

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

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«25» мая 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационная защита 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– 2023

Лист согласования рабочей программы дисциплины

Программу составил (а)

ДОЦ.,К.Т.Н.,ДОЦ.

(должность, уч. степень, звание)



25.05.23

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«25» мая 2023 г, протокол № 10

Заведующий кафедрой № 33

Д.Т.Н.,ДОЦ.

(уч. степень, звание)



25.05.23

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Ответственный за ОП ВО 10.05.05(05)

ДОЦ.,К.Т.Н.,ДОЦ.

(должность, уч. степень, звание)



25.05.23

(подпись, дата)

В.А. Мыльников

(инициалы, фамилия)

Заместитель директора института №3 по методической работе

(должность, уч. степень, звание)



25.05.23

(подпись, дата)

Н.В. Решетникова

(инициалы, фамилия)

Аннотация

Дисциплина «Организационная защита 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 «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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

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

Содержание дисциплины охватывает круг вопросов, связанных с угрозами информационной безопасности объекта; организацией службы безопасности объекта; подбором и работой с кадрами в сфере информационной безопасности; организацией и обеспечением режима секретности; охраной объектов.

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

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

Общая трудоемкость освоения дисциплины составляет 10 зачетных единиц, 360 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью дисциплины является формирование знаний по организационному обеспечению информационной безопасности и навыков по организации информационной безопасности для конкретных условий.

Задачи изучения дисциплины - дать знания по вопросам:

угроз информационной безопасности объекта;

организации службы безопасности объекта;

подбора и работы с кадрами в сфере информационной безопасности;

организации и обеспечение режима секретности;

охраны объектов.

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

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

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

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	ОПК-4 Способен выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	ОПК-4.В.1 владеть навыками разработки технической проектной документации с учетом нормативных правовых актов, нормативных и методических документов при организации системы защиты информации
Общепрофессиональные компетенции	ОПК-8 Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих	ОПК-8.3.1 знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области ОПК-8.У.2 уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и

	государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	оценки защищенности компьютерных систем
Общепрофессиональные компетенции	ОПК-11 Способен использовать автоматизированные информационные системы в профессиональной деятельности	ОПК-11.У.1 уметь разрабатывать концептуальную модель прикладной области

2. Место дисциплины в структуре ОП

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

- Введение в специальность
- Уголовное право
- Уголовный процесс
- Правоведение
- Гражданское право
- Служебное право
- Информационное право
- Специальные информационные технологии в правоохранительной деятельности
- Теория информационной безопасности
- Криминалистика

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	
		№7	№8
1	2	3	4
Общая трудоемкость дисциплины, ЗЕ/ (час)	10/ 360	5/ 180	5/ 180
Из них часов практической подготовки			
Аудиторные занятия, всего час.	119	51	68
в том числе:			
лекции (Л), (час)	51	34	17
практические/семинарские занятия (ПЗ), (час)	51	17	34
лабораторные работы (ЛР), (час)			
курсовой проект (работа) (КП, КР), (час)	17		17
экзамен, (час)	90	36	54
Самостоятельная работа, всего (час)	151	93	58

Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз., Экз.	Экз.	Экз.
---	---------------	------	------

Примечание: ** кандидатский экзамен

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

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

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Концептуальные положения организационного обеспечения информационной безопасности	12	6			30
Раздел 2. Организация службы безопасности объекта	12	6			33
Раздел 3. Подбор сотрудников и работа с кадрами	10	5			30
Итого в семестре:	34	17			93
Семестр 8					
Раздел 4. Организация и обеспечение режима секретности на объекте	4	8			10
Раздел 5. Организация аналитической работы по предупреждению утечки конфиденциальной информации	4	8			10
Раздел 6. Организация внутриобъектового режима	4	8			18
Раздел 7. Организация охраны объектов	5	10			20
Выполнение курсовой работы				17	
Итого в семестре:	17	34		17	58
Итого	51	51	0	17	151

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	Принципы, силы, средства и условия организационной защиты информации Виды угроз информационной безопасности на объекте защиты, их характеристика, оценка ущерба вследствие организационных нарушений информационных нарушений информационной безопасности на объекте. Основные направления организационной защиты на объекте. Структура сил и средств информационной защиты информации
2	Функции, задачи и особенности службы безопасности объекта. Принципы организации службы безопасности объекта.

	<p>Типовая структура службы безопасности. Основные документы, регламентирующие деятельность службы безопасности объекта.</p> <p>Способы и формы участия сотрудников в организационной защите информации. Особенности действий сотрудников службы безопасности в чрезвычайных ситуациях и в условиях чрезвычайного положения.</p> <p>Способы и формы взаимодействия службы безопасности с контрразведывательными и правоохранительными органами.</p>
3	<p>Роль персонала в обеспечении информационной безопасности объекта. Требования к сотрудникам организации, допущенных к секретной (конфиденциальной) информации.</p> <p>Основные критерии приема на работу, связанную с сохранением тайны. Состав документов, необходимых при подборе и приеме сотрудников на работу. Методы проверки кандидатов на должности..</p> <p>Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала, ее методы и формы</p> <p>Организация контроля выполнения сотрудниками требований режима и секретности. Цели, задачи и процедуры служебного расследования нарушения режима секретности. Меры по защите информации при увольнении сотрудника.</p>
4	<p>Организация и обеспечение секретного делопроизводства. порядок засекречивания и рассекречивания сведений, документов и продукции; допуск и доступ к конфиденциальной информации и документам</p> <p>Режим секретности при работе с секретными документами и при обработке секретных документов с применением средств вычислительной техники и технических средств иностранного производства.</p> <p>Допуск к секретной (конфиденциальной) информации. Формы допусков. Организация работы по обеспечению контроля за допуском сотрудников и посетителей.</p> <p>Защита информации при публикаторской и рекламной деятельности.</p> <p>Обеспечение режима секретности при деятельности объекта: разработка изделий, испытание, транспортировка. Подготовка и проведение служебного совещания по секретной тематике</p>
5	<p>Понятие информационно-аналитической работы. Направления аналитической работы.</p> <p>Этапы и методы аналитической работы</p>
6	<p>Назначение и требования внутриобъектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Требования к помещениям внутри которых циркулирует защищаемая информация. Категорирование помещений. Обеспечение режима в выделенных помещениях.</p> <p>Определение границы контролируемых зон. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации. Порядок пребывания и контроля посетителей. Обеспечение защиты информации в экстремальных ситуациях и условиях чрезвычайного положения</p>
7	<p>Цели и задачи, объекты, виды и способы охраны. Посты охраны. Связь, взаимодействие с органами правопорядка. использование собак и борьба с собаками нарушителя. Прием и сдача объекта. Средства и методы физической защиты. Технические средства охраны и видеонаблюдения. Оружие, индивидуальная защита от оружия, оборона объекта в случае нападения. Транспортировка</p>

	<p>объектов защиты. Средства противопожарной охраны. Организация пропускного режима. Понятие, цели и задачи пропускного режима. Атрибутные и биометрические идентификаторы людей. Порядок оформления и выдачи пропусков. КПП людей и автотранспорта, их оборудование и организация. Порядок ввоза/вывоза вноса/выноса документов и материальных ценностей</p>
--	---

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7					
1	Изучение законодательных основ организационной защиты информации	групповые дискуссии	3		1
2	Разработка документов, регламентирующих организационную защиту информации	игровое проектирование	3		1
3	Разработка технологии подбора персонала для работы с конфиденциальными документами	игровое проектирование	3		2
4	Организация проведения служебного расследования	занятия по моделированию реальных условий	3		2
5	Организация и обеспечение режима секретности	занятия по моделированию реальных условий	5		3
Семестр 8					
6	Подготовка помещения к проведению совещания	занятия по моделированию реальных условий	4		4
7	Организация охраны объекта в условиях чрезвычайных ситуаций	занятия по моделированию реальных условий	4		4
8	Категорирование помещений объекта, определение контролируемых зон	решение ситуационных задач	5		8
9	Исследование угроз информационной	решение ситуационных задач	6		4

	безопасности на защищаемом объекте				
10	Изучение спецсредств индивидуальной защиты	групповые дискуссии	6		4
11	Разработка системы охраны и пропускного режима объекта	игровое проектирование	10		7
Всего			51		

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
Учебным планом не предусмотрено				
Всего				

4.5. Курсовое проектирование/ выполнение курсовой работы

Цель курсовой работы: разработка системы защиты информации, детальное проектирование организационных аспектов информационной безопасности предприятия.

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

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час	Семестр 8, час
1	2	3	4
Изучение теоретического материала дисциплины (ТО)	93	53	40
Курсовое проектирование (КП, КР)			
Расчетно-графические задания (РГЗ)			
Выполнение реферата (Р)			
Подготовка к текущему контролю успеваемости (ТКУ)	28	20	8
Домашнее задание (ДЗ)			
Контрольные работы заочников (КРЗ)			
Подготовка к промежуточной аттестации (ПА)	28	20	8
Всего:	151	93	58

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 <ul style="list-style-type: none"> 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 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 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 таблице 12.

Таблица 12 – Состав материально-технической базы

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

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.
Выполнение курсовой работы	Экспертная оценка на основе требований к содержанию курсовой работы по дисциплине.

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 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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»	<ul style="list-style-type: none"> – 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	<p>Перечислите виды угроз информационной безопасности РФ.</p> <p>Что является источниками угроз информационной безопасности РФ?</p> <p>Назовите основные задачи обеспечения информационной безопасности РФ. Какие из них требуют безотлагательного решения?</p> <p>Перечислите основные методы обеспечения информационной безопасности РФ и кратко охарактеризуйте их.</p> <p>Какие пункты, оговаривающие процедуру защиты информации предприятия, можно включить в трудовой договор?</p>	ОПК-4.В.1

	<p>В чем заключаются особенности увольнения сотрудников, владеющих конфиденциальной информацией предприятия?</p> <p>Что представляет собой процесс лицензирования деятельности по защите информации в РФ?</p> <p>Что такое сертификат на средство защиты информации? Для чего он нужен?</p> <p>Назовите нормативно-правовые документы РФ, являющиеся базой лицензирования и сертификации в области защиты информации.</p> <p>Какие государственные органы РФ уполномочены на ведение лицензионной деятельности в области защиты информации?</p> <p>На каких принципах основана процедура проведения сертификации средств защиты информации?</p>	
2	<p>Какова структура государственной системы обеспечения информационной безопасности РФ?</p> <p>Что включают организационные методы защиты информации?</p> <p>На что направлена деятельность по защите информации?</p> <p>Какими нормативными документами руководствуется служба безопасности в своей деятельности?</p> <p>Какие функции выполняет служба безопасности на предприятии?</p> <p>Назовите, какие виды пропускных документов применяются при организации внутриобъектового режима предприятия?</p> <p>Для чего организуют внутриобъектовый режим на предприятии?</p> <p>Как оценивается эффективность системы защиты предприятия?</p> <p>Назовите, какие существуют виды охраны объектов?</p> <p>Для чего на объекте организуется многорубежная защита?</p> <p>Какими достоинствами обладает такой вид организации защиты объекта?</p>	ОПК-8.3.1
3	<p>Какие задачи обеспечения информационной безопасности решаются на организационном уровне?</p> <p>Что такое система безопасности предприятия?</p> <p>На основе каких принципов осуществляется функционирование системы безопасности предприятия?</p> <p>Каким требованиям должна удовлетворять система безопасности предприятия?</p> <p>Сформулируйте правила, которые следует соблюдать при работе с конфиденциальными документами.</p> <p>Назовите основные этапы профотбора сотрудников для работы на коммерческом предприятии.</p> <p>Назовите группы людей, от которых могут исходить угрозы информационным ресурсам предприятия.</p> <p>Приведите примеры тестовых методик, применяемых при отборе сотрудников.</p> <p>Какова структура заключительного собеседования?</p> <p>Какие функции должна выполнять служба безопасности по проверке сотрудников предприятия на благонадежность?</p> <p>Какие методы сбора информации о гражданах могут использовать сотрудники службы безопасности предприятия?</p> <p>В чем состоит особенность проверки благонадежности кандидатов на замещение руководящих должностей?</p> <p>В какой момент времени работнику следует подписать обязательства о неразглашении конфиденциальных сведений предприятия?</p>	ОПК-8.У.2
4	<p>Что является компонентами комплексной модели информационной безопасности?</p>	ОПК-11.У.1

	<p>Перечислите виды объектов защиты. Назовите возможные пути утраты информации. Дайте характеристику основным элементам системы защиты предприятия. Что такое защитные действия? Приведите классификацию защитных действий. Что следует сделать для того, чтобы исключить неправомерное овладение конфиденциальной информацией? Что является основными целями защиты информации в информационных системах?</p>	
--	--	--

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

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

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

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

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	<ol style="list-style-type: none"> 1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей. 3. Анализ методов и средств анализа защищенности беспроводных сетей. 4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 5. Виброакустические средства современных систем обеспечения информационной безопасности. 6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 8. Средства обеспечения информационной безопасности банков данных. 9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации. 11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 15. Инструментальные средства анализа рисков информационной безопасности. 16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).

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
	<p>1. Выберите правильный ответ Основным источником права в области обеспечения информационной безопасности в России является</p> <p>а) Уголовный кодекс б) Конституция в) государственные и отраслевые стандарты г) Документы Гостехкомиссии</p> <p>2. Выберите правильный ответ В статье 42 Конституции РФ говорится о том, что</p> <p>а) каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений б) сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются в) каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом г) каждый имеет право на достоверную информацию о состоянии окружающей среды</p> <p>3. Дополните предложение Федеральные законы и другие нормативные акты предусматривают разделение информации на категории свободного и _____ доступа.</p> <p>4. Выберите правильный ответ В соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную и служебную тайну, осуществляет коллегиальный орган</p> <p>а) ФАПСИ б) ФСБ в) Гостехкомиссия г) Главная научно-исследовательская организация по защите информации</p> <p>5. Выберите правильный ответ Со совокупность норм гражданского права, регулирующих отношения по признанию авторства и охране имущественных и неимущественных прав авторов и правообладателей это определение</p> <p>а) сертификата б) авторского права в) патента г) товарного знака</p> <p>6. Дополните предложение Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения</p>	

7. Выберите правильный ответ

Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы для ЭВМ или базы данных, использовать знак охраны авторского права

- а) ©
- б) ®
- в) тм
- г)

8. Выберите правильный ответ

Символ ® означает

- а) патент
- б) охраняемый знак
- в) торговую марку
- г) авторское право

9. Выберите правильный ответ

Программы для ЭВМ и базы данных к объектам авторского права

- а) относятся
- б) относятся в исключительных случаях
- в) не относятся

10. Дополните предложение

Основной принцип компьютерной стеганографии предполагает использование двух типов файлов – файл-_____, которое должно быть скрыто, и файл-контейнер

1. Выберите правильный ответ

Согласно статьи 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия

- а) возможны в исключительных случаях
- б) проводится постоянно
- в) не допускается

2. Выберите правильный ответ

Каждый имеет право на достоверную информацию о состоянии окружающей среды это выдержка из следующей статьи Конституции РФ

- а) 23
- б) 24
- в) 29
- г) 42

3. Дополните предложение

Государственная тайна относится к информации _____ доступа

4. Выберите правильный ответ

Комплекс действий, проводимых с целью подтверждения соответствия определенным нормам ГОСТ и других нормативных документов называется

- а) лицензированием
- б) сертификацией
- в) авторским правом
- г) торговой маркой

5. Выберите правильный ответ

Способ оформления уникальных идей это определение

- а) сертификата
- б) авторского права
- в) патента
- г) товарного знака

6. Дополните предложение

Авторское право действует с момента создания программы для ЭВМ или базы данных в течение всей жизни автора и ____ лет после его смерти.

7. Выберите правильный ответ

Символ © означает

	а) патент б) охраняемый знак в) торговую марку г) авторское право 8. Выберите правильный ответ Символ TM означает а) патент б) охраняемый знак в) торговую марку г) авторское право 9. Выберите правильные ответы Незаконное использование программ для ЭВМ либо иное нарушение авторских прав на программы для ЭВМ влечет за собой а) гражданско-правовую ответственность б) административную в) уголовную 10. Дополните предложение Компьютерная стеганография относится к методам, предусматривающие наличие _____ авторской «подписи», внедряемой в цифровой файл, как правило, с использованием стеганографических технологий	
--	---	--

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

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

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

11. Методические указания для обучающихся по освоению дисциплины

Целью дисциплины является формирование знаний по организационному обеспечению информационной безопасности и навыков по организации информационной безопасности для конкретных условий.

Задачи изучения дисциплины - дать знания по вопросам:

- угроз информационной безопасности объекта;
- организации службы безопасности объекта;
- подбора и работы с кадрами в сфере информационной безопасности;
- организации и обеспечение режима секретности;
- охраны объектов.

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;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

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

Структура предоставления лекционного материала:

- Раздел 1. Концептуальные положения организационного обеспечения информационной безопасности
- Раздел 2. Организация службы безопасности объекта
- Раздел 3. Подбор сотрудников и работа с кадрами
- Раздел 4. Организация и обеспечение режима секретности на объекте
- Раздел 5. Организация аналитической работы по предупреждению утечки конфиденциальной информации
- Раздел 6. Организация внутриобъектового режима
- Раздел 7. Организация охраны объектов

Методические указания для обучающихся по прохождению практических занятий

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

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

Планируемые результаты при освоении обучающимся практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;
- обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Функции практических занятий:

- познавательная;

- развивающая;
- воспитательная.

По характеру выполняемых обучающимся заданий по практическим занятиям подразделяются на:

- ознакомительные, проводимые с целью закрепления и конкретизации изученного теоретического материала;
- аналитические, ставящие своей целью получение новой информации на основе формализованных методов;
- творческие, связанные с получением новой информации путем самостоятельно выбранных подходов к решению задач.

Формы организации практических занятий определяются в соответствии со специфическими особенностями учебной дисциплины и целями обучения. Они могут проводиться:

- в интерактивной форме (решение ситуационных задач, занятия по моделированию реальных условий, деловые игры, игровое проектирование, имитационные занятия, выездные занятия в организации (предприятия), деловая учебная игра, ролевая игра, психологический тренинг, кейс, мозговой штурм, групповые дискуссии);
- в не интерактивной форме (выполнение упражнений, решение типовых задач, решение ситуационных задач и другое).

Методика проведения практического занятия может быть различной, при этом важно достижение общей цели дисциплины.

Требования к проведению практических занятий

- Студент должен получить тему и список вопросов и заданий до проведения практического занятия;
- Студент должен уметь ответить на любой вопрос из списка;
- Студент должен решить предложенную преподавателем задачу или задание;
- Ответы и решенные задачи оцениваются баллами, которые суммируются.
- По окончании всех практических занятий студент получает допуск к экзамену.

Методические указания для обучающихся по прохождению курсового проектирования/ работы

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

Курсовой проект/ работа позволяет обучающемуся:

- систематизировать и закрепить полученные теоретические знания и практические умения по профессиональным учебным дисциплинам и модулям в соответствии с требованиями к уровню подготовки, установленными программой учебной дисциплины, программой подготовки специалиста соответствующего уровня, квалификации;
- применить полученные знания, умения и практический опыт при решении комплексных задач, в соответствии с основными видами профессиональной деятельности по направлению/ специальности/ программе;
- углубить теоретические знания в соответствии с заданной темой;
- сформировать умения применять теоретические знания при решении нестандартных задач;
- приобрести опыт аналитической, расчётной, конструкторской работы и сформировать соответствующие умения;
- сформировать умения работы со специальной литературой, справочной, нормативной и правовой документацией и иными информационными источниками;

- сформировать умения формулировать логически обоснованные выводы, предложения и рекомендации по результатам выполнения работы;
- развить профессиональную письменную и устную речь обучающегося;
- развить системное мышление, творческую инициативу, самостоятельность, организованность и ответственность за принимаемые решения;
- сформировать навыки планомерной регулярной работы над решением поставленных задач.

Структура пояснительной записки курсовой работы / проекта

Изучение курса «Организационная защита информации» заканчивается выполнением курсовой работы по проектированию корпоративной системы информационной безопасности (организационной подсистемы). Содержание курсового проекта излагается в программе курса для соответствующих специальностей и должно соответствовать приведенному в приложении заданию на курсовое проектирование. Бланк задания на курсовое проектирование должен быть подшит в пояснительную записку перед введением.

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

- титульный лист;
- индивидуальное задание;
- пояснительную записку;
- программы и спецификации на электронном носителе;

Пояснительная записка содержит разделы:

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

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

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

Листинги программ с подробными комментариями должны быть приведены в приложениях.

Задачи курсового проекта:

1. Описание предметной области.
2. Построение инфологической модели бизнес-процессов предприятия и анализ этой модели.
3. Создание модели угроз информационной безопасности предприятия.
4. Проектирование организационных мер обеспечения информационной безопасности.
5. Описание и обоснование модели защиты.
6. Построение иерархии форм приложения.
7. Проектирование локального программного приложения.

Требования к оформлению пояснительной записки курсовой работы / проекта

В виду принадлежности курсового проекта к дисциплинам связанным с информационными технологиями и электронно-вычислительными машинами пояснительная записка должна быть оформлена при помощи любого программного инструмента и распечатана на листах формата А4 (210×297 мм), листы должны быть

пронумерованы и сшиты. Поля листа должны составлять левое 25 мм, верхнее и нижнее 20 мм, правое 15 мм. Текст записки должен быть набран удобочитаемым шрифтом по размеру и начертанию соответствующий «Times New Roman» в 14 пт. Межстрочный интервал должен соответствовать полуторному. В записке также должен быть предусмотрен карман для помещения в него диска с работоспособным приложением и всеми исходными текстами программ. Допускается помещать на дискету архив в формате zip или rar.

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

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

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