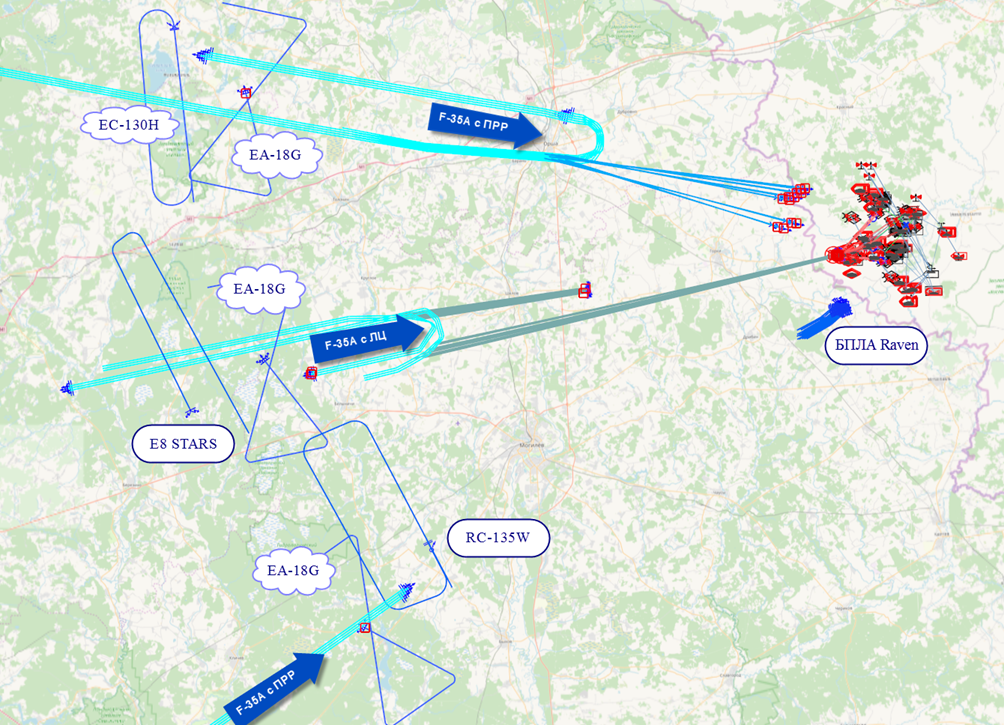


Рисунок 10 - Общая схема построения налётов при проведении тренировок боевых расчетов

Траектории полета самолетов, рубежи и высота применения оружия, наряды самолетов, направленных на подавление выбранной цели, могут корректироваться инструкторами в зависимости от создаваемой воздушной обстановки.

Варианты сценариев могут иметь в своем составе следующие средства воздушного нападения:

Группа обеспечения:

* 1 разведывательный самолет RC-135W Rivet Joint;
* 1 самолет управления и радиоэлектронной борьбы EC-130H Compass Call;
* 1 самолет боевого управления и целеуказания Е-8C Joint STARS;
* 3 самолета постановщика активных помех EA-18G.

Группа прикрытия: истребители ПВО F-22A.

Группа подавления ПВО:

* варьируется от 1 до 20 самолетов F-35A, каждый из которых вооружен 4 ПРР AGM-88E;
* 6 самолетов F-35А, каждый из которых несет 4 ложные цели MALD.

Группа разведывательных БПЛА: до 20 БПЛА Raven.

**4.2.2.1 Сценарий 1 удар по ЗРК одиночным самолетом F-35A**

Удар по ЗРК выполняет 1 самолёт F-35A. Тактика действий F-35A заключается в следующем: приближается к позиции ЗРК со своего азимутального направления (устанавливается инструктором), осуществляя полёт на постоянной высоте 12000 м со скоростью 500 м/с до дальности 3 км до позиций ЗРК, после чего возвращается на аэродром.

## 4.2.2.2 Сценарий 2 удар по ЗРК одиночным самолетом F-35A совершающим маневр змейка

Удар по ЗРК выполняет 1 самолёт F-35A. Тактика действий F-35A заключается в следующем: приближается к позиции ЗРК со своего азимутального направления (устанавливается инструктором), осуществляя полёт на высоте от 5000 до 8000 м со скоростью 200-500 м/с до дальности 3000 м до позиций ЗРК, после чего возвращается на аэродром. В процессе полета осуществляет маневр змейка в вертикальной плоскости с перегрузкой не менее 3ց и амплитудой 3000 м.

## 4.2.2.3 Сценарий 3 удар по ЗРК одиночным самолетом F-35A совершающим маневр кабрирование (пикирование)

## Удар по ЗРК выполняет 1 самолёт F-35A. Тактика действий F-35A заключается в следующем: приближается к позиции ЗРК со своего азимутального направления (устанавливается инструктором), осуществляя полёт на высоте от 5000 со скоростью 500 м/с на дальности 50000 м до позиции ЗРК осуществляет маневр кабрирование (пикирование) на высоту 8000 (2000) м и затем совершает полёт на высоте от 8000 (2000) со скоростью 500 м/с до дальности 3000 м до позиций ЗРК, после чего возвращается на аэродром. В процессе полета осуществляет маневр змейка в вертикальной плоскости с перегрузкой не менее 3ց и амплитудой 3000 м.

## 4.2.2.4 Сценарий 4 удар по ЗРК группой самолетом F-35A построением ромб (квадрат).

Удар по ЗРК выполняют 4 самолёта F-35A. Тактика действий F-35A заключается в следующем: приближаются к позиции ЗРК со своего азимутального направления построением ромб (квадрат) с дистанцией по фронту до 500 м, осуществляя полёт на высоте 5000 м со скоростью 500 м/с до дальности 3000 м до позиций ЗРК, после чего совершают разворот и возвращаются на аэродром. В процессе полета на дальности 30000 м от позиций ЗРК осуществляет маневр по скорости с перегрузкой до 10 ց.

## 4.2.2.5 Сценарий 5 удар по ЗРК группой самолетом F-35A построением клин

Удар по ЗРК выполняют 4 самолёта F-35A. Тактика действий F-35A заключается в следующем: приближаются к позиции ЗРК со своего азимутального направления построением клин с дистанцией по фронту до 500 м, осуществляя полёт на высоте 5000 м со скоростью 500 м/с до дальности 3000 м до позиций ЗРК, после чего совершают разворот и возвращаются на аэродром.

## 4.2.2.6 Сценарий 6 удар по ЗРК группой самолетом F-35A построением фронт

Удар по ЗРК выполняют 4 самолёта F-35A. Тактика действий F-35A заключается в следующем: приближаются к позиции ЗРК со своего азимутального направления построением фронт с дистанцией по фронту до 500 м и углом раскрыва строя 90 градусов, осуществляя полёт на высоте 8000 м со скоростью 500 м/с до дальности 3000 м до позиций ЗРК, после чего совершают разворот и возвращаются на аэродром.

## 4.2.2.7 Сценарий 7 удар по ЗРК зависающим вертолетом

Удар по ЗРК выполняют 1 вертолет «Апач». Тактика действий вертолета заключается в следующем: приближаются к позиции ЗРК со своего азимутального направления, осуществляя полёт на высоте 1000 м со скоростью до 200 м/с до дальности 3000 м до позиций ЗРК, после чего совершают разворот и возвращаются на аэродром. В процессе полета с осуществляет зависания на дальностях 30000, 25000, 20000, 15000, 10000, 5000 м от позиции ЗРК с высотой 15-50 м.

## 4.2.2.8 Сценарий 8 удар по ЗРК имитацией авианалета

В сценарии рассматривается действие зенитного ракетного дивизиона средней дальности. Средства воздушного нападения противника осуществляют удары с больших высот без захода в зону поражения ЗРК средней дальности действия. Численный состав средств воздушного нападения противника, участвующих в авиаударе, представлен в таблице 3.

На первом этапе применяются самолёты РЭБ ЕA-18G. Каждый самолёт ЕA-18G ставит заградительную шумовую помеху в диапазонах работы выявленных с помощью радиотехнической разведки РЛС ПВО.

На втором этапе самолёты F-35A применяются как носители ПРР и как носители ложных целей. Каждый самолёт-носитель ПРР проводит радиотехническую разведку радиоизлучающих целей и вооружён четырьмя противорадиолокационными ракетами AGM-88E AARGM. Каждый самолёт-носитель ложных целей оснащён четырьмя ложными целями типа ADM-160.

На третьем этапе применяются ударные беспилотные летательные аппараты (БПЛА) типа Avenger. Каждый БПЛА оснащён системой оптико-электронного обнаружения наземных целей и вооружён восемнадцатью управляемым ракетами класса «воздух-поверхность» типа AGM-114 с лазерной системой наведения.

Таблица 3 – Количественный состав авиационных налётов противника в сценарии 8

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Варианты  налёта | F-35A с ПРР | ПРР | БПЛА  с УРВП | УРВП | ЕA-18G РЭБ | F-35A с ЛЦ | ЛЦ | Самолетов  и БПЛА  в налёте |
| 1 | 1 | 4 | 4 | 72 | 1 | 1 | 4 | 7 |

На дальности 145 – 155 км от места предполагаемой дислокации подавляемой ЗРС барражируют один самолёт РЭБ ЕA-18G. Самолёт РЭБ прикрывает отдельное азимутальное направление заградительной шумовой помехой. Плотность мощности помехи составляет 2000 Вт/МГц в диапазонах работы СОУ и РПН «Бук‑М3» и 600 Вт/МГц в диапазонах работы СОЦ «Бук‑М3».

Самолёт РЭБ барражирует на высоте 8000 м по траектории типа «восьмёрка» длиной около 42 км и шириной около 18 км. «Восьмёрка» ориентирована перпендикулярно направлению на ЗРК (рисунок 11). Прикрываемые заградительной шумовой помехой азимутальные направления: «северное» – азимут 70– 85°; «западное» – азимут 93– 108°; «южное» – азимут 115– 130° (меняются инструкторами в зависимости от создаваемой воздушной обстановки и направлением авианалета).

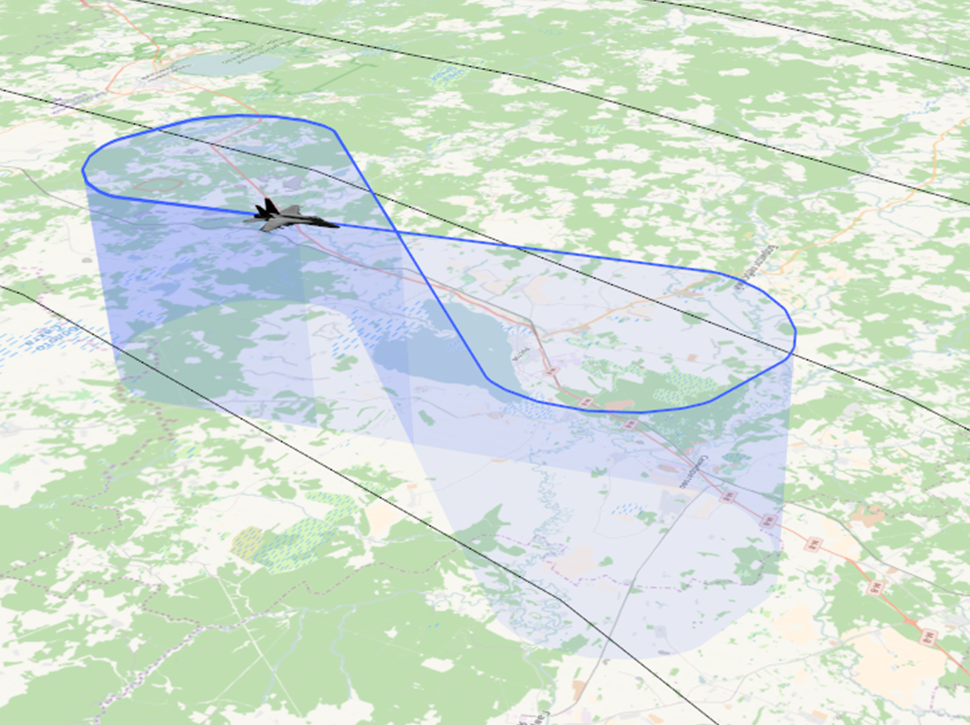


Рисунок 11 – Траектория полета самолета РЭБ

Атака ЗРК самолётом тактической авиации F-35A производится с «северного» направления (меняются инструкторами в зависимости от создаваемой воздушной обстановки) под прикрытием самолётов РЭБ на всём протяжении налёта. Прикрытие РЭБ необходимо для скрытия факта пуска ПРР и затруднения их обнаружения вплоть до момента поражения средств ПВО и для скрытия факта разделения одиночной цели, самолёта-носителя ЛЦ, на множественные цели. Включение помех производится за 20-30 секунд до пуска ЛЦ. Выключение – после окончания пуска ЛЦ и отворота самолёта-носителя ЛЦ.

Пуск ложных целей производится по четыре ЛЦ. Самолёт-носитель ЛЦ производит пуск ЛЦ с такими расчётом, чтобы ЛЦ были обнаружены станцией кругового обзора и станциями наведения зенитных ракет до применения ПРР самолетом, а также продолжали провоцировать работу наибольшего числа РЛС всё время, необходимое для обнаружения указанных РЛС, пуска по ним ПРР и подлёта ПРР к цели. Таким образом, исключается возможность выключения РЛС с целью защиты. Вторая волна пуска ЛЦ обеспечивает выявление оставшихся радиолокационных средств ПВО.

Удар по ЗРК выполняет 1 самолёт F-35A. Сначала производится обнаружение излучения и целенаправленный удар ПРР AGM-88E по обзорным станциям ЗРК. Приоритетные цели при целераспределении – станции обнаружения целей, затем – все остальные РЛС при наличии боекомплекта.

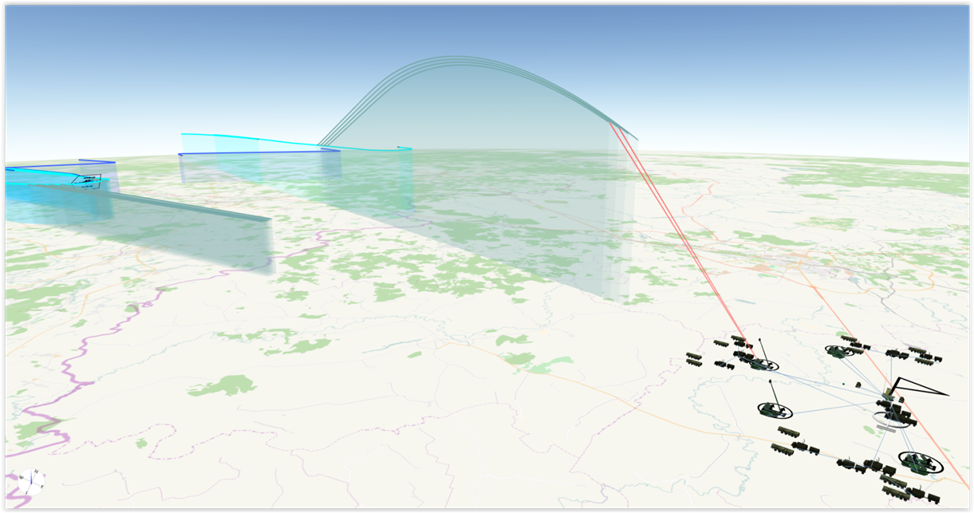


Рисунок 12 – Применение ПРР тактической авиации

Тактика действий авиации F-35A на втором этапе одинаковая и заключается в следующем. F-35A приближается к позиции ЗРК со своего азимутального направления (меняются инструкторами в зависимости от создаваемой воздушной обстановки), осуществляя полёт на постоянной высоте 12000 м со скоростью 500 м/с. По достижении рубежа атаки (80÷90 км от позиций ЗРК) F-35A осуществляет пуск ПРР по обнаруженным радиоизлучающим средствам ЗРК, после чего возвращается на аэродром. Скорость ПРР на участке пикирования на дальностях перехвата составляет величину в диапазоне от 400 м/с до 1100 м/с, а угол места подхода к цели – около 35– 40°.

При проведении расчётов вероятность уничтожения РЛС с помощью ПРР принята 0,8. ЭПР противорадиолокационной ракеты принята равной 0,06 кв.м в диапазоне длин волн СОУ и 0,334 кв.м. в диапазоне длин волн СОЦ «Бук‑М3».

Атака ЗРК беспилотными летательными аппаратами производится с одного направления: «северное» – азимут 60°; (меняются инструкторами в зависимости от создаваемой воздушной обстановки).

Действует одна группа БПЛА Avenger из четырёх БПЛА. Группа приближаются к позиции ЗРК одновременно на высоте 60 м. По достижении рубежа начала атаки (12÷15 км) группы поднимаются на высоту 1000 м. Далее группа БПЛА атакует наземные цели управляемыми ракетами класса «воздух-поверхность» типа AGM-114 с лазерной системой наведения с дальности порядка 3 ÷ 4.5 км. При проведении расчётов вероятность поражения наземной цели ракетой типа AGM-114 была принята равной 0,8. ЭПР AGM-114 принята равной 0,06 кв.м в диапазоне длин волн СОУ и 0,34 кв.м. в диапазоне длин волн СОЦ «Бук‑М3».

## 4.2.2.9 Сценарий 9 удар по ЗРК имитацией авианалета

В сценарии рассматривается действие зенитного ракетного дивизиона средней дальности. Средства воздушного нападения противника осуществляют удары с больших высот без захода в зону поражения ЗРК средней дальности действия. Численный состав средств воздушного нападения противника, участвующих в авиаударе, представлен в таблице 4.

На первом этапе применяются 2 самолёта РЭБ ЕA-18G. Каждый самолёт ЕA-18G ставит заградительную шумовую помеху в диапазонах работы выявленных с помощью радиотехнической разведки РЛС ПВО с разных направлений (задаются инструкторами в зависимости от создаваемой воздушной обстановки).

На втором этапе самолёты F-35A применяются как носители ПРР и как носители ложных целей. Каждый самолёт-носитель ПРР проводит радиотехническую разведку радиоизлучающих целей и вооружён четырьмя противорадиолокационными ракетами AGM-88E AARGM. Каждый самолёт-носитель ложных целей оснащён четырьмя ложными целями типа ADM-160.

На третьем этапе применяются ударные беспилотные летательные аппараты (БПЛА) типа Avenger. Каждый БПЛА оснащён системой оптико-электронного обнаружения наземных целей и вооружён восемнадцатью управляемым ракетами класса «воздух-поверхность» типа AGM-114 с лазерной системой наведения.

Таблица 4 – Количественный состав авиационных налётов противника в сценарии 2

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Варианты  налёта | F-35A с ПРР | ПРР | БПЛА  с УРВП | УРВП | ЕA-18G РЭБ | F-35A с ЛЦ | ЛЦ | Самолетов  и БПЛА в налёте |
| 2 | 2 | 8 | 8 | 144 | 2 | 2 | 32 | 14 |

На дальности 145 – 155 км от места предполагаемой дислокации подавляемой ЗРС барражируют два самолёта РЭБ ЕA-18G. Каждый самолёт РЭБ прикрывает отдельное азимутальное направление заградительной шумовой помехой (задаются инструкторами в зависимости от создаваемой воздушной обстановки). Плотность мощности помехи составляет 2000 Вт/МГц в диапазонах работы СОУ и РПН «Бук-М3» и 600 Вт/МГц в диапазонах работы СОЦ «Бук-М3».

Каждый самолёт РЭБ барражирует на высоте 8000 м по траектории типа «восьмёрка» длиной около 42 км и шириной около 18 км. «Восьмёрка» ориентирована перпендикулярно направлению на подавляемую ЗРК (рисунок 2). Прикрываемые заградительной шумовой помехой азимутальные направления: «северное» – азимут 70– 85°; «западное» – азимут 93– 108° (задаются инструкторами в зависимости от создаваемой воздушной обстановки).

Атака ЗРК самолётами тактической авиации F-35A производится с «северного» и «западного» направлений под прикрытием самолётов РЭБ на всём протяжении налёта. Прикрытие РЭБ с «северного» и «западного» направлений необходимо для скрытия факта пуска ПРР и затруднения их обнаружения вплоть до момента поражения средств ПВО. С «западного» направления прикрытие самолётом РЭБ необходимо для скрытия факта разделения одиночной цели, самолёта-носителя ЛЦ, на множественные цели. Включение помех производится за 20-30 секунд до пуска ЛЦ. Выключение – после окончания пуска ЛЦ и отворота самолёта-носителя ЛЦ.

Пуск ложных целей производится в две волны по шестнадцать ЛЦ на каждой. В первой волне самолёт-носитель ЛЦ производит пуск ЛЦ с такими расчётом, чтобы ЛЦ были обнаружены станцией кругового обзора и станциями наведения зенитных ракет до применения ПРР ударными самолетами с ПРР №1 и №2, а также продолжали провоцировать работу наибольшего числа РЛС всё время, необходимое для обнаружения указанных РЛС, пуска по ним ПРР и подлёта ПРР к цели.

Удар по системе ПВО последовательно выполняют 2 самолёта F-35A. Сначала с «северного» направления самолет №1 производит обнаружение излучения и целенаправленный удар ПРР AGM-88E по обзорным станциям ЗРС. Сразу после завершения удара самолета №1 аналогичные действия тем же оружием и с «западного» направления выполняет самолет №2. Приоритетные цели при целераспределении – станции обнаружения целей, затем – все остальные РЛС при наличии боекомплекта.

Каждый следующий самолет F-35A наносит удар через промежуток времени, достаточный для поражения намеченных целей противорадиолокационными ракетами, пущенными предыдущей группой.

Тактика действий всех F-35A одинаковая и заключается в следующем. Каждая группа приближается к позиции ЗРС со своего азимутального направления, осуществляя полёт на постоянной высоте 12000 м со скоростью 500 м/с. По достижении рубежа атаки (80÷90 км от ЗРС) F-35A осуществляет пуск ПРР по обнаруженным радиоизлучающим средствам ЗРС, после чего возвращается на аэродром. Скорость ПРР на участке пикирования на дальностях перехвата составляет величину в диапазоне от 400 м/с до 1100 м/с, а угол места подхода к цели – около 35– 40°.

При проведении расчётов вероятность уничтожения РЛС с помощью ПРР принята 0,8. ЭПР противорадиолокационной ракеты принята равной 0,06 кв.м в диапазоне длин волн СОУ и 0,334 кв.м. в диапазоне длин волн СОЦ «Бук М3».

Атака ЗРК беспилотными летательными аппаратами производится с двух направлений: «северное» – азимут 60°, «западное» – азимут 100° (задаются инструкторами в зависимости от создаваемой воздушной обстановки).

На каждом направлении действует одна группа БПЛА Avenger из четырёх БПЛА. Группы со всех направлений приближаются к позиции ЗРК одновременно на высоте 60 м. По достижении рубежа начала атаки (12-15 км) группы поднимаются на высоту 1000 м, обнаруживают и распознают наземные цели с помощью бортовой оптико-электронной станции. Далее группы БПЛА атакуют наземные цели управляемыми ракетами класса «воздух-поверхность» типа AGM-114 с лазерной системой наведения с дальности порядка 3 - 4.5 км. ЭПР AGM-114 принята равной 0,06 кв.м в диапазоне длин волн СОУ и 0,34 кв.м. в диапазоне длин волн СОЦ «Бук М3».

**4.2.2.10** **Сценарий 10 осуществление доразведки средств ЗРК с помощью БПЛА с последующим нанесением удара самолетами F-35A, вооруженными планирующими бомбами**

Самолеты RC-135W, EC-130H, EA-18G, E-8C Joint STARS, F-22A, входящие в группу обеспечения и группу прикрытия, совершают барражирование в отведенных им зонах на удалении около 150 км от позиций ЗРК «Бук-М3» в течение всего налета. Самолет RC-135W обеспечивает разведку наземных целей с высоты 10 км. Самолет EC-130H и самолеты EA-18G создают сложную помеховую обстановку заградительной шумовой помехой в диапазонах работы выявленных с помощью бортовых систем РТР РЛС ПВО противника. Плотность мощности помехи в зависимости от диапазона работы и ширины полосы РЛС для различных средств ЗРК составляет 400 Вт/МГц для СОЦ «Бук-М3». Барражируя на высоте 10 км, E-8C Joint STARS обеспечивает связь и синхронизацию действий во время всей операции. Самолеты F-22A выполняют задачу воздушного прикрытия. Зоны барражирования у этих групп находятся на высоте 8 км.

|  |
| --- |
|  |

|  |
| --- |
| Рисунок 13 – Зоны барражирования самолетов обеспечения |

В сценарии 3 группа подавления ПВО снижает эффективность ПВО в такой степени, что этого достаточного для эффективного решения задач доразведки объектов войсковой группировки с помощью БПЛА с последующим нанесением удара по полученной от беспилотников информации самолетами F-35A, вооруженными планирующими бомбами.

Запуск БПЛА Raven численностью до 20 штук производится с передовых рубежей (около 30 км от позиций средств ЗРК). Осуществляя пролет со скоростью 20 м/с над позициями ЗРК, они производят доразведку (рисунок 14) позиций, обнаруженных RC-135W и другими средствами разведки, и передают уточненные координаты для ударной группы F-35A.

После получения точных координат объектов по информации от БПЛА, ударные группы F-35A, несущие по 20 ПАБ GBU-53 Stormbreaker-II на каждом самолете, кратковременно набирают высоту в 12 км для применения ПАБ на дальностях около 60 км и возвращаются на аэродром (рисунок 15). Такая тактика применения обеспечивает необходимую дальность полета планирующих бомб.

|  |
| --- |
|  |

|  |
| --- |
| Рисунок 14 – Доразведка позиций артиллерии БПЛА Raven |

|  |
| --- |
|  |

|  |
| --- |
| Рисунок 15 – Применение ПАБ GBU-53 Stormbreaker-II |

Каждая из трех групп производит пуск бомб только по выделенной ей группе целей (СОЦ, ПБУ, СОУ, РПН). Цели, которые не удалось доразведать с помощью БПЛА (ПУ), обстрелу не подвергаются.

**5 Расчеты, подтверждающие работоспособность и надежность СОЦ ПО**

Надежность СОЦ ПО задана в ТЗ в виде показателя безотказности - средней наработки на отказ Т0 которая должна быть не менее 2000 часов. СОЦ ПО предназначена для эксплуатации в наземной аппаратуре группы 1.3.

Показателем надежности составных частей является интенсивность отказов λ. В таблице 3 приведен перечень составных частей входящих в состав СОЦ ПО с учетом условий эксплуатации (группа 1.3).

Таблица 5. Составные части СОЦ ПО и их расчетные уровни надежности

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Наименование ЭРИ | Кол-во | k | Интенсивность отказов | |
| Одного элемента  λ\*10-6 1/ч | Всех элементов с учетом k  λ\*10-6 1/ч |
| 1 | ЭВМ РАМЕК РАМЭК-113 | 3 | 0,7 | 200 | 420 |
| 2 | Коммутатор/экран локальной вычислительной сети ТЕЦА.468367.026-02.03 | 1 | 0,5 | 100 | 50 |

Для каждого типа составной части в таблице 3 определены суммарные значения интенсивности отказов. В целом по СОЦ ПО по данным таблицы определена суммарная интенсивность отказов по формуле:

λита стс= *i*

где, λi – интенсивность отказов i-ого элемента,

ki – коэффициент влияния на общую надежность блока.

Величина, обратная λита стс, представляет собой среднюю наработку на отказТо  СОЦ ПО в целом:

То=1/ λита стс.

Исходя из данных таблицы 2, λита стс= 470\*10-6.

Соответственно, средняя наработка на отказ ВМК СВ составит:

То = 2127 часа.

Полученный результат расчета То ориентировочный и несколько выше требуемого. По нему устанавливается только возможность достижения заданных требований, что в данном расчете обеспечивается.

**6 Ожидаемые технико-экономические показатели**

**6.1 Технико-экономическое обоснование стоимости**

Технико-экономическое обоснование стоимости работ по СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» разработано с учетом требований ТЗ между АО «УМЗ» и АО «НИИП имени В.В. Тихомирова».

**6.1.1 Ожидаемые стоимостные показатели этапов СЧ ОКР**

При определении сметы расходов на СЧ ОКР использовались затратный и аналоговый методы их определения.

Оценка необходимых трудозатрат произведена с учетом имеющихся данных по трудоемкости работ по ОКР «Бук-М3».

При расчете использованы экономические нормативы АО «НИИП имени В.В. Тихомирова» на 2019г. и 2020г., утвержденные протоколом согласования экономических нормативов АО «НИИП имени В.В. Тихомирова» и согласованные 516 ВП МО РФ, применяемые при формировании договорных цен на продукцию оборонного назначения на 2019-2020гг.

Экономические показатели и исходные данные для расчёта приведены в таблице 1.

Таблица 1

Условия расчета стоимости СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО»

|  |  |
| --- | --- |
| Показатель | **Значение**  **для АО «НИИП имени В.В. Тихомирова»** |
| средняя основная заработная плата (ОЗП): | 71 000,00руб. |
| дополнительная заработная плата (ДЗП) | 9,2% |
| страховые взносы во внебюджетные фонды | 30,2% |
| Накладные расходы | 126,78% |
| Норматив рентабельности | 20% от собственных затрат и 1% от привнесенных затрат |

Расчет основной заработной платы по работам 2021 – 2024гг. произведен по нормативу 2020 года с учетом индекса потребительских цен (ИПЦ), умноженного на реальную заработную плату, в соответствии с письмом Минэкономразвития РФ №33198-ПБ/ДОЗи от 01.10.19 и п. 5 «Порядка применения индексов цен и индексов-дефляторов по видам экономической деятельности, а также иных показателей в составе прогноза социально-экономического развития Российской Федерации при формировании цен на продукцию, поставляемую по государственному оборонному заказу», утвержденного приказом Минэкономразвития РФ №190 от 01.04.2020.

Исходя из вышеуказанного, средняя основная заработная плата в:

2020 году – 71 000,00 руб.

2021 году – 75 320,42 руб. (на 2021/2020: ИПЦ – 103,7% х реал. з/п 102,3%);

2022 году – 80 291,57 руб. (на 2022/2021: ИПЦ – 104,0% х реал. з/п 102,5%);

2023 году – 85 590,81 руб. (на 2023/2022: ИПЦ – 104,0% х реал. з/п 102,5%);

2024 году – 91 328,82 руб. (на 2024/2023: ИПЦ – 104,0% х реал. з/п 102,6%).

Перечень работ, затраты на которые включены в стоимость этапов СЧ ОКР, составлялся в соответствии с ГОСТ РВ 15.203‑2001 г.

В соответствии с ГОСТ РВ 15.203‑2001 г. СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» должна включать следующие этапы, которые указаны в таблице 2:

Таблица 2

|  |  |
| --- | --- |
| № этапа | Наименование работ |
| 1 | Разработка технического проекта СОЦ ПО. |
| 2 | Разработка рабочей конструкторской документации (РКД) СОЦ ПО. |
| 3 | Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ ПО. |
| 4 | Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ ПО, корректировка и утверждение РКД СОЦ ПО по результатам испытаний. |
| 5 | Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М. |
| 6 | Утверждение РКД СОЦ ПО для серийного производства. |

Длительность проведения СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по предварительным прогнозам составит не менее 3,58 лет. Распределение длительности по этапам работ указано в таблице 3.

Таблица 3

|  |  |  |
| --- | --- | --- |
| № этапа | Наименование работ | Длительность ( год ) |
| 1 | Разработка технического проекта СОЦ ПО. | 0,25 |
| 2 | Разработка рабочей конструкторской документации (РКД) СОЦ ПО. | 0,5 |
| 3 | Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ. | 1,75 |
| 4 | Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ, корректировка и утверждение РКД СОЦ ПО по результатам испытаний. | 0,42 |
| 5 | Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М. | 0,58 |
| 6 | Утверждение РКД СОЦ ПО для серийного производства. | 0,08 |
|  | Итого | 3,58 |

Результаты расчета стоимости этапов работ по СЧ ОКР с учетом начала работ 01.11.2020 приведены в сводной таблице 4.

Исходными данными для расчета стоимости работ по этапам являются статистические данные по трудоемкости и распределению трудозатрат по этапам аналогичных ОКР, выполненных АО «НИИП имени В.В. Тихомирова». Экономические нормативы, согласованные ВП МО на 2019 год и 2020 год указаны в таблице 1.

Цены этапов приведены к годам выполнения работ на основе письма Минэкономразвития РФ №33198-ПБ/ДОЗи от 01.10.19 и п. 5 «Порядка применения индексов цен и индексов-дефляторов по видам экономической деятельности, а также иных показателей в составе прогноза социально-экономического развития Российской Федерации при формировании цен на продукцию, поставляемую по государственному оборонному заказу», утвержденного приказом Минэкономразвития РФ №190 от 01.04.2020.

**Расчетно-калькуляционные материалы даны в Приложении.**

Расходы на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО»

Таблица 4, руб.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ЭТАПЫ СЧ ОКР: | «Разработка технического проекта СОЦ ПО» | «Разработка рабочей конструкторской документации (РКД) СОЦ ПО» | «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ» | «Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ, корректировка и утверждение РКД СОЦ ПО по результатам испытаний» | «Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М» | «Утверждение РКД СОЦ ПО для серийного производства» | ИТОГО |
| **Цена** | **7 859 932,71** | **58 004 436,42** | **105 003 419,31** | **15 048 976,95** | **17 720 874,45** | **4 126 693,75** | **207 764 333,59** |

Ориентировочная стоимость СЧ ОКР будет уточняться на каждом на этапе выполнения работ путем формирования фиксированной цены по этапу.

**6.1.2 Ожидаемые стоимостные показатели серийного образца**

Стоимость изготовления серийного образца СОЦ ПО приведена в ценах 2022 года и составляет 22 134 684,94 рублей, в т.ч. НДС 20%. При этом использовались имеющиеся данные по стоимости блоков-аналогов, входящих в его состав.

**Расчетно-калькуляционные материалы даны в Приложении.**

**Приложение:**

1. Плановая калькуляция затрат на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по этапу 1 «Разработка технического проекта СОЦ ПО»;
2. Расшифровка основной заработной платы по этапу 1 «Разработка технического проекта СОЦ ПО»;
3. Расчет и обоснование прибыли по этапу 1 «Разработка технического проекта СОЦ ПО»;
4. Плановая калькуляция затрат на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по этапу 2 «Разработка рабочей конструкторской документации (РКД) СОЦ ПО»;
5. Расшифровка основной заработной платы по этапу 2 «Разработка рабочей конструкторской документации (РКД) СОЦ ПО»;
6. Расчет затрат на командировки по этапу 2 «Разработка рабочей конструкторской документации (РКД) СОЦ ПО»;
7. Расчет и обоснование прибыли по этапу 2 «Разработка рабочей конструкторской документации (РКД) СОЦ ПО»;
8. Плановая калькуляция затрат на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по этапу 3 «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ»;
9. Расшифровка затрат на приобретение комплектующих изделий по этапу 3 «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ»;
10. Расшифровка основной заработной платы по этапу 3 «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ»;
11. Расшифровка прочих прямых затрат по этапу 3 «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ»;
12. Расчет затрат на командировки по этапу 3 «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ»;
13. Расчет и обоснование прибыли по этапу 3 «Изготовление двух комплектов о.о. СОЦ ПО, разработка и изготовление рабочего места настройки и испытаний СОЦ ПО, настройка двух комплектов о.о. СОЦ ПО. Проведение предварительных испытаний комплекта о.о. СОЦ ПО. Доработка и корректировка РКД СОЦ ПО по результатам настройки и испытаний. Участие в изготовлении о.о. модуля СОЦ»;
14. Плановая калькуляция затрат на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по этапу 4 «Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ, корректировка и утверждение РКД СОЦ ПО по результатам испытаний»;
15. Расшифровка основной заработной платы по этапу 4 «Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ, корректировка и утверждение РКД СОЦ ПО по результатам испытаний»;
16. Расчет затрат на командировки по этапу 4 «Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ, корректировка и утверждение РКД СОЦ ПО по результатам испытаний»;
17. Расчет и обоснование прибыли по этапу 4 «Участие в проведении межведомственных и предварительных испытаний о.о. модуля СОЦ, корректировка и утверждение РКД СОЦ ПО по результатам испытаний»;
18. Плановая калькуляция затрат на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по этапу 5 «Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М»;
19. Расшифровка основной заработной платы по этапу 5 «Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М»;
20. Расчет затрат на командировки по этапу 5 «Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М»;
21. Расчет и обоснование прибыли по этапу 5 «Участие в проведении государственных испытаний о.о. ЕКУТС 9К317М»;
22. Плановая калькуляция затрат на СЧ ОКР «Разработка аппаратно-программного комплекса для модуля СОЦ из состава единого комплекса учебно-тренировочных средств ЗРК 9К317М», шифр «ЕКУТС-Б-СОЦ-ПО» по этапу 6 «Утверждение РКД СОЦ ПО для серийного производства»;
23. Расшифровка основной заработной платы по этапу 6 «Утверждение РКД СОЦ ПО для серийного производства»;
24. Расчет и обоснование прибыли по этапу 6 «Утверждение РКД СОЦ ПО для серийного производства»;
25. Плановая калькуляция затрат на изготовление серийного образца СОЦ ПО;
26. Расшифровка затрат на приобретение комплектующих изделий на изготовление серийного образца СОЦ ПО;
27. Расшифровка основной заработной платы на изготовление серийного образца СОЦ ПО;
28. Расшифровка прочих прямых затрат на изготовление серийного образца СОЦ ПО;

Расчет и обоснование прибыли на изготовление серийного образца СОЦ ПО.

**7 Уровень стандартизации и унификации**

**7.1 Унификация аппаратурного состава СОЦ ПО с аппаратурным составом АРМ ИКТ, ПБУ ПО, РПН ПО, СОУ ПО, ЦВС ПУ, ЦВС ПЗУ**

В СОЦ ПО используется 2 типа составных частей:

- ЭВМ типа РАМЭК 113 (3 шт), на базе которой разрабатываются ЭВМ РМИ, ЭВМ с адаптированным ПО Багет-23В и ЭВМ имитатор аппаратуры СОЦ;

- сетевой коммутатор типа ТЕЦА.468367.026-02.03 (1 шт).

Тип базовой ЭВМ и коммутатора выбирались таким образом, чтобы на базе базовой ЭВМ можно было разработать все ЭВМ для всех модулей комплексного тренажера. Соответственно коммутатор подбирался так, чтобы его можно было использовать во всех модулях комплексного тренажера.

Таким образом, по аппаратному составу СОЦ ПО будет полностью унифицирована с модулямиАРМ ИКТ, ПБУ ПО, РПН ПО, СОУ ПО, ЦВС ПУ, ЦВС ПЗУ.

Так же будет унифицировано и системно ПО для всех модулей. В качестве операционной системы будет использоваться ОС на базе Astra Linux SE 1.6 с предустановленным программным обеспечением АРМ АБИ и программами защиты от несанкционированного доступа.

Таким образом, отличия аппаратуры используемой в СОЦ ПО, от аппаратуры, используемой в модулях АРМ ИКТ, ПБУ ПО, РПН ПО, СОУ ПО, ЦВС ПУ, ЦВС ПЗУ будет заключаться только в отличиях функционального программного обеспечения.

**Заключение**

В результате проведения эскизно технического проектирования определены назначение, область применения, состав и структура СОЦ ПО. Приведено описание конструкции СОЦ ПО и общего процесса функционирования СОЦ ПО. Проведен анализ требований ТЗ и составлен перечень основных задач (программных модулей) с кратким описанием. Выбрана операционная система и среда программирования. Оценены возможности обеспечения и подобраны средства для обеспечения защиты СОЦ ПО от несанкционированного доступа. Рассчитана ориентировочная надежность СОЦ ПО.

В результате проработки подтверждена возможность создания СОЦ ПО отвечающего всем требованиям ТЗ на СЧ ОКР. Рассчитаны предварительная стоимость проведения ОКР, стоимость создания опытного образца и стоимость серийного образца.