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. Бегзатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Теория информационной безопасности»
(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)

доц.,к.э.н.,доц.	24.06.21	Т.Н. Елина
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. Бегзатеев
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 «Теория информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» специализация «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-12 «способность работать с различными источниками информации, инфорационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации»;

профессиональных компетенций:

ПК-1 «способность формировать и 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»,

ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»,

ПК-17 «способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов»,

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

ПК-19 «способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности».

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 диффренцированного зачета.

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

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-12 «способность работать с различными источниками информации, инфорационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации»:

знать:
- математические программы для числовых и символьных вычислений на компьютере для качественного исследования свойств различных математических моделей;

уметь:
- строить математические модели и алгоритмы обработки данных;
- разрабатывать алгоритмы логического вывода задач классификации и кластеризации, алгебраических вычислений и оптимизации;

владеть:
- методами дискретного анализа данных;

иметь опыт деятельности:
- при накоплении и обработки информации с применением ПК;
- решением задач дискретной оптимизации;
- построением простых математических моделей классификации

ПК-1 «способность формировать и 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»:

знать - вопросы обеспечения информационной безопасности государства; методологии создания систем защиты информации;
уметь - квалифицированно оценивать область применения элементов СЗИ;
владеть навыками - аппаратом исследования различных систем КЗИ;
иметь опыт деятельности - построения, эксплуатации и использования систем СЗИ;

ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»:

знать - основные функции, назначение составных частей и принципы построения систем компьютерной безопасности;
уметь - объяснять назначение отдельных уровней защиты и задачи их работы;
владеть навыками - адекватно управлять системой информационной безопасности;
иметь опыт деятельности - менеджмента современных систем информационной безопасности;

ПК-17 «способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов»:

знать - о проблемах построения систем зашиты информации (СЗИ) и организации её функционирования, а также об основных направлениях решения этих проблем и направлениях дальнейшего развития;
уметь - грамотно использовать элементы СЗИ при решении практических задач;
владеть навыками - навыками освоения и внедрения новых систем комплексной защиты информации (КЗИ);
иметь опыт деятельности – участия и игровых ситуациях пресечения и раскрытия правонарушений и преступлений в качестве специалиста;

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

знать - о проблемах построения систем зашиты информации (СЗИ) и организации её функционирования, а также об основных направлениях решения этих проблем и направлениях дальнейшего развития;
уметь - грамотно использовать элементы СЗИ при решении практических задач;
владеть навыками - навыками освоения и внедрения новых систем комплексной защиты информации (КЗИ);
иметь опыт деятельности – участия и игровых ситуациях пресечения и раскрытия правонарушений и преступлений в качестве специалиста;

ПК-19 «способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности»:
знать - отличия в реализации основных механизмов функционирования систем защиты; методики проведения сравнительного анализа систем защиты информации;
уметь - использовать все возможности, предоставляемые системой защиты;
владеть навыками - навыками сопровождения и управления системами КЗИ;
иметь опыт деятельности - анализа структуры и содержания информационных массивов и информационных процессов на предмет выявления угроз безопасности.

2. Место дисциплины в структуре ОП

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

- Криминалистика
- Основы информационной безопасности
- Теория информации

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

- Методология защиты информации
- Правовая защита информации
- Технологии защиты от скрытой передачи данных
- Организационная защита информации
- Криптографическая защита информации
- Защита компьютерных сетей

- Техническая защита информации
- Методология защиты информации
- Безопасность сетей ЭВМ
- Защита от вредоносных программ

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
		№6
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	14	14
Аудиторные занятия, всего час., ***В том числе***	34	34
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)		
Самостоятельная работа, всего	74	74
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Дифф. Зач.	Дифф. Зач.

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)	ЛР (час)	КП (час)	СРС (час)
Семестр 6					
Раздел 1. Информационная безопасность	2		2		10

Раздел 2. Общее содержание защиты информации	4		3		10
Раздел 3. Предмет и объект защиты информации	3		2		14
Раздел 4. Угрозы информационной безопасности	4		4		20
Раздел 5. Системное обеспечение защиты информации	5		6		20
Итого в семестре:	17		17		74
Итого:	17	0	17	0	74

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
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

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 дисципли-ны
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 6				
1	Рассмотрение и анализ доктрины информационной безопасности Российской Федерации	2	1	1
2	Определение целей защиты информации на предприятии регионального уровня	1	1	2
3	Составление программы информационной безопасности на предприятии регионального уровня	2	1	2
4	Рассмотрение особенностей объекта защиты информации	2	1	3
5	Определение угроз информационной безопасности на предприятии	2	2	4
6	Анализ рисков на предприятии	2	2	4
7	Определение комплекса практических мероприятий, направленных на обеспечение информационной безопасности предприятия	2	2	5
8	Построение концепции безопасности предприятия	2	2	5
9	Составление программы информационной безопасности предприятия	2	2	5
Всего:		17	14	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 6, час
1	2	3
Самостоятельная работа, всего	74	74
изучение теоретического материала дисциплины (ТО)	40	40
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	34	34
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 студентов 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.

10. Таблица 12 – Состав материально-технической базы

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

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

11.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Дифференцированный зачёт	Список вопросов; Тесты.

11.2. 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-12 «способность работать с различными источниками информации, инфорационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации»	
1	Математика. Аналитическая геометрия и линейная алгебра
1	Математика. Математический анализ
1	Иностранный язык
1	Общая теория государства и права
1	Актуальные проблемы государственного права
1	Промышленная экология
1	Конституционное право
1	Экология
2	Дискретная математика
2	Физика
2	Иностранный язык

2	Математика. Математический анализ
2	Математика. Аналитическая геометрия и линейная алгебра
2	Культурология
3	Иностранный язык
3	Средства вычислительной техники
3	Математика. Теория вероятностей и математическая статистика
3	Физика
4	Административное право
4	Криминалистика
4	Правоведение
4	Иностранный язык
4	Прикладная математика
4	Административный процесс
5	Основы электро-, радиоизмерений
5	Математические основы обработки информации
5	Микропроцессорные системы
5	Профессиональная этика и служебный этикет
5	Организация ЭВМ и вычислительных систем
5	Теория информации
7	Техническая защита информации
8	Технологии защиты от скрытой передачи данных
8	Психология профессиональной деятельности
8	Защита и обработка документов ограниченного доступа
9	Научно-технический семинар
9	Технологии защищенного документооборота
10	Научно-технический семинар
ПК-1 «способность формировать и 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»	
4	Криминалистика
6	Теория информационной безопасности
6	Теория кодирования
6	Программно-аппаратная защита информации
6	Производственная (эксплуатационная) практика
7	Методология защиты информации
8	Правовая защита информации
8	Технологии защиты от скрытой передачи данных
8	Организационная защита информации
ПК-2 «способность применять технические и программно-аппаратные средства обработки и защиты информации»	
2	Основы программирования
3	Основы программирования
3	Средства вычислительной техники

5	Криптографическая защита информации
5	Организация ЭВМ и вычислительных систем
5	Основы электро-, радиоизмерений
5	Микропроцессорные системы
6	Программно-аппаратная защита информации
6	Системы и сети передачи данных
6	Теория информационной безопасности
6	Криптографическая защита информации
6	Производственная (эксплуатационная) практика
7	Защита компьютерных сетей
7	Техническая защита информации
7	Методология защиты информации
7	Безопасность сетей ЭВМ
8	Правовая защита информации
8	Защита от вредоносных программ
ПК-17 «способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов»	
6	Теория информационной безопасности
6	Базы данных
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей
7	Информационное право
7	Базы данных
7	Методология защиты информации
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
9	Управление информационной безопасностью
10	Производственная преддипломная практика
ПК-19 «способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности»	
4	Основы информационной безопасности
5	Теория информации
6	Теория информационной безопасности
7	Методология защиты информации

11.3. 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.

11.4. 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
	Учебным планом не предусмотрено

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
	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. 7. Какие основные проблемы международного сотрудничества стоят на повестке дня сегодня? 8. Перечислите основные документы в области 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. 12. Что понимается под термином безопасность информации? 13. Что включает в себя защита информации? 14. Какие цели преследует защита информации? 15. Какое место занимается защита информации в информационной безопасности? 16. Какие уровни задействованы в обеспечении информационной безопасности? 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. 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? 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? 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?

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

	Учебным планом не предусмотрено

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

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	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 … , … , … .

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
	Примерный перечень тем рефератов 1. Основные понятия информационной безопасности. Цель защиты информации в частном и государственном секторе. 2. Современные требования к системе информационной безопасности организации. 3. Основные этапы создания системы защиты информации в организации. 4. Функциональное построение системы защиты информации. 5. Организационное построение системы защиты информации в организации. Семирубежная модель защиты. 6. Практические проблемы обеспечения информационной безопасности. 7. Место информационной безопасности в системе национальной безопасности Российской Федерации. 8. Структура Государственной системы обеспечения информационной безопасности Российской Федерации. 9. Структура и задачи Федеральной службы по техническому и экспортному контролю, и ее роль в управлении информационной безопасностью в РФ. 10. Иерархия законодательства Российской Федерации в области информационной безопасности. 11. ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ от 9 сентября 2000 г. № Пр-1895. 12. ФЕДЕРАЛЬНЫЙ ЗАКОН ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ от 27 июля 2006 года N 149-ФЗ. 13. Федеральный закон Российской Федерации "Об электронной подписи” от 6 апреля 2011 г. N 63-ФЗ. 14. Федеральный закон Российской Федерации “О персональных данных” от 27 июля 2006 г. N 152-ФЗ. 15. Основные направления обеспечения информационной безопасности на предприятии. 16. Многоуровневая структура системы защиты информации на предприятии. 17. Стратегии организации защиты информации на предприятии. 18. Архитектура системы защиты конфиденциального документооборота на

	предприятии. 19. Основные направления формирования конфиденциальных документов на предприятии. 20. Предпосылки отнесения информации к категории конфиденциальной и выявление конфиденциальных сведений на предприятии. 21. Порядок документирования конфиденциальных сведений. 22. Основные носители конфиденциальных сведений и угрозы конфиденциальному документообороту. 23. Жизненный цикл конфиденциального документа. 24. Структура документированной системы защиты в РФ. 25. Цели и задачи Политики информационной безопасности на предприятии 26. Уровни Политики информационной безопасности на предприятии. 27. Разработка Концепции безопасности информации и Регламента обеспечения безопасности информации на предприятии. 28. Понятие Профиль защиты и его составляющие. 29. Система физической защиты (СФЗ): основные задачи и способы их решения на предприятии. 30. Сценарии последовательности действий нарушителя СФЗ. 31. Организация инженерно-технических средств охраны. 32. Международные стандарты в области информационной безопасности. 33. Цели, задачи и стадии проведения аудита информационной безопасности. 34. Виды аудита информационной безопасности, применяемые на различных стадиях жизненного цикла обследуемого объекта. 35. Состав работ по проведения аудита информационной безопасности.

11.5. 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».

12. 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