Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

В. В. Подтопельный

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебно-методическое пособие по выполнению курсовых проектов
для студентов специальности 10.05.03 «Информационная безопасность
автоматизированных систем»
специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2026

УДК 004.056.5(075)

Рецензент

кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности института информационных технологий ФГБОУ ВО «Калининградский государственный технический университет» Н. Я. Великите

Подтопельный, В. В.
Программно-аппаратные средства защиты информации: учебно-методическое пособие по выполнению курсовых проектов для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2026. – 75 с.

Учебно-методическое пособие включают в себя комплекс вопросов, связанных с подготовкой, написанием и оформлением курсовых проектов по дисциплине «Программно-аппаратные средства защиты информации».

Учебно-методическое пособие предназначено для студентов 4–5-х курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей.

Табл. 16, список лит. – 14 наименований

Учебно-методическое пособие рекомендовано в качестве локального электронного методического материала для использования в учебном процессе методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 29 сентября 2026 г., протокол № 7

УДК 004.056.5(075)

© Федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет», 2026 г.
© Подтопельный В. В., 2026 г.

ОГЛАВЛЕНИЕ

Введение…….…….…4
1 Условия выбора темы и порядок разработки ……7
1.1 Выбор и утверждение темы курсового проекта ……..…....7
1.2 Порядок выполнения курсовых проектов…….....8
2 Требования к структуре, объему, содержанию и оформлению курсового проекта……..…..12
2.1 Требование к содержанию курсового проекта…….…...12
2.2 Состав и объём структурных элементов курсового проекта ..…….....13
2.3 Требования к оформлению курсового проекта.……..……....28
3 Организация выполнения курсового проекта ……..41
4 Критерии и нормы оценки курсового проекта ……....44
5 Список рекомендованных источников …….……...47
Заключение…….…….54
Список использованных источников……....55
Приложения…….57
Приложение А. Примерные темы курсового проекта ……...56
Приложение Б. Краткие правила форматирования…….…60
Приложение В. Пример титульного листа……63
Приложение Г. Пример оформления структурного элемента курсового проекта «Содержание»……..…….....65
Приложение Д. Пример оформления структурного элемента «Введение» курсового проекта на тему «Разработка ПО по идентификации USB носителя при мгновенном разъединении с компьютерной системой» ……66
Приложение Е. Пример оформления структурного элемента «Список использованных источников» ……..……..……..68
Приложение Ж. Примеры оформления иллюстраций ……...69
Приложение З. Пример оформления таблиц и формул… ……71
Приложение И. Примеры оформления библиографических описаний различных источников……...73

ВВЕДЕНИЕ

Дисциплина «Программно-аппаратные средства защиты информации» читается студентам специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем» на 4, 5-м (8 и 9-й семестры) курсах, курсовой проект выполняется в 9-м семестре.

Цели каждого отдельного курсового проекта должны раскрывать выбранную студентом тему. Курсовой проект предназначен для углубления студентами теоретических и практических навыков в области обеспечения информационной безопасности информационных систем.

Современные квалификационные требования, предъявляемые к выпускникам направлений подготовки в области информационной безопасности, предполагают не только фундаментальное освоение теоретических основ и принципов функционирования информационных технологий, но и формирование устойчивых профессиональных компетенций на всех этапах жизненного цикла информационных систем – от проектирования и разработки до эксплуатации и сопровождения.

В соответствии с этим будущие специалисты должны обладать целостным представлением обо всех этапах создания и эксплуатации информационных технологий, владеть методологией обоснованного выбора из широкого арсенала современных средств и методов защиты информации, а также уметь применять наиболее адекватные из них для решения конкретных профессиональных задач.

Курсовой проект представляет собой одну из форм учебной (творческой и научно-исследовательской) работы, выполнение которой является обязательным элементом образовательной программы для студентов очной формы обучения.

Принципиальное различие между курсовой работой и курсовым проектом состоит в следующем: курсовой проект в обязательной практической части предполагает решение сложной расчётной и (или) проектной задачи, содержит описание хода решения задач и отчётные данные. Как правило, курсовой проект характерен для информационных или инженерных направлений и специальностей.

Выполнение курсового проекта представляет собой самостоятельное решение студентом под руководством преподавателя частной задачи или проведение исследования по одному из вопросов, изучаемых в цикле специальных дисциплин (по ГОС ВО) либо в дисциплинах профессионального цикла (по ФГОС ВО).

Основной целью выполнения курсовых проектов является закрепление, углубление и обобщение знаний, полученных студентом за время теоретического и практического обучения, а также расширение объёма профессионально значимых умений и навыков. Содержание курсовых проектов должно отвечать учебным задачам дисциплины и увязываться с последующей проектной деятельностью выпускников по специальности или направлению подготовки.

В соответствии с поставленной целью в задачи курсового проекта входят:

1. Закрепление практических навыков настройки политик безопасности информационных систем, полученных на лабораторных занятиях по дисциплине «Программно-аппаратные средства защиты информации».
2. Углубление теоретических и практических знаний в области методологии отладки функций безопасности информационных систем.
3. Развитие навыков самостоятельного планирования задач защиты операций и ключевой информации информационных систем.
4. Получение опыта сбора и анализа регистрируемых событий безопасности.
5. Приобретение навыков создания резервных копий данных информационных систем и обеспечения их восстановления.

При выполнении курсового проекта обучающимся рекомендуется использование элементов дистанционных образовательных технологий с применением информационных и учебно-методических ресурсов. При этом график курсового проектирования должен определять количество часов, указанных в учебном плане.

Важнейшими требованиями при выполнении курсового проекта для студента являются:

– самостоятельность работы – студент несёт персональную ответственность за содержание, достоверность и обоснованность представленных материалов;

– актуальность тематики – тема курсового проекта должна быть связана с решением вопросов проектирования систем защиты информации промышленных, исследовательских организаций и коммерческих структур;

– использование современной программной и аппаратной базы – работа должна выполняться с применением актуальных технологий и инструментальных средств;

– опора на справочные материалы и нормативные документы – при проектировании необходимо руководствоваться действующими стандартами и рекомендациями;

– применение новейших методов организации расчётов, проектирования и исследований – работа должна демонстрировать владение современной методологией научно-исследовательской и проектной деятельности.

В результате выполнения курсового проекта обучающийся должен:

знать:

- основные средства и способы обеспечения безопасности информации, а также принципы построения систем защиты информации;
- программно-аппаратные средства обеспечения защиты информации автоматизированных систем;
- способы реализации угроз безопасности в автоматизированных системах;

уметь:

- проводить выбор и настройку программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности;

владеть:

- навыками обоснования и внедрения перечня сертифицированных и несертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы.

Таким образом, курсовой проект является неотъемлемой составляющей профессиональной подготовки специалистов в области информационной безопасности. Он обеспечивает интеграцию теоретических знаний и практических навыков, формирует компетенции, необходимые для самостоятельной проектной и исследовательской деятельности, и служит связующим звеном между учебным процессом и будущей профессиональной деятельностью выпускника.

1 УСЛОВИЯ ВЫБОРА ТЕМЫ И ПОРЯДОК РАЗРАБОТКИ КУРСОВОГО ПРОЕКТА

1.1 Выбор и утверждение темы курсового проекта

Выбор темы курсового проекта является начальным и одновременно одним из наиболее ответственных этапов курсового проектирования. От правильности и обоснованности выбора темы во многом зависят успешность выполнения проекта, глубина проработки материала и практическая значимость полученных результатов.

Обучающийся выбирает тему из числа предложенных кафедрой или предлагает собственную тему проекта с последующим утверждением таковой ведущим преподавателем, руководствуясь собственными научными интересами, уровнем подготовки, а также наличием доступа к необходимым информационным и материально-техническим ресурсам. Перечень примерных тем курсовых проектов приводится в приложении А к настоящему пособию. Студент вправе предложить собственную тему с обоснованием целесообразности её разработки, однако такое предложение подлежит обязательному согласованию с заведующим кафедрой и научным руководителем.

Выбранная тема должна быть утверждена ведущим дисциплину преподавателем. Внесение изменений в тему после её утверждения допускается только при наличии веских оснований и с письменного согласия руководителя.

Список типовых тем приведен **в приложении А.**

При выборе темы курсового проекта рекомендуется учитывать следующие обстоятельства:

– соответствие темы содержанию дисциплины, по которой выполняется проект, и учебным задачам курса;

– актуальность рассматриваемой проблемы для современной теории и практики обеспечения информационной безопасности;

– наличие достаточного объёма специальной литературы, нормативно-правовых документов и возможности получения фактических данных, необходимых для анализа и проектирования;

– соответствие темы собственным научным интересам и способностям обучающегося;

– возможность использования материалов, полученных в ходе предыдущих учебных практик и выполнения других курсовых проектов;

– недопустимость дублирования тем курсовых проектов, выполняемых другими студентами в рамках одной учебной группы.

Самостоятельно определяя тему, студент должен реально оценить свой опыт в выбранной сфере, наличие соответствующих знаний и навыков, а также доступность необходимого программного обеспечения и аппаратных средств для практической реализации проекта.

Важную роль в успешном выполнении проекта играет систематическое взаимодействие с ведущим дисциплину преподавателем. Студенту рекомендуется периодически информировать преподавателя о ходе выполнения работы, консультироваться по вопросам, вызывающим затруднения, своевременно сообщать о возможных проблемах, связанных с выполнением проекта или изменением его содержания.

1.2 Порядок выполнения курсовых проектов

Курсовой проект выполняется студентом в период семестра, когда по учебному плану изучается соответствующая дисциплина.

Курсовой проект представляет собой решение практической, научно-исследовательской задачи одной из актуальных проблем в области защиты информационных систем.

Объектами дипломного проекта могут быть методы поиска уязвимостей информационных систем, методы анализа уязвимости информационных, способы повышения защищенности информационных систем, специфика комплектования системного обеспечения в целях повышения информационной безопасности.

При выполнении курсового проекта должно быть предусмотрено:

– обоснование актуальности и важности решаемой задачи обеспечения информационной безопасности выбранного объекта;

– анализ проблемной области защиты информации;

– определение, анализ возможных путей и способов исследования и описание выбранных методов и средств решения поставленных задач;

– формализация задач проектирования;

– методы и проектные решения проблем безопасности информации.

Процесс курсового проектирования представляет собой последовательную реализацию нескольких взаимосвязанных этапов. Курсовой проект предусматривает **следующие обобщённые этапы:**

Первый этап: подготовительный заключается в изучении научной и учебно-методической литературы по выбранной проблеме, сборе и систематизации исходных данных, необходимых для последующего проектирования. На данном этапе студент анализирует цели функционирования объекта проектирования, оценивает текущее состояние его защищённости, выявляет существующие уязвимости и угрозы. Собранные материалы

впоследствии используются при написании введения и теоретической части проекта.

Второй этап: проектный (этап разработки) предполагает непосредственную разработку темы. На основе собранных и обобщённых материалов студент формулирует способы решения поставленных задач, разрабатывает алгоритмы, определяет специфику и последовательность их реализации. На этом этапе создаётся проектный продукт – программный модуль, настроенная система защиты, алгоритм обнаружения угроз или иной практический результат. Разработка сопровождается обоснованием эффективности принятых решений и исследованием их устойчивости к дестабилизирующим факторам.

Третий этап: оформительский включает систематизацию всех материалов курсового проекта, отбор содержания для основной части, составление структуры изложения и подготовку иллюстративного материала. В рамках этого этапа определяются основные направления и содержание предложений, выявляется необходимость дополнительного сбора материалов, формируется черновой вариант пояснительной записки в целом. После сбора дополнительных материалов проводится детальная разработка и обоснование выдвинутых предложений, уточняются аналитическая и исследовательская части проекта, выполняется редактирование и окончательное оформление отобранного материала.

Четвёртый этап: заключительный состоит в предъявлении завершённого курсового проекта научному руководителю. К этому моменту проект должен быть полностью оформлен, подписан студентом и представлен на кафедру в установленный срок.

Подробное рассмотрение этапов проектирования приведено в таблице 1. Целесообразно придерживаться следующего обобщённого плана разработки курсового проекта:

1. Точная формулировка темы, целей и задач проектирования.
2. Изучение специфики проблемной области, анализ существующих решений и оценка их эффективности.
3. Обоснование предлагаемых решений проблем в области защиты информации информационных систем.
4. Практическая реализация предложенных средств и методов защиты, исследование уровня защищённости информационных систем и их компонентов.
5. Проверка и оценка эффективности предложенных мер защиты.

Соблюдение указанной последовательности и своевременное выполнение каждого из этапов является необходимым условием успешного завершения курсового проектирования.

Таблица 1 – Поэтапная процедура проектирования курсового проекта

№ п/п	Наименование этапа	Содержание работ	Ожидаемый результат	Форма отчётности
1	Организационно-подготовительный	Выбор темы из перечня, предложенного кафедрой, либо формулирование собственной темы; согласование темы с научным руководителем; уточнение целей, задач и границ проекта; определение объекта и предмета проектирования	Утверждённая тема курсового проекта; предварительная формулировка цели и задач	Заявление на утверждение темы и или запись в журнале регистрации курсовых проектов
2	Аналитический (предпроектное обследование)	Изучение научной и учебно-методической литературы, нормативных документов, стандартов; анализ предметной области; выявление существующих решений и оценка их эффективности; описание объекта защиты и его уязвимостей	Аналитический обзор; перечень угроз и уязвимостей; обоснование актуальности темы	Черновой вариант раздела 1 пояснительной записки (теоретическая часть); список источников
3	Формулирование требований и разработка технического задания	Определение функциональных, технических и эксплуатационных требований к проектируемому решению; уточнение критериев оценки эффективности; согласование ТЗ с руководителем	Техническое задание на разработку (по шаблону приложения К)	Подписанное руководителем ТЗ
4	Выбор и обоснование проектных решений	Сравнительный анализ возможных методов, средств и подходов; обоснование выбора конкретных программно-аппаратных средств; определение архитектуры решения	Обоснование выбора средств защиты; описание архитектуры проектного решения	Раздел 2 пояснительной записки (проектная часть, теоретическая составляющая)
5	Проектно-конструкторский (разработка)	Разработка алгоритмов и структурных схем; написание программного кода либо настройка средств защиты; конфигурирование компонентов; подготовка исходных данных и рабочей	Работающий прототип (программный модуль, настроенная система, алгоритм);	Демонстрация промежуточного результата руководителю; черновые материалы практической

№ п/п	Наименование этапа	Содержание работ	Ожидаемый результат	Форма отчётности
		среды	исходные тексты программ	части
6	Экспериментально-испытательный (тестирование)	Разработка методики тестирования; проведение испытаний по сценариям; фиксация входных данных, ожидаемых и фактических результатов; анализ расхождений; оценка технической и эксплуатационной эффективности	Протоколы испытаний; таблицы результатов; подтверждение работоспособности решения	Протокол тестирования; раздел практической части с результатами экспериментов
7	Оформительский	Систематизация материалов; окончательное оформление пояснительной записки в соответствии с требованиями раздела 2.3; подготовка иллюстраций, таблиц, формул; оформление списка использованных источников и приложений	Завершённая пояснительная записка с приложениями	Печатный вариант пояснительной записки; электронный файл в формате .docx/.odt
8	Подготовка к защите	Составление текста доклада (5–7 мин); подготовка презентационных материалов по структуре приложения Л; проработка возможных вопросов; проверка комплектности документов	Доклад и презентация; готовность к публичной защите	Текст доклада; презентация; подписанный руководителем отзыв
9	Защита проекта	Публичное представление результатов; ответы на вопросы; обсуждение; выставление оценки	Оценка по четырёх-балльной шкале (при рейтинговой системе – по 100-балльной шкале)	Ведомость; зачётная книжка; размещение электронной версии в ЭИОС

Контрольные точки, в которых студент обязан представить промежуточные результаты руководителю, соответствуют завершению этапов

3, 5 и 7. Непредставление промежуточных результатов в установленные сроки рассматривается как нарушение графика курсового проектирования и учитывается при итоговой оценке.

2 ТРЕБОВАНИЯ К СТРУКТУРЕ, ОБЪЁМУ, СОДЕРЖАНИЮ И ОФОРМЛЕНИЮ КУРСОВОГО ПРОЕКТА

2.1 Требования к содержанию курсового проекта

Решение поставленных задач курсового проекта по дисциплине «Программно-аппаратные средства защиты информации» должно реализовать обеспечение информационной защиты операционной системы в следующих направлениях.

В рамках проекта по специальности, связанной с информационной безопасностью, студент может провести комплексное исследование и разработку, охватывающее следующие ключевые аспекты:

1. Анализ и оптимизация механизмов распределения прав доступа в информационных системах, включая оценку их алгоритмической стойкости и разработку стратегий защиты от потенциальных угроз.
2. Проведение аудита событий безопасности, направленных на выявление и предотвращение инцидентов, связанных с нарушением целостности, доступности и конфиденциальности данных.
3. Разработка и внедрение систем контроля целостности компонентов информационных систем, обеспечивающих непрерывную проверку и верификацию ключевых элементов.
4. Комплектование компонентного состава информационных систем с акцентом на интеграцию элементов защиты, включая сборку и настройку ядра операционной системы с учетом требований безопасности.
5. Обеспечение криптографической защиты информационных систем, включая анализ особенностей функционирования криптографических алгоритмов и методов их применения.
6. Реализация функций идентификации и аутентификации пользователей, направленных на обеспечение аутентификации субъектов доступа и предотвращение несанкционированного доступа.
7. Защита от обратного проектирования программных систем, включая разработку стратегий и методов, затрудняющих анализ и модификацию исходного кода.
8. Использование встроенных антивирусных средств операционной системы, функционирующих как надстраиваемые подсистемы, обеспечивающие защиту от вредоносного программного обеспечения.

9. Контроль и мониторинг процессов информационных систем, включая разработку систем мониторинга и анализа, направленных на своевременное выявление и реагирование на инциденты безопасности.

Курсовой проект может также включать следующие направления исследований и разработок:

1. Разработка специализированных программных защитных средств, включая создание новых алгоритмов и методов защиты информации.
2. Внедрение, настройка и проверка систем распределения прав доступа с акцентом на оценку их алгоритмической стойкости и адаптацию к изменяющимся условиям.
3. Комплектование компонентного состава информационных систем в защищенном исполнении, включая разработку и интеграцию элементов защиты на всех уровнях системы.
4. Сборка и проверка ядра операционной системы с элементами защиты, включая анализ и оптимизацию процессов сборки и настройки.
5. Разработка требований, нормативно-правовой базы и процедур по обеспечению безопасности информационных систем, включая создание стандартов и регламентов.
6. Исследование и анализ методов обеспечения средств защиты информации, включая сравнительный анализ существующих подходов и разработку новых методик.

Таким образом, курсовой проект предоставляет студенту возможность продемонстрировать глубокие знания и компетенции в области информационной безопасности, а также развить навыки практического применения теоретических знаний в реальных условиях.

2.2 Состав и объём структурных элементов дипломного проекта

Курсовой проект должен отражать высокий уровень теоретической подготовки студента и его глубокие знания по выбранной теме. Работа должна иметь грамотно составленную библиографию, логичную структуру, позволяющую полно раскрыть тему. Текст должен быть написан литературным и профессиональным языком, с правильным оформлением научного аппарата. Краткое информация об особенностях форматирования изложена **в приложении Б**.

Минимальный объем курсового проекта 20 печатных тысяч знаков, 25 страниц (шрифт 14 пт., полуторный интервал, отступ 1,27).

Курсовой проект содержит следующие структурные элементы:

– титульный лист;

– содержание (оглавление);

– введение;

– основную часть (состоит из минимально из двух глав);

– заключение;

– список использованных источников;

– приложения.

Титульный лист курсового проекта содержит следующие элементы (бланк оформления титульного листа курсового проекта приведён **в приложении В.**):

– полное наименование вышестоящего органа (Министерство науки и высшего образования Российской Федерации), университета института и кафедры (кафедр), название дисциплины (модуля); название темы курсового проекта;

– сведения об исполнителе (Ф.И.О. обучающегося, группа, подпись); сведения о научном руководителе (Ф.И.О., ученая степень, ученое звание);

– наименование места и год выполнения.

Содержание (Оглавление) включает порядковые номера и наименование структурных элементов курсового проекта с указанием номера страницы, на которой они помещены. Введение и список использованных источников не нумеруются, (см. **Приложение Г**).

Структура проекта – краткое содержание глав и параграфов основной части проекта. Последовательность рубрик должна соответствовать приведенному перечню, наименование каждой рубрики выделяется в тексте жирным шрифтом.

Содержание размещается на отдельной странице.

Содержание курсового проекта включает:

– введение;

– наименования всех глав (разделов), параграфов (подразделов) и пунктов (если последние имеют наименования), заключение;

– список использованных источников и наименование приложений с указанием номеров страниц.

Оформление содержания. Слово «СОДЕРЖАНИЕ» пишут заглавными буквами и выравнивают по центру. Каждый пункт содержания оформляют как отдельный абзац, выровненный по ширине.

Номера страниц указывают по правому краю поля. Они должны быть связаны с названием раздела или подраздела с помощью точек.

Подразделы и пункты обозначают с отступом в два и четыре знака соответственно. Если заголовок раздела, подраздела или пункта не помещается на одной строке, его продолжают с того же уровня, на котором он начался.

Условные обозначения и сокращения. Малопонятные термины, сокращения и символы, которые встречаются в проекте реже трёх раз, следует вынести в отдельный список. Если же они повторяются чаще, расшифровку дают при первом упоминании в тексте.

Введение характеризует актуальность темы проекта – обоснование теоретической и практической важности выбранной для проектирования проблемы. Во введении излагаются общие сведения по тематике разработки или исследования, определяется актуальность выбранного направления, кратко отмечаются проблемные вопросы, степень их решения в конкретной предметной области. Введение завершается четкой формулировкой цели выполняемой проекта и перечислением основных решаемых задач. Цель и задачи курсового проекта – краткая и четкая формулировка цели проведения исследования и нескольких задач, решение которых необходимо для достижения поставленной цели.

Объем введения, как элемента курсового проекта должен составлять около 1,5 страниц. Образец оформления введения в части изложения, касающейся актуальности темы исследования, предмета и объекта исследования, а также постановки целей и задач, приведён **в приложении Д**.

Особенности оформления. Введение не нумеруется. Слово «ВВЕДЕНИЕ» пишется прописными буквами без точки в конце и центрируется.

Основная часть курсового проекта может содержать следующие части:

– главы;

– разделы (параграфы);

– пункты;

– подпункты.

Основная часть курсового проекта

Основная часть курсового проекта подчинена логике проектирования, а не логике исследования. Это означает, что каждый её элемент должен отвечать на вопрос «что и как сделано для получения проектного результата», а не «что и почему устроено в изучаемой области». Материал основной части выстраивается как последовательность проектных решений: от постановки проектной задачи через выбор способа её решения к реализации и подтверждению работоспособности полученного результата.

Каждый элемент основной части должен представлять собой законченный в смысловом отношении фрагмент проекта, обладающий самостоятельной ценностью и одновременно встроенный в общую проектную логику. Разделы (параграфы) внутри главы взаимосвязаны: результат предыдущего раздела выступает исходным материалом для последующего.

Главу рекомендуется завершать краткими выводами, в которых фиксируется, какое проектное решение принято и почему оно обеспечивает продвижение к цели проекта.

Глава 1. Проектно-аналитическая часть

Первая глава курсового проекта не является теоретическим обзором в привычном смысле. Её назначение – подготовить обоснование проектных решений. Поэтому материал в ней отбирается не по критерию «полнота освещения темы», а по критерию «необходимость для принятия проектных решений». Всё, что не влияет на выбор способа решения проектной задачи, в первую главу не включается.

В первой главе последовательно раскрываются:

– характеристика объекта проектирования: что представляет собой защищаемая информационная система, какие компоненты в неё входят, какие информационные процессы в ней протекают;

– перечень актуальных угроз и уязвимостей применительно к данному объекту, а не угроз «вообще»;

– анализ существующих проектных решений и средств защиты, пригодных для применения на данном объекте, с оценкой их применимости, ограничений и условий использования;

– формулировка проектной задачи: что именно требуется спроектировать, разработать или настроить, какие требования предъявляются к результату, какими критериями будет оцениваться его работоспособность.

Обзор литературы и нормативных документов в первой главе подчинён проектной задаче. Он не должен превращаться в самостоятельный реферативный раздел. Ссылки на источники приводятся там, где они обосновывают конкретное проектное решение, а не там, где требуется продемонстрировать начитанность.

Первая глава завершается выводами, в которых фиксируются: характеристика объекта проектирования, выявленные угрозы, обоснованный выбор направления проектирования и сформулированная проектная задача. Эти выводы являются исходным пунктом для второй главы.

Глава 2. Проектно-технологическая часть

Вторая глава представляет собой ядро курсового проекта. В ней описывается процесс создания проектного результата: от выбора средств и методов до подтверждения работоспособности разработанного решения. Содержание этой главы должно быть таково, чтобы можно было воспроизвести выполненную работу и получить аналогичный результат.

Во второй главе последовательно излагаются:

– обоснование выбора программных и аппаратных средств, применяемых для решения проектной задачи, с указанием их версий, конфигураций и условий применения;

– описание архитектуры проектного решения: состав компонентов, их взаимосвязи, принципы взаимодействия, распределение функций между компонентами;

– описание алгоритмов и логики работы разработанного решения, при необходимости – с блок-схемами, диаграммами, схемами взаимодействия;

– пошаговое описание процесса реализации: какие действия выполнялись, в какой последовательности, с какими параметрами, какие промежуточные результаты были получены;

– описание процесса тестирования: какие сценарии проверялись, какие данные подавались на вход, какие результаты ожидались и какие были получены фактически, как интерпретируются расхождения;

– оценка эффективности полученного проектного решения по заранее определённым критериям: обеспечивает ли оно защиту от заявленных угроз, каковы его эксплуатационные характеристики, каковы ограничения и условия применимости.

Экспериментальная проверка является обязательным элементом второй главы. Она не сводится к демонстрации скриншотов работающей программы или настроенной системы. Эксперимент должен быть спланирован, его условия – описаны, результаты – зафиксированы и проанализированы. Если по результатам тестирования выявлены недостатки, в тексте отражается, каким образом они устранялись или почему признаны несущественными в рамках поставленной задачи.

Если в ходе проектирования решалась задача совершенствования существующей системы защиты, во второй главе приводится описание исходной конфигурации, обоснование необходимости доработки, описание внесённых изменений и результаты проверки того, что достигнутый уровень защищённости соответствует предъявленным требованиям.

Вторая глава завершается выводами, в которых фиксируется: что разработано, подтверждена ли работоспособность, какие характеристики получены, какие ограничения выявлены, какие направления развития проектного решения представляются перспективными.

Учитывая содержание таблицы 1, следует обратить внимание и разобрать основные этапы формирования проекта, результаты которых фиксируются в тексте курсового проекта.

1. Пояснение к этапу 3. Формулирование требований и разработка технического задания

Этот этап является переходным от аналитической работы к собственно проектированию. На предыдущем этапе студент изучил объект, выявил угрозы и проанализировал существующие решения. Теперь эти результаты должны быть преобразованы в формализованный документ, который зафиксирует, **что именно** предстоит спроектировать, **какими свойствами** должен обладать проектный результат и **по каким критериям** он будет оцениваться.

Техническое задание (ТЗ) выполняет в курсовом проекте двойную функцию. Во-первых, это рабочий документ, который дисциплинирует проектирование: он не позволяет студенту «расплыться» по теме и отклониться от поставленной задачи. Во-вторых, это отчётный документ, который предъявляется руководителю и впоследствии включается в приложение к пояснительной записке. Наличие подписанного ТЗ свидетельствует о том, что студент и руководитель согласовали границы проекта до начала разработки, а не после её завершения.

Работа над ТЗ включает три последовательные операции. Первая – определение функциональных требований: что проектируемое решение должно **делать**. Например, если разрабатывается средство обнаружения вредоносных объектов в документах, функциональные требования описывают, какие типы документов оно должно обрабатывать, какие виды вредоносных объектов выявлять, какие действия предпринимать при обнаружении.

Вторая операция – определение технических требований: **как** решение должно быть реализовано и **какими характеристиками** обладать. Сюда относятся требования к программной среде, к составу компонентов, к производительности, к совместимости с существующей инфраструктурой, к надёжности.

Третья операция – определение эксплуатационных требований: **как** решение будет использоваться. Это требования к удобству работы пользователя, к документированности, к возможности настройки и сопровождения, к разграничению прав доступа к самому средству защиты.

Отдельно формулируются критерии оценки эффективности. Они должны быть такими, чтобы по завершении проекта можно было однозначно ответить на вопрос: достигнут ли запланированный результат. Например: «средство должно обнаруживать не менее 90 % тестовых образцов», «время сканирования документа объёмом 10 МБ не должно превышать 5 секунд», «ложные срабатывания не должны превышать 5 %».

Завершается этап согласованием ТЗ с руководителем. Это неформальность: руководитель проверяет, соответствует ли заявленный объём

работ возможностям студента и срокам курсового проектирования, достаточно ли обоснованы требования, реалистичны ли критерии.

Результатом является подписанный руководителем документ – техническое задание на разработку. Шаблон ТЗ приведён в приложении К к пособию. ТЗ может быть оформлено как отдельный документ, а может быть включено в состав пояснительной записки в качестве приложения.

ТЗ опирается на результаты аналитического этапа (этап 2): перечень угроз, характеристику объекта, анализ существующих решений. Без этого анализа требования будут произвольными. В свою очередь, ТЗ определяет содержание всех последующих этапов: выбор проектных решений (этап 4) осуществляется в рамках требований ТЗ, разработка (этап 5) ведётся по ТЗ, тестирование (этап 6) проверяет соответствие результата требованиям ТЗ.

Внесение в текст курсового проекта

В пояснительной записке ТЗ не дублируется полностью в основном тексте. Однако его содержание отражается в двух местах. Во-первых, во введении формулируются цель и задачи проекта — они должны соответствовать ТЗ. Во-вторых, в первой главе (проектно-аналитической части) приводится обоснование требований: почему выдвинуты именно такие функциональные, технические и эксплуатационные требования. Само ТЗ помещается в приложение, а в тексте делается ссылка на него.

2. Пояснение к этапу 4. Выбор и обоснование проектных решений

На этом этапе студент отвечает на вопрос: **каким способом** будет решена проектная задача. Существует, как правило, несколько путей достижения одной и той же цели. Задача студента – не просто выбрать один из них, но и обосновать выбор, то есть показать, почему выбранное решение предпочтительнее альтернативных применительно к данному объекту проектирования и данным требованиям.

Этот этап является ключевым с точки зрения оценки качества проекта. Именно здесь проявляется способность студента к инженерному мышлению: умение сопоставлять варианты, учитывать ограничения, прогнозировать последствия выбора.

Работа на этом этапе включает сравнительный анализ возможных методов, средств и подходов. Сравнение ведётся по критериям, которые должны быть явно сформулированы. Для средств защиты информации типичными критериями сравнения являются: уровень обеспечиваемой защищённости, сложность внедрения, стоимость, совместимость с существующей инфраструктурой, требования к квалификации персонала, ресурсоёмкость, наличие документации и поддержки.

Результатом сравнения является обоснование выбора конкретных программно-аппаратных средств. Обоснование должно быть аргументированным, а не декларативным. Формулировки типа «выбрано средство X, потому что оно хорошее» недопустимы. Корректная формулировка: «выбрано средство X, поскольку оно обеспечивает требуемый уровень защиты при меньших затратах на внедрение по сравнению со средством Y, а также совместимо с используемой операционной системой».

Завершается этап определением архитектуры проектного решения. Архитектура описывает состав компонентов, их взаимосвязи, распределение функций, принципы взаимодействия. Архитектурное описание может быть представлено в виде схемы или диаграммы с пояснениями.

Результатом являются два взаимосвязанных материала: обоснование выбора средств защиты и описание архитектуры проектного решения. Эти материалы имеют не только проектный, но и методический характер: они демонстрируют, что студент понимает, почему его решение устроено именно так.

Выбор проектных решений осуществляется в границах, заданных ТЗ (этап 3). Если в ходе выбора выясняется, что требования ТЗ невыполнимы или нуждаются в корректировке, ТЗ уточняется по согласованию с руководителем. Архитектура, определённая на этом этапе, является исходным материалом для разработки (этап 5): алгоритмы и код создаются в соответствии с архитектурой. Тестирование (этап 6) проверяет, соответствует ли реализованная архитектура заявленным требованиям.

Материалы этого этапа входят в первую главу пояснительной записки (проектно-аналитическую часть). Логика изложения такова: сначала приводится описание объекта и требований, затем – сравнительный анализ вариантов, затем – обоснование выбора, затем – описание архитектуры. Вторая глава (проектно-технологическая часть) открывается кратким напоминанием о принятых решениях, после чего переходит к их реализации.

3. Пояснение к этапу 5. Проектно-конструкторский (разработка)

Сущность этапа

Это центральный этап курсового проектирования, на котором проектные решения превращаются в работающий результат. Если на предыдущих этапах студент работал с текстами, схемами и обоснованиями, то здесь он создаёт то, что можно запустить, настроить, проверить в действии.

Работа на этом этапе включает несколько видов деятельности, соотношение между которыми зависит от типа проекта.

Для проектов, связанных с разработкой программного обеспечения, основным содержанием является написание программного кода. Код должен

быть структурирован, снабжён комментариями, соответствовать принятым в данной области соглашениям о стиле. Разработка ведётся итеративно: сначала создаётся минимально работающий прототип, затем он расширяется и дорабатывается.

Для проектов, связанных с настройкой средств защиты, основным содержанием является конфигурирование компонентов: установка, задание параметров, определение политик, разграничение прав доступа. Настройка должна быть документирована: какие параметры изменялись, какие значения устанавливались, почему выбраны именно эти значения.

Для проектов, связанных с разработкой алгоритмов, основным содержанием является разработка алгоритмов и структурных схем: описание последовательности действий, определение условий ветвления, оценка вычислительной сложности.

Общим для всех типов проектов является подготовка исходных данных и рабочей среды: тестовых документов, контрольных примеров, изолированного стенда или виртуальной машины, на которой будет проверяться решение.

Результатом является работающий прототип проектного решения. В зависимости от типа проекта это может быть программный модуль, настроенная система защиты, реализованный алгоритм. Прототип должен демонстрироваться руководителю. Демонстрация – не формальность: она позволяет своевременно выявить проблемы и скорректировать направление работы до того, как проект будет оформлен.

Вторым результатом являются черновые материалы практической части: описание алгоритмов, фрагменты кода, схемы, скриншоты, фиксирующие состояние системы на ключевых этапах настройки.

Разработка ведётся в соответствии с архитектурой, определённой на этапе 4, и в границах требований ТЗ (этап 3). Промежуточные результаты разработки являются исходным материалом для тестирования (этап 6). Если в ходе разработки выясняется, что принятые решения нуждаются в корректировке, студент возвращается к этапу 4 и вносит изменения в архитектуру или выбор средств.

Материалы этого этапа составляют основное содержание второй главы (проектно-технологической части). Логика изложения такова: сначала описывается архитектура решения (кратко, со ссылкой на первую главу), затем – алгоритмы и логика работы, затем – пошаговое описание реализации, затем – ключевые фрагменты кода или конфигурации. Полный исходный код, если он велик, выносится в приложение; в основном тексте приводятся только значимые фрагменты с пояснениями.

4. Пояснение к этапу Этап 6. Экспериментально-испытательный (тестирование)

Тестирование – это не формальное подтверждение того, что «всё работает». Это самостоятельная проектная деятельность, в ходе которой проверяется, соответствует ли разработанное решение требованиям ТЗ и критериям эффективности, сформулированным на этапе 3. Результаты тестирования могут потребовать доработки решения, и это нормально: проект считается качественным не тогда, когда тестирование сразу дало положительный результат, а тогда, когда выявленные проблемы были проанализированы и устранены.

Работа на этом этапе начинается с разработки методики тестирования. Методика должна определять: что именно проверяется, на каких данных, в каких условиях, по каким критериям оценивается результат. Методика разрабатывается до начала испытаний, а не по их ходу.

Затем проводятся испытания по сценариям. Каждый сценарий описывает: входные данные, последовательность действий, ожидаемый результат. По ходу испытаний фиксируются фактические результаты. Расхождения между ожидаемыми и фактическими результатами анализируются: чем они вызваны, являются ли они следствием ошибок в реализации или следствием неверно сформулированных ожиданий.

Оценка эффективности производится по критериям, определённым в ТЗ. Оценивается техническая эффективность (обеспечивает ли решение защиту от заявленных угроз), эксплуатационная эффективность (удобно ли решение в использовании, надёжно ли оно, каковы его ресурсные характеристики). Если проект предполагает экономическое обоснование, оценивается также экономическая эффективность.

Результатом являются протоколы испытаний, таблицы результатов, подтверждение работоспособности решения. Протокол испытаний — это документ, фиксирующий условия, ход и результаты проверки. Он может быть оформлен как таблица, как текстовое описание или как комбинация того и другого.

Тестирование проверяет соответствие результата разработки (этап 5) требованиям ТЗ (этап 3). Если выявлены расхождения, студент возвращается к этапу 5 для доработки решения либо к этапу 4 для пересмотра проектных решений. Результаты тестирования отражаются в выводах по второй главе и в заключении.

Внесение в текст курсового проекта

Материалы этого этапа включаются во вторую главу пояснительной записки, в завершающие её разделы. Логика изложения такова: сначала

описывается методика тестирования, затем – сценарии испытаний, затем – полученные результаты, затем – анализ расхождений и оценка эффективности. Протоколы испытаний могут быть вынесены в приложение, а в основном тексте приведены сводные таблицы результатов.

Приведённый в таблице 2 порядок показывает, что все четыре этапа образуют единую цепочку, в которой результат каждого этапа является исходным материалом для следующего. Разрыв этой цепочки – например, переход к разработке без сформулированных требований или оформление пояснительной записки без проведённого тестирования – приводит к тому, что проект теряет целостность и не может быть оценён как качественно выполненный.

Таблица 2 – Сводная характеристика взаимосвязей этапов

Этап	**Процесс**	**Результат**	**Куда входит в тексте**
1. Формулирование требований и разработка ТЗ	Определение функциональных, технических, эксплуатационных требований; формулировка критериев эффективности; согласование с руководителем	Подписанное ТЗ	Приложение; обоснование требований – в первой главе; цель и задачи – во введении
2. Выбор и обоснование проектных решений	Сравнительный анализ вариантов; обоснование выбора средств; определение архитектуры	Обоснование выбора; описание архитектуры	Первая глава (проектно-аналитическая часть)
3. Проектно-конструкторский (разработка)	Разработка алгоритмов; написание кода или настройка средств; подготовка среды	Работающий прототип; черновые материалы	Вторая глава (проектно-технологическая часть), основное содержание
4. Экспериментально-испытательный (тестирование)	Разработка методики; проведение испытаний; анализ результатов; оценка эффективности	Протоколы испытаний; подтверждение работоспособности	Вторая глава, завершающие разделы; протоколы – в приложении

Пример построения основной части

Тема проекта: «Поиск и удаление вредоносных объектов из DOCX- и PDF-файлов».

Глава 1. Проектно-аналитическая часть

1.1. Характеристика объекта проектирования: документооборот организации и используемые форматы файлов.

1.2. Угрозы, связанные с вредоносными вложениями в DOCX- и PDF-документах, применительно к рассматриваемому объекту.

1.3. Анализ существующих средств обнаружения и удаления вредоносных объектов, оценка их применимости.

1.4. Постановка проектной задачи: разработка средства, обеспечивающего обнаружение и удаление вредоносных объектов из документов указанных форматов.

Глава 2. Проектно-технологическая часть

2.1. Выбор средств реализации и обоснование архитектуры разрабатываемого средства.

2.2. Алгоритм обнаружения вредоносных объектов в DOCX-документах.

2.3. Алгоритм обнаружения вредоносных объектов в PDF-документах.

2.4. Программная реализация: структура модулей, описание ключевых функций.

2.5. Тестирование: сценарии проверки, тестовые документы, полученные результаты.

2.6. Оценка эффективности и ограничений разработанного решения.

Примеры построения проектной части для различных типов заданий

1. Разработка OCR-приложения для обнаружения утечки информации с операционной системы:

– постановка проектной задачи и требования к приложению;

– выбор технологий компьютерного зрения и оптического распознавания символов;

– архитектура приложения и распределение функций между модулями;

– реализация модуля распознавания печатного текста;

– блок-схема работы приложения;

– тестирование на контрольных документах и оценка точности распознавания.

2. Использование AVZ для обнаружения и нейтрализации вредоносного программного обеспечения:

– постановка проектной задачи;

– установка и первичная настройка AVZ;

– разработка сценариев сканирования;

– разработка собственных скриптов для поиска угроз;

– проверка работоспособности сценариев на тестовой среде;

– оценка полноты обнаружения и ограничений применения.

3. Обеспечение безопасности с использованием технологий IoT и NFC:

– техническое задание на разрабатываемую систему;

– выбор комплектующих и обоснование конфигурации;

– схема подключения и её описание;

– алгоритм работы системы;

– программная реализация;

– тестирование и оценка защищённости канала связи.

4. Установка, настройка и сопровождение модуля InfoWatchDeviceMonitor:

– постановка проектной задачи и требования к конфигурации;

– установка и настройка Microsoft SQL Server;

– проверка открытых TCP-портов и настройка сетевого взаимодействия;

– установка и настройка модуля InfoWatchDeviceMonitor;

– настройка контроля общих сетевых ресурсов;

– проверка работоспособности после обновления операционной системы.

5. Исследование стойкости защитных механизмов Unix-подобных операционных систем:

– анализ средств идентификации и аутентификации в выбранной операционной системе;

– выявление уязвимостей, позволяющих изменить права пользователей;

– разработка и применение мер защиты;

– проверка стойкости принятых мер на тестовых сценариях;

– оценка достигнутого уровня защищённости.

Требования к представлению результатов проектирования

В практической части должны быть представлены:

– конфигурации и профили настроек средств защиты;

– параметры регистрации событий безопасности;

– алгоритмы и программные модули, реализующие проектные решения, с описанием их взаимосвязей;

– средства шифрования и криптографические алгоритмы, если они применялись;

– эксплуатационные характеристики средств идентификации и аутентификации;

– порядок применения антивирусных средств;

– настройки аудита информационной безопасности;

– порядок эксплуатации мер защиты, предложенных в проекте.

Все приведённые материалы должны относиться к конкретному объекту проектирования и конкретной проектной задаче, а не носить общий характер.

В списке использованных источников должны быть представлены нормативно-правовые акты, учебная и научно-техническая литература, монографические исследования, статьи, техническая документация производителей программных и аппаратных средств, справочные и интернет-источники. Список должен содержать не менее 10–15 источников, преимущественно изданных не более 10 лет назад относительно года выполнения проекта (за исключением исторических тем). На все приведённые источники должны быть ссылки в тексте.

Заключение

Заключение содержит краткое изложение полученных проектных результатов: что было спроектировано и реализовано, какие характеристики подтверждены экспериментально, в чём состоят ограничения полученного решения и какие направления его развития представляются целесообразными. Выводы заключения должны соотноситься с проектной задачей, сформулированной во введении.

Слово «ЗАКЛЮЧЕНИЕ» пишется прописными буквами без точки в конце и центрируется.

Типовой объем заключения составляет 1–2 страницы.

Список использованных источников включает все материалы, которые вы использовали в курсовом проекте. Важно, чтобы на каждый источник в списке была ссылка в тексте. Общие сведения по теме проекта обычно упоминаются во введении. Источники в списке располагаются в том порядке, в каком они появляются в текст.

При оформлении библиографического описания источников в списке необходимо руководствоваться ГОСТ Р 7.0.100-2018[4]. Список наименований должен содержать не менее 12 источников.

Словосочетание «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ» пишется прописными буквами без точки в конце и центрируется. Пример оформления списка использованных источников приведён **в приложениях Е** и **И** (выдержка из ГОСТ – 7.32.2017).

Приложения. Приложения – вспомогательные иллюстративно-графические, табличные, расчетные и текстовые материалы, которые нецелесообразно (объем более 1 страницы) приводить в основном тексте курсового проекта.

Приложения к курсовому проекту (проекту) могут включать в себя;

– материалы, дополняющие текст проекта;

– промежуточные вычисления, расчеты, выкладки;

– экспериментальные материалы; инструкции;

– описание методик, технологий, программных средств и т. п.;

– протоколы испытаний (экспериментов);

– заключения экспертизы, акты внедрения и т. д.

Приложения помещают в конце курсового проекта.

Каждое приложение должно начинаться с новой страницы и иметь заголовок.

Приложения нумеруются арабскими цифрами порядковой нумерации. Номер приложения размещается в правом верхнем углу над заголовком после слова «Приложение» (например, Приложение 1).

Приложения должны иметь общую с остальной частью курсового проекта сквозную нумерацию страниц.

На все Приложения в основной части курсового проекта должны быть ссылки. Последовательность приложений должна соответствовать их упоминанию в тексте.

В приложения рекомендуется включать материалы, связанные с выполненным проектом, которые по каким-либо причинам не могут быть включены в основную часть. В приложения могут быть включены:

− исходные тексты программ;

− распечатки проекта программ;

− чертежи электрических схем;

− промежуточные математические выкладки, доказательства, расчеты;

− таблицы вспомогательных цифровых данных;

− протоколы испытаний;

− описание аппаратуры, приборов и программ, применяемых в проекте;

− инструкции и методики в процессе выполнения проекта;

− иллюстрации вспомогательного характера;

− документы о внедрении (использовании) результатов проекта и др.

Слово «ПРИЛОЖЕНИЕ» пишется прописными буквами без точки в конце и центрируется.

Приложения размещаются в конце пояснительной записки в порядке, соответствующем ссылкам на них. Каждое приложение начинается с новой страницы и включает информативный заголовок. При необходимости текст приложения можно разделить на разделы, подразделы, пункты и подпункты. Нумерация должна соответствовать требованиям для основной части записки. Программная документация, выносимая в приложения, должна оформляться в соответствии с требованиями ЕСПД [2]. В приложении курсового проекта необходимо привести исходный текст программы, включая (если таковые

используются) нестандартные библиотеки. Если исходный текст программы имеет большой объем (превышает 50 страниц), то в приложениях могут быть приведены ключевые элементы полного исходного текста программы, поясняющие принцип ее действия,

2.3 Требования к оформлению курсового проекта

Так как курсовой проект носит характер практической реализации, то этим определяются требования к его структуре, содержанию и оформлению, **ГОСТ Р 2.105-2019** [3].

Следует отметить особенности оформления (таблицы 3–15).

Таблица 3 – Общие параметры оформления пояснительной записки

Параметр	**Значение / требование**
Нормативный документ	ГОСТ Р 2.105-2019
Язык записки	русский
Формат бумаги	А4 (210 × 297 мм)
Печать	Односторонняя, принтер
Межстрочный интервал	Полуторный
Шрифт	Times New Roman Cyr, 14 пт
Цвет шрифта	Чёрный
Поля: левое	30 мм
Поля: правое	15 мм
Поля: верхнее, нижнее	20 мм
Выравнивание текста	По ширине, без переносов
Абзацный отступ	1,27 см
Акцентирование	Допускается разными шрифтами для терминов, формул, теорем

В работе можно использовать компьютерные средства, чтобы выделить важные термины, формулы и теоремы разными шрифтами.

Специфика оформления структурных элементов, заголовков, требования к качеству текста приведены в таблицах 4–6.

Таблица 4 – Общие требования к качеству текста

№ п/п	**Требование**
1	Плотность, контрастность и чёткость одинаковы на всех страницах
2	Все буквы, цифры и знаки – чёткие, чёрные, без размытости
3	Опечатки и графические ошибки исправляются перепечаткой страниц
4	Листы с повреждениями, помарками, следами старого текста не допускаются
5	Фамилии, названия организаций, фирм, изделий – на языке оригинала; при первом упоминании допускается перевод с оригиналом в скобках

Таблица 5 – Оформление заголовков структурных элементов

Элемент	**Правило оформления**
«СОДЕРЖАНИЕ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ»	Прописными буквами, по центру, без точки в конце, без подчёркивания
Заголовки разделов, подразделов, пунктов	С абзацного отступа 1,27 см, строчными буквами (кроме первой прописной), полужирным шрифтом 14 пт, без точки в конце
Несколько предложений в заголовке	Разделяются точками
Нумерация разделов	Порядковая, в пределах всего текста, кроме приложений
Точка после номера раздела, подраздела, пункта, подпункта	Не ставится

Элемент	Правило оформления
Переносы слов в заголовках	Не допускаются
Многострочный заголовок	Вторая и последующие строки выравниваются по началу первой строки

Пример 1. Приведен фрагмент нумерации глав, параграфов и пунктов курсового проекта:

2 Практическая часть

2.1 Алгоритмы

2.1.1 Алгоритмы контроля

Пример оформления (выдержка из ГОСТ 7.32-2017):

Пример 2. Приведен фрагмент нумерации глав, параграфов и пунктов курсового проекта:

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

2.1 Рубрикатор ВИНИТИ

2.1.1 Структура и функции рубрикатора

Особенности оформления заголовков, нумерации структурных элементов определяется по таблицам 6, 7.

Таблица 6 – Интервалы и размещение заголовков

Ситуация	Интервал
Между идущими подряд заголовками	3 межстрочных интервала (пропуск одной строки)
Между заголовком и последующим текстом	3 межстрочных интервала
Между текстом и последующим заголовком	4,5 межстрочных интервала (пропуск двух строк)
Начало структурного элемента или раздела	С новой страницы

Ситуация	Интервал
Заголовок и текст на разных страницах	Не допускается
Недостаток места после заголовка	Заголовок переносится на следующую страницу

Таблица 7 — Нумерация структурных элементов

Ситуация	Правило
Глава (раздел) состоит из одного подраздела	Подраздел не нумеруется
Подраздел состоит из одного пункта	Пункт не нумеруется
Текст делится только на пункты	Нумерация порядковая в пределах всей записки
Пункты делятся на подпункты	Нумерация в пределах каждого пункта: 3.2.1.1, 3.2.1.2 и т. д.
Перечисления	Перед каждым – дефис; допускается нумерация арабскими цифрами со скобкой
Детализация перечислений	Арабские цифры со скобкой, запись с абзацного отступа 1,27 см

Пример 1. Информационно-сервисная служба для обслуживания удалённых пользователей включает следующие модули:

– удалённый заказ;

– виртуальная справочная служба;

– виртуальный читальный зал.

Пример 2. Проект по оцифровке включала следующие технологические этапы:

1. Первичный осмотр и структурирование исходных материалов;
2. Сканирование документов;
3. Обработка и проверка полученных образов;
4. Структурирование оцифрованного массива;
5. Выходной контроль качества массивов графических образов.

Страницы курсового проекта нумеруют арабскими цифрами, соблюдая сквозную нумерацию по всему тексту, включая приложения. Титульный лист включают в общую нумерацию страниц записки. На титульном листе номер не ставят (таблица 8).

Таблица 8 – Нумерация страниц

Параметр	**Правило**
Нумерация	Арабскими цифрами, сквозная, включая приложения
Титульный лист и реферат	Включаются в общую нумерацию, но номер не ставится
Место номера	Внизу по центру листа, без точки
Иллюстрации и таблицы на отдельных листах	Включаются в общую нумерацию
Листы альбомной ориентации	Номер не проставляется
Листы формата А3	Учитываются как одна страница
Листы более А3	Выносятся в приложения

Особенности стиля изложения, используемого в курсовом проекте, приведены в **таблице 9.**

Таблица 9 – Стилистические требования

Аспект	**Требование**
Обязательные требования	Слова «следует», «должен», «необходимо»; допускается повествовательная форма («указывают», «применяют»)
Стиль	Строгий литературный, как в научно-технических отчётах
Жаргонизмы, вульгаризмы	Не допускаются

Аспект	Требование
Терминология	Один термин для одного понятия; синонимы перечисляются при первом упоминании
Иностранные слова	Избегать при наличии русскоязычных эквивалентов
Аббревиатуры	Только общепринятые
Авторство	Безличные конструкции: «известно», «предложено», «рассмотрено»; местоимения «я», «мы» не используются
Сокращения функциональных элементов	Понятные, не вызывающие путаницы; совпадение названий в тексте и на иллюстрациях

Специфика оформления иллюстративного материала, таблиц, формул, приложений, особенности использования сокращений, оформления библиографии приведены **в таблицах 10–16.**

Таблица 10 – Оформление иллюстраций

Параметр	Правило
Количество	Достаточно для пояснения текста; практическая часть не может состоять в основном из иллюстраций и скриншотов
Ссылки	Обязательны на все иллюстрации; слово «рисунок» с номером
Размещение	После первой ссылки в тексте или на следующей странице
Оформление ссылок	«(Рисунок 3)», «как видно на рисунке 8», «как это видно из рисунка 3.8»; не оформлять как самостоятельные фразы
Подрисуночная подпись	Обязательна

Параметр	Правило
Соответствие стандартам	ЕСПД, ЕСКД
Нумерация	Сквозная, арабскими цифрами; допускается в пределах раздела («рисунок 3.1»)
Единственный рисунок	«Рисунок 1»
Порядок элементов	Рисунок → пояснительные данные → наименование
Наименование	«Рисунок» + пробел + номер без точки + пробел + тире + пробел + наименование; по центру; 13 пт; с прописной буквы; без точки в конце; без подчёркивания
Отбивки	Наименование отделяется от пояснительных данных одной пустой строкой; последующий текст – одной пустой строкой
Иллюстрации в приложениях	Отдельная нумерация с обозначением приложения: «рисунок а.3»

Таблица 11 – Оформление таблиц

Параметр	Правило
Нормативный документ	ЕСКД
Ссылки	Обязательны на все таблицы; слово «Таблица» с номером
Нумерация	Сквозная арабскими цифрами; допускается в пределах раздела («Таблица 3.1»)
Таблицы приложений	Отдельная нумерация с обозначением приложения: «Таблица А.3»
Единственная	«Таблица 1» или «Таблица В.1»

Параметр	Правило
таблица	
Название	Над таблицей слева, без абзацного отступа, в одну строку с номером через тире
Оформление названия	14 пт, нормальный интервал, с прописной буквы, без точки в конце, без подчёркивания
Отбивки	Название отделяется от текста и от таблицы одной пустой строкой; текст после таблицы — одной пустой строкой
Продолжение таблицы	«Продолжение таблицы» с номером над другими частями
Разрыв таблицы	Нижняя горизонтальная линия в первой части не проводится
Ограничивающие линии	Слева, справа, сверху, снизу
Размер шрифта	Допускается меньше основного
Высота строк	Не менее 8 мм
Текст в таблице	С переносами, любое приемлемое выравнивание
Заголовки строк	С прописной буквы, в единственном числе
Подзаголовки граф	Со строчной буквы, если одно предложение с заголовком; с прописной – если самостоятельны
Точки в конце заголовков и подзаголовков	Не ставятся
Прочие требования	По ГОСТ Р 2.105-2019 ЕСКД

Таблица 12 – Оформление формул

Параметр	**Правило**
Размещение	Отдельная строка, выравнивание по центру
Отбивки	По одной свободной строке выше и ниже
Знаки препинания	Если формула встроена в текст — соответствующие знаки в конце
Перенос	После знаков =, +, −, ×, : или других; знак повторяется в начале следующей строки
Перенос на умножении	Знак «×»
Выравнивание строк при переносе	По центру или по первому знаку операции
Пояснения к символам	Под формулой, в порядке появления символов
Пояснения после формулы	Запятая, пропуск одной строки, затем пояснения
Начало пояснений	Слово «где» без двоеточия, с левого края без отступа; символ и пояснение через тире
Разделение пояснений	Через точку с запятой, каждое с новой строки
Вторая и последующие строки пояснений	Начинаются с тире, выравниваются по тире табуляцией
Нумерация	Арабскими цифрами, сквозная или в пределах раздела
Нумеруются	Только формулы, на которые есть ссылки
Номер формулы	В круглых скобках; при сквозной нумерации – порядковый номер; при нумерации по разделам – номер раздела и номер формулы через точку

Параметр	Правило
Расположение номера	В той же строке, справа, табуляцией
Многострочная формула	Номер на уровне последней строки
Единственная формула	(1)
Формулы в приложениях	Отдельная нумерация с обозначением приложения: (В.1)
Ссылки на формулы	В круглых скобках: «…как показано в формуле (1)…»
Единицы измерения	СИ или допускаемые с СИ, кратные и дольные
Редактор формул	MicrosoftEquation
Размер шрифта формул	14 пт, как основной текст

Таблица 13 – Цифровой материал, символы, индексы

Элемент	Правило
Цифры	Арабские; исключение – кварталы и полугодия (римские)
Количественные числительные	Без падежных окончаний
Интервалы	Через дефис: 4–8 %, стр. 5–7
Величины с двумя пределами	Единица измерения указывается один раз при второй цифре
Знаки № и %	Только с цифровыми значениями; в тексте словами: «номер», «процент»

Элемент	Правило
Математические знаки (+, −, =, >, <)	Только в формулах; в тексте словами: «плюс», «минус», «равно», «больше», «меньше»
Символы	Буквы русского, латинского, греческого, готического алфавитов
Индексы	Строчные буквы, арабские и римские цифры, штрихи; справа от символа вверху или внизу
Верхний индекс	Обычно степень; одновременное использование верхнего и нижнего не рекомендуется

Таблица 14 – Оформление приложений

Параметр	Правило
Назначение	Дополнительное (справочное) значение; необходимы для полноты освещения темы
Что включается	Материалы, дополняющие основной текст; вспомогательные таблицы и иллюстрации; акты внедрения; фактические данные о проекте; формы выходных документов
Что не включается	Библиографический список, вспомогательные указатели, справочные комментарии и примечания
Размещение	В конце записки, как продолжение на последних страницах
Нумерация внутри приложения	Иллюстрации, таблицы, формулы и уравнения — в пределах каждого приложения
Объём	Не ограничивается
Начало приложения	С нового листа, слово «ПРИЛОЖЕНИЕ» вверху по центру, тематический заголовок с прописной буквы отдельной строкой
Обозначение приложений	«ПРИЛОЖЕНИЕ А», «ПРИЛОЖЕНИЕ Б» и т. д.; без знака №; буквы Ё, З, Й, О, Ч, Ь, Ы, Ъ не

Параметр	Правило
	Используются
Нумерация страниц	Сквозная, продолжает общую нумерацию
Связь с текстом	Через ссылки в тексте
Отражение в оглавлении	Самостоятельная рубрика с полным названием каждого приложения

Таблица 15 – Аббревиатуры и сокращения

Ситуация	Правило
Общепринятые аббревиатуры (РФ, ЕС, вуз)	Используются без расшифровки
Нестандартные аббревиатуры	После первого упоминания полного названия в скобках указывается аббревиатура; далее – только аббревиатура
Сложносокращённые слова	Составляются из сочетания
Сокращение слов в тексте и подписях	Не допускается, кроме общепринятых (РФ и др.)
Собственные сокращения и термины	Не допускаются
Наименования в тексте и на иллюстрациях	Должны совпадать

Таблица 16 – Библиографический список и ссылки

Параметр	Правило
Нормативный документ	ГОСТ 7.1
Размещение	после заключения

Параметр	Правило
Заголовок	«СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ»
Состав	Все литературные источники и материалы, использованные при подготовке записки
Порядок	В порядке упоминания в тексте
Нумерация	Арабскими цифрами с точкой
Оформление позиции	С абзацного отступа; после номера через пробел – данные об источнике
Ссылки в тексте	В квадратных скобках: [2], [1, 3, 5], [6−9], [3–7, 9, 11]
Объекты описания	Книги, сериальные ресурсы, нормативные и технические документы, электронные ресурсы, составные части документов и др.
Завершение описания	Точка
Области описания	Каждая, кроме первой, предваряется знаком «точка и тире»; пробелы до и после предписанного знака – один печатный знак; исключение – точка и запятая (пробел только после)
Скобки	Круглые и квадратные – единый знак; пробел перед открывающей и после закрывающей
Грамматически связанные элементы	Не разделяются предписанной пунктуацией

Следует отметить, что оформление должно соответствовать требованиям государственных стандартов: ЕСПД [2] и ЕСКД [3]. Примеры оформления в приложениях в конце пособия, В частности приведены:

1. Пример оформления иллюстраций приведен **в приложении Ж.**
2. Примеры оформления таблиц можно посмотреть **в приложении З**.
3. Пример оформления формул приведен также **в приложении З**.

4. Примеры библиографического описания различных источников литературы приведены в **приложении Г** и **И**.

3 ОРГАНИЗАЦИЯ ВЫПОЛНЕНИЯ КУРСОВОГО ПРОЕКТА

Преподаватель осуществляет руководство и контроль выполнения курсового проекта. В период написания курсового проекта он выполняет следующие функции:

– согласовывает с обучающимся тему проекта;

– оказывает обучающемуся помощь в составлении плана проекта;

– рекомендует научную литературу, справочные, статистические материалы и другие источники информации по выбранной теме; проводит регулярные консультации;

– осуществляет контроль за ходом выполнения курсового проекта;

– оценивает содержание курсового проекта.

Руководство со стороны преподавателя предполагает:

– определение степени подготовленности студента к написанию курсового проекта по избранной (или рекомендуемой) теме;

– оказание помощи в осмыслении тематики и содержания курсового проекта;

– выдачу рекомендаций по подбору информационных, законодательных, нормативных актов, научной и методической литературы, периодических изданий, справочных материалов и др. источников;

– организацию и оказание помощи при проведении математических, и других исследований;

– консультирование по содержанию и оформлению курсового проекта;

– чтение подготовленного курсового проекта и выявление в нем недостатков и неточностей.

Выполнение предусматривает прохождение студентом процедуры проверки на объем заимствования, которую осуществляют на выпускающих кафедрах на основании соответствующего нормативного акта университета.

Объем заимствования, в том числе содержательного, не должен превышать 50 % от общего объема пояснительной записки.

Курсовой проект допускается к защите при следующих условиях:

– итоговая оценка оригинальности текста курсового проекта не ниже 50 % для проектов;

– печатный вариант соответствует требованиям по оформлению;

– курсовой проект выполнен в соответствии с рекомендациями данного пособия и его содержательная часть, в том числе результаты работы, соответствует заявленной теме.

Курсовой проект передается на кафедру не позднее, чем за 10 рабочих дней до даты защиты, если другие сроки не оговорены специально.

Дата защиты курсового проекта определяется преподавателем в соответствии с учебным графиком дисциплины. Защита курсового проекта проводится до начала экзаменационной сессии.

Защита состоит из доклада обучающегося по теме курсового проекта в течение 5–7 минут и ответов на вопросы преподавателя (преподавателей). Обучающийся должен: логично построить сообщение о выполненного проекта, обосновать выводы и предложения; показать понимание теоретических положений, на основе которых выполнен проект; показать самостоятельность выполнения проекта; дать правильные ответы на вопросы.

Защита предполагает краткое изложения обучающимся сущности выполненной курсовой работы в течение 5–7 минут и ответов на вопросы преподавателя (преподавателей). Обучающийся должен: логично построить сообщение о выполненной работе, обосновать выводы и предложения; показать понимание теоретических положений, на основе которых выполнена работа; показать самостоятельность выполнения работы; дать правильные ответы на вопросы.

Следует последовательно изложить:

− актуальность темы;

− цель, задачи и основные требования работы (анализ задания);

− используемые в работе методы, подходы и средства, отметив проделанную работу по основным разделам, последовательно на всех ее этапах и полученные при этом результаты;

− описание и анализ моделей, экспериментов и их результатов;

− выводы по работе в целом.

Решение об оценке курсового проекта принимается по результатам Решение об оценке курсовой работы принимается по результатам анализа предъявленной курсовой работы, доклада обучающегося на защите и его ответов на вопросы. В случае выполнения группой курсовой работы обязательно присутствие всех обучающихся, участвовавших в ее подготовке, на ее защите. При этом оценка курсовой работы осуществляется по результатам доклада и ответов на вопросы каждого из участвовавших в написании курсовой работы.

Курсовой проект оценивается дифференцированной отметкой: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»:

Положительные оценки по курсовому проекту заносятся в ведомость и зачетную книжку, неудовлетворительные оценки проставляются только в ведомость.

Обучающийся, не предъявивший в установленный срок курсовую проект при соблюдении всех требований, предъявляемых к оформлению и содержанию курсового проекта, или не защитивший его по неуважительной причине, считается имеющим академическую задолженность.

Курсовые проекта (проекты) после их защиты должны сдаваться на кафедры в распечатанном бумажном виде и в электронном (файл, расширение *.docx, *.odt).

Наименование курсового проекта и дисциплина, по которой она выполняется, вносятся в экзаменационные ведомости и зачетные книжки обучающихся.

Электронный вариант защищённой студентом курсового проекта размещается в формате PDF в электронной информационной образовательной среде Университета (по необходимости, в разделе электронное портфолио).

4 КРИТЕРИИ И НОРМЫ ОЦЕНКИ КУРСОВОГО ПРОЕКТА

Преподаватель осуществляет руководство и контроль за выполнением курсового проекта, что включает в себя ряд ключевых функций, направленных на обеспечение высокого качества и научной обоснованности работы. В процессе выполнения проекта преподаватель выполняет следующие задачи:

1. Согласование темы проекта с обучающимся, что позволяет определить научную направленность и актуальность исследования.
2. Оказание помощи в составлении плана проекта, что способствует структурированию работы и обеспечению логической последовательности изложения материала.
3. Рекомендация научной литературы, справочных, статистических материалов и других источников информации, необходимых для глубокого анализа темы.
4. Проведение регулярных консультаций, что позволяет своевременно выявлять и устранять возникающие у обучающегося затруднения.
5. Осуществление контроля за ходом выполнения курсового проекта, включая проверку соответствия содержания и структуры работы заявленной теме и поставленным задачам.
6. Оценка содержания курсового проекта, включающая анализ научной обоснованности выводов и предложений, а также соответствия оформления установленным требованиям.

Руководство со стороны преподавателя также предполагает:

1. Определение степени подготовленности студента к выполнению курсового проекта, что позволяет адаптировать уровень поддержки и рекомендаций в зависимости от индивидуальных особенностей и уровня знаний обучающегося.
2. Оказание помощи в осмыслении тематики и содержания курсового проекта, что способствует формированию у студента глубокого понимания исследуемой проблемы.
3. Выдачу рекомендаций по подбору релевантных информационных, законодательных, нормативных актов, научной и методической литературы, а также периодических изданий и справочных материалов.
4. Организацию и оказание помощи при проведении научных исследований, включая математические и статистические методы анализа.
5. Консультирование по содержанию и оформлению курсового проекта, что обеспечивает соответствие работы установленным стандартам и требованиям.

6. Чтение подготовленного курсового проекта с целью выявления возможных недостатков и неточностей, что позволяет студенту своевременно внести необходимые коррективы.

7. Выполнение курсового проекта включает процедуру проверки на объем заимствования, которая осуществляется на выпускающих кафедрах в соответствии с нормативными актами университета. Объем заимствования, включая содержательные элементы, не должен превышать 50% от общего объема пояснительной записки.

Курсовой проект допускается к защите при выполнении следующих условий:

1. Итоговая оценка оригинальности текста курсового проекта должна быть не ниже 50 %.

2. Печатный вариант проекта должен соответствовать установленным требованиям по оформлению.

3. Содержательная часть проекта, включая результаты работы, должна соответствовать заявленной теме и основным требованиям, изложенным в данном пособии.

Курсовой проект передается на кафедру не позднее чем за 10 рабочих дней до даты защиты, если не установлены иные сроки. Дата защиты определяется преподавателем в соответствии с учебным графиком дисциплины и проводится до начала экзаменационной сессии.

Защита курсового проекта включает доклад обучающегося по теме проекта продолжительностью 5–7 минут, а также ответы на вопросы преподавателя (преподавателей). Обучающийся должен логично построить сообщение о выполненной работе, обосновать выводы и предложения, продемонстрировать понимание теоретических положений, на которых базируется исследование, а также показать самостоятельность выполнения проекта.

В докладе обучающийся должен последовательно изложить:

1. Актуальность темы.

2. Цель, задачи и основные требования работы.

3. Используемые методы, подходы и средства исследования.

4. Описание и анализ моделей, экспериментов и их результатов.

5. Выводы по работе в целом.

Решение об оценке курсового проекта принимается на основе анализа представленной работы, доклада обучающегося и его ответов на вопросы. В случае выполнения проекта группой, обязательно присутствие всех участников на защите. Оценка работы осуществляется по результатам доклада и ответов каждого из участников.

Курсовой проект оценивается дифференцированной отметкой: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно». Положительные оценки заносятся в ведомость и зачетную книжку, неудовлетворительные – только в ведомость.

Обучающийся, не представивший курсовой проект в установленный срок или не защитивший его по неуважительной причине, считается имеющим академическую задолженность.

После защиты курсовой проект должен быть сдан на кафедру в распечатанном виде и в электронном формате (файл, расширение .*docx*или.odt). Наименование проекта и дисциплина, по которой он выполнен, допустимо вносить в экзаменационные ведомости и зачетные книжки обучающихся.

Электронный вариант защищенного проекта размещается в формате PDF в электронной информационной образовательной среде университета, а также в разделе электронного портфолио (при необходимости).

СПИСОК РЕКОМЕНДОВАННЫХ ИСТОЧНИКОВ

Основная литература

1. Никифоров, С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]: учеб. пособие / С.Н. Никифоров. – Электрон. дан. – Санкт-Петербург: Лань, 2018. – 160 с. – Режим доступа: https://e.lanbook.com/book/106734. – Загл. с экрана.
2. Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс]: учеб. пособие / С.Н. Никифоров. – Электрон. дан. – Санкт-Петербург: Лань, 2018. – 96 с. – Режим доступа: https://e.lanbook.com/book/107306. – Загл. с экрана.
3. Никифоров, С.Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс] учеб. пособие / С.Н. Никифоров. – Электрон. дан. – Санкт-Петербург: Лань, 2018. – 124 с. – Режим доступа: https://e.lanbook.com/book/107307. – Загл. с экрана.
4. Никифоров, С.Н. Методы защиты информации. Защищенные сети [Электронный ресурс]: учеб. пособие / С.Н. Никифоров. – Электрон. дан. – Санкт-Петербург: Лань, 2018. – 96 с. – Режим доступа: https://e.lanbook.com/book/110935. – Загл. с экрана.
5. Дойникова, Е. В. Оценивание защищённости и выбор контрмер для управления кибербезопасностью: монография / Е. В. Дойникова, И. В. Котенко. – Москва: РАН, 2021. – 184 с.
6. Краковский, Ю. М. Методы и средства защиты информации: учебное пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с.
7. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба. – Омск: ОмГТУ, 2021. – 119 с.
8. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 / В. В. Подтопельный. – Калининград: БГАРФ, 2023. – Ч. 1. – 171 с.
9. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с.
10. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с.

Дополнительная литература

1. Емельянова, Н. З. Проектирование информационных систем: учеб. пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. – Москва: Форум, 2013. – 432 с.: ил. – (Профессиональное образование). – Библиогр.: с. 362-364. ISBN 978-5-91134-274-6: 260.00 р. (12 экз.)

2. Ищейнов, В. Я. Защита конфиденциальной информации: учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – Москва: ФОРУМ, 2013. – 256 с. (наличие в библиотеке БГАРФ – 15 экз.)

3. Кузнецов, А. В. Основы защиты информации: учеб. пособие / В. А. Иванов, О. П. Пономарев, И. А. Ветров. – Калининград: Изд-во БГАРФ, 2014. – 122 с. (наличие в библиотеке БГАРФ - 110 экз.)

4. Родичев, Ю. А. Информационная безопасность: нормативно-правовые аспекты: учеб. пособие для студентов, обучающихся по спец. «Комплексное обеспечение информационной безопасности автоматизированных систем» / Ю. А. Родичев. – Санкт-Петербург: Питер, 2008. – 272 с. (наличие в библиотеке БГАРФ - 15 экз.)

5. Automating Construction of Machine Learning Models with Clinical Big Data: Proposal Rationale and Methods / L. Gang, B. L. Stone, M. D. Johnson [и др.] // JMIR Research Protocols. – 2017. – Т. 8, № 6. – С. 175.

Методические разработки

1. Подтопельный, В. В. Программно-аппаратные средства защиты информации: учеб. пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / В. В. Подтопельный; Балтийская государственная академия рыбопромыслового флота. – Калининград: Изд-во БГАРФ. – Электрон. версия печ. публикации. – Текст: электронный. Ч. 4 : Настройка подсистем СЗИ. – 2021. – 98 с.

2. Подтопельный, В. В. Комплексное обеспечение информационной безопасности автоматизированных систем: методические указания по выполнению лабораторных проектов для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / В. В. Подтопельный; Балтийская государственная академия рыбопромыслового флота. – Калининград: Изд-во БГАРФ. – Электрон. версия печ. публикации. – Текст: электронный. Ч. 1. – 2021. – 54 с.

3. Подтопельный, В. В. Информационная безопасность распределенных информационных систем: методические указания по выполнению лабораторных проектов для студентов специальности 10.05.03

«Информационная безопасность автоматизированных систем» всех форм обучения / В. В. Подтопельный; Балтийская государственная академия рыбопромыслового флота. – Калининград: Изд-во БГАРФ. – Электрон. версия печ. публикации. – Текст: электронный. Ч. 2. – 2021. – 43 с.

4. Бабаева, А. А. Информационная безопасность автоматизированных информационных систем: методические указания по выполнению лабораторных проектов для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / А. А. Бабаева; Балтийская государственная академия рыбопромыслового флота. – Калининград: Изд-во БГАРФ, 2020. – 45 с.: табл. – Библиогр.: с. 37. – 190.00 р. – Текст: непосредственный.

5. Информационная безопасность автоматизированных информационных систем: метод. указания по выполнению лаб. работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» очной формы обучения / Федер. агентство по рыболовству [и др.]; авт.-сост. А. А. Бабаева. – (изд. 2-е, с доп. и изм.). – Калининград: БГАРФ, 2022. – 46 с.

6. Безопасность операционных систем: метод. указания по выполнению курсовых работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» очной формы обучения / Федер. агентство по рыболовству [и др.]; авт.-сост. В. В. Подтопельный. – Калининград: БГАРФ, 2023. – 53 с.

7. Жестовский, А. Г. Управление информационной безопасностью: учеб.-метод. пособие по выполнению практ. занятий для студентов специальности 10.05.03 – Информ. безопасность автоматизир. систем / А. Г. Жестовский; Калинингр. гос. техн. ун-т. – Калининград: КГТУ, 2023. – 26 с.

8. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Ч. 1. – 171 с.

9. Подтопельный, В. В. Программно-аппаратные средства защиты информации: учеб. пособие по дисциплине «Программно-аппарат. средства защиты информации» для студентов специальности 10.05.03 – Информ. безопасность автоматизир. систем: в 2 ч. / В. В. Подтопельный ; Калинингр. гос. техн. ун-т. – Калининград: КГТУ, 2024. – Ч. 1 : Поиск и удаление вредоносных объектов в информационных системах. – 2024.

10. Высоцкий, Л. Г. Программная инженерия (ПИ): учеб.-метод. пособие по выполнению лаб. практикума по дисциплине «Программная инженерия» для студентов бакалавриата по направлениям подгот. 09.03.01

Информатика и вычисл. техника, 09.03.03 Приклад. информатика / Л. Г. Высоцкий; Калинингр. гос. техн. ун-т. – Калининград: КГТУ, 2024. – 115 с.

11. Ильяшов, А. Н. Безопасность вычислительных сетей: учеб.-метод. пособие по выполнению лаб. работ для студентов специальности 10.05.03 Информ. безопасность автоматизир. систем, специализация «Безопасность открытых информ. систем» / А. Н. Ильяшов, В. В. Подтопельный; Калинингр. гос. техн. ун-т. – Калининград: КГТУ, 2025. – 170 с.

12. Подтопельный, В. В. Программно-аппаратные средства защиты информации: учеб. пособие для студентов специальности 10.05.03 Информ. безопасность автоматизир. систем, специализация «Безопасность открытых информ. систем» / В. В. Подтопельный; Калинингр. гос. техн. ун-т. – Калининград : КГТУ, 2024. – Ч. 2 : Эксплуатация систем защиты информации. – 2025. – 166 с.

Нормативно-правовые акты

1. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации от 5 декабря 2016 г. № 646.
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ).
3. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера».
8. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
9. ГОСТ 24.104-2023. Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования.

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

11. ГОСТ 24.205-80. Комплекс стандартов на автоматизированные системы. Требования к содержанию документов по информационному обеспечению.

12. ГОСТ 24.206-80. Комплекс стандартов на автоматизированные системы. Требования к содержанию документов по техническому обеспечению.

13. ГОСТ 24.207-80. Комплекс стандартов на автоматизированные системы. Требования к содержанию документов по программному обеспечению.

14. ГОСТ 24.208-80. Комплекс стандартов на автоматизированные системы. Требования к содержанию документов стадии «Ввод в эксплуатацию».

15. ГОСТ 24.209-80. Комплекс стандартов на автоматизированные системы. Требования к содержанию документов по организационному обеспечению.

16. ГОСТ 24.210-82. Комплекс стандартов на автоматизированные системы. Требования к содержанию документов по функциональной части.

17. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

18. ГОСТ Р ИСО/МЭК 29100-2013. Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности.

19. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.

20. ГОСТ Р ИСО/МЭК ТО 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

21. ГОСТ 29339-92. Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Общие технические требования.

22. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

23. ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методика испытаний.

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

25. Методический документ: Методика оценки угроз безопасности информации: утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf (дата обращения: 18.10.2026).

26. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/vul/ (дата обращения: 18.10.2026).

27. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

28. 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.

29. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200068822 (дата обращения: 18.10.2026).

30. ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллекта [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200177292 (дата обращения: 18.10.2026).

31. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200048398 (дата обращения: 18.10.2026).

32. Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

33. Приказ ФСТЭК России от11.04.2025 г. № 117 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

34. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

35. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных

системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и представляющих угрозу для безопасности государства».

ЗАКЛЮЧЕНИЕ

Данные методические рекомендации устанавливают общие требования к структуре, содержанию, порядку выполнения курсового проекта, выполняемого студентами очной формы обучения по специальности 10.05.03 «Информационная безопасность автоматизированных систем» на основании стандартов, приказов и положений.

В методических указаниях отражены основные моменты оформления пояснительной записки, приведены примеры, бланки заявлений и их можно использовать как образец оформления.

Методические рекомендации направлены на формирование корректного изложения материала в курсовом проекте, что поможет студенту избежать распространённых ошибок и сосредоточить своё внимание на успешной его защите.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ 7.32-2017. Отчет о научно-исследовательской работе. Структура и правила оформления. – Введ. 2018-07-01. – Москва: Стандартинформ, 2017. – 32 с.

2. ГОСТ 19.401-78. Единая система программной документации. Текст программы. Требования к содержанию и оформлению. – Введ. 1980-01-01. – Москва: Стандартинформ, 2010. – 70 с.

3. ГОСТ Р 2.105-2019. Единая система конструкторской документации. Общие требования к текстовым документам. – Введ. 2020-01-01. – Москва: Стандартинформ, 2019. – 28 с.

4. ГОСТ Р 7.0.100-2018. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления. – Введ. 2019-07-01. – Москва: Стандартинформ, 2018. – 128 с.

5. Методический документ: Методика оценки угроз безопасности информации: утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf (дата обращения: 18.10.2026).

6. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/vul/ (дата обращения: 18.10.2026).

7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Введ. 2011-01-01. – Москва: Изд-во стандартов, 2010.

8. 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. – Введ. 2013-09-01. – Москва: Стандартинформ, 2013.

9. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200068822 (дата обращения: 18.10.2026).

10. ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллекта [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200177292 (дата обращения: 18.10.2026).

11. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных

технологий [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200048398 (дата обращения: 18.10.2026).

12. Приказ Минобрнауки России от 26.11.2020 № 1457 «Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета)». Зарегистрировано в Минюсте России 17.03.2021 № 62532.

13. MITRE ATLAS // MITRE ATT&CK [Электронный ресурс]. – Режим доступа: https://atlas.mitre.org, свободный (дата обращения: 18.10.2026).

14. NIST (National Institute of Standards and Technology) [Электронный ресурс]. – Режим доступа: https://www.nist.gov (дата обращения: 18.10.2026).

ПРИЛОЖЕНИЯ

Приложение А

Примерные темы курсовых проектов

1. Оценка защищённости беспроводных сетей Wi-Fi: сканирование уязвимостей, анализ перехваченных рукопожатий и подбор политик защиты на тестовом стенде.
2. Разработка модуля выявления утечек текстовой информации через скриншоты и файлы с использованием OCR и правил DLP-классификации (на примере DOCX/PDF).
3. Проектирование защищённой IoT-подсистемы на базе микроконтроллера (ESP32/RPi) с аутентификацией по NFC-меткам и шифрованием канала передачи данных.
4. Выявление и нейтрализация вредоносного кода в файлах DOCX и PDF: анализ макросов, встроенных скриптов и объектов OLE; разработка сигнатурного и поведенческого детектора.
5. Анализ защищённости проводных сетей общего пользования: моделирование атак (ARP spoofing, VLAN hopping) и применение аппаратных/программных средств защиты на стенде.
6. Проектирование системы защиты банка данных: разграничение доступа, шифрование на уровне СУБД, аудит операций и журналирование событий.
7. Исследование возможностей AVZ как инструмента анализа и устранения вредоносных объектов: сценарии использования, сравнение с другими утилитами, автоматизация типовых действий.
8. Анализ характеристик линий связи (затухание, наводки, электромагнитная эмиссия) и оценка рисков утечки информации по техническим каналам.
9. Реализация и аудит цепочки доверия при использовании ЭЦП в системе электронного документооборота: проверка сертификатов, валидация подписей, сценарии атак на PKI.
10. Проектирование механизма защиты конфиденциальной информации в распределённой системе разграничения доступа: ролевая модель, токены доступа, аудит сессий.
11. Настройка и тестирование модуля контроля съёмных носителей (на примере InfoWatchDeviceMonitor): сценарии утечек, политики, анализ событий и отчётов.
12. Разработка прототипа системы мониторинга активности сотрудников ИТ-отдела: сбор событий, корреляция, визуализация, пороги срабатывания.

13. Сравнительный анализ инструментальных средств оценки рисков ИБ (CVSS, MITRE ATT&CK, NIST SP 800-30) и их применение для типовой корпоративной сети.

14. Адаптация международных стандартов ИБ (ISO/IEC 27001, NIST CSF) под требования типовой организации: карта соответствия, контрольные меры, план внедрения.

15. Аудит информационной безопасности вычислительной сети: сканирование уязвимостей, тестирование на проникновение, формирование отчёта по стандарту PTES.

16. Разработка стенда для исследования атак на Wi-Fi и тестирования средств защиты: подбор WPA-ключей, анализ трафика, внедрение политик безопасности.

17. Прототип системы обнаружения аномалий сетевого трафика на базе одноплатного компьютера (RaspberryPi) с применением правил Suricata и эвристик.

18. Аппаратно-программный комплекс контроля целостности исполняемых файлов: расчёт хешей, сравнение эталонов, блокировка запуска при нарушении.

19. Исследование атак на протоколы аутентификации (NTLM, Kerberos) в лабораторной сети и разработка рекомендаций по защите.

20. Система контроля доступа на базе RFID/NFC с интеграцией в СКУД и логированием событий на микроконтроллере.

21. Анализ уязвимостей веб-приложений и защита на уровне инфраструктуры: WAF, фильтрация запросов, защита от инъекций.

22. Проектирование сегмента защищённой сети (DMZ, VLAN, межсетевой экран) и тестирование устойчивости к сетевым атакам.

23. Исследование методов защиты от утечки информации по побочным каналам (электромагнитное излучение, акустические каналы) на лабораторном стенде.

24. Разработка прототипа DLP-модуля для контроля передачи данных через USB-накопители: блокировка по типам файлов, журналирование, отчёты.

25. Сравнительное исследование средств анализа уязвимостей (OpenVAS, Nessus, Qualys) на типовом сегменте сети: покрытие, ложные срабатывания, удобство эксплуатации.

26. Применение MITRE ATT&CK для моделирования кибератак и проверки эффективности средств защиты в лаборатории.

27. Проектирование и тестирование системы резервного копирования и восстановления с учётом требований ИБ: шифрование, контроль доступа, проверка целостности.

28. Аппаратно-программный модуль доверенной загрузки на базе UEFI-совместимого стенда: контроль целостности загрузчика, журналирование попыток подмены.

29. Система контроля физического доступа на базе микроконтроллера (ESP32) и RFID-меток с шифрованием канала и защитой от клонирования меток.

30. Исследование утечки информации по электромагнитному каналу на лабораторном стенде: измерение побочных излучений монитора, оценка эффективности экранирования и фильтров.

31. Прототип системы защиты от несанкционированного копирования на съёмные носители: блокировка по типам файлов, журналирование, интеграция с ОС (Windows/Linux).

32. Проектирование сегмента защищённой сети (VLAN, DMZ, межсетевой экран) и тестирование устойчивости к типовым сетевым атакам (ARP spoofing, ICMP flood, сканирование портов).

33. Прототип IDS на одноплатном компьютере (RaspberryPi) с правилами Suricata и эвристиками для обнаружения сканирования портов и brute-force.

34. Анализ защищённости Wi-Fi-сети: захват и разбор рукопожатий (WPA2/WPA3), оценка стойкости паролей, рекомендации по политикам безопасности.

35. Тестирование межсетевого экрана на устойчивость к атакам типа DoS/DDoS и оптимизация правил фильтрации для снижения ложных срабатываний.

36. Модуль выявления утечек конфиденциальной информации в файлах и скриншотах: интеграция OCR, классификация по ключевым словам и регулярным выражениям, правила блокировки.

37. Система мониторинга USB-устройств и контроля передачи данных: журналирование подключений, блокировка по вендору/модели, отчёты по активности.

38. Реализация и аудит цепочки доверия при использовании ЭЦП: проверка сертификатов, валидация подписей, моделирование атак на PKI (MITM, подмена сертификата).

39. Разработка модуля проверки целостности и подлинности обновлений ПО: подпись пакетов, проверка хешей, защита от подмены обновлений.

40. Адаптация стандарта ISO/IEC 27001 под типовую организацию: карта соответствия, контрольные меры, план внедрения и матрица рисков.

41. Применение MITRE ATT&CK для моделирования кибератак и проверки эффективности средств защиты: карта техник, сценарии, отчёт по срабатыванию средств защиты.

42. Лабораторный стенд для исследования атак на протоколы аутентификации (NTLM, Kerberos): разбор атак, меры защиты, отчёт.

Приложение Б

Краткие правила форматирования

Курсовые проекты представляются в виде единого файла в формате текстового редактора *.docx, *.odt..

Требования к тексту:

– формат бумаги: А4;

– ориентация: книжная;

– поля: верхнее, нижнее, левое, правое – 2,0 см;

– гарнитура шрифта: Times New Roman Cyr;

– размер шрифта 14;

– межстрочный интервал – полуторный**;**

– не допускается применять стили при формировании текста; ставить пробелы перед знаками препинания; применять любые разрядки слов;

– необходимо слова внутри абзаца разделять одним пробелом;

– абзац сопровождается отступом 1,27;

– выравнивание шрифта по ширине;

– автоматический перенос слов (набирать текст без принудительных переносов);

– нумерация страниц проставляется с 2-й страницы (1 – это титульный лист);

– номер страницы (колонцифра) проставляется внизу посередине (от края до номера страницы – 2,0 см);

– используется автоматическая вставка таблиц.

Требования к иллюстрациям, таблицам, формулам:

– при определении формата каждой иллюстрации следует исходить из минимума занимаемого места, но при этом помнить, что рисунки будут изданы с уменьшением почти в два раза (максимальный размер рисунка 160 мм по горизонтали и 240 мм – по вертикали);

– иллюстрации нужно вмонтировать в текст и выполнять с использованием текстовых редакторов, формат:

а) bmp, tiff, jpg (цветовое пространство – RGB, разрешение изображений – 300 dpi);

б) cdr;

– рисунки должны быть черно-белыми (допускаются цветные, если цветовая дифференциация несет смысловую нагрузку), четкими, контрастными; на каждый рисунок в тексте необходимо делать ссылку; нумерация должна быть последовательной; если рисунок не умещается на

одной странице, то на последующих страницах пишется: «Рисунок 1. Продолжение (или Окончание)»;

– диаграммы выполняются в форматах MC Graf или MC Excel. Либо в аналогах других общедоступных текстовых редакторов;

– все обозначения на рисунке должны соответствовать обозначениям в тексте;

– номер рисунка и подпись к нему печатаются ниже и выносятся отдельно от файла рисунка (Пример: Рисунок 5 – Алгоритм программы);

– ширина рисунка не должна быть больше ширины полосы набора текста;

– таблицу, по возможности, помещают под текстом, в котором впервые дана ссылка на нее, или на следующей странице; таблицы должны быть пронумерованы и ссылками отражены в тексте; если таблица не уменьшается на одной странице, то на последующих страницах в правом верхнем углу пишется «Продолжение таблицы 1», а на последней странице «Окончание таблицы 1»; относительно заголовков оформление должно быть единообразным: либо с заголовками, либо нет; если шапка таблицы при ее продолжении не повторяется, следует указывать номера граф;

– ширина таблицы не должна быть больше ширины полосы набора текста;

– все формулы набираются в формульном редакторе отдельной строкой; экспликации к ним печатаются в подбор;

– химические символы набирают прямым шрифтом;

– при наличии в тексте ссылок на формулы последние необходимо нумеровать арабскими цифрами; номер формулы ставят в правый ряд страницы в круглых скобках; ссылки в тексте на формулы также дают в круглых скобках;

– если ссылка на номер формулы находится внутри выражения, заключенного в круглые скобки, то их следует заменять квадратными, например: *Используя выражение* [*см. формулу (1.2)], получаем…*

– единицы физических величин следует приводить в международной системе СИ по ГОСТ 8.417-2002. ГСИ. Единицы величин;

– все аббревиатуры в тексте должны быть расшифрованы (разрешаются лишь общепринятые сокращения названия мер, физических и математических величин).

Приложение В

Пример титульного листа

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО РЫБОЛОВСТВУ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»

Институт цифровых технологий

Кафедра _____
наименование кафедры

Курсовой проект допущен к защите

Руководитель:___
(уч. степень, звание, должность*)
_____ И.О. Фамилия
«___» _____ 202__ г.

Курсовой проект защищен с оценкой _____

Руководитель:_____
(уч. степень, звание, должность)
_____ И.О. Фамилия
«___» _____ 202_ г.

ТЕМА КУРСОВОГО ПРОЕКТА

Курсовой проект по дисциплине
«Наименование дисциплины»
КР.ХХ[1].ХХ.ХХ.ХХ[2].Х[3].Х[4]

Проект выполнил:
студент гр.__
_____ И.О.Фамилия
«___» _____ 20__ г.

Калининград
202__

Пояснения

Обозначения в шифре

КП.ХХ[1].ХХ.ХХ.ХХ[2].Х[3].ХХ[4].П

З КР – Курсовой проект.

КП – курсового проект.

ХХ[1] – номер кафедры.

ХХ.ХХ.ХХ[2]– шифр направления подготовки

Х[3] – последняя цифра года, когда выполнена проект (например, 2022 год, будет цифра 2).

ХХ[4] – номер варианта курсового проекта.

ПЗ – пояснительная записка

*

Ученую степень и звание следует сокращать в соответствии с рекомендациями Министерства науки РФ, например:

Сокращение	**Полное написание**
Учёные степени	
д-р биол. наук	доктор биологических наук
д-р с.-х. наук	доктор сельскохозяйственных наук
д-р техн. наук	доктор технических наук
канд. с.-х. наук	кандидат сельскохозяйственных наук
канд. техн. наук	кандидат технических наук
канд. хим. наук	кандидат химических наук
Учёные звания	
доц.	доцент
проф.	профессор

Приложение Г

Пример оформления структурного элемента курсового проекта «Содержание»

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ 3
ВВЕДЕНИЕ 5
1 Теоретическая часть 7
1.1 Анализ существующих методов выявления сетевых угроз 7
1.2 Методы обучения моделей для выявления сетевых угроз 10
1.3 Современные архитектуры систем обнаружения вторжений и их классификация 14
1.4 Переход к разработке архитектуры системы обнаружения нелегитимного трафика 17
2 Практическая часть 23
2.1 Разработка архитектуры двухкомпонентной системы 23
2.2 Реализация компонента перехвата и первичной классификации (инспектор) 40
2.3 Реализация компонента анализа угроз и генерации рекомендаций 53
2.4 Объединение компонентов в единое приложение 63
2.5 Тестирование, оценка эффективности и практические сценарии применения 73
2.6 Защита компонентов системы от компрометации 84
3 Оценка эффективности предложенных решений и разработка рекомендаций по внедрению 89
3.1 Методика и показатели оценки качества 89
3.2 Результаты тестирования и анализ производительности 91
3.3 Рекомендации по внедрению и масштабированию системы 94
ЗАКЛЮЧЕНИЕ 98
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 100
ПРИЛОЖЕНИЕ А 101
ПРИЛОЖЕНИЕ Б 102
ПРИЛОЖЕНИЕ В 103
ПРИЛОЖЕНИЕ Г 104
ПРИЛОЖЕНИЕ Д 105
ПРИЛОЖЕНИЕ Е 106
ПРИЛОЖЕНИЕ Ж 107
ПРИЛОЖЕНИЕ З 108

Рисунок 1 – Пример оформления структурного элемента курсового проекта «Содержание»

Приложение Д

Пример оформления структурного элемента «Введение» курсового проекта на тему «Разработка ПО по идентификации USB-носителя при мгновенном разъединении с компьютерной системой»

ВВЕДЕНИЕ

В современном мире смартфоны, работающие на системе Android, стали неотъемлемой частью нашей жизни. Они хранят огромные объемы конфиденциальной информации, включая банковские реквизиты, личные данные и другую важную информацию. Однако вместе с повсеместным использованием мобильных устройств растет и угроза кибербезопасности, связанная с ними. Одна из наиболее распространенных проблем — это вредоносные приложения, которые могут похищать данные, отслеживать действия пользователей или вымогать деньги.

Защита мобильных устройств от злонамеренных атак является первостепенной задачей для обеспечения конфиденциальности и безопасности пользователей. События безопасности, такие как атаки вредоносного ПО, попытки взлома и несанкционированный доступ, представляют собой серьезные угрозы, которые могут привести к утечке конфиденциальных данных, нарушению конфиденциальности и значительным финансовым потерям.

Для эффективного противодействия этим угрозам необходимы надежные средства анализа событий безопасности, способные точно идентифицировать и классифицировать злонамеренные действия. Традиционные методы анализа безопасности, такие как сигнатуры вредоносного ПО и эвристические подходы, часто оказываются недостаточными для борьбы с изощренными угрозами.

Для защиты смартфонов от таких угроз необходимы эффективные меры безопасности. Одна из многообещающих областей, которая может повысить возможности обнаружения вредоносных программ, – это машинное обучение.

Машинное обучение позволяет системам обучаться на основе данных и распознавать закономерности, которые могут быть незаметны для человека.

Объектом исследования в данной работе являются средства обнаружения вредоносных Android приложений.

Предметом исследования являются методы и подходы обнаружения вредоносного ПО с использованием методов машинного обучения.

Для достижения поставленной цели в работе были поставлены следующие задачи:

– исследовать принципы работы Android-приложений, основные функции приложений и всей системы Android;

– проанализировать существующие виды атак при помощи вредоносных приложений и методы зашиты от них;

– разработать модель машинного обучения, которая обнаруживает вредоносные приложения и будет устойчива к состязательным атакам на этапе обучения;

– разработать основные компоненты программного обеспечения по выявлению вредоносных приложений.

Приложение Е

Пример оформления структурного элемента «Список использованных источников»

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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

2. Приказ Минобразования РФ от 19 декабря 2013 г. N9 1367 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета. программам магистратуры». – URL: http://www. consullant.ru/ document/cons_doc_LAW_159671/(дата обращения: 04.08.2016).

3. ISO 25964-1:2011. Information and documentation – Thesauri and interoperabdity with other vocabularies — Part 1: Thesauri for information retrieval. – URL: http://www.iso.org/iso/catalogue detail.htm?csnumber=53657 (дата обращения: 20.10.2016).

4. Литвиненко, Н. А. Л64 Технология программирования на C++. Win32 API-приложения. – Санкт-Петербург: БХВ-Петербург, 2010. – 288 с.: ил. – (Учебное пособие)

5. Пирогов, В. Ю. Ассемблер для Windows / В. Ю. Пирогов. – Москва: БХВ-Петербург, 2007. – 896 с

6. Рихтер Дж. Windows для профессионалов: создание эффективных Win32 приложений с учетом специфики 64-разрядной версии Windows / Пер. с англ. – 4-е изд. – Санкт-Петербург: Питер; Москва: Издательство «Русская Редакция»; 2008. – 720 стр.: ил.

7. Руссинович, Марк. Внутреннее устройство Microsoft Windows. Основные подсистемы ОС / Марк Руссинович. – Москва: Питер, 2015. – 486 с.

8. Техническая документация Microsoft: [Электронный ресурс] – URL: https://docs.microsoft.com/ru-ru/. (Дата обращения: 25.05.2022).

Приложение Ж

Примеры оформления иллюстраций

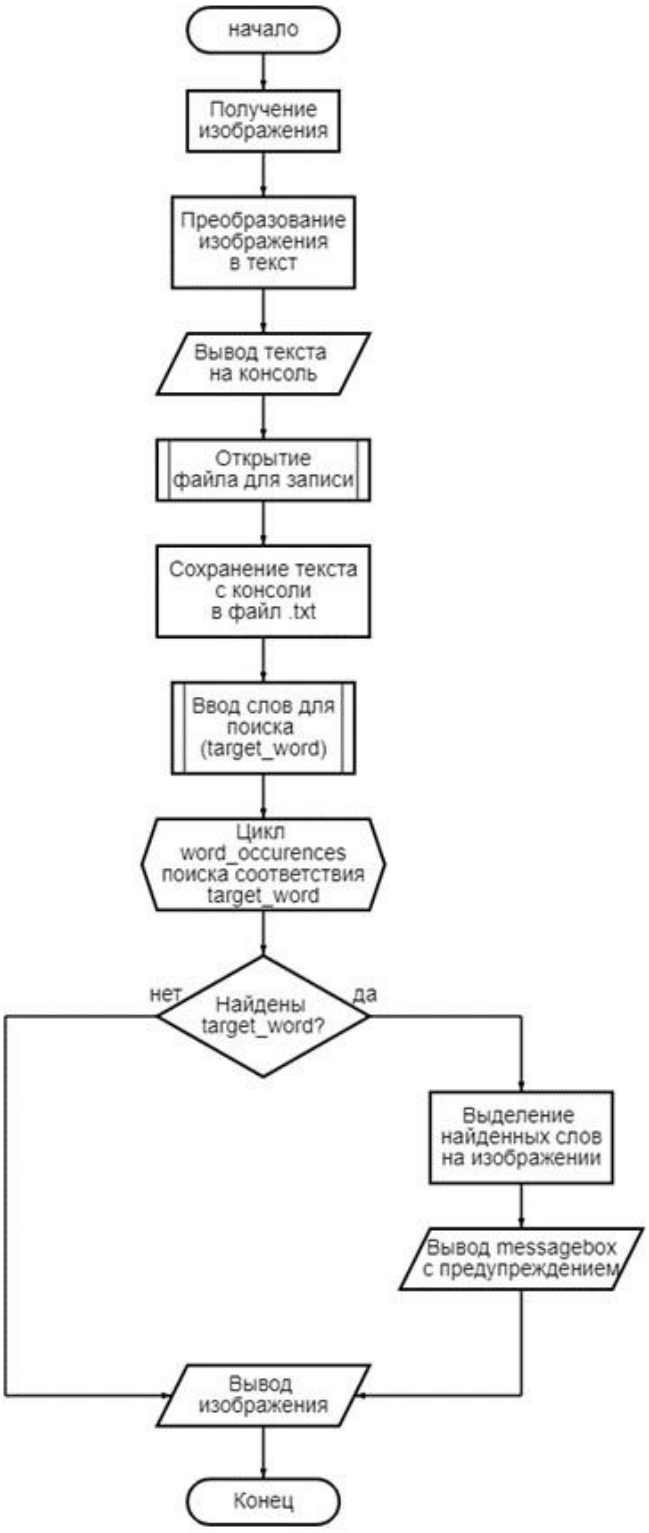


Рисунок 1 – Блок-схема программы

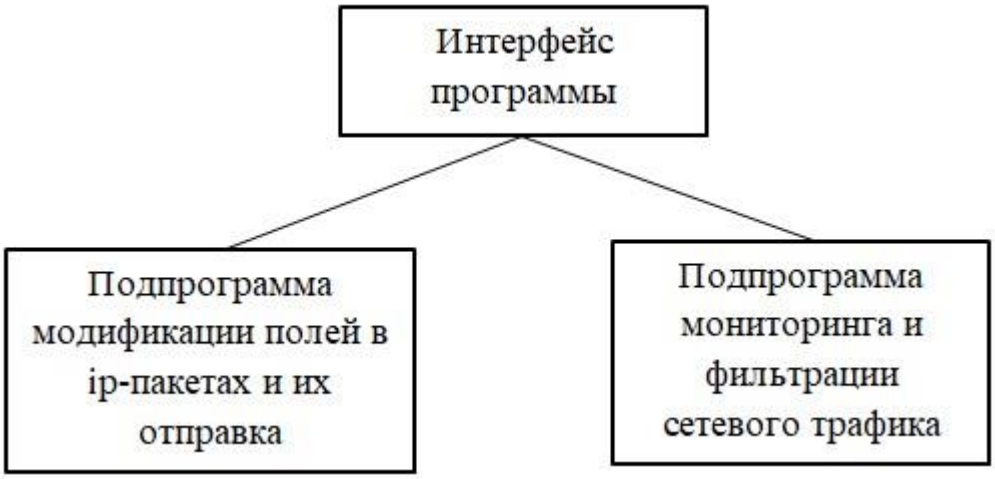


Рисунок 2 – Общая архитектура программы

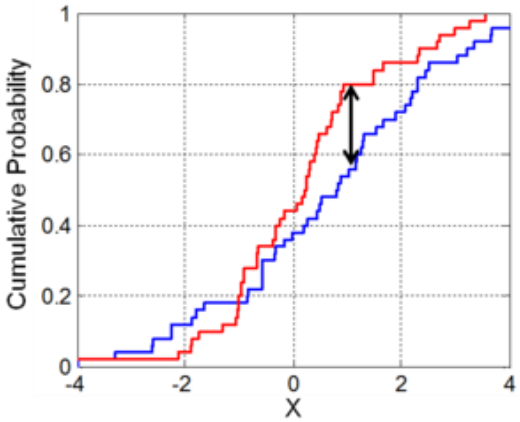


Рисунок 3 – Статистика теста Колмогорова-Смирнова

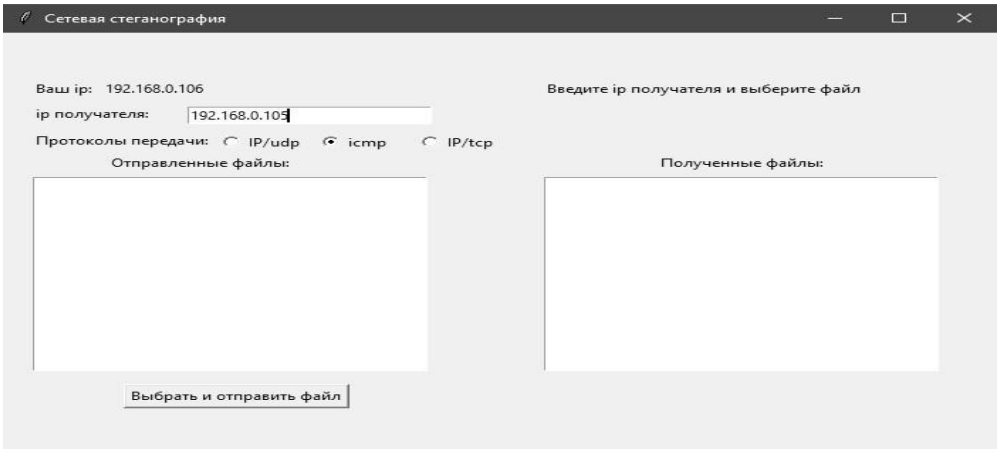


Рисунок 4 – Интерфейс программы

Приложение 3

Пример оформления таблиц и формул

Решение		
	Не отвергать H_0	Отвергнуть H_0
Справедлива H_0	Правильное с вероятностью $1-\alpha$	Ошибочное с вероятностью α
Справедлива H_1	Ошибочное с вероятностью β	Правильное с вероятностью $1-\beta$

Таблица 2 – Результаты исследования

Таблица 3.1 – Сравнение результатов моделей

Классификатор	**Точность**	**Полнота**	**Мера F1**	**ROC AUC**
KNN	0.8974	0.9264	0.9117	0.8914
Логистическая регрессия	0.8995	0.9666	0.9318	0.8682
Стохастический градиентный спуск	0.8991	0.9844	0.9398	0.8746

Продолжение Таблицы 3.1

Случайные леса	0.9005	0.9518	0.9254	0.9263
XGBoost	0.8992	0.9469	0.9224	0.9323
Градиентный бустинг	0.8979	0.99990	0.9461	0.8249
Метод опорных векторов	0.8977	0.9607	0.9281	0.8960

Пример 1:

$$W = AC, \qquad (1)$$

где:

B – первый сомножитель;

C – второй сомножитель.

Пример 2:

$$AUC_{ROC_{ovo}} = \frac{1}{c(c-1)} \sum_{j=1}^{c} \sum_{k>j} \left(AUC_{ROC}(j|k) + AUC_{ROC}(k|j) \right), \quad (2)$$

,

где c – количество классов, а $AUC(j|k)$ – метрика класса j относительно k, где j класс является положительным, а k – отрицательным.

Пример 3:

Сумма интенсивностей отказов рассчитываться следующим образом:

$$Y = \sum_{i=1}^{n} y_i, \quad (3)$$

где Y – интенсивность отказов комплекса средства защиты;

y_i – интенсивность отказа отдельного средства защиты (средства ИБ можно объединять в группы, избегая излишней детализации при необходимости).

Приложение И

Примеры оформления библиографических описаний различных источников

Статья в периодических изданиях и сборниках статей:

1. Намиот, Д. Е. Схемы атак на модели машинного обучения / Д. Е. Намиот // Internationaljournalofopeninformationtechnologies. – 2023. – Т. 11, № 5. – С. 68-86.

2. Zheng, J., Defending SDN-based IoT Networks Against DDoS Attacks Using Markov Decision Process / J. Zheng, A.S. Namin. // Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018 – 2018 – P. 4589 – 4592

Книги, монографии:

1. Бурков, А. Машинное обучение без лишних слов. / А. Бурков. – Санкт-Петербург: Питер, 2020. – 192 с.

2. Кохендерфер, М. Алгоритмы принятия решений. / М. Кохендерфер, Т. Уилер, К. Рэй. – Москва: ДМК Пресс, 2023. – 684 с.

Тезисы докладов, материалы конференций:

1. Подтопельный, В. В. Особенности использования марковских процессов принятия решений при моделировании атак на системы искусственного интеллекта / В. В. Подтопельный // Актуальные проблемы радиоэлектроники и телекоммуникаций: Материалы Всероссийской научно-технической конференции, Самара, 23–26 апреля 2024 года. – Самара: ООО «Артель», 2024. – С. 236–240.

2. Подтопельный, В. В. Особенности описания вектора сетевых атак с использованием Марковских процессов принятия решений / В. В. Подтопельный // Социотехнические и гуманитарные аспекты информационной безопасности: материалы V Всероссийской научно-практической конференции, Пятигорск, 25–27 апреля 2024 года. – Пятигорск: ФГБОУ ВО «Пятигорский государственный университет», 2024. – С. 178–184.

3. Ильяшов, А. Н. Анализ научных подходов к определению и прогнозированию компьютерных атак / А. Н. Ильяшов, В. В. Подтопельный, А. Г. Жестовский // Балтийский морской форум : материалы XII Международного Балтийского морского форума: в 6 т., Калининград, 30 сентября – 04 2024 года. Том 2. XII Национальная научная конференция с международным участием «Морская техника и технологии. Безопасность

морской индустрии». – Калининград: Балтийская государственная академия рыбопромыслового флота, Калининградский государственный технический университет, 2024. – С. 286–289.

Патентная документация согласно стандарту ВОИС:

1. BY (код страны) 18875 (N9 патентного документа) C1 (код вида документа). 2010 (дата публикации).

Электронные ресурсы:

1. Federated Learning Under Attack: Exposing Vulnerabilities through Data Poisoning Attacks in Computer Networks / E. Nowroozi, I. Haider, R. Taheri, M. Conti – Текст: электронный // arXiv: электронный журнал. – 2024. – URL: https://arxiv.org/abs/2403.02983 (дата обращения: 05.09.2024)
2. Federated Learning Under Attack: Exposing Vulnerabilities through Data Poisoning Attacks in Computer Networks / E. Nowroozi, I. Haider, R. Taheri, M. Conti [Электронный ресурс]. – arXiv, 2024. – Режим доступа: https://arxiv.org/abs/2403.02983, свободный (дата обращения: 05.09.2024)
3. Backdoor Attacks Against Dataset Distillation / Y. Liu, Z. Li, M. Backes, Y. Shen [Электронный ресурс]. – arXiv, 2024. – Режим доступа: https://arxiv.org/pdf/2107.09258, свободный (дата обращения: 06.09.2024)

Нормативные документы:

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

2 Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). – 83 с. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g, свободный (дата обращения: 25.07.2024).

3 ISO 25964-1:2011. Information and documentation – Thesauri and interoperabdity with other vocabularies – Part 1: Thesauri for information retrieval. – URL: http://www.iso.org/iso/catalogue detail.htm?csnumber=53657 (дата обращения: 20.10.2016).

Локальный электронный методический материал

Владислав Владимирович Подтопельный

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 5,3. Печ. л. 4,7.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1