МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)
КУРСОВОЕ ПРОЕКТИРОВАНИЕ 2

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Курсовое проектирование 2» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FBC60C
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью написания курсового проекта по специальности является углубление знаний по дисциплинам, формирование и развитие навыков самостоятельной научно исследовательской и практической деятельности, оформления полученных результатов в соответствии с принятыми стандартами, умения представить результаты работы в виде научного доклада и убедительно защитить их в дискуссии со специалистами

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.2к : Внедряет программные и программно-аппаратные средства защите информации в информационных системах	РД1	Умение	выделить основные угрозы информационной безопасности предприятия
			РД2	Навык	определение основных направлений на снижение возникающих угроз

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Развитие патриотизма и гражданской ответственности	Созидательный труд	Внимательность к деталям
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Взаимопомощь и взаимоуважение	Любознательность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Гражданственность	Внимательность к деталям
Формирование коммуникативных навыков и культуры общения		

Развитие умения эффективно общаться и сотрудничать	Гражданственность	Внимательность к деталям

2 Место дисциплины (модуля) в структуре ОПОП

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Безопасность операционных систем», «Безопасность систем баз данных», «Криптографические протоколы». На данную дисциплину опираются "Аудит информационной безопасности».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.В	10	7	51	0	0	0	1	50	201	КП

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Подготовка обзора по теме курсовой работы	РД1, РД2	0	0	0	36	выполнение заданий курсовой работы
2	Выполнение практической части курсовой работы	РД1, РД2	0	0	0	120	
3	Подготовка доклада и презентации по результатам выполнения курсовой работы.	РД1, РД2	0	0	0	24	
Итого по таблице			**0**	**0**	**0**	**180**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Подготовка обзора по теме курсовой работы.

Содержание темы: Сбор и изучение литературы по теме. Составление примерного содержания работы. Написание введения с описанием актуальности проблемы. Формулировка цели и задачи. Работа с литературой. Подготовка обзора по теме курсовой работы. Уточнение темы исследования с руководителем работы. Изучение прикладного программного обеспечения, необходимых для выполнения работы приборов и технических средств.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: самостоятельны работа по изучению литературы.

Виды самостоятельной подготовки студентов по теме: изучение литературы по тематике.

Тема 2 Выполнение практической части курсовой работы.

Содержание темы: Анализ литературы по теме исследования. Написание теоретической части курсовой работы. Выбор методов исследования. Выполнение практической части работы. Обсуждение результатов работы с научным руководителем.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: самостоятельны работа по изучению литературы и материалов для написания практической части.

Виды самостоятельной подготовки студентов по теме: изучение литературы и практики по тематике.

Тема 3 Подготовка доклада и презентации по результатам выполнения курсовой работы.

Содержание темы: Подготовка доклада и презентации по результатам выполнения курсовой работы. Оформление курсовой работы. Изучение правил оформления курсовой работы. Написание основной части курсовой работы, всесторонне раскрывающих тему, заключения. Формулировка кратких, но емких выводов по теме. Оформление курсовой работы по ГОСТу. Оформление списка литературы. Подготовка презентации и научного доклада.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: .

Виды самостоятельной подготовки студентов по теме: изучение литературы и практики по тематике.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Выбор и закрепление темы курсового проекта

В качестве объекта исследования в курсовом проекте может быть выбран любой хозяйствующий субъект. В то же время следует отдать предпочтение тому предприятию, организации, которая станет объектом дипломного проектирования. В курсовом проекте могут быть рассмотрены темы, которые условно можно подразделить на следующие типы:

– темы, отражающие комплекс вопросов построения и совершенствования системы информационной безопасности;

– темы, отражающие отдельные технологические и научые разработки и их применение в практической деятельности.

Тема курсового проекта выбирается студентом самостоятельно из примерной тематики, приведенной ниже либо может быть предложена студентом самостоятельно. Выбранная тема согласовывается с руководителем.

Студент на основании имеющейся информации может предложить тему, не входящую в рекомендованный перечень, но являющуюся актуальной для предприятия, организации или фирмы. При этом необходимо учитывать возможность получения соответствующей информации, необходимой для оценки состояния рассматриваемых вопросов на предприятии, а также наличие научной литературы и других источников информации, посвященной проблематике курсового проекта. Студент должен собрать и обработать необходимую информацию, проверить ее достоверность и согласованность.

Сбор информации

На этом этапе на основе исходных данных, приведенных в задании на выполнение курсового проекта (назначение разрабатываемого изделия или процесса, область его применения, условия эксплуатации, требования к техническим характеристикам и. т.д.) осуществляется сбор информации для выбора направления и методов решения поставленных задач. Для выполнения курсового проекта рекомендуются следующие источники информации:

1. Литературные источники: непериодические (учебники, монографии, справочники и.т.п.) и периодические издания. Основные непериодические издания, определяющие состояние научно-технической проблемы, как правило, предлагаются студенту руководителем курсового проектирования.

2. Нормативно-техническая документация: ГОСТы, Технические описания, Технические условия, инструкции по эксплуатации и т.д. Особенно важно найти нормативно-технические документы на аналоги и прототип разрабатываемого изделия или процесса.

3. Отчеты по научно-исследовательским работам. Как правило, доступ к ним обеспечивает руководитель курсового проектирования.

4. Описания патентов на изобретения. Рефераты патентов на изобретения содержатся в реферативных журналах, в журнале «Изобретения в России и за рубежом».

5. Электронные ресурсы: внутренние – библиотека ВВГУ, внешние – Интернет.

Индивидуальные задания к курсовому проектированию

Курсовая работа должна быть оформлена в соответствии с правилами оформления, приведенными ниже, ее структура и содержание должны соответствовать принятым правилам. По решению кафедры студенту может быть назначена публичная защита курсовой работы.

Требования к курсовой работе:

Структура курсовой работы Курсовая работа состоит из двух частей: пояснительной записки (текст курсовой работы) и приложений.

Пояснительная записка должна иметь следующую структуру:

1) титульный лист по принятому образцу;

2) оглавление с постраничной разметкой;

3) сокращения и обозначения – не обязательно;

4) введение с кратким обзором по рассматриваемому вопросу и обоснованием выбора направления курсовой работы (обзор можно вынести и в отдельную главу);

5) основной текст работы, который необходимо разбить на главы в соответствии с поставленными задачами или на разделы;

6) заключение;

7) список использованной литературы.

Пояснительная записка и приложения сшиваются и сдаются вместе. Изложение материала записки должно быть кратким, точным и технически правильным. Работа не должна иметь грамматических, стилистических, пунктуационных ошибок и опечаток. Повествование во всем тексте работы рекомендуется вести в безличной форме («можно

сделать вывод…» и т.п.), либо от третьего лица, либо от первого, но во множественном числе (т.к. подразумевается, что работа выполняется совместно с научным руководителем) – «Авторами предложено…», «В работе рассматривается…». Введение включает в себя следующее: - обоснование выбора темы работы, её актуальности и новизны; - определение целей и задач исследования, а также методов их решения; - анализ степени разработанности темы в отечественной и зарубежной литературе, краткий обзор исторического развития вопроса.

Объем введения не должен превышать 3-5 страниц (примерно 10% от основного текста). Актуальность работы. Чем важна, интересна в плане научного исследования Ваша работа. Вот именно только здесь, как и в любом реферате, допустимо небольшое художественное вступление в свободной форме. Цель. Какую цель планируется достичь написанием данной курсовой работы. Цель определяется одна, максимум - две. В цели упоминаются конкретные понятия. Время, скорость, цена, сила. Если понятия расплывчатые, например «эффективность» или «комфорт», нужно четко сказать, какой смысл в них вкладывается. Например, «под повышением эффективности работы алгоритма распознавания букв понимается сокращение времени работы при уровне ошибок, не превышающем 1%». Задачи. Перечислить какие задачи необходимо решить для достижения поставленной цели, с использованием каких методов.

Основная часть текста должна состоять из двух-трех глав и содержать теоретическую и практическую части. Каждая глава должна заканчиваться промежуточным выводом по данной главе.

Теоретическая часть включает в себя описание предметной области, объекта, предмета исследования, обзор литературы, программных продуктов, существующих алгоритмов, теоремы, обзор и ссылки на законы по защите информации и пр.

Практическая часть обязательна для курсовой работы студентов и должна содержать описание того, что именно было сделано автором, что, при необходимости, можно вынести на защиту.

Желательно, чтобы разделы были одинаковыми по объему. То же самое относится и к подразделам. В заключении формулируются общие выводы, отражается оценка работы, подводятся итоги по каждой выполненной задаче и работе в целом. Задачи. В результате работы были выполнены следующие задачи… Цели. После выполнения задач были достигнуты следующие цели… Заключительное слово – выводы. Объем заключения примерно равен объему введения и составляет не более 10% от всего основного текста.

Примерные темы курсовых работ:

1. Система нормативных актов РФ в области защиты от НСД
2. Угрозы и уязвимости современных автоматизированных систем
3. Классы защищённости современных автоматизированных систем и программно-аппаратных средств
4. Авторизация как процесс доступа
5. Межсетевые экраны как средство защиты информации от несанкционированного доступа
6. Анализ рынка средств усиления парольной защиты
7. Разработка элементов политики информационной безопасности для организации
8. Архитектура корпоративной системы защиты информации предприятия
9. Анализ современных способов разграничения доступа
10. Анализ защищённости внутренней инфраструктуры сети организации
11. Применения инструментальных средств анализа защищённости внутренней инфраструктуры сети
12. Анализ рынка программно-аппаратных средств защиты информации от несанкционированного доступа

13 Разработка генератора случайной последовательности на микроконтроллереSTM32

14 Выявление сетевых атак на основе методов машинного обучения

15 Безопасность управления устройством через системы мгновенных сообщений

16 Анализ проблем при внедрении систем физической защиты информации напредприятиях

17 Стратегические цели и основные направления. принципы и общие методыобеспечения обеспечения информационной безопасности в ……..

18 Автоматизированная информационная система как объект защиты в …….

19 Аудит информационной безопасности….

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843184 (Дата обращения - 05.09.2025)

2. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169702 (дата обращения: 31.05.2026)

3. Пушкин, П. Ю. Организационно-правовое обеспечение информационной безопасности : учебно-методическое пособие / П. Ю. Пушкин, Д. А. Головченко, Е. О. Карамышева. — Москва : РТУ МИРЭА, 2023. — 32 с. — ISBN 978-5-7339-1916-4. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/382658 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1898839 (дата обращения: 31.05.2026)
2. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2026. — 337 с. — (Среднее профессиональное образование). - ISBN 978-5-16-019432-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2221361 (дата обращения: 31.05.2026)

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры

Программное обеспечение:

- Microsoft Office 2010 Suites and Apps Russian

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

КУРСОВОЕ ПРОЕКТИРОВАНИЕ 2

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ПКВ-2 : Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.	ПКВ-2.2к : Внедряет программные и программно-аппаратные средства защите информации в информационных системах

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ПКВ-2 «Способен разрабатывать модели угроз безопасности и формировать требования к защите информации в организации.»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ПКВ-2.2к : Внедряет программные и программно-аппаратные средства защите информации в информационных системах	РД 1	Умение	выделить основные угрозы информационной безопасности предприятия	выполнение задания на курсовую работу
	РД 2	Навык	определение основных направлений на снижение возникающих угроз	выполнение задание курсовой работы

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения	Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
		Текущий контроль	Промежуточная аттестация
Очная форма обучения			

РД1	Умение : выделить основные угрозы информационной безопасности предприятия	1.1. Подготовка обзора по теме курсовой работы	Курсовая работа	Защита проекта
		1.2. Выполнение практической части курсовой работы	Курсовая работа	Защита проекта
		1.3. Подготовка доклада и презентации по результатам выполнения курсовой работы.	Курсовая работа	Защита проекта
РД2	Навык : определение основных направлений на снижение возникающих угроз	1.1. Подготовка обзора по теме курсовой работы	Курсовая работа	Защита проекта
		1.2. Выполнение практической части курсовой работы	Курсовая работа	Защита проекта
		1.3. Подготовка доклада и презентации по результатам выполнения курсовой работы.	Курсовая работа	Защита проекта

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Оценочное средство		Итого
Курсовая работа	Защита курсовой работы	
50		50
	50	50
50	50	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Темы курсовых работ

1. Система нормативных актов РФ в области защиты от НСД
2. Угрозы и уязвимости современных автоматизированных систем
3. Классы защищённости современных автоматизированных систем и программно-аппаратных средств
4. Авторизация как процесс доступа
5. Межсетевые экраны как средство защиты информации от несанкционированного доступа
6. Анализ рынка средств усиления парольной защиты
7. Разработка элементов политики информационной безопасности для организации
8. Архитектура корпоративной системы защиты информации предприятия
9. Анализ современных способов разграничения доступа
10. Анализ защищённости внутренней инфраструктуры сети организации
11. Применения инструментальных средств анализа защищённости внутренней инфраструктуры сети
12. Анализ рынка программно-аппаратных средств защиты информации от несанкционированного доступа
13 Разработка генератора случайной последовательности на микроконтроллереSTM32
14 Выявление сетевых атак на основе методов машинного обучения
15 Безопасность управления устройством через системы мгновенных сообщений
16 Анализ проблем при внедрении систем физической защиты информации напредприятиях
17 Стратегические цели и основные направления. принципы и общие методыобеспечения обеспечения информационной безопасности в ……..
18 Автоматизированная информационная система как объект защиты в …….
19 Аудит информационной безопасности….

Краткие методические указания

Тема курсовой работы может зависить от выбранного объекта исследования и согласовывается с руководителем

Шкала оценки

Оценка	Баллы*	Описание
5	40-50	В работа соответсвует заданию, тема раскрыта
4	20-39	В работа соответсвует заданию, тема раскрыта, но используются устаревшие данные
3	10-19	В работа соответсвует заданию, тема раскрыта не полностью
2	0-9	В работа не соответсвует заданию или тема не раскрыта

5.2 защита проекта

Какие факторы определили выбор именно вашего предприятия для исследования?

Какие конкретно угрозы информационной безопасности выявлены в ходе анализа?

Что представляет собой понятие "окно уязвимости"? Приведите конкретные примеры из вашего исследования.

Почему выбранные вами информационные потоки являются критически важными для функционирования предприятия?

Какой способ документирования полученных результатов оказался наиболее эффективным?

Чем обусловлен выбор методов анализа угроз информационной безопасности?

Краткие методические указания

Для ответов на поставленные вопросу студенту необходимо максимально полно ознакомиться как с практическим, так и с теоретическими аспектами исследования

Шкала оценки

Оценка	Баллы*	Описание
5	40-50	Раскрыты ответы на вопросы
4	20-39	Ответы корректные, но не полные не может обосновать выбранную позицию
3	10-19	Ответы ошибочны
2	0-9	Ответы на вопрос не даны