НЕГОСУДАРСТВЕННОЕ АККРЕДИТОВАННОЕ НЕКОММЕРЧЕСКОЕ
ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«АКАДЕМИЯ МАРКЕТИНГА И СОЦИАЛЬНО-ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – ИМСИТ»
(г. Краснодар)

Институт информационных технологий и инноваций

Кафедра математики и вычислительной техники

Рассмотрено и одобрено на заседании кафедры математики и вычислительной техники Академии ИМСИТ, протокол №3 от 13 октября 2023 года, зав. кафедрой МиВТ, доцент Н.П. Исикова

УТВЕРЖДАЮ

Проректор по учебной работе, доцент Н.И. Севрюгина
20 ноября 2023 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ КУРСОВОГО ПРОЕКТА

по дисциплине «Проектирование защищенных автоматизированных систем»

для обучающихся направления подготовки бакалавров
10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы
«Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Квалификация (степень) выпускника
«Бакалавр»

Краснодар
2023

Методические указания по выполнению курсового проекта по дисциплине «Проектирование защищенных автоматизированных систем» для обучающихся всех форм обучения направления подготовки 10.03.01 Информационная безопасность направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)» – Краснодар: Академия маркетинга и социально-информационных технологий – ИМСИТ (г. Краснодар).

Методические указания по выполнению курсового проекта содержат требования к составу и содержанию, рекомендации по выполнению и защите курсового проекта по дисциплине «Проектирование защищенных автоматизированных систем».

Методические указания составлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от «17» ноября 2020 г. № 1427 направленность (профиль) образовательной программы «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)».

Составитель, канд. техн. наук, доцент К.Н. Цебренко

Методические указания рассмотрены и рекомендованы на заседании кафедры Математики и вычислительной техники от 13.10.2023 г., протокол №3

Зав. кафедрой математики и вычислительной
техники, канд. экон. наук, доцент Н.П. Исикова

Рабочая программа утверждена на заседании Научно-методического совета Академии ИМСИТ протокол № 3 от 20 ноября 2023 г.

Председатель Научно-методического Совета Академии ИМСИТ, профессор Н.Н. Павелко

Согласовано:
Проректор по учебной работе, доцент Н.И. Севрюгина

Проректор по качеству образования, доцент К.В. Писаренко

Рецензенты:

Видовский Л.А., д.т.н., профессор, профессор кафедры информационных систем и программирования КубГТУ
Глебов О.В., директор АО «ЮГ-СИСТЕМА ПЛЮС»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от «17» ноября 2020 г. № 1427 и разработанным на его основе учебным планом Академии маркетинга и социально-информационных технологий – ИМСИТ для студентов всех форм обучения предусмотрены выполнение и защита курсового проекта по дисциплине «Проектирование защищенных автоматизированных систем».

Курсовой проект по дисциплине «Проектирование защищенных автоматизированных систем» представляет комплексную проектную практическую внедренческую работу студента, предшествующую выполнению выпускной квалификационной работы и вобравшую в себя совокупность ранее выполненных проектных и практических наработок по дисциплинам кафедры. В их числе Основы информационной безопасности, Организационное и правовое обеспечение информационной безопасности.

Таким образом, интегрируя результаты учебно-творческого процесса за несколько лет напряженного труда студента настоящую курсовой проект, выстраивает их в систему, на базе которой реализуется современное наукоемкое проектирование по специальности.

Объем и трудности выполнения курсового проекта, возложенная на него ответственность по интенсификации подготовки специалиста, определяют сквозной характер проектирования на два семестра изучения базовой для этого проекта дисциплины «Проектирование защищенных автоматизированных систем».

Для выполнения курсового проекта требуется предварительное изучение курсов: "Основы информационной безопасности", " Организационное и правовое обеспечение информационной безопасности ".

Процесс выполнения работы на формирование следующих компетенций:

ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах

ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении

Цель настоящих методических указаний – оказать помощь обучающимся в выборе темы курсового проекта, определении ее содержания и организации процесса ее написания и защиты. Знание методики написания курсовых необходимо обучающимся не только для успешного освоения основной образовательной программы направления подготовки 10.03.01 Информационная безопасность, но и будущей профессиональной деятельности.

Выполнение курсового проекта (КП) является одним из основных этапов в изучении дисциплины «Проектирование защищенных автоматизированных систем», и имеет целью закрепление, углубление и обобщение знаний, полученных студентами в процессе изучения лекционного курса, а также умений и навыков, полученных при выполнении практических и лабораторных

работ, и применение этих знаний, умений и навыков к решению конкретных инженерных задач, развитие навыков работы со специальной литературой и навыков инженерного проектирования.

При выполнении курсового проекта решаются следующие задачи:

- формализация постановки задачи, разработка и согласование требований технического задания (ТЗ) на разработку или модернизацию информационной системы, комплекса или технологии, системы защиты информации (далее - объекта разработки);
- анализ научно-технической литературы, нормативно-правовой, справочной и др. документации, необходимой в процессе выполнения курсовой работы;
- выбор базовых принципов, концепций, структур построения объекта разработки с учетом требований ТЗ, проведение соответствующего методологического и теоретического обоснования разработки;
- построение функциональной, информационной, динамической модели функционирования объекта разработки, анализ основных показателей качества, эффективности и путей их улучшения;
- выбор программных и аппаратных средств, технологической документации, оборудования, экспериментальной базы, проведение расчетно-теоретических и экспериментальных исследований, моделирование работы объекта разработки и проверка правильности его функционирования, тестирование;
- составление рабочей документации (пояснительной записки) к объекту разработки с описанием ТЗ, принципов построения, результатов исследования и моделирования, расчетов основных показателей и характеристик, рекомендаций по применению и т.д.;
- защита курсового проекта.

В ходе курсового проектирования студент самостоятельно принимает решения и затем их защищает. Поэтому в процессе работы студент обязан проявить творческую активность, инициативу, самостоятельность и чувство ответственности. За принятые в работе технические решения, правильность всех вычислений, оформление в соответствии с требованиями государственных стандартов отвечает автор работы – студент.

Методические указания по выполнению курсового проекта содержат требования к составу и содержанию, рекомендации по выполнению курсового проекта по дисциплине «Проектирование защищенных автоматизированных систем» и являются обязательными для студентов всех форм обучения направления подготовки 10.03.01 Информационная безопасность.

1 Структура и оформление курсового проекта

1.1 Структура курсового проекта

Материал курсового проекта должен быть изложен чётко и логически последовательно с конкретным описанием результатов научно-технического исследования и выводов.

План курсового проекта студент составляет самостоятельно и затем согласует с ведущим преподавателем учебной дисциплины, научным руководителем курсового проекта.

Рекомендуемая структура курсового проекта выглядит следующим образом:

1. Титульный лист (см. приложение 1).
2. Задание на курсовой проект (см. приложение 2).
3. Реферат (приложение 8)
4. Содержание
5. Введение
6. Обоснование выбранного направления исследований и общую методику достижения поставленной цели;
7. Теоретические и (или) экспериментальные исследования;
8. Обобщение и оценку результатов исследований
9. Заключение.
10. Список использованных источников.
11. Приложения (при необходимости).

Структура работы согласовывается с руководителем курсового проекта и может отличатся от рекомендуемой.

Компетенции формируемые в процессе выполнения курсового проекта

Индекс	Разделы курсового проекта
ПК-3, ПК-4	Обоснование выбранного направления исследований и общую методику достижения поставленной цели
ПК-3, ПК-4	Теоретические и (или) экспериментальные исследования
ПК-3, ПК-4	Обобщение и оценку результатов исследований

1.2 Оформление текста курсового проекта

Реферат должен содержать:

- сведения об общем объеме работы, иллюстраций, таблиц, использованных источников, приложений;
- перечень ключевых слов;

- текст реферата.

Перечень ключевых слов должен включать от 5 до 15 слов или словосочетаний из текста работы, которые в наибольшей мере характеризуют его содержание и обеспечивают возможность информационного поиска.

Текст реферата должен отражать:

- объект исследования или разработки;
- цель работы;
- методы или методологию проведения работы;
- результаты работы и их новизну;
- область применения результатов;
- рекомендации по внедрению или итоги внедрения результатов работы;
- экономическую эффективность или значимость работы;
- прогнозные предположения о развитии объекта исследования.

Если работа не содержит сведений по какой-либо из перечисленных структурных частей реферата, то в тексте реферата она опускается, при этом последовательность изложения сохраняется.

Оптимальный объем текста реферата - 850 печатных знаков, но не более одной страницы машинописного текста.

Содержание включает введение, наименование всех разделов и подразделов, пунктов (если они имеют наименование), заключение, список использованных источников и наименования приложений с указанием номеров страниц, с которых начинаются эти элементы курсового проекта.

В элементе "СОДЕРЖАНИЕ" приводят наименования структурных элементов работы, порядковые номера и заголовки разделов, подразделов (при необходимости - пунктов) основной части работы, обозначения и заголовки ее приложений (при наличии приложений). После заголовка каждого элемента ставят отточие и приводят номер страницы работы, на которой начинается данный структурный элемент.

Обозначения подразделов приводят после абзацного отступа, равного двум знакам, относительно обозначения разделов. Обозначения пунктов приводят после абзацного отступа, равного четырем знакам относительно обозначения разделов.

При необходимости продолжение записи заголовка раздела, подраздела или пункта на второй (последующей) строке выполняют, начиная от уровня начала этого заголовка на первой строке, а продолжение записи заголовка приложения - от уровня записи обозначения этого приложения.

Введение должно содержать оценку современного состояния решаемой научно-технической проблемы, основание и исходные данные для разработки темы, обоснование необходимости проведения курсового проекта, сведения о планируемом научно-техническом уровне разработки, о патентных исследованиях и выводы из них, сведения о метрологическом обеспечении работы. Во введении должны быть отражены актуальность и новизна темы, связь данной работы с другими научно-исследовательскими работами.

В основной части работы приводят данные, отражающие сущность, методику и основные результаты выполненной работы.

Основная часть должна содержать:

- выбор направления исследований, включающий обоснование направления исследования, методы решения задач и их сравнительную оценку, описание выбранной общей методики проведения исследований и реализации проекта;

- процесс теоретических и (или) экспериментальных исследований, включая определение характера и содержания теоретических исследований, методы исследований, методы расчета, обоснование необходимости проведения экспериментальных работ, принципы действия разработанных объектов, их характеристики;

- обобщение и оценку результатов работы, включающих оценку полноты решения поставленной задачи и предложения по дальнейшим направлениям работ, оценку достоверности полученных результатов и технико-экономической эффективности их внедрения и их сравнение с аналогичными результатами отечественных и зарубежных работ, обоснование необходимости проведения дополнительных исследований, отрицательные результаты, приводящие к необходимости прекращения дальнейших исследований.

Она должна содержать:

- структурную схему автоматизированной информационной системы;
- обоснование проектных решений по автоматизации информационных процессов;
- структурную схему подсистемы защиты информации;
- обоснование проектных решений по защите информации;
- структура ресурсов, таблица разграничения доступа;
- протоколы и отчеты экспериментальных исследований;

Заключение должно содержать:

- краткие выводы по результатам выполненной работе или отдельных ее этапов;

- оценку полноты решений поставленных задач;

- разработку рекомендаций и исходных данных по конкретному использованию результатов работы;

- результаты оценки эффективности внедрения;

- результаты оценки научно-технического уровня выполненной работы в сравнении с лучшими достижениями в этой области.

Страницы текста курсового проекта и включенные в нее иллюстрации и таблицы должны соответствовать формату А4 по ГОСТ 9327. Допускается применение формата А3 при наличии большого количества таблиц и иллюстраций данного формата.

Работа должна быть выполнена любым печатным способом на одной стороне листа белой бумаги формата А4 через полтора интервала.

Цвет шрифта должен быть черным, размер шрифта - не менее 12 пт (рекомендуется использовать 14 пт). Рекомендуемый тип шрифта для основного текста работы - Times New Roman. Полужирный шрифт применяют только для заголовков разделов и подразделов, заголовков структурных элементов. Использование курсива допускается для обозначения объектов

(биология, геология, медицина, нанотехнологии, генная инженерия и др.) и написания терминов (например, in vivo, in vitro) и иных объектов и терминов на латыни.

Для акцентирования внимания может применяться выделение текста с помощью шрифта иного начертания, чем шрифт основного текста, но того же кегля и гарнитуры. Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Текст работы следует печатать, соблюдая следующие размеры полей: левое - 30 мм, правое - 15 мм, верхнее и нижнее - 20 мм. Абзацный отступ должен быть одинаковым по всему тексту работы и равен 1,25 см.

Вне зависимости от способа выполнения работы качество напечатанного текста и оформления иллюстраций, таблиц, распечаток программ должно удовлетворять требованию их четкого воспроизведения.

При выполнении работы необходимо соблюдать равномерную плотность и четкость изображения по всей работе. Все линии, буквы, цифры и знаки должны иметь одинаковую контрастность по всему тексту работы.

Фамилии, наименования учреждений, организаций, фирм, наименования изделий и другие имена собственные в работе приводят на языке оригинала. Допускается транслитерировать имена собственные и приводить наименования организаций в переводе на язык работы с добавлением (при первом упоминании) оригинального названия по ГОСТ 7.79.

Сокращения слов и словосочетаний на русском, белорусском и иностранных европейских языках оформляют в соответствии с требованиями ГОСТ 7.11, ГОСТ 7.12.

Наименования структурных элементов работы: "СПИСОК ИСПОЛНИТЕЛЕЙ", "РЕФЕРАТ", "СОДЕРЖАНИЕ", "ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ", "ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ", "ВВЕДЕНИЕ", "ЗАКЛЮЧЕНИЕ", "СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ", "ПРИЛОЖЕНИЕ" служат заголовками структурных элементов работы.

Заголовки структурных элементов следует располагать в середине строки без точки в конце, прописными буквами, не подчеркивая. Каждый структурный элемент и каждый раздел основной части работы начинают с новой страницы.

Основную часть работы следует делить на разделы, подразделы и пункты. Пункты при необходимости могут делиться на подпункты. Разделы и подразделы работы должны иметь заголовки. Пункты и подпункты могут не иметь заголовков.

Заголовки разделов и подразделов основной части работы следует начинать с абзацного отступа и размещать после порядкового номера, печатать с прописной буквы, полужирным шрифтом, не подчеркивать, без точки в конце. Пункты и подпункты могут иметь только порядковый номер без заголовка, начинающийся с абзацного отступа, а могут иметь заголовок после порядкового номера, печатать с прописной буквы, обычным шрифтом, не подчеркивать, без точки в конце.

Если заголовок включает несколько предложений, их разделяют точками.

Переносы слов в заголовках не допускаются.

Страницы работы следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту работы, включая приложения. Номер страницы проставляется в центре нижней части страницы без точки. Приложения, которые приведены в работе и имеющие собственную нумерацию, допускается не перенумеровать.

Титульный лист включают в общую нумерацию страниц работы. Номер страницы на титульном листе не проставляют.

Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц работы. Иллюстрации и таблицы на листе формата А3 учитывают как одну страницу.

Разделы должны иметь порядковые номера в пределах всей работы, обозначенные арабскими цифрами без точки и расположенные с абзацного отступа. Подразделы должны иметь нумерацию в пределах каждого раздела. Номер подраздела состоит из номеров раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится. Разделы, как и подразделы, могут состоять из одного или нескольких пунктов.

Если работа не имеет подразделов, то нумерация пунктов в нем должна быть в пределах каждого раздела и номер пункта должен состоять из номеров раздела и пункта, разделенных точкой. В конце номера пункта точка не ставится.

Если работа имеет подразделы, то нумерация пунктов должна быть в пределах подраздела и номер пункта должен состоять из номеров раздела, подраздела и пункта, разделенных точками.

Пример - Приведен фрагмент нумерации раздела, подраздела и пунктов работы:

3 Принципы, методы и результаты разработки и ведения классификационных систем ВИНИТИ

3.1 Рубрикатор ВИНИТИ

3.1.1 Структура и функции рубрикатора

3.1.2 Соотношение Рубрикатора ВИНИТИ и ГРНТИ

3.1.3 Место рубрикатора отрасли знания в рубрикационной системе ВИНИТИ

Если раздел или подраздел состоит из одного пункта, то пункт не нумеруется.

Если текст работы подразделяется только на пункты, они нумеруются порядковыми номерами в пределах работы.

Пункты при необходимости могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта: 4.2.1.1, 4.2.1.2, 4.2.1.3 и т.д.

Внутри пунктов или подпунктов могут быть приведены перечисления. Перед каждым элементом перечисления следует ставить тире. При необходимости ссылки в тексте работы на один из элементов перечисления вместо тире ставят строчные буквы русского алфавита со скобкой, начиная с

буквы "а" (за исключением букв е, з, й, о, ч, ъ, ы, ь). Простые перечисления отделяются запятой, сложные - точкой с запятой.

При наличии конкретного числа перечислений допускается перед каждым элементом перечисления ставить арабские цифры, после которых ставится скобка.

Перечисления приводятся с абзацного отступа в столбик.

Пример 1

Информационно-сервисная служба для обслуживания удаленных пользователей включает следующие модули:

- удаленный заказ,
- виртуальная справочная служба,
- виртуальный читальный зал.

Пример 2

Работа по оцифровке включала следующие технологические этапы:

а) первичный осмотр и структурирование исходных материалов,

б) сканирование документов,

в) обработка и проверка полученных образов,

г) структурирование оцифрованного массива,

д) выходной контроль качества массивов графических образов.

Пример 3

8.2.3 Камеральные и лабораторные исследования включали разделение всего выявленного видового состава растений на четыре группы по степени использования их копытными:

1) случайный корм,

2) второстепенный корм,

3) дополнительный корм,

4) основной корм.

Пример 4

7.6.4 Разрабатываемое сверхмощное устройство можно будет применять в различных отраслях реального сектора экономики:

- в машиностроении:

1) для очистки отливок от формовочной смеси;

2) для очистки лопаток турбин авиационных двигателей;

3) для холодной штамповки из листа;

- в ремонте техники:

1) устранение наслоений на внутренних стенках труб;

2) очистка каналов и отверстий небольшого диаметра от грязи.

Заголовки должны четко и кратко отражать содержание разделов, подразделов. Если заголовок состоит из двух предложений, их разделяют точкой.

В работе рекомендуется приводить ссылки на использованные источники. При нумерации ссылок на документы, использованные при составлении работы, приводится сплошная нумерация для всего текста работы в целом или для отдельных разделов. Порядковый номер ссылки (отсылки) приводят арабскими цифрами в квадратных скобках в конце текста ссылки. Порядковый

номер библиографического описания источника в списке использованных источников соответствует номеру ссылки.

Ссылаться следует на документ в целом или на его разделы и приложения.

При ссылках на стандарты и технические условия указывают их обозначение, при этом допускается не указывать год их утверждения при условии полного описания стандарта и технических условий в списке использованных источников в соответствии с ГОСТ 7.1.

Примеры

1 ..... приведено в работах [1] - [4].

2 ..... по ГОСТ 29029.

3 ..... в работе [9], раздел 5.

1.3 Оформление иллюстраций курсового проекта

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в работе непосредственно после текста, где они упоминаются впервые, или на следующей странице (по возможности ближе к соответствующим частям текста работы). На все иллюстрации в работе должны быть даны ссылки. При ссылке необходимо писать слово "рисунок" и его номер, например: "в соответствии с рисунком 2" и т.д.

Чертежи, графики, диаграммы, схемы, помещаемые в работе, должны соответствовать требованиям стандартов Единой системы конструкторской документации (ЕСКД).

Количество иллюстраций должно быть достаточным для пояснения излагаемого текста работы. Не рекомендуется в Курсовому проекту приводить объемные рисунки.

Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается: Рисунок 1.

Пример - Рисунок 1 - Схема прибора

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения: Рисунок А.3.

Допускается нумеровать иллюстрации в пределах раздела работы. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 2.1.

Иллюстрации при необходимости могут иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок", его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком без точки в конце.

Пример - Рисунок 2 - Оформление таблицы

Если наименование рисунка состоит из нескольких строк, то его следует записывать через один межстрочный интервал. Наименование рисунка

приводят с прописной буквы без точки в конце. Перенос слов в наименовании графического материала не допускается.

1.4 Оформление таблиц в Курсовому проекту

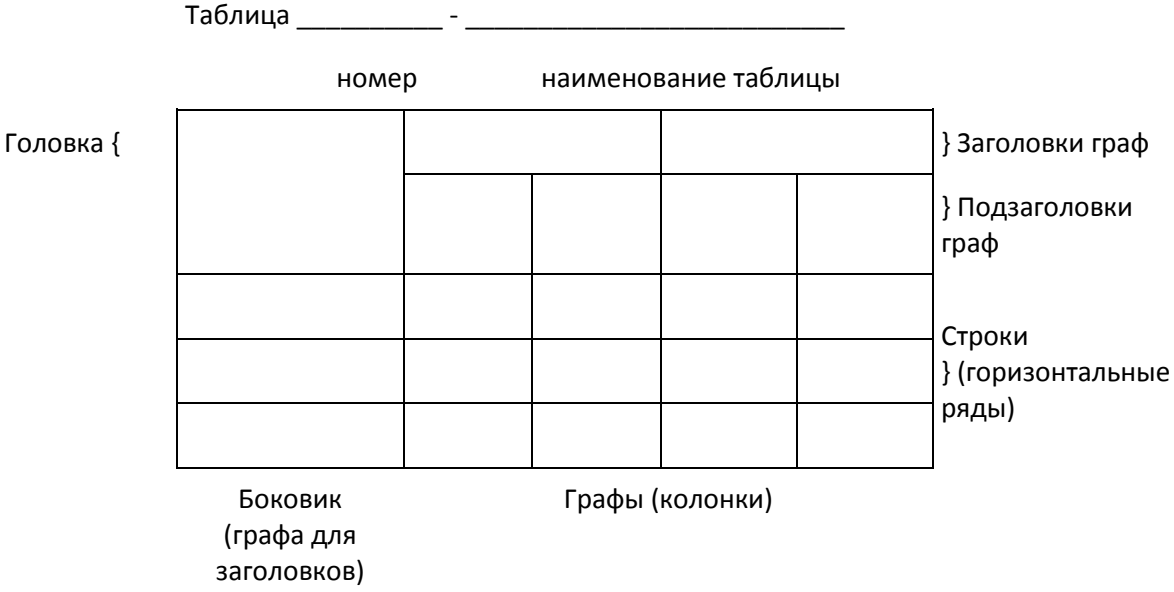
Цифровой материал должен оформляться в виде таблиц. Таблицы применяют для наглядности и удобства сравнения показателей. Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице. все таблицы в работе должны быть ссылки. При ссылке следует печатать слово "таблица" с указанием ее номера.

Наименование таблицы, при ее наличии, должно отражать ее содержание, быть точным, кратким. Наименование следует помещать над таблицей слева, без абзацного отступа в следующем формате: Таблица Номер таблицы - Наименование таблицы. Наименование таблицы приводят с прописной буквы без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал.

Таблицу с большим количеством строк допускается переносить на другую страницу. При переносе части таблицы на другую страницу слово "Таблица", ее номер и наименование указывают один раз слева над первой частью таблицы, а над другими частями также слева пишут слова "Продолжение таблицы" и указывают номер таблицы.

При делении таблицы на части допускается ее головку или боковик заменять соответственно номерами граф и строк. При этом нумеруют арабскими цифрами графы и (или) строки первой части таблицы. Таблица оформляется в соответствии с таблицей 1.

Таблица 1 – Заголовок таблицы



Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы каждого приложения обозначаются отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Если в работе одна таблица, она должна быть обозначена "Таблица 1" или "Таблица А.1" (если она приведена в приложении А).

Допускается нумеровать таблицы в пределах раздела при большом объеме работы. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой: Таблица 2.3.

Заголовки граф и строк таблицы следует печатать с прописной буквы, а подзаголовки граф - со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставятся. Названия заголовков и подзаголовков таблиц указывают в единственном числе.

Таблицы слева, справа, сверху и снизу ограничивают линиями. Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Заголовки граф выравнивают по центру, а заголовки строк - по левому краю.

Горизонтальные и вертикальные линии, разграничивающие строки таблицы, допускается не проводить, если их отсутствие не затрудняет пользование таблицей.

Текст, повторяющийся в строках одной и той же графы и состоящий из одиночных слов, заменяют кавычками. Ставить кавычки вместо повторяющихся цифр, буквенно-цифровых обозначений, знаков и символов не допускается.

Если текст повторяется, то при первом повторении его заменяют словами "то же", а далее кавычками. В таблице допускается применять размер шрифта меньше, чем в тексте работы.

2 Тематика курсовых работ

Тематика курсового проекта должна соответствовать основным разделам программы дисциплины «Проектирование защищенных автоматизированных систем». Теоретическая часть курсового проекта должна базироваться на лекционном материале дисциплины и определяется практическими потребностями предприятий в области информационных технологий. Курсовой проект должна содержать углубленную разработку вопросов проектирования защищённых автоматизированных систем.

Тематика курсовых работ определяется преподавателем, рассматривается на заседании кафедры и утверждается научно-методическим советом академии. При этом выбор основывается как на государственном стандарте, так и на направлениях научно-исследовательской и учебно-методической работы, актуальных направлениях работы других организаций, деятельность которых связана с разработкой математического, информационного и программного обеспечения ЭВМ. Студенту предоставляется право выбора одной из предложенных тем или предложения своей темы с обоснованием

целесообразности ее разработки. Темой курсового проекта может быть любая проблема из организационной, технической или экономической области, с которой сталкиваются в практической деятельности предприятия.

Тема курсового проекта: «Разработка эскизного проекта системы защиты автоматизированной информационной системы организации».

Задание на курсовой проект включает в себя разработку эскизного проекта подсистемы защиты информации от несанкционированного доступа для определенной в задании защищенной автоматизированной информационной системы (ЗАС) предприятия.

Задание предусматривает разработку и реализацию студентом одного из элементов политики безопасности учреждения (предприятия) в виде таблицы разграничения доступа (ТРД), а также экспериментальную проверку и оптимизацию выбранных решений (контрмер) по организации защиты ЗАС путем управления информационными рисками на основе моделей угроз и информационных потоков в среде программного комплекса Digital Security Office или другим способом.

При выполнении курсового проекта студент должен выполнить:

Определение перечня защищаемых ресурсов и их критичности.

Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности.

Определение особенностей расположения, функционирования и построения средств ЗАС.

Определение угроз безопасности информации и класса защищенности ЗАС.

Формирование требований к построению СЗИ.

Определение уязвимостей автоматизированной системы и выбор средств защиты информации.

Проведение экспериментальных проверок и оптимизацию выбранных решений (контрмер) по организации защиты ЗАС

Оформить пояснительную записку и графическую часть проекта.

Кроме того, по решению кафедры в состав проекта могут быть включены дополнительные разделы, связанные с научно-исследовательской работой.

Примерный список тем выглядит следующим образом:

1. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации муниципального подчинения на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу голосовых сообщений.
2. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу голосовых сообщений.
3. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей

4. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу видеоизображений.

5. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.

6. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, поддерживающей передачу голосовых сообщений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования

7. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края, поддерживающей передачу голосовых сообщений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования

8. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района с сервисом электронной почты на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования

9. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, поддерживающей передачу видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования

10. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края, поддерживающей передачу голосовых сообщений, на базе локальной вычислительной сети

11. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ

12. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с сервисом электронной посты на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ

13. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края с использованием механизмов операционных систем на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ

14. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей, поддерживающей передачу видеоизображений и голосовых сообщений.

15. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с использованием механизмов операционных систем на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.

16. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с сервисом электронной посты на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.

17. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края с ограничением пользователей в допуске к различным разделам информационной базы для распределенной вычислительной сети, состоящей из локальных вычислительных сетей.

18. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, с сервисом передачи видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования

19. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с ограничением пользователей в допуске к различным разделам информационной базы для комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования

20. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с использованием механизмов операционных систем на базе локальной вычислительной сети

21. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с применением программно-аппаратных средств защиты от несанкционированного доступа на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.

22. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей, где ЭВМ системы расположены в нескольких контролируемых зонах.

23. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации муниципального подчинения

24. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района

25. Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края

26. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе комплекса локальных вычислительных сетей вычислительной сети, соединенных каналами общего пользования

27. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе локальной вычислительной сети

28. Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из отдельных ЭВМ

3 Исходные данные для курсового проекта

Вариант индивидуального задания формируется в соответствии с номером задания по таблице, приведенной в приложении 6. Для формирования индивидуального задания исполнителю необходимо выбрать из списка вариантов значений исходных данных те, которые соответствуют его варианту индивидуального задания.

Уточнение индивидуальных заданий и конкретизация требований к разрабатываемым элементам защищенной автоматизированной системы производится руководителем на начальном этапе разработки курсового проекта.

Примерный перечень элементов, из которых формируется задание на курсовой проект, изложен ниже.

Разработать проект подсистемы защиты информации от несанкционированного доступа для автоматизированной системы

Звено управления. (Первый символ)

организация муниципального подчинения (1)

учреждение администрации района (2)

учреждение администрации края (3)

Данный элемент предназначен для использования на этапе информационного обследования АС с целью определения круга лиц органов управления, для работы которых создается АС, определения основных информационных потоков в ходе управления подразделениями, степени секретности и тематики информации, предназначенной для автоматизированной обработки.

Таблица 2 - Уровень конфиденциальности информации

Уровень конфиденциальности информации	1	2	3
общедоступная информация	+	+	+
персональные данные	+		
сведения, составляющие служебную тайну	+	+	+
секретные сведения	+	+	
совершенно секретные сведения		+	+
сведения особой важности			+

Тип автоматизированной системы (архитектура). (Второй символ)

Автономные компьютеры соединенные каналами передачи данных на основе телефонной сети. (1)

Локальная вычислительная сеть. (2)

Распределенная вычислительная сеть, состоящая из отдельных ЭВМ. (3)

Распределенная вычислительная сеть, состоящая из локальных вычислительных сетей. (4)

Комплекс локальных сетей, соединенных каналами передачи данных коллективного пользования (общедоступных). (5)

Условия расположения автоматизированной системы. (Третий символ)

Все ЭВМ и каналы связи расположены в одной контролируемой зоне. (1)

ЭВМ системы расположены в нескольких контролируемых зонах. (2)

Пункты 1.2 и 1.3 используются для определения архитектуры АС, размещения элементов системы и определения специфических каналов утечки информации и других информационных угроз системы.

Распределение полномочий пользователей. (Четвертый символ)

Все пользователи имеют одинаковый уровень допуска. (1)

Пользователи имеют разные уровни допуска. (2)

Состав информационной базы. (Пятый символ)

Все пользователи имеют допуск ко всем тематическим разделам информационной базы. (1)

Пользователи ограничены в допуске к различным разделам информационной базы. (2)

Пункты 1.4 и 1.5 используются при определении класса защищенности АС и выбора основной модели разграничения доступа для СЗИ.

Построение системы защиты информации от несанкционированного доступа. (Шестой символ)

На основе механизмов операционных систем. (1)

С применением специальных программных средств защиты от несанкционированного доступа. (2)

С применением программно-аппаратных средств защиты от несанкционированного доступа. (3)

Данный пункт является основанием для определения концепции построения системы защиты информации в исследуемой АС и распределения функций защиты информации по элементам АС.

Реализуемые информационные сервисы (Седьмой символ)

Таблица 3 – Варианты индивидуального задания

Реализуемые информационные сервисы	Символ варианта индивидуального задания																	
	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т
обмен файлами	+	+	+	+	+	+		+	+	+	+	+		+	+	+	+	+
доступ в ИВС высшего звена		+	+	+		+	+	+	+	+		+	+	+	+		+	
электронная почта	+		+		+		+		+		+		+		+		+	+
вывод документов на печать			+	+	+		+	+	+	+		+		+	+	+	+	+
обмен сообщениями в реальном масштабе времени		+				+		+		+	+		+			+		+
доступ в базы данных	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
электронный документооборот	+		+	+	+	+		+	+	+		+	+	+	+	+	+	+

передача голосовых сообщений	+	+		+	+		+				+	+		+		+		+
передача видеоизображения		+				+					+				+			+

Разработать структуру ресурсов (каталогов) для заданного количества пользователей АС, приведенных в таблице (Восьмой символ)

Таблица 4 - Структура ресурсов (каталогов) для заданного количества пользователей АС

Вариант	Количество начальников отделов	Количество зам.начальников отделов	Количество специалистов в отделах
А	1	3	3
Б	2	2	4
В	3	1	5

Разработать и реализовать таблицу разграничения доступа для пользователей в соответствии с их должностным положением и возможностями прав доступа NTFS к каталогам по их смысловому содержанию. Например, каталог «Общие документы» доступен по чтению для группы «Все специалисты», каталог «Распоряжения начальника отдела» доступен по чтению для группы «Сотрудники отдела» и имеет полный доступ для начальника отдела, каталог «Донесения Зам.начальника отдела» доступен по чтению для начальника отдела, по добавлению для зам.начальника отдела и недоступен для остальных.

Провести экспериментальную проверку выбранных решений по результатам эскизного проектирования системы защиты ЗАС (например с использованием программного комплекса Digital Security Office). Для этого:

1. Произвести расчет рисков ЗАС на основе модели угроз и уязвимостей.
2. Используя модуль управления рисками, на основе расчета эффективности каждой предложенной контрмеры выбрать наиболее оптимальные, которые позволят снизить риск до необходимого уровня с наименьшими затратами.
3. Произвести расчет рисков ЗАС на основе модели информационных потоков.
4. Используя модуль управления рисками, на основе расчета эффективности каждой предложенной контрмеры выбрать наиболее оптимальные, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

Например, вариант (1-2-2-1-1-1-В-Б), означает следующее:

1. Разработать проект системы защиты информации от несанкционированного доступа для автоматизированной системы организации

муниципального подчинения, создаваемой в виде локальной вычислительной сети, некоторые компоненты которой вынесены за пределы контролируемой зоны. Все зарегистрированные клиенты сети имеют одинаковые полномочия, как по уровню допуска, так и по доступу ко всей информационной базе системы. Управление разграничением доступа к ресурсам системы осуществляется на основе механизмов сетевой операционной системы.

2. Разработать и реализовать структуру ресурсов (каталогов) для пользователей АС - 2-х начальников отделов, 2-х заместителей и 4-х специалистов в каждом отделе.

Провести экспериментальную проверку выбранных решений по результатам эскизного проектирования системы защиты ЗАС. Для этого:

Произвести расчет рисков ЗАС на основе модели угроз и уязвимостей. Используя модуль управления рисками, на основе расчета эффективности каждой предложенной контрмеры выберите наиболее оптимальные, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

Произвести расчет рисков ЗАС на основе модели информационных потоков. Используя модуль управления рисками, на основе расчета эффективности каждой предложенной контрмеры выберите наиболее оптимальные, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

Окончательный вариант системы защиты ЗАС организации выбрать по результатам всех расчетов.

Форма задания приведена в приложении 2.

4 Порядок выполнения курсового проекта

Курсовой проект в основном выполняется в часы самостоятельной работы студентов. Консультации проводятся преподавателями кафедры.

Для своевременного завершения курсового проекта необходимо правильно спланировать время для ее выполнения. При этом можно руководствоваться следующей ориентировочной оценкой трудоемкости отдельных этапов в соответствии с примерным графиком работы (таблица 5).

Таблица 5 - Примерный график выполнения курсового проекта

№ этапа	**Этап выполнения**	**Объем этапа, %**	**Общий объем, %**
1	Выдача варианта индивидуального задания на курсовой проект.		
2	Уточнение индивидуальных заданий и конкретизация требований к разрабатываемым элементам защищенной автоматизированной системы.	5	5
3	Проведение информационного и технического обследования системы управления.	10	15
4	Обоснование проектных решений по автоматизации информационных процессов и разработка структурной схемы корпоративной информационной системы.	5	20

5	Разработка политики информационной безопасности: • определение класса защищенности ЗАС; • разработка концепции защиты информации; • структура ресурсов, таблица разграничения доступа.	15	35
6	Обоснование проектных решений по защите информации и разработка структурной схемы системы защиты информации (СЗИ).	10	45
7	Для разработанной первоначальной конфигурации СЗИ проверка и оптимизация выбранных решений (контрмер) по организации защиты ЗАС (например в среде программного комплекса Digital Security Office) по показателю ROSI.	20	65
8	Формирование протоколов и отчетов экспериментальных исследований.	5	70
9	Оформление пояснительной записки, устранение замечаний руководителя.	10	80
10	Подготовка доклада и презентации к защите курсового проекта.	10	90
11	Защита курсового проекта.	10	100

5 Разработка проекта системы защиты автоматизированной информационной системы организации

5.1 Порядок разработки системы защиты защищенной автоматизированной информационной системы

Процесс разработки системы программно-аппаратной защиты информации от НСД в АС является итеративным, т.е. требует возвращения к некоторым этапам при получении новых данных на других этапах.

Общая последовательность разработки АС состоит из следующих этапов.

1. Проводиться информационное и техническое обследование системы управления Заказчика. Специалист, проводящий обследование изучает организационно-штатную и техническую (если она имеется) структуру системы управления и проводит бланочный опрос должностных лиц и технического персонала, входящих в эту структуру.

В результате информационного обследования составляется схема информационных потоков, на которой указываются элементы системы управления, направления потоков информации между ними, а также прогнозируемые характеристики информационных потоков (объемы передаваемых данных, их вид, приоритетность, конфиденциальность и т.п.). Характеристики информационных потоков могут объединяться в сводные таблицы.

В результате технического обследования выясняется существующая структура и характеристики автоматизированных участков системы управления Заказчика.

2. На основании результатов информационного обследования определяются объекты информатизации (пункты управления, отделы, службы и должностные лица), информационная деятельность которых подлежит

автоматизации, а также выполняемые ими функции и информационные службы, которые необходимо реализовать в АС для удовлетворения информационных потребностей выделенных объектов информатизации, в том числе потребности по защите информации от НСД. Сведения о степени секретности (конфиденциальности) информации и должностных лицах, которые должны иметь к ним доступ, включаются в Перечни защищаемых ресурсов АС, представляемых отделами и службами.

3. На основании результатов информационного и технического обследования составляется предварительная схема построения АС и определяется:

назначение, состав и характеристики автоматизированных рабочих мест (АРМ) должностных лиц;

назначение, состав, логическая структура и характеристики локальных вычислительных сетей (ЛВС);

назначение, состав и характеристики сетевых серверов;

логическая структура сети передачи данных (СПД) между удаленными узлами АС с учетом имеющихся и планируемых к развертыванию каналов передачи данных.

4. В соответствии с исходными данными разрабатывается политика информационной безопасности:

определяется класс защищенности АС и требования по защите информации, которые должны быть реализованы в АС данного класса;

разрабатывается концепция защиты информации АС, которая должна отражать основные угрозы информационной безопасности, замысел по защите информации от НСД и организационно-технические мероприятия, обеспечивающие поддержку системы защиты информации от НСД.

5. Составляется предварительная схема построения защищенной АС, в которой определяется состав, назначение и логика взаимодействия программно-аппаратных средств защиты информации от НСД.

При необходимости структура АС корректируется для удовлетворения требований по защите информации от НСД.

6. Производится технико-экономическое обоснование принятых организационно-технических решений по построению защищенной АС.

7. Уточняются принятые решения и составляется спецификация на программное и аппаратное обеспечение, необходимое для построения АС.

8. Оформляется пояснительная записка и графические материалы.

9. Разрабатывается презентация для демонстрации предлагаемых организационно-технических решений по созданию защищенной АС.

5.2 Рекомендации по разработке политики информационной безопасности

Под политикой информационной безопасности автоматизированного участка системы управления (СУ) понимается совокупность принципов, правил, и практических рекомендаций, на основе которых строится управление,

защита и распределение защищаемой информации в конкретной АС, зафиксированных документально.

Под автоматизированной системой будем понимать организационно-техническую структуру, представляющую собой совокупность взаимосвязанных компонентов: технических средств обработки и передачи; методов и алгоритмов обработки данных; информации на различных носителях; персонала, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации с целью решения задач управления.

Под информационной архитектурой понимается организационно-техническая структура системы управления. Она отражает логику взаимодействия элементов информационной системы в ходе обработки данных при решении функциональных задач.

Информационная архитектура может быть представлена набором функциональных схем, таблиц и других документов, содержащих следующую информацию:

- состав структурных подразделений и должностных лиц организации, в чьих интересах будет функционировать информационная система, а также подразделений и должностных лиц информационных служб, с указанием функциональных обязанностей и порядка взаимодействия при решении задач управления;
- перечни функциональных задач и задач по обработке информации, которые предполагается решать в системе с указанием их характеристик;
- перечень информационных массивов, которые необходимо формировать и поддерживать в ходе решения задач, с указанием носителей информации, предназначенных для их хранения, и ответственных за их актуализацию должностных лиц;
- структура физической и логической топологии информационной системы с указанием планируемых информационных потоков между элементами СУ и каналов связи между ними;
- организационно-техническая структура автоматизированных участков СУ с указанием технических средства обработки и передачи данных, методов и алгоритмов обработки данных в виде пакетов общего и специального программного обеспечения;
- других характеристик системы и ее компонентов, способных оказать влияние на ход информационного процесса.

Порядок разработки программно-аппаратной системы защиты информации от НСД в АС зависит от стадии жизненного цикла, на которой находится СУ, существующего уровня автоматизации и степени изученности.

Объективно существует три ситуации, в которых может приниматься решение на создание системы защиты информации:

1. Создается новая СУ. Планируется решение задач управления с обработкой информации ограниченного доступа. Необходимые исходные данные для создания системы защиты информации разрабатываются

параллельно с проектированием АС на основе информационного обследования функциональных задач СУ.

2. СУ уже существует. Имеются задачи управления, решение которых требует обработки информации ограниченного доступа. Часть необходимых исходных данных для создания системы защиты информации формируется в результате информационного и технического обследования организационно-штатной структуры и существующей информационной архитектуры СУ.

3. СУ уже существует и в ее интересах функционирует АС, которая автоматизирует обработку данных на некоторых участках или во всей системе. СУ планируется настроить на решение задач управления, обрабатывающих информацию ограниченного доступа.

Если система только проектируется, то имеется возможность включить требования по безопасности информации в проект системы и учитывать их при разработке информационной инфраструктуры организации.

Если СУ уже существует и требуется автоматизация информационных процессов, то организационно-штатная структура уже сложилась, должностные лица и подразделения имеют функциональные задачи и, в целом, функциональные требования к АС уже слабо управляемы. Необходимо провести информационное и техническое обследование информационной архитектуры СУ, выявить все взаимодействующие информационные объекты, их функциональные задачи и информационные потоки между ними и разработать архитектуру АС в защищенном исполнении.

В случае создания системы защиты информации для уже функционирующей АС задачи по разработке системы защиты информации остаются те же, однако модификация архитектуры АС уже требует больших затрат. Создание системы защиты информации для существующей АС является сложной задачей из-за невозможности выполнить некоторые требования по безопасности и обеспечить требуемый класс защиты АС от НСД к информации.

5.3 Определение перечня защищаемых ресурсов и их критичности

5.3.1. Определение необходимости формирования политики безопасности

При автоматизации информационных процессов в системах управления необходимо иметь четко сформулированную на основе законодательных и нормативно-руководящих документов политику информационной безопасности.

Политика безопасности АС должна быть отражена в организационно-распорядительных документах, разрабатываемых при принятии решения на создание системы, а также на этапах ее проектирования, ввода в эксплуатацию и функционирования.

Исходными данными для формулирования политики безопасности АС являются:

- законы, указы и другие государственные законодательные акты, регулирующие правовые отношения в области информационной безопасности;

• руководящие, нормативные и методические документы, регламентирующие вопросы обеспечения безопасности информации, которые разрабатываются федеральными и ведомственными органами, входящими в систему защиты государственной тайны;

• информационная архитектура конкретной СУ (формируется в ходе обследования организационно-штатной структуры СУ);

• архитектура автоматизированного участка защищаемой СУ (формируется в ходе обследования состава и структуры существующей или в ходе проектирования создаваемой АС);

• варианты построения систем защиты информации в АС;

• тактико-технические характеристики средств вычислительной техники (СВТ) и защиты информации.

Система защиты информации, которая создается для обеспечения безопасности информации в автоматизированных системах, должна реализовать необходимые и достаточные требования по защите информации.

Состав требований по защите информации для конкретной АС формируется с учетом организационно-штатной структуры системы управления, характеристик решаемых задач и обрабатываемых данных, условий расположения, режимов функционирования и архитектуры комплекса технических средств обработки информации, в том числе средств вычислительной техники.

Основой для построения защиты информации в АС является формальная модель политики безопасности, которая представляет собой взаимосвязанную совокупность следующих элементов:

• множество защищаемых ресурсов информационной системы R={ri}, ri=(idi, rpi,), где id — идентификатор ресурса, rp — уровень безопасности;

• множество пользователей информационной системы U={uj}, uj=(idj,ulj), id — идентификатор пользователя, ul — уровень доступа;

• совокупность правил разграничения доступа пользователей к ресурсам информационной системы M=RxU;

• совокупность правил поведения пользователей системы;

• множество источников угроз безопасности информации и соответствующих им угроз S={sk}, sk={tl,pl,dl}, t — угроза безопасности, p — вероятность проявления угрозы, d — величина наносимого ущерба;

• множество механизмов защиты информации M={mn,}, mn=(fn, cn), fn — реализуемая функция, cn — стоимость реализации механизма;

• совокупность правил управления механизмами защиты и средствами их интеграции;

• совокупность оценок результатов применения механизмов защиты информации Rt=SxM;

• множество мероприятий по поддержанию и восстановлению работоспособности информационной системы.

Формулирование и разработка политики информационной безопасности проводится в два этапа.

На первом этапе высшими звеньями управления определяются общие требования к политике информационной безопасности. Соответствующие органы и должностные лица определяют важность (ценность) сведений, обрабатываемых в информационной системе, выделяют тематические разделы и информационные службы, которые нуждаются в особой защите с точки зрения обеспечения целостности, доступности и конфиденциальности информации.

На втором этапе разрабатывается политика информационной безопасности и, соответствующая, модель разграничения доступа для конкретной АС, с привлечением специалистов службы защиты информации, и согласуется с разработчиками защищенной АС.

Под службой защиты информации (СЗИ) понимается специальное штатное подразделение, создаваемое в установленном порядке на этапах ввода объектов АС или их отдельных элементов в эксплуатацию с соответствующим штатным расписанием.

Действие политики информационной безопасности распространяется на объект защиты (АС, объект вычислительной техники), пользователей и администраторов системы.

Под пользователем понимается должностное лицо, которое самостоятельно обрабатывает информацию на СВТ или в чьих интересах производится ее автоматизированная обработка.

При наличии информации ограниченного доступа принимается решение на создание системы защиты информации, и определяются структурные подразделения организации, информация которых наиболее критична. Для информации ограниченного доступа определяются грифы секретности или категории доступа (тематики), соответствующие их важности с точки зрения защиты. В то же время определяются наиболее важные направления обеспечения безопасности информации в разных подразделениях, т.е. выделяются информационные компоненты, которые являются более зависимыми от нарушения их целостности и/или доступности и/или конфиденциальности.

5.3.2. Классификация защищаемой информации

Классификация информации по грифам секретности или категориям доступности производится на основании законодательства РФ и ценности защищаемой информации, которая устанавливается ее собственником.

Исходными данными для проведения классификация информации являются:

- уровень звена управления, для которого проектируется АС;
- организационно-штатная структура СУ с перечнем должностных лиц и структурных подразделений, в интересах которых будет функционировать АС;
- функциональные задачи, которые предполагается решать в интересах подразделений и должностных лиц;
- архитектура АС.

Для каждой АС отрабатываются общий Перечень защищаемых ресурсов и Перечни защищаемых ресурсов подразделений или отдельных объектов ВТ, входящих в состав АС в качестве относительно независимых функциональных компонентов.

Перечни разрабатываются в процессе информационного и технического обследования АС и анализа решаемых функциональных задач, состава автоматизированных рабочих мест, организуемых банков данных, возможностей и режимов использования программных средств, а также средств, обеспечивающих обмен информацией между объектами АС. В Перечнях защищаемых ресурсов указываются сведения о допуске к этим ресурсам соответствующих подразделений или должностных лиц организации. Составление Перечней защищаемых ресурсов осуществляется совместно представителями подразделений, органов автоматизации, связи и защиты информации.

Перечни защищаемых ресурсов оформляются в виде официального распорядительного документа с приложением к нему сводного перечня задач, которые планируется решать в АС.

Примерная форма Перечня защищаемых ресурсов представлена в таблице 6.

Таблица 6 - Перечень защищаемых ресурсов на объекте ВТ ЛВС оперативного отдела и отдела кадров

№ п.п.	Защищаемый ресурс			К ресурсу допущены
	полное наименование	условное наименование	категория доступа	
1	2	3	4	5
1	Ключевой набор данных	RNLM2	Секретно	специалист по ОБИ (СЗИ)
2	АРМы операционного отдела	АРМ1	Секретно	работники операционного отдела
3	АРМ начальника операционного отдела	АРМ2	Секретно	Начальник и зам. начальника операционного отдела
4	АРМ отдела кадров	АРМ3	Конфиденц.	работники отдела кадров
5	Сервер ЛВС	С1	Секретно	Администратор безопасности ЛВС
6	ОС Windows	ОС336790422	Несекретно	Администратор безопасности ЛВС
…				

5.4. Определение категорий персонала и программно-аппаратных средств, на которые распространяется политика безопасности

5.4.1. Определение правил разграничения доступа к информации между различными категориями персонала

На основе анализа особенностей информационного обмена между подразделениями и штатного состава подразделений определяются:

- необходимость работы некоторых штатных категорий должностных лиц с различными информационными ресурсами, содержащими сведения ограниченного доступа;
- должностные лица, ответственные за поддержание актуальности различных разделов информационной базы;
- перечень типов операций с различными категориями документов (чтение, изменение, уничтожение, создание и т.п.) для отдельных категорий пользователей.

5.4.2. Определение категорий персонала, на которые распространяются требования политики безопасности

Часть сотрудников может иметь свои штатные автоматизированные рабочие места (АРМ), другая часть может совместно использовать автоматизированные рабочие места коллективного пользования. Некоторым должностным лицам может предоставляться право доступа к информационным ресурсам из-за пределов АС (удаленные или мобильные пользователи).

В целях регламентации использования различных технических средств, в том числе носимых компьютеров, множительной аппаратуры, средств печати документов, средств связи, необходимо определить порядок их использования, ответственных должностных лиц, отвечающих за безопасность информации при их использовании.

Результатом работы должны стать таблицы разграничения доступа (ТРД) категорий должностных лиц подразделений к информационным массивам:

- общая для всей организации;
- по каждому отдельному структурному подразделению.

Для обеспечения функционирования системы разграничения доступа к информации и техническим средствам вычислительного комплекса, ответственным по защите информации разрабатывается таблица разграничения доступа к защищаемым ресурсам.

Исходными данными для составления ТРД к защищаемым ресурсам являются перечни защищаемых ресурсов, заявки начальников структурных подразделений организации на должностных лиц, допущенных к работе с этими ресурсами, списки подразделений и должностных лиц, предоставляющих информационные службы, с их функциональными обязанностями и обязанностями по защите информации.

Основанием для включения должностных лиц в ТРД и предоставления им определенных полномочий к информационным ресурсам с указанием типов разрешенных доступов являются заявки на должностных лиц структурных подразделений организации.

Заявки могут иметь форму, приведенную в таблице 3. Возможно применение других разрешенных типов доступов. Количество и наименование граф 5-7 может меняться в зависимости от типов доступов к ресурсам, которые способны регулировать используемые средства разграничения доступа.

Таблица 7 - Примерная форма заявок на должностных лиц структурных подразделений организации

№ п/п	Должностные лица, допущенные к защищаемым ресурсам ОВТ	Защищаемые ресурсы				
		полное наименование ресурса	условное наименование ресурса	разрешенные виды доступа к ресурсу		
				чтение	запись	запуск
1	2	3	4	5	6	7
1	Начальник службы защиты информации	Папка «Документы начальника СЗИ»	Документы начальника СЗИ	да	да	-
		Файл verba.exe	EC025	-	-	да
		Файл verba.txt	FC376	да	да	-
2	Начальник операционного отдела	Папка «Документы начальника ОО»	Документы начальника ОО	да	да	-
		Файл verba.exe	EC025	-	-	да
3	…					

5.5 Определение особенностей расположения, функционирования и построения средств АС. Определение угроз безопасности информации и класса защищенности АС

Формирование набора требований по защищенности информации осуществляется на основании РД Гостехкомиссии /5, 6/, в которых указаны требования по защищенности для соответствующих классов АС и СВТ, а также информации, полученной при анализе или проектировании информационной архитектуры системы управления и АС, которые определяют особенности расположения, функционирования и построения средств компьютерной системы.

5.5.1. Информационное обследование системы

5.5.1.1. Определение информационных потребностей должностных лиц структурных подразделений

Для формирования детальных требований к построению защищенной АС необходимо выделить основные информационные задачи, решаемые должностными лицами различных подразделений.

Определяются места хранения информационных массивов, возможности совместного хранения информационных массивов различными подразделениями, способы и режимы обмена информацией между подразделениями и необходимость такого обмена.

5.5.1.2. Формирование перечня информационных услуг, предоставляемых информационной системой пользователям

Пользователи информационной системы нуждаются в определенных информационных услугах, которые представляются им в функциональном виде. Однако, чтобы основные службы могли функционировать, необходимо установить ряд вспомогательных служб. Имеются в виду серверы баз данных, почтовые серверы, сетевые службы, службы удаленного доступа, серверы

печати и т.п. Операционные системы и оборудование также можно отнести к вспомогательным службам.

На этом этапе необходимо сформировать отображение основных информационных служб на вспомогательные службы (конкретные компоненты информационной системы).

Типовой набор вспомогательных служб (информационных служб):

• совместное хранение информации;

• совместная обработка информации;

• совместное использование устройств печати документов;

• электронная почта;

• удаленный доступ внешних пользователей к ресурсам системы;

• доступ к внешним информационным ресурсам; и др.

5.5.1.3. Определение особенностей программно-аппаратной организации информационной системы, способов и средств связи самостоятельных компонент системы с внешней информационной средой

В защите нуждаются все информационные службы и коммуникационные каналы между ними. Для определения перечня необходимых механизмов безопасности нужно разработать или проанализировать программно-аппаратную конфигурацию всех серверов, рабочих мест, каналов связи информационной системы, а также других коммуникационных систем, особенно связанных с элементами информационной системы.

Результатом работы должна быть структурная схема информационной системы, на которой отображаются:

• основные серверы системы (если они есть), в том числе выделяются серверы, доступные извне, с указанием применяемых операционных систем;

• элементы системы, которые являются узлами связи различных компонент (сегментов) информационной системы;

• рабочие места, непосредственно связанные с выделенными для этого серверами, а также имеющие возможность организации связи с другими серверами, с указанием применяемых операционных систем;

• рабочие места или локальные сети, из которых возможно осуществление доступа к внешним информационным службам, с указанием средств, при помощи которых осуществляется доступ;

• реализация сетевых взаимодействий и особенности построения кабельной инфраструктуры.

5.5.1.4. Определение особенностей размещения основных систем и служб информационной системы, а также прокладки и использования кабельной системы, линий и каналов связи

Для исключения физического доступа посторонних лиц к элементам информационной системы необходимо проанализировать их размещение и возможности предотвращения или затруднения несанкционированного контакта с техническими средствами, в том числе:

• помещения, где располагаются основные серверы и рабочие места, контролируемость подходов к ним, способы охраны, в том числе противопожарной, и сигнализации;

• размещение в помещениях технических средств, особенно там, где возможно появление посетителей, с точки зрения недоступности для визуального обзора посторонними лицами;

• построение и размещение кабельных систем, расположения посторонних кабелей, способы и средства контроля за целостностью кабелей;

• особенности реализации связи с удаленными подразделениями.

5.5.1.5. Определение особенностей расположения и использования элементов систем коммуникаций и жизнеобеспечения

Для функционирования системы, особенно с точки зрения обеспечения целостности ресурсов и правильности их функционирования, важным является построение систем жизнеобеспечения, в том числе системы электропитания, пожаротушения и других.

Другой стороной систем жизнеобеспечения является их взаимосвязь с общедоступными системами и большая разнесенность по территории, что критично с точки зрения предотвращения утечки информации за счет электромагнитных наводок.

Результаты работы по этому разделу являются основой для формирования детальных описаний политики безопасности в виде правил разграничения доступа к ресурсам конкретных информационных служб, а также для выявления существующих угроз безопасности информации и выбора необходимых дополнительных механизмов безопасности.

5.5.2. Формулирование политики информационной безопасности структурных подразделений и информационных служб

Работы данного этапа выполняются отдельно для каждого функционального подразделения или информационной службы совместно начальником подразделения, администраторами системы и специалистами службы защиты информации.

5.5.2.1. Определение особенностей функционирования службы

Определение особенностей функционирования службы заключаются в уточнении:

• конфигурации применяемых аппаратных и программных средств;

• режимов функционирования, временных интервалов работы;

• распределения обязанностей между обслуживающим персоналом;

• интенсивности информационного обмена;

• перечня и характера связей с другими компонентами;

• зависимости от функционирования других компонент информационной системы;

• построения и надежности источников электропитания и других систем обеспечения.

5.5.2.2. Определение перечня ресурсов, относительно которых решаются задачи обеспечения целостности и конфиденциальности, а также доступности для легитимных пользователей

Если информационной основой организации является вычислительная сеть, то в число аппаратных активов следует включить компьютеры, периферийные устройства, внешние интерфейсы, кабельное хозяйство и

сетевое оборудование.

К программным активам, относятся операционные системы, прикладное программное обеспечение, инструментальные средства, программы управления сетью и отдельными системами. Важно зафиксировать, в каких узлах сети хранится программное обеспечение, и из каких узлов используется.

Третьим, и наиболее важным, видом активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, а также способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

5.5.2.3. Определение способов реализации правил разграничения доступа пользователей к информационным ресурсам

На основе разработанной политики информационной безопасности определяется модель разграничения доступа, которая будет являться базой формирования правил разграничения доступа и выбора конкретных средств защиты информации.

Руководящие документы Гостехкомиссии РФ определяют необходимость реализации дискреционного управления доступом для информационных систем, обрабатывающих информацию одного уровня конфиденциальности (секретности) и применения мандатного управления доступом для систем, обрабатывающих информацию разных уровней конфиденциальности (секретности).

5.5.2.4. Определение лиц, ответственных за ведение информационных массивов службы, а также возможностей их модификации другими пользователями

Главной задачей является определение лиц, ответственных за поддержание надлежащего состояния каждого конкретного ресурса (собственников ресурсов).

Результат работы можно представить в виде списков пользователей с разделением по категориям:

- администраторы системы;
- администраторы рабочих групп (подразделений);
- владельцы информационных ресурсов;
- операторы информационных служб;
- привилегированные пользователи;
- рядовые пользователи;
- внешние пользователи.

Для каждой категории необходимо определить максимальные полномочия по изменению конфигурации системы и обрабатываемой информации в соответствии с возможностями, предоставляемыми средствами информационной службы.

К таким полномочиям можно отнести, например, следующие:

- включение в систему новых устройств и программ;
- изменение режимов функционирования системы;
- включение новых пользователей;

• возможность работы с удаленных рабочих мест и др.

5.5.2.5. Формирование исчерпывающего набора правил разграничения доступа конкретных пользователей к конкретным объектам информационной службы

Для каждого сервера, относящегося к информационной системе, определяются поименные перечни пользователей, для которых будут созданы (или уже созданы) учетные записи с соответствующими атрибутами доступа к информации и дополнительными полномочиями.

5.5.2.6. Формулирование и оформление в виде организационно-распорядительных документов правил работы с конкретными информационными службами

Для регламентации поведения пользователей на рабочих местах и организации работы администраторов должны быть разработаны типовые инструкции для каждого рабочего места (частные инструкции по защите информации).

В инструкциях для администраторов информационных служб определяются основные положения политики безопасности применительно к данной службе и подходы к распределению полномочий пользователей.

В инструкциях для пользователей определяются правила работы в каждой информационной службе, а также действия в нестандартных и аварийных ситуациях.

Особенно детально должны быть расписаны правила работы пользователей, которые осуществляют связь с внешними информационными системами, а также в сегментах системы, в которые разрешен доступ внешних пользователей.

5.5.3. Определение класса защищенности АС

Для того чтобы сформировать набор требований по безопасности, которым должна отвечать АС, необходимо определить ее класс защищенности. Класс защищенности согласно руководящему документу Гостехкомиссии «Классификация АС и требования по защите информации» /5/ определяется на основании:

• перечня защищаемых ресурсов АС и их уровней конфиденциальности;

• перечня лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;

• матрицы доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;

• режимов обработки данных в АС.

При исследовании или проектировании информационной архитектуры системы необходимо определить:

• режимы обработки информации (коллективный или индивидуальный);

• полномочия пользователей по доступу к конкретным информационным ресурсам и штатным средствам АС;

• уровни секретности и категории защищаемой информации.

Для обработки секретной информации разрешается использовать только АС категорий 3А, 2А, 1В, 1Б, 1А.

Если АС состоит из одной или нескольких автономных АРМ, каждая из которых предназначена для индивидуального использования одним из пользователей, который допущен ко всей информации, располагаемой на этом АРМ и информация имеет один уровень секретности (не важно какой!), то АС относится к классу 3А.

Если в АС пользователи имеют одинаковые права доступа (полномочия) ко всей информации, обрабатываемой в АС и имеющей различные уровни секретности, то система относится к классу защищенности 2А.

Если в АС при тех же прочих условиях, что и для класса 2А, не все пользователи имеют доступ ко всей информации в системе, то система относится к первой группе. Определение классов защищенности АС первой группы по обработке информации различных уровней секретности производится на основании требований Гостехкомиссии.

Определение класса защищенности АС по обработке конфиденциальной информации производится на основании рекомендаций и требований Гостехкомиссии, изложенных в СТР-К.

5.6. Формирование требований к построению защищенной АС

На основе класса защищаемой АС выбираются средства вычислительной техники (СВТ), которые должны иметь соответствующие классы защищенности СВТ:

- для класса защищенности АС 1В используются СВТ не ниже 4 класса;
- для класса защищенности АС 1Б используются СВТ не ниже 3 класса;
- для класса защищенности АС 1А используются СВТ не ниже 2 класса.

Необходимо использовать данные действующих редакций документов.

Для классов защищенности АС 3А и 2А выбираются СВТ классов защищенности не ниже 4, 3, и 2 в зависимости от грифа секретности обрабатываемой информации, соответственно «секретной», «совершенно секретной» и «особой важности» /5/.

Требования, предъявляемые к межсетевым экрана (МЭ), не исключают требований, предъявляемых к СВТ и АС. При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться /5/.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

- при обработке информации с грифом «секретно» - не ниже 3 класса;
- при обработке информации с грифом «совершенно секретно» - не ниже 2 класса;
- при обработке информации с грифом «особой важности» - не ниже 1 класса.

Необходимо использовать данные действующих редакций документов.

Полный набор требований по безопасности к АС называется Заданием по безопасности, выполнение которого должно дать определенные гарантии защищенности информации.

5.7 Определение уязвимостей автоматизированной системы. Выбор средств защиты информации

Выделение угроз безопасности преследует цель ранжирования их по степени опасности для функционирования информационной системы.

5.7.1. Выбор компонент информационной системы, для которых возможно нарушений безопасности

На основе работ, выполненных при анализе информационной системы, получено достаточно информации, чтобы определить направления, на которых наиболее вероятно возникновение угроз безопасности информации. В зависимости от построения системы можно задать уровень детальности рассмотрения на основе, например, следующих градаций:

- информационная система в целом;
- сегменты информационной системы и средства связи между ними;
- серверы информационных служб и используемые сетевые технологии;
- рабочие станции различного назначения и их конфигурации;
- межсегментные устройства;
- средства связи с удаленными корреспондентами.

5.7.2. Определение точек информационного контакта анализируемых компонент с внешней информационной средой, через которые возможны нарушения безопасности информации

Определяются элементы системы, в которых возможен физический контакт с внешней информационной средой, и который может явиться основой для проявления угроз безопасности

Контролируемой зоной будем называть территорию организации (ЗАС), на которой исключено или существенно затруднено пребывание посторонних лиц.

При реализации угрозы безопасности в точках контакта информационной системы с внешней средой возникает канал утечки информации или канал проникновения в информационную систему.

Утечка информации может происходить за счет:

- разглашения информации;
- разведки информации;
- несанкционированного доступа в информационную систему.

Существование канала утечки информации всегда приводит к нарушению конфиденциальности информации.

Канал проникновения в информационную систему в большинстве случаев приводит к нарушению целостности или доступности информации.

5.7.3. Формирование моделей источников угроз безопасности информации

Угрозы безопасности можно разделить на несколько категорий относительной следующих классификационных признаков:

По наличию нарушителя:

- естественные, связанные со стихийными явлениями или авариями обеспечивающих систем;
- искусственные, связанные с деятельностью людей.
- по наличию умысла:
- случайные, когда умысел отсутствуют;
- умышленные, в противоположном случае.

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознанно со злым умыслом или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п.

Исследовав причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть или внешними.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об АС:

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;
- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые.

По уровню возможностей (используемым методам и средствам):

- применяющий агентурные методы получения сведений;

• применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);

• использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;

• применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

• в процессе функционирования АС (во время работы компонентов системы);

• в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);

• как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

• без доступа на контролируемую территорию организации;

• с контролируемой территории без доступа в здания и сооружения;

• внутри помещений, но без доступа к техническим средствам АС;

• с рабочих мест конечных пользователей (операторов) АС;

• с доступом в зону данных (баз данных, архивов и т.п.);

• с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

• работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;

• нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников;

• НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

5.7.3.1. Информационные каналы, выходящие за пределы контролируемой зоны

Информационные каналы можно подразделить на:

• выделенные каналы (предназначенные для передачи особо ценной информации);

• каналы, по которым передается конфиденциальная информация;

• каналы, по которым передается несекретная информация.

Кроме того, каналы связи можно разделить на общедоступные и ведомственные.

Для организации информационных каналов первых двух видов предпочтительнее использовать ведомственные системы связи, так как для них легче организовать применение технических средств защиты и контроля их целостности. Ведомственные каналы, как правило, недоступны для активного вмешательства, или такое вмешательство легко обнаруживается.

5.7.3.2. Побочные электромагнитные и другие излучения и наводки

Основные каналы утечки информации, возникающие за счет физических полей, можно проиллюстрировать следующей таблицей:

Таблица 8 - Основные каналы утечки информации

Каналы утечки информации	Виды перехватываемой информации
Акустический канал	Речевые и прочие акустические сигналы
Виброакустический канал	Речевые и прочие акустические сигналы
Утечка по проводному каналу (токонесущим инженерным коммуникациям)	Речевые и прочие акустические сигналы. Факсимильная, телеграфная, телетайпная информация. Информация, обрабатываемая на ЭВМ, или транслируемая по модемным каналам.
Электромагнитные поля	Информация передаваемая по радиотелефону и радиосвязи. Информация передаваемая по радиомодему
Побочные электромагнитные излучения и наводки	Информация, обрабатываемая на ЭВМ. ПЭМИН вспомогательного оборудования, промодулированные полезным акустическим сигналом
Оптический	Скрытая фото-, кино-, видеосъемка Видеонаблюдение из вне зоны охраны.

Данные каналы характеризуются их объективным существованием в пространстве, окружающем информационную систему. Практически не существует способов полного перекрытия данных каналов, однако выполнение мероприятий и применение специальных технических средств позволяет снизить вероятность проявления угрозы и существенно затруднить возможности злоумышленника по получению информации.

5.8 Выбор механизмов и средств защиты информации от НСД

5.8.1. Выбор защитных механизмов для предотвращения выявленных угроз безопасности информации или для усиления системы защиты и способы их реализации

Механизмы защиты информации являются достаточно специфичными и направленными на решение ограниченного круга задач безопасности. Для определения способов реализации механизмов защиты информации производится анализ возможных задач защиты из следующего перечня:

• введение избыточности элементов системы;

• резервирование элементов системы;
• регулирование доступа к элементам системы;
• защитное преобразование данных;
• контроль элементов системы;
• регулирование использования элементов системы;
• регистрация сведений об использовании элементов системы;
• уничтожение информации, потерявшей актуальность;
• сигнализация о попытках нарушения безопасности;
• реагирование на попытки нарушения безопасности.\

Таблица 9 - Способы нанесения ущерба

Способы нанесения ущерба	Объекты воздействий			
	оборудование	программы	данные	персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкциони-рованное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение “троянских коней”	Искажение, модификация	Вербовка персонала
Нарушение работоспособност и автоматизиро-ванной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Основу любой защищенной АС составляет совокупность некоторых механизмов защиты информации, которые можно выделить на основе различных критериев. Обычно выделяют следующие механизмы (или службы безопасности):

• идентификацию и аутентификацию;
• управление доступом;
• протоколирование и аудит;
• криптографию;
• экранирование.

Выбор способа реализации механизмов защиты информации и решения задач защиты заключается в выборе типа средств, которые планируется

использовать для решения каждого из механизмов организационные, инженерно-технические (физические), программно-технические, криптографические.

5.8.2. Определение функциональных компонент (информационных служб), в которых предполагается использовать выбранные механизмы защиты

Реализация политики безопасности информации в разных компонентах системы, как правило, строится на основе разных подходов и преследует разные цели в соответствии с тем, что в разных информационных службах главный упор делается на разные свойства информации (целостность, доступность, конфиденциальность).

Реализация механизмов защиты информации базируется на двух подходах:

• использование встроенных в основные информационные службы (в том числе операционные системы, прикладные программы и др.) средств защиты;

• использование дополнительных экранирующих (навесных) средств защиты.

Целью распределения механизмов защиты по компонентам является построение наиболее экономичной и наиболее эффективной системы защиты информации. Рациональным подходом в данном случае может рассматриваться использование одного механизма (или одного набора средств) для обслуживания некоторой группы взаимодействующих информационных служб.

Основное внимание уделяется недостатком используемых аппаратных и системных программных средств для определения необходимости применения в отдельных элементах информационной системы дополнительных средств защиты информации.

5.8.3. Определение способов интеграции механизмов безопасности в комплексную систему защиты информации

В настоящее время имеется большое количество разнообразных средств защиты информации, ориентированных на различные вычислительных платформы.

Задача интеграции средств защиты информации стоит особенно остро, если АС создавалась длительное время из разнородных компонентов. При этом может появиться общая проблема интеграции самих компонент информационной системы.

Лучшим подходом к интеграции средств защиты информации для разнородной информационной системы является выбор средств защиты на основе однотипных сетевых технологий. Это позволит организовать информационный обмен между элементами комплексной системы защиты и построить основу для создания централизованной системы управления защитой информации.

Дополнительным основанием для объединения средств защиты может служить соответствие их общепринятым международным (или государственным) стандартам.

При организации работ в разнородных информационных системах необходимо обращать внимание на достижение непротиворечивости и полноты

реализации функций защиты информации в информационной системе в целом.

Для построения АС, обрабатывающих информацию ограниченного доступа, должны выбираться только сертифицированные СВТ и криптографические средства защиты информации. Только в этом случае можно претендовать в суде на возбуждение уголовного дела по факту несанкционированного доступа к информации. Перечни сертифицированных СВТ и криптографических средств защиты информации публикуются подразделениями Гостехкомиссии РФ и ФСБ.

5.8.4. Оценка остаточного риска

После определения конфигурации системы защиты информации необходимо заново оценить оставшиеся угрозы безопасности информации. Оценив новые параметры угроз, необходимо принять решение о применении дополнительных средств защиты информации или сделать выводы о достижении требуемого уровня безопасности информационной системы. Для решения этой задачи используются инструментальные средства анализа рисков и, в частности, программный комплекс Digital Security Office 2006.

5.9 Рекомендации по выполнению практической части курсового проекта

Разработать структуру ресурсов (каталогов) для заданного количества пользователей АС, приведенных в задании.

Разработать и реализовать таблицу разграничения доступа для пользователей в соответствии с их должностным положением и возможностями прав доступа NTFS к каталогам по их смысловому содержанию. Например, каталог «Общие документы» доступен по чтению для группы «Все офицеры», каталог «Распоряжения начальника отдела» доступен по чтению для группы «Офицеры отдела» и имеет полный доступ для начальника отдела, каталог «Донесения Замначальника отдела» доступен по чтению для начальника отдела, по добавлению для замначальника отдела и недоступен для остальных.

Произвести расчет рисков ЗАС на основе модели угроз и уязвимостей.

Для разработанной первоначальной конфигурации СЗИ провести проверку и оптимизацию выбранных решений (контрмер) по организации защиты ЗАС (например в среде программного комплекса Digital Security Office):

- Произвести расчет рисков ЗАС на основе модели угроз и уязвимостей.
- Используя модуль управления рисками, на основе расчета эффективности каждой предложенной контрмеры выбрать наиболее оптимальные, которые позволят снизить риск до необходимого уровня с наименьшими затратами.
- Произвести расчет рисков ЗАС на основе модели информационных потоков.
- Используя модуль управления рисками, на основе расчета эффективности каждой предложенной контрмеры выбрать наиболее оптимальные, которые позволят снизить риск до необходимого уровня с

наименьшими затратами.

- Окончательный вариант системы защиты ЗАС организации выбрать по результатам всех расчетов.

По результатам моделирования и расчетов формируются соответствующие отчеты, которые в виде текстовых файлов приводятся в пояснительной записке.

6 Организация выполнения курсового проекта

6.1 Выбор темы курсового проекта

На первой неделе срока, выделенного учебным планом для выполнения курсового проекта, до сведения студентов доводится список тем курсового проектирования (раздел 2).

Студенту предоставляется право в течение недели выбрать любую тему из предложенного списка. Также студент может сам предложить интересующую его тему, если она соответствует изучаемому предмету и целям курсового проектирования.

При выборе темы курсового проекта рекомендуется консультироваться с преподавателем дисциплины "Проектирование защищенных автоматизированных систем".

Выполнять курсовые работы на одну и ту же тему нескольким студентам из одной учебной группы не рекомендуется.

Выбранная студентом тема утверждается руководителем курсового проектирования, о чем вносится соответствующая запись в бланк задания на подготовку курсового проекта (см. Приложение 2).

Задание на выполнение курсового проекта является нормативным документом, устанавливающим границы и глубину разработки темы, а также сроки представления работы на кафедру в завершенном виде.

6.2 Контроль выполнения курсового проекта

После утверждения темы курсового проекта студент обязан изучить исходные данные к Курсовому проекту, подобрать и изучить литературу по теме проекта, составить план, регулярно посещать консультации руководителя, дорабатывать отдельные части проекта по замечаниям руководителя, своевременно подготовить и сдать на проверку законченный Курсовой проект и защитить его.

На руководителя возлагается ответственность за постоянное наблюдение за разработкой всех разделов курсового проекта в соответствующие сроки и оказание студенту необходимой помощи на всех этапах выполнения проекта.

В процессе проектирования для студентов проводятся в соответствии с утвержденным кафедрой графиком групповые и индивидуальные консультации.

Руководитель обязан:

- установить студенту календарный график выполнения этапов проектирования и занести его в бланк задания на подготовку курсового проекта (см. Приложение 2);
- регулярно проводить консультации в соответствии с графиком при уточнении темы, разработке плана, составлении списка литературы, обобщении материала и т.д.;
- контролировать соблюдение календарных сроков и качество выполнения как отдельных частей, так и проекта в целом. Если при проверке обнаружатся ошибки, неполнота объема, незавершенность проектирования или низкое качество оформления, то проект возвращается студенту для доработки;
- принять (по-возможности, совместно с комиссией) защиту курсового проекта.

6.3 Подведение итогов и защита курсового проекта. Подготовка презентации

В качестве отчетных материалов по проекту студент должен представить пояснительную записку.

Подведение итогов подготовки курсового проекта включает следующие этапы:

- сдача курсового проекта на проверку руководителю;
- доработка курсового проекта с учетом замечаний руководителя;
- сдача готовой курсового проекта на защиту;
- защита курсового проекта.

Срок сдачи готовой курсового проекта определяется заведующим кафедрой. График защиты курсовых работ вывешивается на доске объявлений.

Срок доработки курсового проекта устанавливается руководителем с учетом сущности замечаний и объема необходимой доработки.

Выполненная курсовой проект подписывается студентом и представляется на защиту. Курсовой проект, удовлетворяющий предъявленным требованиям, допускается к защите и прошедшая проверку на объем заимствований.

На проверенную курсовой проект руководитель в обязательном порядке пишет отзыв по строго установленной в академии форме (Приложение 9).

В отзыве дается оценка уровня сформированности компетенций, соответствия работы предъявляемым требованиям, содержание и структура работы, степень самостоятельности, теоретическая и практическая значимость выводов и предложений, а также уровень грамотности (общий и специальный). В отзыве отмечаются положительные качества работы и недостатки.

Если, по мнению руководителя, курсовой проект заслуживает неудовлетворительной оценки и подлежит переработке, то в отзыве

указываются недостатки, которые следует устранить и/или доработать. После устранения недостатков работа представляется на повторную проверку. Если представляется несколько курсовых работ с идентичным содержанием, что не отражает степень самостоятельности выполнения работы, все эти работы возвращаются исполнителям на переработку и повторное рецензирование, после чего обучающийся приступает к процедуре защиты работы.

Защита курсового проекта на комиссии в составе руководителя курсового проекта и одного или двух преподавателей кафедры может быть организована разными методами: индивидуально или группой, с привлечением оппонентов из числа студентов.

По-возможности, защита курсового проекта должна проводиться публично в присутствии группы.

Руководитель работы определяет требования к содержанию и продолжительности доклада при защите, устанавливает регламент для оппонентов.

Защита курсового проекта, как правило, состоит в коротком докладе (5 - 7 мин) студента и ответах на вопросы по существу проекта. За такое время можно представить примерно 2 - 3 страницы стандартного машинописного текста.

Доклад представляет конспект выступления студента. В докладе студент должен раскрыть цель и задачи курсового проекта, его актуальность, кратко изложить содержание, делая акцент на выводах. Основное требование к докладу - обеспечение логической последовательности между разделами, подчиненной четкому и полному изложению цели.

Желательно к защите подготовить презентационный материал, поскольку он помогает студенту успешно защищать свою работу, свои идеи и представлять их в самом выгодном свете. Представленная презентация должна быть последовательно и жестко связана с содержанием доклада.

Все слайды, используемые на защите, должны быть представлены в пояснительной записке как последнее приложение.

Презентацию следует оформлять в Microsoft PowerPoint.

Для того чтобы такая презентация действительно делала выступление более эффективным, необходимо соблюдение определенных требований. Эти требования кажутся очевидными. Тем не менее, практика показывает, что они часто нарушаются не только начинающими, но и квалифицированными пользователями и специалистами в области информационных технологий.

Во-первых, информация на слайдах должна хорошо читаться. Это обеспечивается выбором оптимального цветового решения, размера и типа шрифта, объема и структуры информации на слайде.

Выбор цветового решения - соотношения цветов фона слайда и текста - диктуется условиями показа. Для демонстрации презентации на экране монитора или с помощью проектора в хорошо затемненном помещении вполне оправдан выбор ярких цветов, темного фона слайдов и светлого цвета текста. Типичной же ситуацией является отсутствие затемнения, поэтому оптимальным для электронной презентации является светлый фон слайдов и темный цвет текста.

Размер шрифта, позволяющий сделать текст приемлемым для чтения на экране, предусмотрен в шаблонах презентаций, поэтому имеет смысл размещать на слайде такой объем текста, который бы не приводил к автоматическому уменьшению размера шрифта.

Кроме того, нужно помнить, что на экране лучше воспринимаются шрифты без засечек (такие как, например, Tahoma, Verdana, Arial), поэтому использовать привычный для печатных текстов шрифт Times New Roman в презентациях не рекомендуется, также как не рекомендуется использовать курсивное начертание.

Текст презентации не должен служить конспектом для докладчика. В презентациях, иллюстрирующих публичное выступление, каковым является защита курсового проекта, текст должен быть свернут до ключевых слов и фраз. Полные развернутые предложения на слайдах таких презентаций используются только при необходимости цитирования. Текст каждого слайда должен быть кратким, но содержательным и хорошо структурированным.

Списки на слайдах не должны включать более 5-7 элементов. Если элементов списка все-таки больше, их лучше расположить в две колонки.

В таблицах не должно быть более 4 строк и 4 столбцов - в противном случае данные в таблице будет просто невозможно увидеть. Ячейки с названиями строк и столбцов и наиболее значимые данные рекомендуется выделять цветом.

Гистограммы не должны включать более 4 категорий, а организационные диаграммы - более 5 элементов.

Если требуются более объемные таблицы и диаграммы, лучше подготовить их для раздаточных материалов с помощью других программ.

Во-вторых, выбранные средства визуализации должны быть адекватными содержанию.

Информация, которая плохо воспринимается на слух - даты, имена, новые термины, названия - должна быть обязательно представлена на слайдах.

При графическом представлении информации должны использоваться адекватные средства визуализации, т.е. подбираться соответствующие содержанию типы графиков и диаграмм, иллюстрации, таблицы.

Средства динамического представления информации (перемещение или разновременное появление фрагментов текста и графических объектов, другие анимационные эффекты и эффекты смены слайдов) должны служить для дозирования информации, привлечения внимания слушателей к той ее части, о которой идет речь в определенный момент выступления, и показа явлений в динамике.

В презентации должно быть не менее 5 слайдов. Количество слайдов определяется исходя из потребностей доклада. Количество и содержание слайдов должны быть адекватны содержанию и продолжительности выступления.

Избыточное количество слайдов приводит не только к нарушению регламента, но и к утомлению слушателей и рассеиванию их внимания.

Все слайды (кроме первого и последнего, которые не включаются и в приложения пояснительной записки) должны быть пронумерованы в порядке следования. После номера ставится точка ".", пробел " " и с большой буквы приводится заголовок слайда без точки на конце, например: "1. Наименование слайда". Если логически однородный материал разбивается на несколько слайдов, то в их нумерации используют русские буквы, например: "2.А. Наименование слайда", "2.Б. Наименование слайда". Все заголовки слайда должны выделяться большим размером шрифта, жирностью и цветом. Слайды могут содержать подзаголовки.

Первый слайд презентации является слайдом - приветствием, на котором необходимо разместить:

- наименование ВУЗа, в котором обучается студент;
- вид работы (Курсовой проект);
- тема курсового проекта;
- наименование выпускающей кафедры;
- фамилия, имя, отчество студента;
- шифр группы, в которой обучается студент;
- фамилия, имя и отчество руководителя курсового проектирования с указанием его научной степени и звания;
- место защиты и год защиты.

Последний слайд сообщает о завершении доклада. На нем помещаются фразы «Спасибо за внимание. Доклад окончен».

Необходимо помнить, что чрезмерное увлечение дизайном, звуковым сопровождением, анимацией может отвлечь слушателей от сути выступления.

Курсовой проект оценивается по 100-балльной шкале с выставлением оценки по пятибалльной системе. Оценка зависит от качества выполнения и защиты курсового проекта. Критерии оценки качества исполнения курсового проекта приведены в таблице 10.

Таблица 10 - Критерии оценки качества исполнения курсового проекта *($О_{работа}$)*

№ п/п	Критерии оценки	Оценка работы (по 100-балльной шкале)	
		min количество баллов	max количество баллов
1.	Соответствие содержания курсовой работы утвержденной теме	0-10	10
2.	Выполнение поставленных целей и задач	0-5	5
3.	Оценка работы в разрезе структурных элементов	0-28	28
3.1	Введение	0-5	5
3.2	Основная часть	0-32	32
3.5	Заключение	0-6	6

4.	Общая характеристика работы (сбалансированность по объему теоретической, аналитической и проектной частей, правильность интерпретации результатов)	0-4	4
5.	Оформление работы	0-10	10
	ИТОГОВАЯ ОЦЕНКА по Курсовому проекту	0-100	100

*Максимальное количество баллов ставится только в случае полного выполнения того или иного критерия.

Защита курсового проекта - обязательная процедура, которая оказывает существенное влияние на выставление итоговой оценки проведённого исследования. Качество исполнения курсового проекта оценивается руководителем *($О_{работа}$)*, а результаты защиты либо только руководителем, либо членами комиссии по защите курсовых работ *($О_{защита}$)* (если это решение было приято на заседании кафедры).

Оценка руководителя ставится на основании отзыва на курсовой проект. Качество исполнения и защиты курсового проекта оценивается по 100-балльной (рейтинговой) системе в соответствии со следующими критериями оценки (таблица 11).

Таблица 11 - Критерии оценки защиты курсового проекта *($О_{защита}$)*

№ п/п	Критерии оценки	Оценка защиты курсовой работы (по 100-балльной шкале)
1.	Владение содержанием курсового проекта	30
2.	Логическая последовательность изложения материала	5
3.	Краткость изложения работы	5
4.	Умение вычленить главную мысль работы	10
3.	Умение обосновать собственный вклад в работу	20
4	Полнота и грамотность ответов на вопросы при защите	20
5	Наличие подготовленного иллюстрационного материала	10
	ИТОГОВАЯ ОЦЕНКА по защите курсового проекта	100

Итоговая оценка за курсовой проект рассчитывается по формуле:

$$О_{итог} = 0,4 \cdot О_{работа} + 0,6 \cdot О_{защита}$$

Полученное количество баллов трансформируется в оценку и проставляется в зачетную книжку обучающегося и зачетную ведомость для курсовых работ.

Результаты выполнения и защиты курсовых работ определяются оценками:

90-100 баллов - «отлично»;

70-89 баллов - «хорошо»;

50-69 баллов - «удовлетворительно»;

0-49 баллов - «неудовлетворительно».

Результат защиты курсового проекта студента оценивается в форме зачета с оценкой (дифференцированного зачета) по бально-рейтинговой и пятибальным системам. Кафедра разрабатывает критерии оценки, в соответствии с которыми устанавливается качество сформированности у студента компетенций, которые он должен приобрести при подготовке курсового проекта и продемонстрировать в ходе ее защиты, а также уровень знаний, владений (навыков), которые студент должен продемонстрировать для подтверждения освоенных компетенций.

Оценка зачтено (с оценкой *«отлично»),* зачтено *(с оценкой «хорошо»),* зачтено *(с оценкой «удовлетворительно»*) проставляется в зачетную книжку студента и зачетную ведомость для защиты курсовых работ. Отрицательная оценка в зачетную книжку не вносится. Полное наименование курсовых работ вносится в зачетную книжку и в приложение к Курсовому проекту.

Студент, не представивший курсовой проект или получивший неудовлетворительную оценку, считается студентом, имеющим академическую задолженность по учебной дисциплине.

По решению кафедры для защиты курсовых работ может быть утверждена комиссия. Число членов комиссии для защиты курсового проекта должно составлять не более трех человек. Состав комиссии определяется заведующим кафедрой.

Повторная защита курсовых работ для обучающихся, которые по уважительной причине не вышли на защиту курсового проекта, назначается либо в период проведения зачётной недели, либо в дополнительную сессию по решению кафедры.

Хранение курсовых работы осуществляется согласно номенклатуре дел кафедры.

6.4 Порядок размещения в ЭБС и автоматизированной (компьютерной) проверке на объем и характер заимствования курсовой работы

Проверка курсовых работ на объем и характер заимствования курсовых и выпускных квалификационных работ по направлениям подготовки/специальностям высшего образования является составной частью реализуемого в академии процесса контроля соблюдения академических норм при выполнении и защите курсовых работ.

Проверка работ на наличие неправомерных заимствований осуществляется с помощью программных продуктов электронных систем проверки заимствований.

При наличии в Курсовому проекту менее 45% оригинального текста, она отправляется на доработку при сохранении ранее установленной темы и после этого подвергается повторной проверке.

При повторной проверке курсовой проект, имеющая менее 45% оригинального текста, в течение 3-х дней должна быть доработана при сохранении ранее установленной темы и после этого подвергается окончательной проверке. Если после проведения научным руководителем окончательной проверки уровень оригинальности не достигает установленного минимального рубежа в 45%, курсовой проект не допускается к защите.

Итоговая проверка курсового проекта осуществляется с помощью программных продуктов электронных систем проверки заимствований должна быть выполнена за месяц до начала экзаменационной сессии и сдачи экзамена по дисциплине, по которой учебным планом предусмотрено выполнение курсового проекта.

Обучающийся, не допущенный к защите курсового проекта, считается имеющим академическую задолженность по дисциплине, по которой предусмотрено выполнение курсового проекта.

Все курсовые работы обучающихся (полный текст) подлежат загрузке в электронную среду академии.

Доступ лиц к текстам курсовых работ должен быть обеспечен в соответствии с законодательством Российской Федерации, с учетом изъятия производственных, технических, экономических, организационных и других сведений, в том числе о результатах интеллектуальной деятельности в научно-технической сфере, о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, в соответствии с решением правообладателя.

После проведения проверок курсового проекта научным руководителем формируется справка-заключение о проверке на наличие незаконных заимствований и прикладывается к Курсовому проекту (Приложение10).

7 Оценочные средства для проведения аттестации уровня сформированности компетенций обучающихся при выполнении курсового проекта

7.1 Перечень компетенций, с указанием этапов их формирования в процессе освоения образовательной программы

Перечень компетенций и их структура в виде знаний, умений и владений содержится в таблице 12 «Перечень планируемых результатов обучения дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы».

Таблица 12 - Критерии оценивания уровня сформированности компетенции обучающихся в результате выполнения и защиты курсового по дисциплине «Проектирование защищенных автоматизированных систем»

ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах	
ПК-3.1: Фиксирует возникновение инцидентов информационной безопасности	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Фиксирует возникновение инцидентов информационной безопасности
Уровень 2	Уровень знаний Фиксирует возникновение инцидентов информационной безопасности в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Фиксирует возникновение инцидентов информационной безопасности в объёме, соответствующем программе подготовки, без ошибок
ПК-3.2: Использует методы и средства резервного копирования информации	
Уметь	
Уровень 1	Продемонстрированы основные умения Использует методы и средства резервного копирования информации,
Уровень 2	Продемонстрированы все основные умения Использует методы и средства резервного копирования информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме,
Уровень 3	Продемонстрированы все основные умения Использует методы и средства резервного копирования информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все
ПК-3.3: Устраняет уязвимости в автоматизированной системе	
Владеть	
Уровень 1	Имеется минимальный набор навыков Устраняет уязвимости в автоматизированной системе с негрубыми
Уровень 2	Продемонстрированы базовые навыки Устраняет уязвимости в автоматизированной системе с некоторыми
Уровень 3	Продемонстрированы навыки Устраняет уязвимости в автоматизированной системе без ошибок и
ПК-3.4: Соотносит изменения в конфигурации автоматизированной системы с её защищенностью	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Соотносит изменения в конфигурации автоматизированной
Уровень 2	Уровень знаний Соотносит изменения в конфигурации автоматизированной системы с её защищенностью,
Уровень 3	Уровень знаний Соотносит изменения в конфигурации автоматизированной системы с её защищенностью без
Уметь	
Уровень 1	Продемонстрированы основные умения Использует методы и средства резервного копирования информации,

Уровень 2	Продемонстрированы все основные умения Использует методы и средства резервного копирования информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме,
Уровень 3	Продемонстрированы все основные умения Использует методы и средства резервного копирования информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все
Владеть	
Уровень 1	Имеется минимальный набор навыков Устраняет уязвимости в автоматизированной системе с негрубыми
Уровень 2	Продемонстрированы базовые навыки Устраняет уязвимости в автоматизированной системе с некоторыми
Уровень 3	Продемонстрированы навыки Устраняет уязвимости в автоматизированной системе без ошибок и

ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном	
ПК-4.1: Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
ПК-4.2: Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем	
Уметь	
Уровень 1	Продемонстрированы основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми
Уровень 3	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными
ПК-4.3: Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Проверяет программы и алгоритмы на предмет соответствия требованиям
ПК-4.4: Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме

Уровень 2	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми
Уровень 3	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными
Владеть	
Уровень 1	Имеется минимальный набор навыков Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Проверяет программы и алгоритмы на предмет соответствия требованиям
ПК-4.5: Предлагает конфигурации и состав автоматизированной системы	
Знать	
Уровень 1	Минимальный необходимый уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем
Уровень 2	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с негрубыми
Уровень 3	Продемонстрированы все основные умения Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем, решены все основные задачи с отдельными
Владеть	
Уровень 1	Имеется минимальный набор навыков Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки Проверяет программы и алгоритмы на предмет соответствия требованиям

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии оценивания уровня сформированности компетенции обучающегося, формируемые в результате выполнения курсового проекта по дисциплине «Проектирование защищенных автоматизированных систем» представлены в таблице10.

7.3 Примерный перечень основных вопросов для защиты курсового проекта.

1. Чем вызван Ваш выбор темы для своего исследования? В чем заключается ее актуальность?

2. Как отражена в Вашем исследовании связь с актуальными проблемами защиты автоматизированных систем в России?

3. Какие цели и задачи Вы ставили в своем исследовании? Что Вы хотели доказать?

4. Что нового Вы узнали в изучаемом Вами дополнительном материале по сравнению с учебной литературой?

5. На каких основных источниках Вы основывали написание своей курсового проекта? Что показалось Вам интересным в той или иной работе, что конкретно Вы использовали в своем Курсовому проекту?

6. Какие выводы и предложения по своей теме курсового проекта Вы сделали, каков основной итог Вашей работы?

7. Собираетесь ли Вы продолжать свои исследования по данной теме в будущем? Если да, то по каким основным направлениям?

8. Чем Вам могут помочь знания, полученные в данной области, в Вашей дальнейшей работе?

9. Чем обусловлен выбор средств защиты информации в проектируемой системе?

8 Условия обучения лиц с ограниченными возможностями здоровья

Для студентов из числа лиц с ограниченными возможностями здоровья обучение проводится Академией с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья.

При проведении обучения по дисциплине обеспечивается соблюдение следующих общих требований:

− проведение обучения для лиц с ограниченными возможностями здоровья в одной аудитории совместно со студентами, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для них в процессе обучения;

− присутствие в аудитории ассистента, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем);

− пользование необходимыми обучающимся техническими средствами при выполнении практических и других работ в соответствии с учебным планом с учетом их индивидуальных особенностей;

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья образовательная среда Академии обеспечивает выполнение следующих требований при обучении и проведении промежуточной и итоговой аттестации:

а) для слепых:

− задания и иные материалы для аттестации зачитываются ассистентом;

− письменные задания надиктовываются обучающимся ассистенту;

б) для слабовидящих:

− задания и иные учебно-методические материалы оформляются увеличенным шрифтом;

− обеспечивается индивидуальное равномерное освещение не менее 300

− люкс;

− при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

− обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

− по их желанию аттестационные испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

− письменные задания надиктовываются ассистенту;

− по их желанию все аттестационные испытания проводятся в устной форме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Основная литература

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1035570. - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1865598
2. Семеновых, В. И. Проектирование автоматизированных систем : учебное пособие / В. И. Семеновых, А. А. Перминов. - Москва ; Вологда : Инфра-Инженерия, 2022. - 116 с. - ISBN 978-5-9729-1060-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1903144
3. Макаренко, С.И.. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : Учебное пособие / С.И. Макаренко, А.А. Ковальский, С.А. Краснов — Санкт-Петербург : Наукоемкие технологии, 2020. — 358 с. — ISBN 978-5-6044429-8-2. — URL: https://book.ru/book/942928
4. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2023. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: https://doi.org/10.29039/01848-4. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/2038247

Дополнительная литература

1. Коваленко, Ю. И., Нормативное обеспечение информационных систем в защищенном исполнении : монография / Ю. И. Коваленко, М. М. Тараскин, О. И. Торба. — Москва : Русайнс, 2020. — 233 с. — ISBN 978-5-4365-1811-4. — URL: https://book.ru/book/934104
2. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). — www.dx.doi.org/10.12737/2248. - ISBN 978-5-16-009519-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1036519
3. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1212394
4. Королёв, М. В., Обеспечение защищенности речевой информации при использовании систем виброакустического зашумления : монография / М.

В. Королёв. — Москва : Русайнс, 2022. — 127 с. — ISBN 978-5-4365-9826-0. — URL: https://book.ru/book/944860
5. Енютина, Т. А. Расчет и проектирование систем обеспечения безопасности : учебное пособие / Т. А. Енютина, Л. В. Кулагина. - Красноярск : Сибирский федеральный университет, 2022. - 190 с. - ISBN 978-5-7638-4599-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2092915
6. Царегородцев, А. В. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем : монография / А.В. Царегородцев, С.В. Романовский, С.Д. Волков. — Москва : ИНФРА-М, 2024. — 198 с. - (Научная мысль). - DOI 10.12737/2049718. - ISBN 978-5-16-018719-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/2049718

ПРИЛОЖЕНИЕ 1
(обязательное)
Титульный лист курсового проекта

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар)
(НАН ЧОУ ВО Академия ИМСИТ)

Институт информационных технологий и инноваций

Кафедра математики и вычислительной техники

КУРСОВОЙ ПРОЕКТ
по дисциплине: «Проектирование защищенных автоматизированных систем»

на тему: РАЗРАБОТКА ЭСКИЗНОГО ПРОЕКТА СИСТЕМЫ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) образовательной программы
«Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

Работу выполнил студент
4 курса очной формы
обучения, группы 24-ИБ-01 _____ А.В. Ермоленко

Научный руководитель:
канд. техн. наук, доцент _____ К.Н. Цебренко

Работа защищена с оценкой «_____»

Краснодар 2029

ПРИЛОЖЕНИЕ 2
(обязательное)
Форма задания на курсовой проект

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования «Академия маркетинга и социально-информационных технологий – ИМСИТ» (г. Краснодар)
Кафедра математики и вычислительной техники

УТВЕРЖДАЮ
Зав. кафедрой _____
_____
«____» _____ 20___ г.

З А Д А Н И Е
на курсовой проект

Студенту:_____ группы_____ курса
(Ф.И.О.) (№ группы и курса)

факультета _____
направления _____
_____
(шифр и наименование)

Тема работы:_____

Содержание задания:_____
_____

Объем работы:
а) пояснительная записка к работе _____ с.
б) задачи

Рекомендуемая литература:_____

Срок выполнения работы: с "___" _____по"___"____20__г.
Срок защиты: "___"____20__г.
Дата выдачи задания: "___"____20__г.
Дата сдачи проекта на кафедру: "___"____20__г.
Руководитель работы _____
(подпись, ф.и.о., звание, степень)

Задание принял студент _____
(подпись, дата)

ПРИЛОЖЕНИЕ 3
(справочное)
Оформление рисунка

	Название задачи	Длительность	Начало	Окончание
1	Получение задания на курсовое проектирование	1 день	Пн 18.02.08	Пн 18.02.08
2	Подписание заявления	1 день	Вт 19.02.08	Вт 19.02.08
3	Сбор необходимых материалов по предметной области	10 дней	Ср 20.02.08	Пт 29.02.08
4	Составление примерного проекта в MS Project	3 дней	Ср 20.02.08	Пт 22.02.08
5	Написание технического задания	7 дней	Сб 23.02.08	Пт 29.02.08
6	Описание предметной области	3 дней	Вт 26.02.08	Чт 28.02.08
7	Анализ и выбор инструмента моделирования	3 дней	Пт 29.02.08	Вс 02.03.08
8	Создание диаграмм и IDEF-комплекта	8 дней	Пн 03.03.08	Пн 10.03.08
9	Создание физической модели	3 дней	Вт 11.03.08	Чт 13.03.08
10	Создание логической модели	3 дней	Пт 14.03.08	Вс 16.03.08
11	Создание диаграмм UML	5 дней	Пн 17.03.08	Пт 21.03.08
12	Создание эскизного проекта	5 дней	Сб 22.03.08	Ср 26.03.08
13	Представление работы в электронном виде	1 день	Чт 27.03.08	Чт 27.03.08
14	Исправление ошибок	3 дней	Пт 28.03.08	Вс 30.03.08
15	Предзащита работы	1 день	Пн 31.03.08	Пн 31.03.08
16	Сдача в печать	1 день	Вт 01.04.08	Вт 01.04.08
17	Защита работы	1 день	Ср 02.04.08	Ср 02.04.08

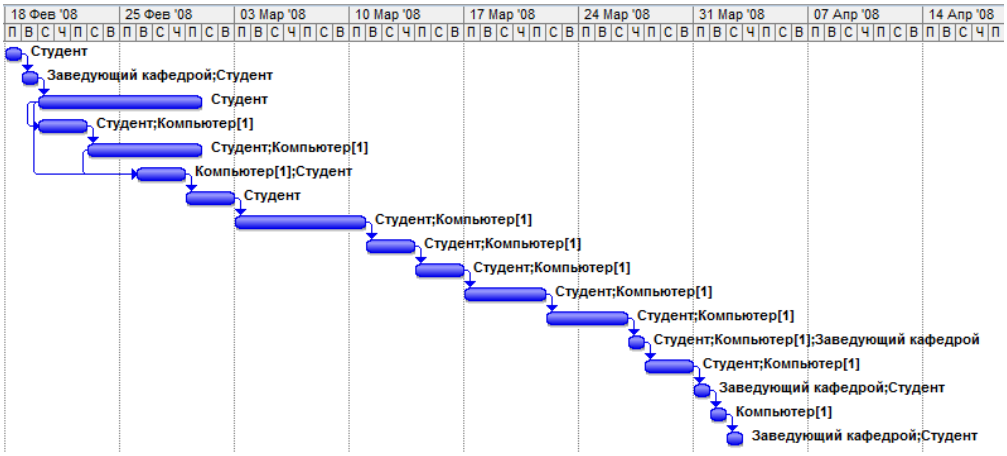


Рисунок 3.1 – Диаграмма Ганта

ПРИЛОЖЕНИЕ 4
(справочное)

Краткий перечень международных стандартов, применяемых при проектировании автоматизированных систем

ISO 9000:2000. Системы менеджмента качества. Основные положения и словарь.

ISO 9001:2000. Системы менеджмента качества. Требования.

ISO 9004:2000. Системы менеджмента качества. Рекомендации по улучшению деятельности.

ISO 19011:2002. Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента

ISO/IEC 90003:2004. Техника программного обеспечения. Рекомендации по применению ISO 9001:2000 к компьютерному программному обеспечению.

ISO/IEC 15288:2002. Системотехника. Процессы жизненного цикла системы.

ISO/IEC TR 19760:2003. Системотехника. Руководство по применению ISO/IEC 15288 (Процессы жизненного цикла системы)

ISO/IEC 15504-1:2004. Информационные технологии. Оценка процессов. Часть 1. Общие понятия и словарь.

ISO/IEC 15504-2:2003. Информационные технологии. Оценка процессов. Часть 2. Выполнение оценки

ISO/IEC 15504-3:2004. Информационные технологии. Оценка процесса. Часть 3. Руководство по выполнению оценки.

ISO/IEC 15504-4:2004. Информационные технологии. Оценка процесса. Часть 4. Руководство для усовершенствования процессов и определения их результативности.

ISO/IEC TR 15504-5:1999. Информационные технологии. Оценка процессов программного обеспечения. Часть 5. Оценочная модель и руководящие указания по индикации.

ISO/IEC 14756:1999. Информационные технологии. Измерение и оценка эксплуатационных характеристик автоматизированных систем программного обеспечения.

ISO/IEC TR 14759:1999. Разработка программного обеспечения. Макет и прототип. Категоризация моделей макета и прототипа программного обеспечения и их применение.

ISO/IEC TR 12182:1998. Информационные технологии. Классификация программного обеспечения

ISO/IEC 12207:1995. Информационные технологии. Процессы жизненного цикла программного обеспечения.

ISO/IEC TR 15271:1998. Информационные технологии. Руководство по применению ISO/IEC 12207 (Процессы жизненного цикла программных средств).

ISO/IEC TR 16326:1999. Разработка программного обеспечения. Руководство по применению ISO/IEC 12207 к управлению проектом.

ISO/IEC 12207:1995/Amd.1:2002. Информационные технологии. Процессы жизненного цикла программного обеспечения. Изменение 1

ISO/IEC 12207:1995/Amd.2:2004. Информационные технологии. Процессы жизненного цикла программного обеспечения. Изменение 2.

ISO/IEC 16085:2004. Информационные технологии. Процессы жизненного цикла программного обеспечения. Управление рисками.

ISO/IEC TR 19759:2005. Совокупность знаний о разработке программного обеспечения. Руководство.

ISO/IEC 15026:1998. Информационные технологии. Системные и программные уровни целостности.

ISO/IEC 25000:2005. Технология программного обеспечения. Требования и оценка качества программного продукта. Руководство.

ISO/IEC 9126-1:2001. Программная инженерия. Качество продукта. Часть 1. Модель качества.

ISO/IEC TR 9126-2:2003. Программная инженерия. Качество продукта. Часть 2. Внешние метрики.

ISO/IEC TR 9126-3:2003. Программная инженерия. Качество продукта. Часть 3. Внутренние метрики.

ISO/IEC TR 9126-4:2004. Программная инженерия. Качество продукта. Часть 4. Показатели качества в использовании.

ISO/IEC 12119:1994. Информационные технологии. Пакеты программ. Требования к качеству и тестирование.

ISO/IEC 14598-1:1999. Информационные технологии. Оценка программного продукта. Часть 1. Общий обзор.

ISO/IEC 14598-2:2000. Разработка программного обеспечения. Оценка программного продукта. Часть 2. Планирование и руководство.

ISO/IEC 14598-3:2000. Разработка программного обеспечения. Оценка программного продукта. Часть 3. Процесс для разработчиков.

ISO/IEC 14598-4:1999. Разработка программного обеспечения. Оценка продукта. Часть 4. Процесс для закупщика.

ISO/IEC 14598-5:1998. Информационные технологии. Оценка программного продукта. Часть 5. Процесс для оценщика.

ПРИЛОЖЕНИЕ 5
(справочное)

Краткий перечень национальных стандартов, применяемых при проектировании автоматизированных систем

ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь.

ГОСТ Р ИСО 9001-2001. Системы менеджмента качества. Требования. ГОСТ Р ИСО 9004-2001. Системы менеджмента качества. Рекомендации по улучшению деятельности.

ГОСТ Р ИСО 19011-2003. Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента.

ГОСТ Р ИСО/МЭК ТО 12182-2002. Информационная технология. Классификация программных средств.

ГОСТ Р ИСО/МЭК 12207-99. Информационная технология. Процессы жизненного цикла программных средств.

ГОСТ Р ИСО/МЭК ТО 15271-2002. Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств).

ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом.

ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств.

ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению.

ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование.

ГОСТ Р ИСО/МЭК ТО 9294-93. Информационная технология. Руководство по управлению документированием программного обеспечения.

ГОСТ Р ИСО/МЭК 15910-2002. Информационная технология. Процесс создания документации пользователя программного средства.

ГОСТ Р ИСО 9127-94. Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.

ГОСТ Р ИСО/МЭК 14764-2002. Информационная технология. Сопровождение программных средств.

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51583-2014 Защита информации. Порядок создания

автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения

ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. Общие требования.

ГОСТ Р 51904-2002. Программное обеспечение встроенных систем. Общие требования к разработке и документированию.

ГОСТ 28195-89. Оценка качества программных средств. Общие положения.

ГОСТ 28806-90. Качество программных средств. Термины и определения.

ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

ГОСТ 34.602-2020. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

ГОСТ Р 59792-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем.

ГОСТ Р 59793–2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»

ГОСТ 34.201-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

ГОСТ 7.32-2017. Система стандартов по информации, библиографическому и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.

ГОСТ Р 2.105-2019 Единая система конструкторской документации. Общие требования к текстовым документам

ГОСТ 2.316-2008 ЕСКД. Правила нанесения надписей, технических требований и таблиц на графических документах. Общие положения

ГОСТ Р 1.5-2012 Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения.

ГОСТ Р 7.0.97-2016 Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов

ГОСТ Р 7.0.100-2018 Система стандартов по информации, библиотечному

и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления

ГОСТ 8.417-2002 Государственная система обеспечения единства измерений. Единицы величин.

ГОСТ Р 15.011-2022 Система разработки и постановки продукции на производство. Патентные исследования. Содержание и порядок проведения

ГОСТ 34.602-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 19.101–77 Единая система программной документации. Виды программ и программных документов

ГОСТ 19.102-77. Единая система программной документации. Стадии разработки

ГОСТ 19.105-78. Единая система программной документации. Общие требования к программным документам

ГОСТ 19.201-78. Единая система программной документации. Техническое задание. Требования к содержанию и оформлению

ГОСТ 19.301-79. Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению

ГОСТ 19.601-78. Единая система программной документации. Общие правила дублирования, учета и хранения и внесения изменений

ГОСТ Р 59853-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 15971-90. Системы обработки информации. Термины и определения

ПРИЛОЖЕНИЕ 6
(справочное)
ЗАКРЕПЛЕНИЕ ВАРИАНТОВ ИНДИВИДУАЛЬНЫХ ЗАДАНИЙ НА КУРСОВОЙ ПРОЕКТ

№ п.п.	Номер варианта индивидуального задания	Фамилия и инициалы исполнителя	Тема курсового проекта	Фамилия и инициалы руководителя
1	2	3	4	5
1.	141212 АА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации муниципального подчинения на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу голосовых сообщений.	К.Н. Цебренко
2.	342121 ОА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу голосовых сообщений.	К.Н. Цебренко
3.	241113 ЗА		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей	К.Н. Цебренко
4.	241222 БА		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей и поддерживающей передачу видеоизображений.	К.Н. Цебренко

5.	341213 ВБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.	К.Н. Цебренко
6.	151212 ГА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, поддерживающей передачу голосовых сообщений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования	К.Н. Цебренко
7.	351112 ЖВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края, поддерживающей передачу голосовых сообщений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования	К.Н. Цебренко
8.	251213 ДА		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района с сервисом электронной почты на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования	К.Н. Цебренко
9.	351212 ЕБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, поддерживающей передачу видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования	К.Н. Цебренко
10.	321112 ЖВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края, поддерживающей передачу голосовых сообщений, на базе локальной вычислительной сети	К.Н. Цебренко

11.	131113 ЗА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ	К.Н. Цебренко
12.	231121 ИБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с сервисом электронной посты на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ	К.Н. Цебренко
13.	331121 КВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края с использованием механизмов операционных систем на базе распределенной вычислительной сети, состоящей из отдельных ПЭВМ	К.Н. Цебренко
14.	141211 ЛА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей, поддерживающей передачу видеоизображений и голосовых сообщений.	К.Н. Цебренко
15.	242111 МБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с использованием механизмов операционных систем на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.	К.Н. Цебренко
16.	242121 НВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с сервисом электронной посты на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.	К.Н. Цебренко

17.	342121 ОА		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края с ограничением пользователей в допуске к различным разделам информационной базы для распределенной вычислительной сети, состоящей из локальных вычислительных сетей.	К.Н. Цебренко
18.	152121 ПБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации, с сервисом передачи видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования	К.Н. Цебренко
19.	252121 РВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с ограничением пользователей в допуске к различным разделам информационной базы для комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования	К.Н. Цебренко
20.	322121 СА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с использованием механизмов операционных систем на базе локальной вычислительной сети	К.Н. Цебренко
21.	142213 ТБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации с применением программно-аппаратных средств защиты от несанкционированного доступа на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей.	К.Н. Цебренко

22.	242213 ГВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из локальных вычислительных сетей, где ЭВМ системы расположены в нескольких контролируемых зонах.	К.Н. Цебренко
23.	121121 АБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации муниципального подчинения	К.Н. Цебренко
24.	232212 БА		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации района	К.Н. Цебренко
25.	342123 ВВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы учреждения администрации края	К.Н. Цебренко
26.	152212 ДА		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе комплекса локальных вычислительных сетей вычислительной сети, соединенных каналами общего пользования	К.Н. Цебренко
27.	221121 ЕВ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе локальной вычислительной сети	К.Н. Цебренко
28.	332213 ЖБ		Разработка эскизного проекта системы защиты автоматизированной информационной системы организации на базе распределенной вычислительной сети, состоящей из отдельных ЭВМ	К.Н. Цебренко

ПРИЛОЖЕНИЕ 7
(справочное)

Примеры библиографических описаний документов

Статья в периодических изданиях и сборниках статей:

1 Гуреев В.Н., Мазов Н.А. Использование библиометрии для оценки значимости журналов в научных библиотеках (обзор)//Научно-техническая информация. Сер. 1. - 2015. - N 2. - С. 8 - 19.

2 Колкова Н.И., Скипор И.Л. Терминосистема предметной области "электронные информационные ресурсы": взгляд с позиций теории и практики//Научн. и техн. б-ки. - 2016. - N 7. - С. 24 - 41.

Книги, монографии:

1 Земсков А.И., Шрайберг Я.Л. Электронные библиотеки: учебник для вузов. - М: Либерея, 2003. - 351 с.

2 Костюк К.Н. Книга в новой медицинской среде. - М.: Директ-Медиа, 2015. - 430 с.

Тезисы докладов, материалы конференций:

1 Леготин Е.Ю. Организация метаданных в хранилище данных//Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов/отв. за вып. С.Д. Ваулин; Юж.-Урал. гос. ун-т. Т. 2. - Челябинск: Издательский центр ЮУрГУ, 2011. - С. 128 - 132.

2 Антопольский А.Б. Система метаданных в электронных библиотеках//Библиотеки и ассоциации в меняющемся мире: Новые технологии и новые формы сотрудничества: Тр. 8-й Междунар. конф. "Крым-2001"/г. Судак, (июнь 2001 г.). - Т. 1. - М., 2001, - С. 287 - 298.

3 Парфенова С.Л., Гришакина Е.Г., Золотарев Д.В. 4-я Международная научно-практическая конференция "Научное издание международного уровня - 2015: современные тенденции в мировой практике редактирования, издания и оценки научных публикаций"//Наука. Инновации. Образование. - 2015. - N 17. - С. 241 - 252.

Патентная документация согласно стандарту ВОИС:

1 BY (код страны) 18875 (N патентного документа) C1 (код вида документа), 2010 (дата публикации).

Электронные ресурсы:

1 Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. - 2006. - URL: http://bookhamber.ru/stat_2006.htm (дата обращения 12.03.2009).

2 Прогноз научно-технологического развития Российской Федерации на период до 2030 года. - URL: http://government.ru/media/files/41d4b737638891da2184/pdf (дата обращения 15.11.2016).

3 Web of Science. - URL: http://apps.webofknowledge.com/(дата обращения 15.11.2016).

Нормативные документы:

1. ГОСТ 7.0.96-2016 Система стандартов по информации, библиотечному и издательскому делу. Электронные библиотеки. Основные виды. Структура. Технология формирования. - М.: Стандартинформ, 2016. - 16 с.

2 Приказ Минобразования РФ от 19 декабря 2013 г. N 1367 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры". - URL: http://www. consultant.ru/document/cons_doc_LAW_159671/(дата обращения: 04.08.2016).

3 ISO 25964-1:2011. Information and documentation - Thesauri and interoperability with other vocabularies - Part 1: Thesauri for information retrieval. - URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber53657 (дата обращения: 20.10.2016).

ПРИЛОЖЕНИЕ 8
(обязательное)
Пример оформления реферата

РЕФЕРАТ

Курсовой проект 44 с., 15 рис., 1 табл., 20 источн., 1 прил.

АВТОМАТИЗИРОВАННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, СРЕДСВА ЗАЩИТЫ, РИСКИ, ТЕХНИЧЕСКОЕ ЗАДАНИЕ, УГРОЗЫ, ВЫБОР СРЕДСТВ ЗАЩИТЫ, МОДЕЛЬ УГРОЗ, ПРОЕКТИРОВАНИЕ

Объектом исследования является системы защиты автоматизированной информационной системы организации.

Цель работы: разработка эскизного проекта системы защиты автоматизированной информационной системы организации, с сервисом передачи видеоизображений, на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования.

Методы исследования: экспериментальный, методы системного анализа, методы аналогий и сравнений.

Основные результаты: разработан эскизный проект системы защиты автоматизированной информационной системы организации на базе комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования.

Область применения системы – организации с ограничением пользователей в допуске к различным разделам информационной базы для комплекса локальных сетей, соединенных каналами передачи данных коллективного пользования.

Разработанный проект готов для внедрения при разработке системы защиты автоматизированной информационной системы организации.

Эффективность разработки заключается в разработке оригинальной архитектуре системы защиты автоматизированной информационной системы организации.

Предметом дальнейших исследования является разработка системы защиты автоматизированной информационной системы организации.

ПРИЛОЖЕНИЕ 9
(обязательное)
Образец отзыва руководителя на курсовой проект

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования "Академия маркетинга и социально-информационных технологий - ИМСИТ" (г. Краснодар)
Кафедра Математики и вычислительной техники

РЕЦЕНЗИЯ РУКОВОДИТЕЛЯ
на курсовой проект обучающегося
по дисциплине Проектирование защищенных автоматизированных систем

_____

Фамилия, имя, отчество обучающегося

Тема курсового проекта:_____
_____
Регистрационный номер_____ Курс_____ Группа_____
Направление подготовки: _____

код, направление

Сформированность компетенций у обучающегося по итогам выполнения заданий на курсовой проект

Задания*	Уровень сформированности компетенций
1) разработка модели угроз;	
2) выбор средств защиты;	
3)	

*Сформулировать задания в соответствии с содержанием курсового проекта

Соответствие курсового проекта требованиям

Наименование требования	Заключение о соответствии требованиям (отметить «соответствует», «соответствует не в полной мере», или «не соответствует»)
1. Актуальность темы	
2.Соответствие содержания теме	
3. Полнота, глубина и обоснованность решения поставленных задач	
4. Корректность проектных решений	
5. Практическая значимость	
6. Оценка личного вклада автора	
7. Наглядность (информативность) представления	

результатов исследования	

Достоинства содержательной части курсового проекта:

_____

_____

_____

Ошибки и недостатки содержательной части курсового проекта:

_____

_____

_____

Общее заключение научного руководителя о соответствии курсового проекта требованиям, установленным федеральным государственным образовательным стандартом и основной профессиональной образовательной программой по направлению подготовки 10.03.01 Информационная безопасность

Курсовой проект соответствует требованиям ФГОС и ОПОП по направлению

Обобщенная оценка содержательной части
курсового проекта* Соответствует

*соответствует / частично соответствует / не соответствует

_____

_____

Руководитель:

Полное наименование должности и основного
места работы, ученая степень, ученое звание _____

Подпись расшифровка подписи

«_____»_____20___г.

ПРИЛОЖЕНИЕ 10
(обязательное)
Образец заключения

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования "Академия маркетинга и социально-информационных технологий - ИМСИТ" (г. Краснодар)

Кафедра Математики и вычислительной техники

ЗАКЛЮЧЕНИЕ

ФАМИЛИЯ ИМЯ ОТЧЕСТВО ОБУЧАЮЩЕГОСЯ ……
…….
Форма обучения _____ Курс _____ Группа _____
НАПРАВЛЕНИЕ/СПЕЦИАЛЬНОСТЬ _____

Курсовой проект по дисциплине _____, выполненная на тему:
_____
_____
_____
в соответствии с «Положением о порядке размещения в ЭБС и автоматизированной (компьютерной) проверке на объем и характер заимствования курсовых и выпускных квалификационных работ по направлениям подготовки/специальностям высшего образования» курсовой проект по дисциплине _____ **прошла** автоматизированный анализ в Программной системе для обнаружения заимствований в учебных и научных работах.

Доля авторского текста (оригинальности) в результате автоматизированной проверки составила _____%.

Зав. кафедрой
математики и вычислительной
техники, доцент Н.П. Исикова

« _____» _____