

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

Кафедра № 33

УТВЕРЖДАЮ  
Руководитель направления  
проф. д.т.н., доц.  
(должность, уч. степень, звание)  
С.В. Безугаев  
(инициалы, фамилия)  
(подпись)  
«26» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Управление информационной безопасностью»  
(наименование дисциплины)

Код направления подготовки/ специальности	10.05.05
Наименование направления подготовки/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Организация и технологии защиты информации (в информационных системах)
Форма обучения	очная

Лист согласования рабочей программы дисциплины

Программу составил (а)  
проф., к.т.н., проф. \_\_\_\_\_ 26.05.22 С.Г. Фомицина  
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33  
«27» мая 2022 г., протокол № 10

Заведующий кафедрой № 33  
д.т.н., доц. \_\_\_\_\_ 26.05.22 С.В. Безугаев  
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Ответственный за ОП ВО 10.05.05(05)  
доц., к.т.н., доц. \_\_\_\_\_ 26.05.22 В.А. Мильников  
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №3 по методической работе  
\_\_\_\_\_ 26.05.22 Н.В. Решетникова  
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

## Аннотация

Дисциплина «Управление информационной безопасностью» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» направленности «Организация и технологии защиты информации (в информационных системах)». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-4 «Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации»

ОПК-5 «Способен планировать проведение работ по комплексной защите информации на объекте информатизации»

ОПК-8 «Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз»

ОПК-9 «Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности»

ОПК-11 «Способен использовать автоматизированные информационные системы в профессиональной деятельности»

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, практические занятия, 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 4 зачетных единицы, 144 часа.

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 организациях; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в организациях РФ; развитие способностей по использованию существующей системы управления информационной безопасности.

1.2. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

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

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	ОПК-4.3.2 знать структуру и общий состав нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Общепрофессиональные компетенции	ОПК-5 Способен планировать проведение работ по комплексной защите информации на объекте информатизации	ОПК-5.У.1 уметь оценивать угрозы несанкционированного перехвата сведений по каналам передачи данных ОПК-5.У.2 уметь анализировать текущее состояние IT-инфраструктуры предприятия и прогнозировать изменения ее внешней и внутренней среды ОПК-5.В.2 владеть навыками восстановления информационных систем при повреждении ОПК-5.В.3 владеть навыками создания копий баз данных, критичных для

		предприятия
Общепрофессиональные компетенции	ОПК-8 Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ОПК-8.3.4 знать порядок ввода объекта информатизации системы технической защиты информации в эксплуатацию, порядок проведения категорирования технических средств и систем и аттестации объектов информатизации требованиям безопасности информации, порядок сертификации технических средств защиты информации ОПК-8.У.1 уметь анализировать и оценивать угрозы информационной безопасности объекта информатизации ОПК-8.В.2 владеть методами и средствами выявления угроз безопасности объекта информатизации, формирования требований по защите информации, методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов
Общепрофессиональные компетенции	ОПК-9 Способен применять технологии получения, накопления, хранения, обработки, интерпретации и использования информации в ходе профессиональной деятельности	ОПК-9.В.1 владеть навыками построения систем управления данными, извлечения информации из баз данных, ее анализа и использования в профессиональной деятельности ОПК-9.В.2 владеть навыками обоснованного выбора современных систем управления базами данных и обработки информации
Общепрофессиональные компетенции	ОПК-11 Способен использовать автоматизированные информационные системы в профессиональной деятельности	ОПК-11.У.2 уметь проводить анализ и оценку автоматизированных систем в профессиональной деятельности

## 2. Место дисциплины в структуре ОП

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

- «Теория вероятностей и математическая статистика»
- «Математическая логика и теория алгоритмов»
- «Дискретная математик»
- «Вычислительная математика»
- «Информатика и информационные технологии в правоохранительной деятельности»
- «Математические основы обработки информации»
- «Языки программирования»

- «Технологии и методы программирования»
- «Основы информационной безопасности»
- «Программно-аппаратная защита информации»
- «Системы и сети передачи информации»
- «Теория систем и системный анализ»
- «Моделирование систем»
- «Интеллектуальные системы и технологии»

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

- Производственная практика по профилю специализации
- Государственная итоговая аттестация

### 3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№9
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	4/ 144	4/ 144
<b>Из них часов практической подготовки</b>		
<b>Аудиторные занятия, всего час.</b>	85	85
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	27	27
<b>Самостоятельная работа, всего (час)</b>	32	32
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: \*\* кандидатский экзамен

### 4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 9					
Раздел 1. Основы управления ИБ					
Тема 1.1. Введение Понятие процесса управления ИБ	4	4	4		4
Тема 1.2. Политика государства в области информационной безопасности					
Тема 1.3. Базовые вопросы управления ИБ					

Тема 1.4. Стандартизация в области управления ИБ					
Раздел 2. Политика безопасности организации Тема 2.1. Назначение и содержание политики безопасности Тема 2.2. Управление активами. Безопасность, связанная с управлением персоналом Тема 2.3. Жизненный цикл политики безопасности	6	4	6		6
Раздел 3. Системы управления ИБ Тема 3.1. Процессный подход к управлению ИБ Тема 3.2. Область деятельности СУИБ Тема 3.3. Ролевая структура СУИБ Тема 3.4. Политика СУИБ	6	2	6		6
Раздел 4. Основы управления рисками ИБ Тема 4.1. Угрозы и нарушители безопасности информации Тема 4.2. Рискология ИБ Тема 4.3. Методы анализа рисков ИБ	6	2	6		6
Раздел 5. Процессы управления ИБ Тема 5.1. Основные процессы СУИБ Тема 5.2. Внедрение разработанных процессов Тема 5.3. Внедрение мер (контрольных процедур) по обеспечению ИБ Тема 5.5. Процесс «Управление инцидентами ИБ» Тема 5.6 Процесс «Обеспечение непрерывности ведения бизнеса» Тема 5.7. Эксплуатация и независимый аудит СУИБ	6	2	6		6
Раздел 6. Системы обнаружения и предотвращения компьютерных атак Тема 6.1. Требования к системам обнаружения и предотвращения компьютерных атак Тема 6.2, Системы анализа защищенности. Системы обнаружения атак Тема 6.3. Системы контроля целостности бмин Системы анализа журналов регистрации Тема 6.4. Критерии выбора систем обнаружения и предотвращения компьютерных атак	6	1	6		4
Итого в семестре:	34	17	34		32
Итого	34	17	34	0	32

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	<b>Основы управления ИБ</b> Тема 1.1. Введение Понятие процесса управления ИБ (демонстрация слайдов) Тема 1.2. Политика государства в области информационной безопасности (демонстрация слайдов) Тема 1.3. Базовые вопросы управления ИБ (демонстрация слайдов) Тема 1.4. Стандартизация в области управления ИБ (демонстрация слайдов)

<b>2</b>	<b>Политика безопасности организации</b> Тема 2.1. Назначение и содержание политики безопасности (демонстрация слайдов) Тема 2.2. Управление активами. Безопасность, связанная с управлением персоналом (демонстрация слайдов) Тема 2.3. Жизненный цикл политики безопасности (демонстрация слайдов)
<b>3</b>	<b>Системы управления ИБ</b> Тема 3.1. Процессный подход к управлению ИБ (демонстрация слайдов) Тема 3.2. Область деятельности СУИБ (демонстрация слайдов) Тема 3.3. Ролевая структура СУИБ (демонстрация слайдов) Тема 3.4. Политика СУИБ (демонстрация слайдов)
<b>4</b>	<b>Основы управления рисками ИБ</b> Тема 4.1. Угрозы и нарушители безопасности информации (демонстрация слайдов) Тема 4.2. Рискология ИБ (демонстрация слайдов) Тема 4.3. Методы анализа рисков ИБ (демонстрация слайдов)
<b>5</b>	<b>Процессы управления ИБ</b> Тема 5.1. Основные процессы СУИБ (демонстрация слайдов) Тема 5.2. Внедрение разработанных процессов (демонстрация слайдов) Тема 5.3. Внедрение мер (контрольных процедур) по обеспечению ИБ (демонстрация слайдов) Тема 5.5. Процесс «Управление инцидентами ИБ» (демонстрация слайдов) Тема 5.6. Процесс «Обеспечение непрерывности ведения бизнеса» (демонстрация слайдов) Тема 5.7. Эксплуатация и независимый аудит СУИБ (демонстрация слайдов)
<b>6</b>	<b>Системы обнаружения и предотвращения компьютерных атак</b> Тема 6.1. Требования к системам обнаружения и предотвращения компьютерных атак (демонстрация слайдов) Тема 6.2. Системы анализа защищенности. Системы обнаружения атак (демонстрация слайдов) Тема 6.3. Системы контроля целостности бинарных Системы анализа журналов регистрации (демонстрация слайдов) Тема 6.4. Критерии выбора систем обнаружения и предотвращения компьютерных атак (демонстрация слайдов)

#### 4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 9					
1	Выбор области действия СУИБ	решение ситуационных задач	4	2	1-3
2	Разработка Политики ИБ	решение ситуационных задач	4	2	2
3	Выбор методики оценки рисков ИБ	занятия по моделированию реальных условий	2	1	4
4	Проведение оценки рисков ИБ системы	занятия по моделированию реальных условий	2	1	4

5	Разработка плана проведения внутреннего аудита ИБ	решение ситуационных задач	2	1	4,5
6	Проведение внутреннего аудита ИБ	занятия по моделированию реальных условий	2	1	4,5
7	Планирование работы службы безопасности предприятия	Деловая игра	1	-	6
Всего			17		

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 9				
1	Разработка модели угроз безопасности информации	6	4	1-3
2	Формирование заданий по безопасности и SIEM-экосистемы	8	4	2,3
3	Сбор логов событий информационной безопасности в AirSIEM	10	6	4-6
4	Регистрация инцидентов в AirSIEM	10	6	4-5
Всего		34		

#### 4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

#### 4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 9, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)	-	-
Расчетно-графические задания (РГЗ)	-	-
Выполнение реферата (Р)	-	-
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Домашнее задание (ДЗ)	-	-
Контрольные работы заочников (КРЗ)	-	-
Подготовка к промежуточной аттестации (ПА)	12	12



Всего:	32	32
--------	----	----

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

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
37 Г 72	Государственная итоговая аттестация : методические указания по подготовке к государственному экзамену и написанию и защите выпускной квалификационной работы / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост.: С. Г. Фомичева, Т. Н. Елина, В. А. Мыльников. - Санкт-Петербург : Изд-во ГУАП, 2021. - 79 с. : рис., табл. - Библиогр.: с. 79 (10 назв.). - Б. ц. - Текст : непосредственный.	5
004 Ф 76	Фомичева, Светлана Григорьевна. Обработка информации в распределенных системах : учебное пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 132 с. ; 131 с. : рис. - Библиогр.: с. 123 (17 назв.). - ISBN 978-5-8088-1487-5 : Б. ц. - Текст : непосредственный	5
004 Б 39	Беззатеев, Сергей Валентинович (д-р техн. наук, доц.). Программирование задач по обеспечению информационной безопасности : лабораторный практикум / С. В. Беззатеев, С. Г. Фомичева ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2020. - 89 с. : рис., табл. - Библиогр.: с. 88 (10 назв.). - Б. ц. - Текст : непосредственный.	5
004 3-62	Зима, В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. - 2-е изд. - СПб. : БХВ - Петербург, 2015. - 368 с. : рис. - (Мастер систем). - Библиогр.: с. 351 - 353 (31 назв.). - Предм. указ.:с. 354 - 362. - ISBN	7

	978-5-94157-213-7 : 419.00 р. - Текст : непосредственный	
007 В 67	Волкова, В. Н. Теория систем и системный анализ : учебник для академического бакалавриата / В. Н. Волкова, А. А. Денисов ; Нац. исслед. С.-Петерб. гос. политехн. ун-т. - 2- е изд., перераб. и доп. - М. : Юрайт, 2015. - 616 с. : рис. - (Бакалавр. Академический курс). - Предм. указ.: с. 600 - 606. - Имен. указ.: с. 607 - 609. - Библиогр.: с. 610 - 616 (109 назв.). - ISBN 978-5-9916-4783-0 : 870.87 р. - Текст : непосредственный. Имеет гриф УМО высшего образования	10
004 И 85	Исаев, Г. Н. Проектирование информационных систем : учебное пособие / Г. Н. Исаев. - 2- е изд., стер. - М. : ОМЕГА-Л, 2015. - 424 с. : рис., табл. - (Высшее техническое образование). - Библиогр.: с. 421 - 424 (61 назв.). - ISBN 978-5-370-03507-4 : 401.60 р. - Текст : непосредственный. На стр. 7 - 8: Список сокращений	5
004 Б 24	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. : рис., табл. - (Высшее образование). - Библиогр.: с. 313 - 316 (56 назв.). - ISBN 978-5-369-01450-9 (РИОР). - ISBN 978-5- 16-011164-3 (ИНФРА-М) : 942.63 р. - Текст : непосредственный. Имеет гриф УМО по образованию в области прикладной информатики	5
004.4 И 46	Ильина, Дарья Викторовна. Проектирование и разработка безопасных веб-приложений : учебное пособие / Д. В. Ильина ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт- Петербург : Изд-во ГУАП, 2019. - 43 с. : рис. - Библиогр.: с. 42 (2 назв.). - ISBN 978- 5-8088-1434-9 : Б. ц. - Текст : непосредственный.	5
004.7 К 95	Кучин, Николай Валентинович (доц.). Многоуровневые системы и облачные вычисления : учебное пособие / Н. В. Кучин, А. Ю. Молчанов ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2018. - 136 с. : рис. - Библиогр.: с. 133 (14 назв.). - ISBN 978-5- 8088-1250-5 : Б. ц. - Текст :	4

	непосредственный	
--	------------------	--

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
<a href="http://www.intuit.ru/studies/courses/10/10/info">http://www.intuit.ru/studies/courses/10/10/info</a>	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)
<a href="https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti#syllabus">https://ru.coursera.org/learn/management-informacionnoi-bezopasnosti#syllabus</a>	Сорокин Александр Владимирович. Менеджмент информационной безопасности

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	
3	Класс для деловой игры	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

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

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«отлично» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>– уверенно, логично, последовательно и грамотно его излагает;</li> <li>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>– умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>– делает выводы и обобщения;</li> <li>– свободно владеет системой специализированных понятий.</li> </ul>
«хорошо» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> <li>– не формулирует выводов и обобщений.</li> </ul>

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код
-------	--	-----

		индикатора
1.	Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.	ОПК-4.3.2
2.	Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?	ОПК-5.У.1
3.	Охарактеризуйте шифрование (криптографию) в качестве основного сервиса безопасности ИС.	ОПК-5.У.2
4.	Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?	ОПК-5.В.2
5.	Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует?	ОПК-5.В.3
6.	Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации.	ОПК-8.3.4
7.	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.	ОПК-8.У.1
8.	В чем заключается основная задача аудита, как сервиса безопасности?	ОПК-8.В.2
9.	Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации.	ОПК-9.В.1
10.	Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?	ОПК-9.В.2
11.	Что такое протоколирование? Прокомментируйте особенности применения данного сервиса безопасности.	ОПК-11.У.2
12.	Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?	ОПК-4.3.2
13.	В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?	ОПК-5.У.1
14.	Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.	ОПК-5.У.2
15.	Перечислите основные виды конфиденциальной информации, нуждающейся в защите.	ОПК-5.В.2
16.	Прокомментируйте возможности биометрической идентификации (аутентификации).	ОПК-5.В.3
17.	Перечислите основные угрозы конфиденциальности информации.	ОПК-8.3.4
18.	Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне.	ОПК-8.У.1

	Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности	
19.	Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?	ОПК-8.В.2
20.	Охарактеризуйте основные угрозы целостности конфиденциальной информации.	ОПК-9.В.1
21.	Дайте определение защищаемой информации и охарактеризуйте ее основные признаки.	ОПК-9.В.2
22.	Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?	ОПК-11.У.2
23.	Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?	ОПК-4.3.2
24.	Раскройте содержание политических, Экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ.	ОПК-5.У.1
25.	Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?	ОПК-5.У.2
26.	Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность.	ОПК-5.В.2
27.	Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня.	ОПК-5.В.3
28.	Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.	ОПК-8.3.4
29.	Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.	ОПК-8.У.1
30.	Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации.	ОПК-8.В.2
31.	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?	ОПК-9.В.1
32.	Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?	ОПК-9.В.2
33.	Перечислите важнейшие задачи обеспечения информационной безопасности РФ.	ОПК-11.У.2
34.	Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности? Приведите примерный список решений верхнего уровня политики безопасности.	ОПК-4.3.2
35.	Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна	ОПК-5.У.1

	опасности?	
36.	Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?	ОПК-5.У.2
37.	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.	ОПК-5.В.2
38.	Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.	ОПК-5.В.3
39.	Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?	ОПК-8.3.4
40.	Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?	ОПК-8.У.1
41.	Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.	ОПК-8.В.2
42.	Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.	ОПК-9.В.1
43.	Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процессами?	ОПК-8.3.4
44.	Что понимается под системой управления безопасностью?	ОПК-11.У.2
45.	Каков функционал SIEM-систем?	ОПК-9.В.2

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код

		индикатора
1.	К какой разновидности моделей управления доступом относится модель Белла-Ла Падулы? а) модель дискреционного доступа; б) модель мандатного доступа; в) ролевая модель.	ОПК-4.3.2
2.	Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?	ОПК-5.У.1
3.	К каким мерам защиты относится политика безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным.	ОПК-5.У.2
4.	В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу? а) ACL; б) списки полномочий субъектов; в) атрибутные схемы.	ОПК-5.В.2
5.	Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность	ОПК-5.В.3
6.	К основным принципам построения системы защиты АИС относятся: а) открытость; б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота	ОПК-8.3.4
7.	Какие из следующих высказываний о модели управления доступом RBAC справедливы? а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей; б) роли упорядочены в иерархию; в) с каждым объектом доступа ассоциировано несколько ролей ; г) для каждой пары «субъект-объект» назначен набор возможных разрешений	ОПК-8.У.1
8.	. Диспетчер доступа... а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа; б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;	ОПК-8.В.2
9.	Какие предположения включает неформальная модель нарушителя?	ОПК-9.В.1



	<ul style="list-style-type: none"> <li>а) о возможностях нарушителя;</li> <li>б) о категориях лиц, к которым может принадлежать нарушитель;</li> <li>в) о привычках нарушителя;</li> <li>г) о предыдущих атаках, осуществленных нарушителем;</li> <li>д) об уровне знаний нарушителя</li> </ul>	
10.	<p>Что представляет собой доктрина информационной безопасности РФ?</p> <ul style="list-style-type: none"> <li>а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;</li> <li>б) федеральный закон, регулирующий правоотношения в области информационной безопасности;</li> <li>в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;</li> <li>г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации</li> </ul>	ОПК-9.В.2
11.	<p>К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?</p> <ul style="list-style-type: none"> <li>а) политика безопасности верхнего уровня;</li> <li>б) политика безопасности среднего уровня;</li> <li>в) политика безопасности нижнего уровня;</li> <li>г) принцип минимизации привилегий;</li> <li>д) защита поддерживающей инфраструктуры.</li> </ul>	ОПК-11.У.2
12.	<p>Какие из перечисленных ниже угроз относятся к классу преднамеренных?</p> <ul style="list-style-type: none"> <li>а) заражение компьютера вирусами;</li> <li>б) физическое разрушение системы в результате пожара;</li> <li>в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);</li> <li>г) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;</li> <li>д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;</li> <li>е) вскрытие шифров криптозащиты информации</li> </ul>	ОПК-4.3.2

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

## 11. Методические указания для обучающихся по освоению дисциплины

### 11.1. 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 обучающимися 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;
- научиться 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

### 11.2. Методические указания для обучающихся по участию в семинарах- *учебным планом не предусмотрено*

### 11.3. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

#### Планируемые результаты при освоении обучающимися практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;

- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

#### Требования к проведению практических занятий

В рамках проведения практических занятий проводится опрос по пройденному теоретическому материалу. Студенту ставится оценка по результатам опроса, которая учитывается при промежуточной аттестации.

11.4. Методические указания для обучающихся по выполнению 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 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

##### **Лабораторная работа № 1 «Разработка модели угроз безопасности информации»**

Цель лабораторной работы № 1: Построение различных моделей, отображающих архитектуру автоматизированной системы и ограничений доступа к информации. Проведение анализа мест и видов утечки информации. Оценка угроз, уязвимостей и степени защищенности информации.

Задание к лабораторной работе №1

- 1) Выполнить оценку актуальности разрабатываемой информационной
- 2) системы
- 3) Провести структурный системный анализ бизнес-процессов
- 4) предметной области. Построить диаграммы IDEF0 (AS-IS), DFD (ASIS), (при необходимости – IDEF3 (AS-IS)).
- 5) Описать разработанные диаграммы
- 6) Выделить активы, подлежащие информационной защите
- 7) Построить модель угроз разрабатываемой информационной системы
- 8) Построить модель нарушителя
- 9) Сформировать реестр актуализированных угроз для каждого актива
- 10) Сформировать векторы уязвимостей. Оценить возможные риски
- 11) Оценить степень защищенности информации

#### Структура и форма отчета о лабораторной работе

Отчет по лабораторным работам должна отражать не факт спроектированной системы защиты, а процесс проектирования, показывающий всю работу над проектом начиная от полученного исходного материала и наброска будущей защищенной

информационной системы и заканчивая разработанным и протестированным программным пакетом, с обоснованием всех принятых в процессе проектирования решений. В содержании должна быть отражена структура отчета. Введение должно характеризовать ту сферу человеческой деятельности, для которой будет проектироваться система защиты информации. При описании диаграмм должны быть изложены основные функциональные возможности будущей системы защиты информации, а также виды информации которые придется хранить и обрабатывать для достижения поставленной цели. В последующих лабораторных работах должны быть изложены этапы конструирования и функционирования программно-технических устройств защиты информации и технических объектов от несанкционированного доступа

#### Требования к оформлению отчета о лабораторной работе

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен 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.

Ссылка на материалы ЛР1 - <https://pro.guap.ru/get-task/b25b17c8140089be72add01c1e078f59>

### **Лабораторная работа № 2 «Формирование заданий по безопасности и SIEM-экосистемы»**

Цель лабораторной работы № 2: На основании формулированных целей безопасности сформировать профили защиты и задания по безопасности информационной системы и СЗИ, реализующих требуемый уровень защищенности системы. Развернуть SIEM-экосистему

#### Задание к лабораторной работе №2

- 1) На основании сформулированных целей безопасности сформировать профили защиты информационной (автоматизированной) системы и/или СЗИ.
- 2) В профилях защиты построить таблицы, которые взаимосвязывают Цели безопасности с угрозами и ПолиБ. Взаимосвязи обосновать и описать.
- 3) Сформулировать функциональные требования, требования доверия и требования к среде
- 4) Разработать задание по безопасности. Выделить правила безопасности, реализованные в технических политиках безопасности, которые предстоит реализовать в подсистеме анализа (корреляций) SIEM-системы.
- 5) Развернуть SIEM-экосистему, используя проект AirSIEM <https://github.com/fisher85/AirSIEM>
- 6) Исходный код ядра корреляции - <https://github.com/fisher85/AirSIEM/tree/master/AirSIEM>
- 7) Оформить отчет по лабораторной работе

#### 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

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;

- Отчет по лабораторной работе должен 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

Ссылка на материалы ЛР2 - <https://pro.guap.ru/get-task/29751f9f3e45be1a6db3dba4876f9ab5>

**Лабораторная работа № 3** «Сбор логов событий информационной безопасности в AirSIEM»

Цель лабораторной работы № 3: разработать систему, которая позволяет анализировать регистрируемые в защищаемой инфраструктуре события, поступающие от различных источников, и обнаруживать атаки/сценарии атак/подозрительные действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности.

Задание к лабораторной работе №3

- 1) Сформировать технические политики ИБ
- 2) На основании разработанных политик информационной безопасности, профилей защиты и заданий по безопасности информационной (автоматизированной) системы и/или СЗИ, разработать архитектуру SIEM-системы
- 3) Реализовать подсистему сбора и хранения поступающих событий безопасности;
- 4) Оформить отчет по лабораторной работе.

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

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен 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

Ссылка на материалы ЛР3 - <https://pro.guap.ru/get-task/1586365b0a7f4af9f6c2e921c0a1206a>

**Лабораторная работа № 4** «Регистрация инцидентов в AirSIEM»

Цель лабораторной работы № 4: разработать систему, которая позволяет анализировать регистрируемые в защищаемой инфраструктуре события, поступающие от различных источников, и обнаруживать атаки/сценарии атак/подозрительные действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности.

Задание к лабораторной работе №4

- 1) Реализовать обработку и анализ зарегистрированных событий безопасности;
- 2) Разработать подсистему обнаружения атак и нарушений политик безопасности в реальном времени (близком к реальному времени);
- 3) Реализовать выявление и разбор инцидентов безопасности.
- 4) Оформить отчет по лабораторной работе.

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

- Отчет по лабораторной работе предоставляется в печатном/или электронном виде;
- должна соответствовать структуре и форме отчета, представленной выше;
- Отчет по лабораторной работе должен 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

Ссылка на материалы ЛР4 - <https://pro.guap.ru/get-task/2deea4a227cabcc77748f9e39303882f>

11.5. Методические указания для обучающихся по прохождению курсового проектирования/выполнения курсовой работы- *учебным планом не предусмотрено.*

11.6. 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).

11.7. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины..

11.8. 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