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. Безгатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Комплексные системы защиты информации в правоохранительной сфере»
(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. Безгатеев
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. Арнашова-Тельник
должность, уч. степень, звание | подпись, дата | инициалы, фамилия

Аннотация

Дисциплина «Комплексные системы защиты информации в правоохранительной сфере» 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-7 «способность к логческому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии»;

профессиональных компетенций:

ПК-4 «способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации»,

ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»,

ПК-6 «способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»,

ПК-30 «способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации»;

профессионально-специализированных компетенций:

ПСК- 1.2 «способность использовать технологии разработки объектов профессиональной деятельности в правоохранительной сфере».

Содержание дисциплины охватывает круг вопросов, связанных с раскрытием сущности и задач КСЗИ; принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ; определение и нормативное закрепление состава защищаемой информации; определение объектов защиты; анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию; определение потенциальных каналов и методов несанкционированного доступа к информации; определение возможностей несанкционированного доступа к защищаемой информации; определение компонентов КСЗИ; определение условий функционирования КСЗИ; разработка модели КСЗИ; технологическое и организационное построение КСЗИ; кадровое обеспечение функционирования КСЗИ; материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ; назначение, структура и содержание управления КСЗИ; принципы и методы планирования функционирования КСЗИ; сущность и содержание контроля функционирования КСЗИ; управление КСЗИ в условиях чрезвычайных ситуаций; состав методов и моделей оценки эффективности КСЗИ.

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

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

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целями освоения дисциплины являются раскрытие сущности и задач КСЗИ; принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ; определение и нормативное закрепление состава защищаемой информации; определение

объектов защиты; анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию; определение потенциальных каналов и методов несанкционированного доступа к информации; определение возможностей несанкционированного доступа к защищаемой информации; определение компонентов КСЗИ; определение условий функционирования КСЗИ; разработка модели КСЗИ; технологическое и организационное построение КСЗИ; кадровое обеспечение функционирования КСЗИ; материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ; назначение, структура и содержание управления КСЗИ; принципы и методы планирования функционирования КСЗИ; сущность и содержание контроля функционирования КСЗИ; управление КСЗИ в условиях чрезвычайных ситуаций; состав методов и моделей оценки эффективности КСЗИ.

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОК-7 «способность к логческому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии»:

знать – основы логического вывода;
уметь – использовать логические выводы при проектировании систем защиты информации;
владеть навыками – ведения дискуссий в области систем защиты информации;
иметь опыт деятельности – написании докладов по системам защиты информации;

ПК-4 «способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации»:

знать – основные требования к системам защиты информации;
уметь – осуществлять оценку соответствия технических и программных средств требованиям защиты информации;
владеть навыками – тестирования информационных систем;
иметь опыт деятельности – по составлению отчетов по тестированию;

ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного населения»:
знать – состав технического обеспечения информационных систем;
уметь – сопровождать и настраивать техническое обеспечение информационных систем;
владеть навыками – настройки и установки компонентов технического обеспечения;
иметь опыт деятельности – по эксплуатации систем защиты информации;

ПК-6 «способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»:
знать – правила администрирования информационных систем;
уметь – осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации;
владеть навыками – поддержки систем обеспечения информационной безопасности;
иметь опыт деятельности – по администрированию информационных систем;

ПК-30 «способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации»:
знать – состав работ по комплексной защите информации;

уметь – осуществлять различные виды планирования;
владеть навыками – планирования работ по комплексной защите информационного объекта;
иметь опыт деятельности - по комплексной защите информации и сведений, составляющих государственную тайну;

ПСК- 1.2 «способность использовать технологии разработки объектов профессиональной деятельности в правоохранительной сфере»:
знать – современные технологии проектирования и разработки систем защиты информации;
уметь – использовать современные технологии проектирования и разработки для систем защиты информации;
владеть навыками – проектирования информационных систем в правоохранительной сфере;
иметь опыт деятельности – по системному анализу бизнес процессов в правоохранительной сфере.

2. Место дисциплины в структуре ОП

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

- Математическая логика и теория алгоритмов
- Введение в специальность
- Уголовное право
- Логика
- Гражданское право
- Служебное право
- Информационное право
- Организационная защита информации
- Правовая защита информации
- Криминология
- Средства вычислительной техники
- Программно-аппаратная защита информации
- Системы и сети передачи данных
- Техническая защита информации

Знания, полученные при изучении материала данной дисциплины, имеют самостоятельное значение.

3. Объем дисциплины в ЗЕ/академ. час

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

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№9
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	2/ 72	2/ 72
Из них часов практической подготовки	11	11
Аудиторные занятия, всего час.,	34	34

В том числе		
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	38	38
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Зачет	Зачет

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

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

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 9					
Раздел 1. Сущность, задачи и принципы организации КСЗИ	2				3
Раздел 2. Факторы, влияющие на организацию КСЗИ	2				5
Раздел 3. Определение объектов защиты	2		4		5
Раздел 4. Дестабилизирующие воздействия на информацию и их нейтрализация	2				5
Раздел 5. Определение возможностей несанкционированного доступа к защищаемой информации	2		4		5
Раздел 6. Определение компонентов КСЗИ	2		4		5
Раздел 7. Разработка модели КСЗИ	2		4		5
Раздел 8. Методы и модели оценки эффективности КСЗИ	3		1		5
Итого в семестре:	17		17		38
Итого:	17	0	17	0	38

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
Раздел 1.	Сущность, задачи и принципы организации КСЗИ Цели, задачи и принципы построения КСЗИ. Цели и задачи защиты информации в автоматизированных системах. Методологические основы организации КСЗИ.

	Разработка политики безопасности предприятия. Требования, предъявляемые к КСЗИ
Раздел 2.	Факторы, влияющие на организацию КСЗИ Влияние формы собственности на особенности защиты информации ограниченного доступ. Состав, объекты и степень конфиденциальности защищаемой информации. Состав, объекты и степень конфиденциальности защищаемой информации
Раздел 3.	Определение объектов защиты Методика выявления состава носителей защищаемой информации. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Состав средств обеспечения, подлежащих защите
Раздел 4.	Дестабилизирующие воздействия на информацию и их нейтрализация Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации. Модели нарушителей безопасности АС. Обеспечение безопасности информации в непредвиденных ситуациях
Раздел 5.	Определение возможностей несанкционированного доступа к защищаемой информации Технические каналы утечки информации, их классификация. Особенности защиты речевой информации. Механизмы обеспечения безопасности информации. Методика выявления нарушителей, тактики их действий и состава интересующей их информации
Раздел 6.	Определение компонентов КСЗИ Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ. Оптимальное построение системы защиты для АС. Проектирование системы зашиты информации для существующей АС
Раздел 7.	Разработка модели КСЗИ Общая характеристика задач моделирования КСЗИ. Формальные модели безопасности и их анализ. Прикладные модели защиты информации в АС. Формализация модели безопасности
Раздел 8.	Методы и модели оценки эффективности КСЗИ Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности КСЗИ

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

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

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 9				
1	Определение объектов защиты информации на объекте	4		3
2	Определение возможностей несанкционированного доступа к защищаемой информации	4	3	5
3	Определение компонентов КСЗИ	4	4	6
4	Разработка модели КСЗИ	4	4	7
5	Методы и модели оценки эффективности КСЗИ	1	4	8
	Всего:	17	11	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 9, час
1	2	3
Самостоятельная работа, всего	38	38
изучение теоретического материала дисциплины (ТО)	30	30
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	8	8
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

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

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

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

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

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

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

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

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

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

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

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

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

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

Состав материально-технической базы представлен в таблице 12.

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
Зачет	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-7 «способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии»	
1	История
1	Математическая логика и теория алгоритмов
1	Введение в специальность
2	Философия
2	Дискретная математика
2	Уголовное право
3	Уголовный процесс
4	Логика
4	Прикладная математика
4	Правоведение
5	Гражданское право
6	Международный бизнес
6	Психология воздействия
6	Гражданский процесс
6	Мировая экономика
6	Производственная (эксплуатационная) практика
7	Служебное право
7	Информационное право
8	Организационная защита информации
8	Производственная практика
8	Правовая защита информации
8	Криминология
9	Научно-технический семинар
9	Комплексные системы защиты информации в правоохранительной сфере
10	Научно-технический семинар
ПК-4 «способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации»	
3	Основы электротехники и радиоэлектроники
4	Основы электротехники и радиоэлектроники
6	Системы и сети передачи данных
6	Производственная (эксплуатационная) практика
8	Организационная защита информации
9	Комплексные системы защиты информации в правоохранительной сфере
9	Технологии защиты электронных платежей
9	Защита банковской информации
ПК-5 «способность осуществлять установку, настройку и эксплуатацию компонентов	

технических систем обеспечения безопасности информации и поддержку их работоспособного населения»	
3	Средства вычислительной техники
3	Основы электротехники и радиоэлектроники
4	Программирование. Методы и технологии программирования
4	Основы электротехники и радиоэлектроники
5	Микропроцессорные системы
5	Организация ЭВМ и вычислительных систем
5	Основы электро-, радиоизмерений
6	Программно-аппаратная защита информации
6	Системы и сети передачи данных
6	Производственная (эксплуатационная) практика
7	Защита компьютерных сетей
7	Безопасность сетей ЭВМ
8	Противодействие преступлениям в сфере информационных технологий
8	Программирование. Языки программирования
9	Комплексные системы защиты информации в правоохранительной сфере
ПК-6 «способность осуществлять администрирование подсистем обеспечения информационной безопасности объекта информатизации»	
3	Средства вычислительной техники
6	Программно-аппаратная защита информации
7	Распределенные информационные системы
7	Техническая защита информации
9	Комплексные системы защиты информации в правоохранительной сфере
ПК-30 «способность планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации»	
7	Распределенные информационные системы
8	Защита информации в распределенных информационных системах
9	Комплексные системы защиты информации в правоохранительной сфере
ПСК- 1.2 «способность использовать технологии разработки объектов профессиональной деятельности в правоохранительной сфере»	
9	Комплексные системы защиты информации в правоохранительной сфере

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
	Цели, задачи и принципы построения КСЗИ. Цели и задачи защиты информации в автоматизированных системах. Методологические основы организации КСЗИ. Разработка политики безопасности предприятия. Требования, предъявляемые к КСЗИ.

	Состав, объекты и степень конфиденциальности защищаемой информации. Методика выявления состава носителей защищаемой информации. Факторы, определяющие необходимость защиты периметра и здания предприятия. Особенности помещений как объектов защиты для работы по защите информации. Состав средств обеспечения, подлежащих защите. Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации. Модели нарушителей безопасности АС. Обеспечение безопасности информации в непредвиденных ситуациях. Технические каналы утечки информации, их классификация. Особенности защиты речевой информации. Механизмы обеспечения безопасности информации. Методика выявления нарушителей, тактики их действий и состава интересующей их информации. Особенности синтеза СЗИ АС от НСД. Методика синтеза СЗИ. Оптимальное построение системы защиты для АС. Проектирование системы зашиты информации для существующей АС. Общая характеристика задач моделирования КСЗИ. Формальные модели безопасности и их анализ. Прикладные модели защиты информации в АС. Формализация модели безопасности. Показатель уровня защищенности, основанный на экспертных оценках. Методы проведения экспертного опроса. Экономический подход к оценке эффективности КСЗИ

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. «Троянскийконь» является разновидностью модели воздействия программных закладок *искажение* уборка мусора наблюдение и компрометация перехват **2. В «Европейских критериях» количество классов безопасности равно** *10*

	12 5 7 **3. В модели политики безопасности Лендвера одноуровневый блок информации называется** *объектом* массивом множеством контейнером **4. В модели политики безопасности Лендвера ссылка на сущность, если это последовательность имен сущностей, называется** *косвенной* сложной циклической прямой **5. Гарнтия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это** *целостность* детерминированность восстанавливаемость доступность **6. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство** *доступность* детерминированность восстанавливаемость целостность **7. Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели** *искажение* наблюдение компрометация перехват **8. Длина исходного ключа у алгоритма шифрования DES (бит)** *56* 128 64 256 **9. Домены безопасности согласно «Оранжевой книге» используются в системах класса** *B3* C3 C2

	В2 **10. Достоинствами программной реализации криптографического закрытия данных являются** *практичность и гибкость* корректность и функциональность безопасность и эффективность высокая производительность и простота **11. Достоинством модели конечных состояний политики безопасности является** *высокая степень надежности* удобство эксплуатации дешевизна простота реализации **12. Единственный ключ используется в криптосистемах** *симметричных* с закрытым ключом с открытым ключом асимметричных **13. Если средство защиты способно противостоять корпоративному злоумышленнику, то согласно «Европейским критериям» безопасность считается** *средней* высокой базовой стандартной **14. Задачей анализа модели политики безопасности на основе анализа угроз системе является** *минимизация вероятности преодоления системы защиты* максимизация затрат для взлома максимизация ресурса для взлома максимизация времени взлома **15. Из перечисленного: 1) администраторы; 2) пользователи; 3) задания; 4) терминалы; 5) программы; 6) файлы — модель политики безопасности Адепт-50 рассматривает следующие группы безопасности** *2, 3, 4, 6* 1, 2, 5, 6 3, 4, 5, 6 1, 2, 3, 4

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

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	1. Напишите программу, реализующую протокол строгой двусторонней аутентифи-кации на основе случайных чисел. Используйте решетку Флейберга в качестве симметричного алгоритма и стандартную функцию

	генерации случайных чисел выбранного языка программирования. 2. Напишите программу, реализующую протокол строгой двусторонней аутентифи-кации на основе случайных чисел. Используйте Шифр Плейфейера в качестве симметричного алгоритма и стандартную функцию генерации случайных чисел выбранного языка программирования. 3. Запрограммируйте линейный конгруэнтный генератор псевдослучайных чисел. 4. Запрограммируйте смешанный квадратичный генератор псевдослучайных чисел 5. Разработайте программу, реализующую модель безопасности Белла-ЛаПадула. Ос-новные функции программы: регистрация пользователей (при регистрации пользо-ватель получает уровень допуска), авторизация, создание текстовых заметок (при создании заметка получает уровень секретности), просмотр и редактирование заме-ток. 6. Разработайте программу, реализующую диспетчер безопасности на основе ACL. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и попытка доступа к объекту. 7. Разработайте программу, реализующую диспетчер безопасности на основе списков полномочий субъектов. Функции программы: регистрация объектов, регистрация субъектов, просмотр и редактирование привилегий, вход от лица субъекта и по-пытка доступа к объекту.

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

Целями освоения дисциплины являются раскрытие сущности и задач КСЗИ; принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ; определение и нормативное закрепление состава защищаемой информации; определение объектов защиты; анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию; определение потенциальных каналов и методов несанкционированного доступа к информации; определение возможностей несанкционированного доступа к защищаемой информации; определение компонентов КСЗИ; определение условий функционирования КСЗИ; разработка модели КСЗИ; технологическое и организационное построение КСЗИ; кадровое обеспечение функционирования КСЗИ; материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ; назначение, структура и содержание управления КСЗИ; принципы и методы планирования функционирования КСЗИ; сущность и содержание контроля функционирования КСЗИ; управление КСЗИ в условиях чрезвычайных ситуаций; состав методов и моделей оценки эффективности КСЗИ.

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:

– Сущность, задачи и принципы организации КСЗИ
– Факторы, влияющие на организацию КСЗИ
– Определение объектов защиты
– Дестабилизирующие воздействия на информацию и их нейтрализация
– Определение возможностей несанкционированного доступа к защищаемой информации
– Определение компонентов КСЗИ
– Разработка модели КСЗИ
– Методы и модели оценки эффективности КСЗИ

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 моделей и алгоритмов комплексной защиты информации:

Определение объектов защиты информации на объекте

Определение возможностей несанкционированного доступа к защищаемой информации

Определение компонентов КСЗИ

Разработка модели КСЗИ

Методы и модели оценки эффективности КСЗИ

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