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
(инициалы, фамилия)

(подпись)
«24» марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория информационной безопасности и методология защиты информации»
(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

Санкт-Петербург – 2021

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н., доц.	24.03.22	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 34
«24» марта 2022 г., протокол № 8

Заведующий кафедрой № 34

д.т.н., доц.	24.03.22	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 10.05.05(05)

доц., д.т.н., доц.	24.03.22	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

См. прил.	24.03.22	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Теория информационной безопасности и методология защиты информации» 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 «№34».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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-10 «Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач»

Содержание дисциплины охватывает круг вопросов, связанных с системой теоретических и методологических знаний и специальных умений в области информационной безопасности и их использования в профессиональной деятельности будущего специалиста.

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 6 зачетных единиц, 216 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Формирование профессиональной компетентности на основе системы теоретических и методологических знаний и специальных умений в области информационной безопасности и их использования в профессиональной деятельности будущего специалиста. В курсе рассматривается основной понятийный аппарат 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-5 Способен планировать проведение работ по комплексной защите информации на объекте информатизации	ОПК-5.З.2 знать внешние и внутренние угрозы информационной безопасности ОПК-5.У.1 уметь оценивать угрозы несанкционированного перехвата сведений по каналам передачи данных
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.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-10 Способен осуществлять аналитическую деятельность с	ОПК-10.З.1 знать основные понятия, принципы и методы теории системного анализа и управления в целях применения в профессиональной сфере

	последующим использованием данных при решении профессиональных задач	ОПК-10.У.3 уметь выявлять пробелы в информации, необходимой для решения профессиональных задач, и проектировать процессы по их устранению

2. Место дисциплины в структуре ОП

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

- Алгебра и геометрия
- Математическая логика и теория алгоритмов
- Информатика и информационные технологии в правоохранительной деятельности
- Математический анализ
- Дискретная математика
- Теория вероятностей и математическая статистика

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

- Теория кодирования
- Моделирование систем

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	
		№6	№7
1	2	3	4
Общая трудоемкость дисциплины, ЗЕ/ (час)	6/ 216	2/ 72	3/ 144
Из них часов практической подготовки			
Аудиторные занятия, всего час.	102	51	51
в том числе:			
лекции (Л), (час)	34	17	17
практические/семинарские занятия (ПЗ), (час)			
лабораторные работы (ЛР), (час)	68	34	34
курсовой проект (работа) (КП, КР), (час)			
экзамен, (час)	45		45
Самостоятельная работа, всего (час)	33	21	12
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Дифф. Зач., Экз.	Дифф. Зач.	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 6					
Раздел 1. Информационная безопасность	2		4		4
Раздел 2. Общее содержание защиты информации	3		6		4
Раздел 3. Предмет и объект защиты информации	4		8		4
Раздел 4. Угрозы информационной безопасности	4		8		4
Раздел 5. Системное обеспечение защиты информации	4		8		5
Итого в семестре:	17		34		21
Семестр 7					
Раздел 6. Автоматизированная информационная система как объект защиты	4		8		3
Раздел 7. Требования информационной безопасности АИС	4		8		3
Раздел 8. Методы защиты информации	4		8		4
Раздел 9. Средства защиты информации	5		10		4
Итого в семестре:	17		34		12
Итого	34	0	68	0	33

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	Раздел 1. Информационная безопасность Тема 1. Проблемы развития теории и практики обеспечения информационной безопасности Тема 2. Основные понятия и определения в области информационной безопасности Термины, определяющие научную основу информационной безопасности Термины, определяющие предметную основу информационной безопасности Термины, определяющие характер деятельности по обеспечению информационной безопасности Тема 3. Определение информационной безопасности в свете информационных проблем современного общества Тема 4. Основные составляющие информационной безопасности Тема 5. Значение информационной безопасности для субъектов информационных отношений Тема 6. Составляющие национальных интересов российской федерации в информационной сфере Стратегия национальной безопасности российской федерации до 2020 года Доктрина информационной безопасности российской федерации Тема 7. Международное сотрудничество в области информационной безопасности: проблемы и перспективы
2	Раздел 2. Общее содержание защиты информации Тема 8. Понятие и сущность защиты информации Тема 9. Цели защиты информации

	Тема 10. Концептуальная модель информационной безопасности
3	Раздел 3. Предмет и объект защиты информации Тема 11. Предмет защиты информации Тема 12. Информация как объект права собственности Тема 13. Объект защиты информации
4	Раздел 4. Угрозы информационной безопасности Тема 14. Случайные угрозы Тема 15. Преднамеренные угрозы Тема 16. Модель гипотетического нарушителя информационной безопасности
5	Раздел 5. Системное обеспечение защиты информации Тема 17. Основные принципы построения системы защиты Тема 18. Методы защиты информации Минимизация ущерба от аварий и стихийных бедствий Дублирование информации Повышение надежности информационной системы Создание отказоустойчивых информационных систем Оптимизация взаимодействия пользователей и обслуживающего персонала Методы и средства защиты информации от традиционного шпионажа и диверсий Методы и средства защиты от электромагнитных излучений и наводок Защита информации от несанкционированного доступа Тема 19. Модели защиты информации Криптографические методы защиты информации
6	Тема 1.1. Архитектура «клиент-сервер» АИС. Тема 1.2. Модели нарушителя и угроз АИС
7	Тема 2.1. Общие требования к построению защищенной АИС. Тема 2.2. Требования к подсистеме аутентификации и управления доступом. Тема 2.3. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Тема 2.4. Требования к подсистемам резервирования /восстановления информации, контроля эталонного состояния информации и рабочей среды. Тема 2.5. Требования к подсистеме управления безопасностью
8	Тема 3.1. Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер». Тема 3.2. Методы защиты информации на физическом уровне модели OSI. Тема 3.3. Методы защиты информации на канальном уровне модели OSI. Тема 3.4. Методы защиты информации на сеансовом уровне модели OSI. Тема 3.5. Методы защиты информации на транспортном уровне модели OSI. Тема 3.6. Методы защиты информации на сеансовом уровне модели OSI. Тема 3.7. Методы защиты информации на прикладном уровне модели OSI.
9	Тема 4.1. Средства защиты информации от несанкционированного доступа. Тема 4.2. Средства защиты информации от вредоносного кода. Тема 4.3. Средства защиты информации от межсетевого воздействия. Тема 4.4. Средства криптографической защиты информации.

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

Учебным планом не предусмотрено					
Всего					

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 6				
1	Рассмотрение и анализ доктрины информационной безопасности Российской Федерации	4		1
2	Определение целей защиты информации на предприятии регионального уровня	2		2
3	Составление программы информационной безопасности на предприятии регионального уровня	4		2
4	Рассмотрение особенностей объекта защиты информации	4		3
5	Определение угроз информационной безопасности на предприятии	4		4
6	Анализ рисков на предприятии	4		4
7	Определение комплекса практических мероприятий, направленных на обеспечение информационной безопасности предприятия	4		5
8	Построение концепции безопасности предприятия	4		5
9	Составление программы информационной безопасности предприятия	4		5
Семестр 7				
10	Требования к построению защищенной АИС и ее элементов	8		2
11	Многоуровневая модель защиты информации в АИС на архитектуре «клиент-сервер»	8		3
12	Методы защиты информации на уровнях модели OSI	10		3
13	Средства защиты информации	8		4
	Всего	68		

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 6, час	Семестр 7, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)	30	10	8
Курсовое проектирование (КП, КР)			
Расчетно-графические задания (РГЗ)			
Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)	20	6	2
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной аттестации (ПА)	19	5	3
Всего:	33	21	13

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)
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	
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	(5)

	с.	
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.	
004/М 87-604316-ED	Мошак Н. Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография / Н. Н. Мошак; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб.: Изд-во ГУАП, 2014. - 197 с.	50
004 М 87	Организация безопасного доступа к информационным ресурсам: учебное пособие / Н. Н. Мошак, Т. М. Татарникова. - СПб.: Изд-во ГУАП, 2014. - 121 с	40
Х404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для СПО / В. Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2016. - 416 с.	10
	Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. http://znanium.com/catalog.php?bookinfo=474838	

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

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	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля 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.
Дифференцированный зачёт	Список вопросов; Тесты; Задачи.

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	

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«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.
«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.
«удовлетворительно» «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.
«неудовлетворительно» «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.

10.3. 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	1. Дайте определение понятию информационная безопасность. 2. Перечислите основные составляющие информационной безопасности. 3. Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений? 4. Каковы интересы РФ в информационной сфере? 5. Определите источники угроз информационной безопасности РФ и постройте их классификацию. 6. Перечислите основные методы обеспечения информационной безопасности РФ.	ОПК-5.З.2
2	7. Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня? 8. Перечислите основные документы в области	ОПК-5.У.1

	международной информационной безопасности. 9. Каково, на ваш взгляд, положение дел в области МИБ сегодня? 10. Проанализируйте различные определения понятия «защита информации» и «информационная безопасность». 11. Дайте определение понятию защита информации.	
3	12. Что понимается под термином безопасность информации? 13. Что включает в себя защита информации? 14. Какие цели преследует защита информации?	ОПК-8.У.1
4	15. Какое место занимается защита информации в информационной безопасности? 16. Какие уровни задействованы в обеспечении информационной безопасности?	ОПК-8.В.2
5	17. Что представляет собой политика безопасности организации? 18. Что входит в анализ рисков? 19.Что представляет собой программа безопасности организации? 20. Определите предмет защиты информации. 21. Сформулируйте основные свойства информации.	ОПК-10.З.1
6	22. Дайте определение конфиденциальной информации. 23. Перечислите уровни секретности государственной тайны. 24. Раскройте сущность основных подходов к измерению количества информации. 25. Раскройте сущность информации как объекта права собственности. 7. Раскройте сущность объекта защиты. 26. Составьте классификацию угроз информационной безопасности. 27. Раскройте основные группы классификации. 28. На основании чего строится модель нарушителя информационной безопасности?	ОПК-10.У.3

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
1	29.Сформулируйте основные принципы построения системы защиты информации. 30. Перечислите основные модели защиты информации и их особенности. 31. В чем заключается сущность методов защиты от случайных угроз? 32. Дайте определение понятиям идентификации и аутентификации. 33. Перечистите основные виды аутентификации. 34. В чем заключается повышение надежности и отказоустойчивости информационных систем?	ОПК-5.З.2
2	Общие требования к построению защищенной АИС. Требования к подсистеме аутентификации и управления доступом. Требования к подсистемам криптографической защиты информации и антивирусной защиты. Требования к подсистемам резервирования	ОПК-5.У.1

	/восстановления информации, контроля эталонного состояния информации и рабочей среды. Требования к подсистеме управления безопасностью Многоуровневая модель защиты информации в АИС на архитектуре «клиентсервер».	
3	Методы защиты информации на физическом уровне модели OSI. Методы защиты информации на канальном уровне модели OSI. Методы защиты информации на сеансовом уровне модели OSI. Методы защиты информации на транспортном уровне модели OSI. Методы защиты информации на сеансовом уровне модели OSI. Методы защиты информации на прикладном уровне модели OSI.	ОПК-8.У.1
4	Средства защиты информации от несанкционированного доступа. Средства защиты информации от вредоносного кода. Средства защиты информации от межсетевого воздействия. Средства криптографической защиты информации.	ОПК-8.В.2
5	35. Какую роль играет подготовленность персонала в построении системы защиты информации? 36. Какие методы и средства используются для организации противодействия традиционным методам шпионажа и диверсий? 37. Раскройте особенность построения защиты от несанкционированного доступа 38. Какие методы защиты информации относятся к криптографическим?	ОПК-10.З.1

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. Свойства информации в форме сообщения: (укажите правильный вариант) a. идеальность b. субъективность c. информационная неуничтожаемость d. динамичность e. материальность f. накапливаемость 2. Свойства информации в форме сведений: (укажите правильный	

	вариант) a. материальность b. измеримость c. сложность d. проблемная ориентированность e. накапливаемость 3. Информационная сфера – это … , … , … , … . 4. Первая классификация национальных интересов: a. интересы … b. интересы … c. интересы … 5. Общие методы обеспечения информационной безопасности: a. … b. … c. … 6. Информация – наиболее ценный … современного общества. 7. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков? a. Документы b. Персонал c. Организационные единицы d. Промышленные образцы e. Научный инструментарий 8. Поставьте в порядке важности национальные интересы: a. Информационное обеспечение государственной политики Российской Федерации. b. Развитие современных информационных технологий, отечественной индустрии информации. c. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею. d. Защита информационных ресурсов от несанкционированного доступа 9. Допишите различные подходы к понятию информации: a. информация … b. информация … c. … информация 10. Составляющие национальной безопасности: a. … b. … c. … d. … e. … f. … g. … h. … 11. Общие методы обеспечения национальной безопасности: a. … b. … c. … 12. Основные объекты воздействия в информационной войне? a. … b. … c. … d. … e. … 13. Перечислите информационное оружие: a. …	

	b. … средства c. … генераторы d. средства … e. средства … 14. Война, есть продолжение … другими, насильственными средствами. 15. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .	

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.

1. Методические указания для обучающихся по освоению дисциплины

Формирование профессиональной компетентности на основе системы теоретических и методологических знаний и специальных умений в области информационной безопасности и их использования в профессиональной деятельности будущего специалиста. В курсе рассматривается основной понятийный аппарат 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

Задание на лабораторные работы представлены по темам изучаемой дисциплины и представляют собой реализацию изучаемых задач:

Рассмотрение и анализ доктрины информационной безопасности российской федерации

Необходимо проанализировать Доктрину ИБ РФ и построить схему органов государственной власти и самоуправления, отвечающих за информационную безопасность и определить их функциональные обязанности; определить положения государственной политики в области обеспечения ИБ, выделить первоочередные мероприятия по обеспечению ИБ, дать им оценку.

Определение целей защиты информации на предприятии регионального уровня

Необходимо проанализировать структуру местного предприятия, рассмотреть виды информации и носители, используемые в его подразделениях. Сформулировать цели защиты информации на данном предприятии. Составить программу информационной безопасности

Рассмотрение особенностей объекта защиты информации

Используя данные предыдущей практической работы, рассмот- реть особенности каждого типа носителей информации, отметить плюсы и минусы каждого типа, условия хранения и обработки.

Определение угроз информационной безопасности и анализ рисков на предприятии

Исходя из целей защиты информации и носителей информации, выявленных на предыдущих занятиях, необходимо определить список угроз ИБ, характерных для данного предприятия. Проанализировать риски, определить степень их допустимости. Составить модели нарушителей информационной безопасности, акту- альных для данного предприятия.

Построение концепции безопасности предприятия

Определите, комплекс практических мероприятий, направленных на обеспечение информационной безопасности предприятия. Составьте программу информационной безопасности предприятия.

Структура и форма отчета о лабораторной работе

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;
3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

Требования к оформлению отчета о лабораторной работе

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники…) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

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