МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф.,д.т.н.,доц.
(должность, уч. степень, звание)
С.В. Беззатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Управление информационной безопасностью»
(Название дисциплины)

Код направления	10.05.05
Наименование направления/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Технологии защиты информации в правоохранительной сфере
Форма обучения	очная

Санкт-Петербург– 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

проф.,д.т.н.,доц.	«24» июня 2021 г.		С.В. Беззатеев
должность, уч. степень, звание		подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34
«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34

проф.,д.т.н.,доц.	«24» июня 2021 г.		С.В. Беззатеев
должность, уч. степень, звание		подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.05(01)

доц.,к.т.н.,доц.		24.06.21	В.А. Мыльников
должность, уч. степень, звание		подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц.,к.э.н.,доц.		24.06.21	Г.С. Армашова-Тельник
должность, уч. степень, звание		подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Управление информационной безопасностью» входит в базовую часть образовательной программы подготовки обучающихся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» направленность «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-5 «способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности»,

ОК-8 «способность принимать организационно-управленческие решения»;

профессиональных компетенций:

ПК-3 «способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации»,

ПК-13 «способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов»,

ПК-14 «способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов»,

ПК-18 «способность разрабатывать предложения по совершенствованию системы управления безопасностью информации».

Содержание дисциплины охватывает круг вопросов, связанных с изучением методов и средств управления информационной безопасностью (ИБ) в организации, а также изучением основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов. Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целями изучения дисциплины «Управление информационной безопасностью» является: формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ; развитие способностей по использованию существующей системы управления информационной безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-5 «способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности»:

знать - подходы к интеграции СУИБ в общую систему управления предприятием; основные стандарты, регламентирующие управление ИБ;
уметь - анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ;
владеть навыками - навыками управления информационной безопасностью простых объектов;
иметь опыт деятельности - разрабатывать и внедрять СУИБ и оценивать ее эффективность;

ОК-8 «способность принимать организационно-управленческие решения»:

знать - современные подходы к управлению ИБ и направлениях их развития; принципы построения СУИБ;
уметь - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
владеть навыками - терминологией и процессным подходом построения систем управления ИБ;
иметь опыт деятельности – в разработке предложений по совершенствованию системы управления безопасностью информации;

ПК-3 «способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации»:

знать - принципы разработки процессов управления ИБ
уметь - применять процессный подход к управлению ИБ в различных сферах деятельности;
владеть навыками - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
иметь опыт деятельности – в применении технологий получения, накопления, хранения, обработки, анализа, интерпретации и использования информации;

ПК-13 «способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов»:

знать - современные подходы к управлению ИБ и направлениях их развития; принципы построения СУИБ;
уметь - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
владеть навыками - терминологией и процессным подходом построения систем управления ИБ;
иметь опыт деятельности – в разработке предложений по совершенствованию системы управления безопасностью информации;

ПК-14 «способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов»:

знать - современные подходы к управлению ИБ и направлениях их развития; принципы построения СУИБ;
уметь - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
владеть навыками - терминологией и процессным подходом построения систем управления ИБ;
иметь опыт деятельности – в разработке предложений по совершенствованию системы управления безопасностью информации;

ПК-18 «способность разрабатывать предложения по совершенствованию системы управления безопасностью информации»:
знать - взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;
уметь - используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
владеть навыками - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом;
иметь опыт деятельности - практически решать задачи формализации разрабатываемых процессов управления ИБ.

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Введение в специальность
- Производственная (технологическая) практика
- Психология воздействия
- Психология профессиональной деятельности
- Криминалистика
- Теория информации
- Защита от вредоносных программ
- Организационная защита информации
- Теория информационной безопасности
- Методология защиты информации
- Защита информации в распределенных информационных системах
- Производственная практика

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Комплексные системы защиты информации в правоохранительной сфере
- Научно-технический семинар
- Производственная преддипломная практика

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№9
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час., ***В том числе***	68	68
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)	17	17
Экзамен, (час)	36	36
Самостоятельная работа, всего	4	4
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 9					
Раздел 1. Основы управления ИБ Тема№ 1. Введение Тема № 2. Базовые вопросы управления ИБ	3				

Тема № 3. Стандартизация в области управления ИБ					
Раздел 2. Системы управления ИБ Тема№ 4. Процессный подход Тема № 5. Область деятельности СУИБ Тема № 6. Ролевая структура СУИБ Тема № 7. Политика СУИБ	4		8		
Раздел 3. Основы управления рисками ИБ Тема № 8. Рискология ИБ Тема № 9. Анализ рисков ИБ	4		8		
Раздел 4. Процессы управления ИБ Тема№ 10. Основные процессы СУИБ Тема № 11. Внедрение разработанных процессов Тема№ 12. Внедрение мер (контрольных процедур) по обеспечению ИБ Тема№ 13. Процесс «Управление инцидентами ИБ» Тема№ 14. Процесс «Обеспечение непрерывности ведения бизнеса» Тема№ 15. Эксплуатация и независимый аудит СУИБ	6		18		4
Выполнение курсовой работы				17	
Итого в семестре:	17		34	17	4
Итого:	17	0	34	17	4

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
Раздел 1. Основы управления ИБ	Тема№ 1. Введение Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Тема № 2. Базовые вопросы управления ИБ Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Тема № 3. Стандартизация в области управления ИБ Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, BS 25999 и др.).
Раздел 2. Системы управления ИБ	Тема№ 4. Процессный подход Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов. Тема № 5. Область деятельности СУИБ Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа). Тема № 6. Ролевая структура СУИБ Понятие роли. Использование ролевого

	принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.). Тема № 7. Политика СУИБ Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.
Раздел 3. Основы управления рисками ИБ	Тема № 8. Рискология ИБ Основные определения и положения рискологии. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Тема № 9. Анализ рисков ИБ Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.
Раздел 4. Процессы управления ИБ	Тема№ 10. Основные процессы СУИБ. Обязательная документация СУИБ Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности». Тема № 11. Внедрение разработанных процессов. Документ «Положение о применимости» 10 Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа. Тема№ 12. Внедрение мер (контрольных процедур) по обеспечению ИБ Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками. Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик. Тема№ 13. Процесс «Управление инцидентами ИБ» Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Тема№ 14. Процесс «Обеспечение непрерывности ведения бизнеса» Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Тема№ 15. Эксплуатация и независимый аудит СУИБ Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисцип-лины
Учебным планом не предусмотрено				
		Всего:		

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
	Семестр 9			
1	Выбор области действия СУИБ	4	2	2
2	Разработка Политики ИБ	4	2	2
3	Разработка методики оценки рисков ИБ	4	2	3
4	Проведение оценки рисков ИБ системы	4	2	3
5	Разработка плана проведения внутреннего аудита ИБ	4	2	4
6	Проведение внутреннего аудита ИБ	4	2	4
7	Планирование работы службы безопасности предприятия	3	1	4
8	Организация работы службы безопасности предприятия	3	2	4
9	Контроль за работой службы безопасности предприятия	4	2	4
	Всего:	34	17	

4.5. Курсовое проектирование (работа)

Цель курсовой работы: освоение способов и методов проектирования информационных систем и систем защиты в них, обеспечивающих решение следующих задач: разграничение и управление доступом, регистрация и учет пользователей системы и их действий, обеспечение целостности данных в системе.

Часов практической подготовки: 17

Примерные темы заданий на курсовую работу приведены в разделе 10 РПД.

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 9, час
1	2	3
Самостоятельная работа, всего	4	4
изучение теоретического материала дисциплины (ТО)		
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	4	4
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.05В 75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	(74)
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с	(8)
Х Я 47	Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.	(9)
	http://e.lanbook.com/books/element.php?pl1_id=3032 Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 М 48	Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с.	(5)
004 Р 98	Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с.	(10)
	http://e.lanbook.com/books/element.php?pl1_id=4959 Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 с.	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
http://www.intuit.ru/studies/courses/10/10/info	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-5 «способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности»	
4	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности (технологическая)
6	Психология воздействия
8	Психология профессиональной деятельности
9	Управление информационной безопасностью
ОК-8 «способность принимать организационно-управленческие решения»	
6	Международный бизнес
9	Прикладная экономика
9	Управление информационной безопасностью
ПК-3 «способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации»	

4	Криминалистика
5	Теория информации
8	Защита от вредоносных программ
8	Организационная защита информации
8	Защита и обработка документов ограниченного доступа
8	Криминология
9	Технологии защищенного документооборота
9	Управление информационной безопасностью
ПК-13 «способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов»	
4	Программирование. Методы и технологии программирования
5	Математические основы обработки информации
6	Гражданский процесс
7	Информационное право
8	Программирование. Языки программирования
8	Правовая защита информации
9	Управление информационной безопасностью
ПК-14 «способность планировать и организовывать служебную деятельность подчиненных, осуществлять контроль и учет ее результатов»	
4	Экономика
9	Научно-технический семинар
9	Управление информационной безопасностью
10	Научно-технический семинар
ПК-18 «способность разрабатывать предложения по совершенствованию системы управления безопасностью информации»	
6	Теория информационной безопасности
7	Методология защиты информации
8	Защита информации в распределенных информационных системах
8	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
9	Управление информационной безопасностью
10	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	

$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \le К \le 84$	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \le К \le 69$	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$К \le 54$	«неудовлетво рительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	1. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни. 2. Что понимается под системой безопасности? 3. Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ? 4. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процесами? 5. Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ. 6. Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ? 7. Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию. 8. Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со

	стороны злоумышленников? 9. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности? 10. Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими? 11. Назовите основные способы неправомерного овладения конфиденциальной информацией. 12. Какие основные понятия рассматриваются в Законе РФ "Об информации, информатизации и защите информации"? 13. Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации. 14. Дайте определение и перечислите основные с пособы НСД к конфиденциальной информации. Охарактеризуйте обобщенную модель взаимодействия способов НСД иисточников конфиденциальной информации. 15. Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации? Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии. 16. Дайте определение информационной безопасности, прокомментируйте его составляющие. Перечислите основные категории информационной безопасности. 17. Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации? 18. Какие Вам известны американские законы, напрямую связанные с ИБ? Что можно сказать о законодательстве ФРГ по вопросам ИБ? 19. Что такое защита информации? 20. Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется? 21. Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь? 22. Охарактеризуйте понятия доступности, целостности и конфиденциальности информации. 23. Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации? 24. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне. 25. Прокомментируйте основные составляющие информационной безопасности РФ. 26. Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности? 27. Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности? Приведите примерный список решений верхнего уровня политики безопасности. 28. Перечислите важнейшие задачи обеспечения информационной безопасности РФ. 29. Что такое угрозы утечки информации? Какие угрозы называются преднамеренными и случайными? 30. Что такое программа безопасности, ее уровни. 31. Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности. 32. Что такое канал НСД? Назовите типовые причины их возникновения. 33. Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками? 34. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность. 35. Назовите основные способы добывания конфиденциальной информации злоумышленником. 36. В чем заключается основная специфика процедурного уровня ИБ? Перечислите основные классы мер процедурного уровня ИБ. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?

	37. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны? 38. Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации. 39. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС. 40. В чем специфика деятельности ФСТЭК России? 41. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз. 42. Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня. 43. Почему уровень ИБ в России в настоящее время не соответствует жизненно важным потребностям личности, общества и государства и к акие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России? 44. Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность. 45. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны? 46. Раскройте содержание политических, Экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ. 47. Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО? 48. Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация? 49. Дайте определение защищаемой информации и охарактеризуйте ее основные признаки. 50. Охарактеризуйте основные угрозы целостности конфиденциальной информации. 51. Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты? 52. Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности 53. Перечислите основные угрозы конфиденциальности информации. 54. Прокомментируйте возможности биометрической идентификации (аутентификации). 55. Перечислите основные виды конфиденциальной информации, нуждающейся в защите. 56. Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ. 57. В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа? 58. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте о сновные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне? 59. Что такое защита от разглашения? 60. Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности. 61. Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? 62. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации. 63. В чем заключается основная задача аудита, как сервиса безопасности? 64. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

	65. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации. 66. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует? 67. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных? 16 68. Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС. 69. Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	1.Подсистема защиты АС «Отдел кадров» 2.Подсистема защиты АС «Магазин цифровых товаров» 3.Подсистема защиты АС «Медицинский центр» 4.Подсистема защиты АС «Комплекс Бар» 5.Подсистема защиты АС «Багетная Мастерская» 6.Подсистема защиты АС «Регистратура Краевой больницы» 7.Подсистема защиты АС «Салон сотовой связи» 8.Подсистема защиты АС «Автосалон» 9. Подсистема защиты АС «Выставочный центр» 10.Подсистема защиты АС «Магазин электроники» 11.Подсистема защиты АС «Парфюмерия» 12.Подсистема защиты АС «Магазин бытовой техники» 13.Подсистема защиты АС «Media Market» 14.Подсистема защиты АС «Магазин запчастей» 15.Подсистема защиты АС «Магазин музыкальных инструментов» 16.Подсистема защиты АС «Зоопарк» 17.Подсистема защиты АС «Автовокзал» 18.Подсистема защиты АС «Бытовые услуги» 19.Подсистема защиты АС «Молочная продукция» 20.Подсистема защиты АС «Комплектующие мототехники» 21.Подсистема защиты АС «Абитуриенты» 22.Подсистема защиты АС «Телефонный справочник» 23.Подсистема защиты АС «Пожарная охрана» 24.Подсистема защиты АС «Библиотека» 25.Подсистема защиты АС «Магазин-склад моющих средств» 26.Подсистема защиты АС «Аудиотехника» 27.Подсистема защиты АС «Салон сотовой связи» 28.Подсистема защиты АС «Спорттовары»

	29.Подсистема защиты АС «Автосервис» 30.Подсистема защиты АС «Видео прокат» 31.Подсистема защиты АС «Магазин компьютерной техники» 32.Подсистема защиты АС «Компьютерный сервис»

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	1. Разработка модели угроз ИБ конкретного объекта. 2. Разработка модели нарушителя ИБ конкретного объекта. 3. Разработка политики ИБ конкретного объекта. 4. Оценка рисков ИБ конкретного объекта. 5. Проектирование отдельного процесса СУИБ конкретного объекта. 6. Разработка структуры СУИБ конкретного объекта. 7. Разработка плана проведения аудита ИБ конкретного объекта.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Целями изучения дисциплины «Управление информационной безопасностью» является: формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ; развитие способностей по использованию существующей системы управления информационной безопасности.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

– Изложение лекционного материала;

– Представление теоретического материала преподавателем в виде слайдов;

– Освоение теоретического материала по практическим вопросам;

– Список вопросов по теме для самостоятельной работы студента (Табл.21).

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

– В задании должно быть четко сформулирована задача, выполняемая в ЛР;

– Описаны входные и выходные данные для проведения ЛР;

– ЛР должна выполняться на основе полученных теоретических знаниях;

– Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;

– ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;

– Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

– Постановка задачи;

– Входные и выходные данные;
– Содержание этапов выполнения;
– Обоснование полученного результата (вывод);
– Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

– Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
– ЛР должна соответствовать структуре и форме отчета представленной выше;
– ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);

Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

Методические указания для обучающихся по прохождению курсового проектирования/ работы

Курсовой проект/ работа проводится с целью формирования у обучающихся опыта комплексного решения конкретных задач профессиональной деятельности.

Курсовой проект/ работа позволяет обучающемуся:

– систематизировать и закрепить полученные теоретические знания и практические умения по профессиональным учебным дисциплинам и модулям в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;
– применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;
– углубить теоретические знания в соответствии с заданной темой;
– сформировать умения применять теоретические знания при решении нестандартных задач;
– приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;
– сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;
– сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;
– развить профессиональную письменную и устную речь обучающегося;
– развить системное мышление, творческую инициативу, самостоятельность, организованность и ответственность за принимаемые решения;
– сформировать навыки планомерной регулярной работы над решением поставленных задач.

Структура пояснительной записки курсовой работы / проекта

Изучение курса «Управление информационной безопасностью» заканчивается выполнением курсовой работы по проектированию баз данных различного назначения. Содержание курсового проекта излагается в программе курса для соответствующих специальностей и должно соответствовать приведенному в приложении заданию на курсовое проектирование. Бланк задания на курсовое проектирование должен быть подшит в пояснительную записку перед введением.

Отчёт по курсовой работе оформляется каждым студентом индивидуально и содержит описание лично выполненной работы, которая включает:

- титульный лист;
- индивидуальное задание;
- пояснительную записку;

- программы и спецификации на электронном носителе;

Пояснительная записка содержит разделы:

- содержание с указанием страниц и разделов;
- введение;
- основную часть;
- список литературы;
- приложения.

В содержании должна быть отражена структура пояснительной записки. Введение должно характеризовать ту сферу человеческой деятельности, для которой будет проектироваться приложение.

Список литературы, помимо книг, использованных при работе над курсовой работой, должен включать ссылки на все электронные материалы, использованные при проектировании.

Листинги программ с подробными комментариями должны быть приведены в приложениях.

Задачи курсового проекта:

-титульный лист;
-задание на курсовую работу;
-аннотация;
-содержание;
-введение;
-основные разделы, предусмотренные заданием;
-заключение;
-список используемой литературы (список источников);
-приложения.

Титульный лист является первым листом пояснительной записки и должен быть оформлен на печатном бланке.

Задание на курсовое проектирование как лист утверждения оформляется на печатном бланке и **не нумеруется**, предусматривается двусторонняя печать листа задания. В задании указываются:

-дисциплина «Управление информационной безопасностью»;
-группа, фамилия, имя, отчество студента;
-тема курсовой работы;
-исходные данные для разработки;
-в разделе "Пояснительная записка" перечисляются подлежащие разработке вопросы;
-дата выдачи и срок окончания курсовой работы;
-фамилия, имя, отчество преподавателя-руководителя.

Аннотацию (лист 3) размещают на отдельной пронумерованной странице с заголовком АННОТАЦИЯ и **не нумеруют** как раздел. В аннотации кратко излагают назначение, содержание и другие особенности курсовой работы. Аннотация носит пояснительный и рекомендательный характер.

Оглавление (лист 4) отражает состав курсового проекта, может быть сформировано в автоматическом режиме. Содержание разделов пояснительной записки представлено перечнем подразделов и пунктов.

Во **Введении** (лист 5) обосновывается и доказывается важность рассматриваемой темы для выбранной специализации: проводится аналитический обзор современных тенденций в области автоматизации обработки данных и их защиты.

Назначение и цели создания системы - указывается вид автоматизируемой деятельности (указать, для управления какими процессами предназначена система), перечень объектов автоматизации, а также описываются цели создания системы защиты данной АС.

Анализ предметной области. Проводится анализ объекта автоматизации и выявление перечня задач, подлежащих автоматизации. При анализе предметной области необходимо собрать и обобщить материал, всесторонне характеризующий деятельность объекта

автоматизации, ознакомиться с перспективами развития объекта автоматизации, обосновать необходимость применения ИС, выявить возможности автоматизации информационных процессов для повышения эффективности, надежности и снижения трудоемкости работ. В процессе анализа предметной области необходимо определить класс защищенности информации в ИС с целью разработки требуемого уровня защиты информации.

В **Описании постановки задачи** должны содержаться следующие сведения:

- характеристики комплекса задач, решаемых в ИС, входная информация, выходная информация;
- защита информации от НСД и определение класса защищенности в соответствии с требованиями ГТК (Государственной Технической Комиссии РФ);
- описание подсистем защиты информации.

Анализ методов решения *– это разработка основных решений по техническому, программному и информационному обеспечению автоматизированной системы. Также должен быть проведен анализ методов решения задачи защищенности ИС (ограничение и разграничение доступа, разделение привилегий на доступ к информации, криптографическое преобразование информации). При этом необходимо рассмотреть использование различных программно-аппаратных способов ЗИ. Необходимо проанализировать организационные мероприятия, необходимые для защиты от НСД и произвести обоснование выбора среды программирования для решения поставленной задачи.*

Информационная модель системы - модель объекта автоматизации, описывающая его существенные параметры, связи между ними, входы и выходы объекта. Она позволяет моделировать возможные состояния объекта путём подачи на модель информации о входных величинах.

Важным этапом разработки любой информационной системы является проектирование - построение модели реальных объектов, явлений или процессов с учетом их взаимосвязей. Информационная система является овеществлением модели, и правильность ее функционирования зависит от точности и непротиворечивости модели, построенной на этапе проектирования.

При создании моделей следует быть особенно внимательным, поскольку исправление ошибок, допущенных на этом этапе, требует самых больших затрат. Концептуальная (инфологическая) модель предметной области после словесного описания чаще всего представляется в виде графической схемы (ER-диаграммы). Целью построения инфологической модели является подробное и точное описание данных, их взаимодействия и методов их обработки. Способы хранения данных, применяемые средства СУБД, языки программирования и все, что имеет отношение к конкретной реализации программы, при построении инфологической модели не упоминается. Это дает возможность разработчику в процессе проектирования сложных систем выбирать для реализации отдельных частей задачи наиболее подходящие средства. Такой подход, не учитывающий применения конкретных программных средств или технологий, позволяет привлекать к разработке концептуальных (инфологических) моделей конечных пользователей, которые могут оперировать объектами и понятиями своей предметной области. Концептуальная модель строится отдельно для каждого пользовательского представления с последующим объединением локальных моделей в глобальную. При объединении производится анализ сущностей пользовательских представлений на предмет их идентичности и производится их объединение, аналогично поступают со связями.

Итак, проектирование базы данных осуществляется поэтапно. На **первом этапе** происходит **концептуальное проектирование** - представление структуры данных при помощи различных технологий моделирования. Самая распространенная среди них - модель «сущность-связь», или ER-моделъ (Entity-relationship), предложенная П. Ченом в 1976 году.

Следующий после построения ER-диаграмм шаг в процессе проектирования базы данных состоит в построении набора предварительных отношений и указании предполагаемого первичного ключа для каждого отношения. Такое моделирование называется логическим. Итогом **второго этапа** - логического проектирования - является построенная **логическая**

модель данных, которая преобразуется из созданной на предыдущем шаге концептуальной модели. Логические модели данных могут быть различных типов, но наибольшее распространение получили сетевые, иерархические и реляционные модели. Выбор того или иного типа модели данных непосредственно связан с вопросом выбора системы управления базой данных по той причине, что СУБД, как правило, поддерживает только одну конкретную модель данных (курс дисциплины «Базы данных», тема «Реляционная модель данных»)

На третьем этапе происходит физическое проектирование, которое связано с выбором конкретной СУБД и проектированием структур данных с учетом особенностей хранения данных в выбранной СУБД. На этом этапе производится формирование набора таблиц (если используется реляционный тип модели данных), вырабатываются методики контроля **целостности** данных и методики **защиты данных**. Если используется реляционная СУБД, то для описания схемы БД используется язык DDL выбранной целевой СУБД. Пользовательские представления создаются в виде запросов к БД на языке SQL

По итогам этого этапа происходит оформление технического проекта.

Разработка программно-информационных компонентов системы - описание разработанных программных средств и баз данных, контрольные пример. При представлении физической реализации решения задачи необходимо описать словесно и представить графически алгоритм решения спроектированной задачи, представить и пояснить вид окон и элементов управления для всех режимов работы (ввод исходных данных, вывод результатов работы). Проектируемая информационная система должна обеспечить выполнение следующих требований:

- разрабатываемый интерфейс должен включать в себя средства редактирования всех используемых для расчета данных и быть простым и понятным в работе не только для разработчика, но и для обычного пользователя;
- система должна обладать максимальной гибкостью — возможность изменения любых настроек и параметров программы. И хотя данное требование в основном реализуется при реализации программы, основа этого должна быть заложена уже на этапе проектирования;
- необходимо ввести четкое разграничение прав доступа и отслеживать любое изменение данных с возможностью выявления даты и ответственного за введенные изменения;
- ввод данных для расчета должен быть максимально автоматизирован. Необходимо предусмотреть защиту от некорректного ввода данных во всех формах интерфейса. Если оператор не имеет представления о корректности введенных данных, то в результате возникает множество ошибок, которые приводят к неправильному результату.

В этом разделе должен быть представлен алгоритм работы системы и описаны программные модули и формы.

Инструкция по эксплуатации. Инструкция по эксплуатации указывает, какие операции, в каком порядке, с какой периодичностью следует выполнять системному администратору и пользователям системы. Однако нет необходимости подробно описывать в ней способ выполнения каждой из этих операций. Необходимо также упомянуть о требованиях техники безопасности.

Заключение. Перечисляются результаты проделанной работы, выводы по результатам разработки, дается заключение о качестве и полноте решения поставленной задачи. Высказываются соображения о направлениях развития разработки, путях дальнейшей автоматизации объекта, оценивается степень ее готовности к практическому использованию и перспективы развития.

Список используемых источников включает все информационные источники для выполнения курсового проекта (в т.ч. ГОСТы). В соответствии с ГОСТ 7.32-2001 список составляется в порядке появления ссылок в пояснительной записке.

Приложение. В приложения следует включать вспомогательный материал, необходимый для полноты изложения результатов проделанной работы в пояснительной записке, например:

- промежуточные математические доказательства, формулы, расчеты;
- таблицы вспомогательных данных;
- иллюстрации вспомогательного характера;
- тексты программ;
- руководства пользователя.

Каждое приложение должно начинаться с нового листа (страницы) с указанием в правом верхнем углу слова «Приложение» и номера арабскими цифрами и иметь тематический заголовок.

В тексте на все приложения даются ссылки.

Например, в Приложении **Техническое задание** должны быть отражены следующие сведения:

1. Полное наименование системы и её условное обозначение.
2. Требования к системе (например, к численности и квалификации персонала системы и режима его работы).
3. Требования безопасности.
4. Требования по эргономике и технической эстетике.
5. Требования по эксплуатации, техническому обслуживанию, ремонту.
6. Требования по сохранности информации.
7. Требования по видам обеспечения (математическое обеспечение).
8. Информационное обеспечение.
9. Программное обеспечение.
10. Техническое обеспечение.
11. Организационное обеспечение.

Требования к оформлению пояснительной записки курсовой работы / проекта

В виду принадлежности курсового проекта к дисциплинам связанным с информационными технологиями и электронно-вычислительными машинами пояснительная записка должна быть оформлена при помощи любого программного инструмента и распечатана на листах формата А4 (210×297 мм), листы должны быть пронумерованы и сшиты. Поля листа должны составлять левое 25 мм, верхнее и нижнее 20 мм, правое 15 мм. Текст записки должен быть набран удобочитаемым шрифтом по размеру и начертанию соответствующий «Times New Roman» в 14 пт. Межстрочный интервал должен соответствовать полуторному. В записке также должен быть предусмотрен карман для помещения в него диска с работоспособным приложением и всеми исходными текстами программ. Допускается помещать на дискету архив в формате zip или rar.

Полный листинг программы должен включать в себя распечатку всех файлов программ, из которых состоит проект. Формы проекта должны быть распечатаны в двух видах: в виде формы и в виде тестового файла. Все файлы форм должны быть сгруппированы в следующей последовательности: сначала форма в процессе разработки, затем форма в текстовом виде и в завершении текст модуля связанный с формой. В записке фрагменты текстов программы, а также тексты распечаток модуля и формы должны быть выполнены шрифтом «Courier New» размером 10 пт., через одинарный интервал.

Титульный лист записки должен быть оформлен в соответствии с образцом, приведенным в приложении №1.

Основные разделы курсовой работы:

По структуре курсовая работа практического характера состоит из:

введения, в котором раскрывается актуальность и значение темы, формулируются цели и задачи работы;

основной части, которая обычно состоит из двух разделов: в первом разделе содержатся теоретические основы разрабатываемой темы; вторым разделом является практическая часть, которая представлена расчётами, графиками, таблицами, схемами и т.п.;

заключения, в котором содержатся выводы и рекомендации относительно возможностей практического применения материалов работы;

списка используемой литературы;

приложений.

По структуре курсовая работа опытно-экспериментального характера состоит из:

введения, в котором раскрывается актуальность и значение темы, формулируются цели и задачи эксперимента;

основной части: в первом разделе содержатся теоретические основы разрабатываемой темы, даны история вопроса, уровень разработанности проблемы в теории и практике; вторым разделом является практическая часть, в которой содержится план проведения эксперимента, характеристики методов экспериментальной работы, обоснование выбранного метода, основные этапы эксперимента, обработка и анализ результатов опытно-экспериментальной работы;

заключения, в котором содержатся выводы и рекомендации относительно возможностей практического применения полученных результатов;

списка используемой литературы;

приложений.

Исходными данными для выполнения курсового проекта являются документы и материалы, собранные на предприятии или в организации (при прохождении практики при очной форме обучения или на рабочем месте студента при заочной форме обучения). Перечисленные выше тематики реализуются в виде курсовых проектов, имеющих практический или опытно-экспериментальный характер.

Студент разрабатывает и оформляет курсовую работу (проект) в соответствие с требованиями ЕСПД.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой