

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

Кафедра № 34


УТВЕРЖДАЮ  
Руководитель направления  
проф. д.т.н., доц.  
(должность, уч. степень, звание)  
С.В. Беззатеев  
(инициалы, фамилия)  
(подпись)  
«27» мая 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
«Стандарты информационной безопасности»  
(Наименование дисциплины)


Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Безопасность открытых информационных систем
Форма обучения	очная

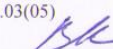
Санкт-Петербург – 2021

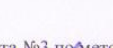
Лист согласования рабочей программы дисциплины

Программу составил (а)  
доц., к.э.н., доц.  24.05.21 Т.Н. Елина  
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 34  
«27» мая 2021 г, протокол № 10

Заведующий кафедрой № 34  
д.т.н., доц.  24.05.21 С.В. Беззатеев  
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Ответственный за ОП ВО 10.05.03(05)  
доц., к.т.н., доц.  24.05.21 В.А. Мыльников  
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №3 по методической работе  
доц., к.э.н., доц.  24.05.21 Г.С. Армашова-Тельник  
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

## Аннотация

Дисциплина «Стандарты информационной безопасности» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№34».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-4 «Способен осуществлять работы по разработке систем защиты информации автоматизированных систем»

ПК-7 «Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа»

ПК-9 «Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»

ПК-11 «Способен проводить оценку уровня информационной безопасности открытых информационных систем»

Содержание дисциплины охватывает круг вопросов, связанных с усвоением знаний по нормативно-правовым основам организации информационной безопасности, изучением стандартов и руководящих документов по защите информационных систем; ознакомлением с основными угрозами информационной безопасности; правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности; формированием научного мировоззрения, навыков индивидуальной самостоятельной работы с учебным материалом.

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

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

Получение обучающимися необходимых знаний и навыков по нормативно-правовым основам организации информационной безопасности, изучением стандартов и руководящих документов по защите информационных систем; ознакомлением с основными угрозами информационной безопасности; правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности; формированием научного мировоззрения, навыков индивидуальной самостоятельной работы с учебным материалом.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, 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
Профессиональные компетенции	ПК-4 Способен осуществлять работы по разработке систем защиты информации автоматизированных систем	ПК-4.В.1 владеть навыками разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах
Профессиональные компетенции	ПК-7 Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа	ПК-7.3.1 знать порядок сертификации средств и систем защиты от несанкционированного доступа
Профессиональные компетенции	ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-9.3.3 знать формальные модели управления доступом
Профессиональные компетенции	ПК-11 Способен проводить оценку уровня информационной безопасности открытых информационных систем	ПК-11.У.2 уметь проводить анализ средств защиты с целью определения уровня обеспечиваемой ими защищенности и доверия

## 2. Место дисциплины в структуре ОП

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

- Введение в специальность
- Информационные технологии
- Основы информационной безопасности

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

- Управление информационной безопасностью
- Организационное и правовое обеспечение информационной безопасности
- Информационная безопасность распределенных информационных систем
- Разработка и эксплуатация защищенных автоматизированных систем

Проектирование безопасных информационных систем

## 3. Объем и трудоемкость дисциплины

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

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№5
1	2	3
<b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>	3/ 108	3/ 108
<b>Из них часов практической подготовки</b>	17	17
<b>Аудиторные занятия, всего час.</b>	51	51
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
<b>Самостоятельная работа, всего (час)</b>	57	57
<b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет	Зачет

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 5					
Раздел 1: Обзор наиболее важных стандартов и	2				2

спецификаций в области информационной безопасности					
Раздел 2: "Общие критерии", часть 1. Основные идеи	2	4			2
Раздел 3: "Общие критерии", часть 2. Функциональные требования безопасности	2				2
Раздел 4: "Общие критерии", часть 3. Требования доверия безопасности	2				2
Раздел 5: Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности	2	5			2
Раздел 6: Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности	2				3
Раздел 7: Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности	2				4
Раздел 8: Рекомендации семейства X.500 84	2				4
Раздел 9: Спецификации Internet-сообщества IPsec	2	4			4
Раздел 10: Спецификация Internet-сообщества TLS	2				4
Раздел 11. Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности"	2				4
Раздел 12. Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия"	2				4
Раздел 13. Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности"	2				4
Раздел 14. Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"	2				4
Раздел 15. Британский стандарт BS 7799	2	2			4
Раздел 16. Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	2	2			4
Раздел 17. Заключение	2				4
Итого в семестре:	34	17			57
Итого	34	17	0	0	57

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	<p>Раздел 1: Обзор наиболее важных стандартов и спецификаций в области информационной безопасности</p> <p>Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности</p> <p>Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса.</p> <p>Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций</p>
2	<p>Раздел 2: "Общие критерии", часть 1. Основные идеи</p> <p>История создания и текущий статус "Общих критериев"</p> <p>Основные понятия и идеи "Общих критериев"</p> <p>Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий"</p>
3	<p>Раздел 3: "Общие критерии", часть 2. Функциональные требования безопасности</p> <p>Классификация функциональных требований безопасности</p> <p>Классы функциональных требований, описывающие элементарные сервисы безопасности</p> <p>Классы функциональных требований, описывающие производные сервисы безопасности</p> <p>Защита данных пользователя</p> <p>Защита функций безопасности объекта оценки</p> <p>Классы функциональных требований, играющие инфраструктурную роль</p>
4	<p>Раздел 4: "Общие критерии", часть 3. Требования доверия безопасности</p> <p>Основные понятия и классификация требований доверия безопасности</p> <p>Оценка профилей защиты и заданий по безопасности</p> <p>Требования доверия к этапу разработки</p> <p>Требования к этапу получения, представления и анализа результатов разработки</p> <p>Требования к поставке и эксплуатации, поддержка доверия</p> <p>Оценочные уровни доверия безопасности</p>
5	<p>Раздел 5: Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности</p> <p>Общие положения</p> <p>Общие предположения безопасности</p> <p>Общие угрозы безопасности</p> <p>Общие элементы политики и цели безопасности</p> <p>Общие функциональные требования</p> <p>Общие требования доверия безопасности</p>
6	<p>Раздел 6: Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности</p> <p>Биометрическая идентификация и аутентификация</p> <p>Требования к произвольному (дискреционному) управлению доступом</p> <p>Требования к принудительному (мандатному) управлению доступом</p> <p>Ролевое управление доступом</p> <p>Межсетевое экранирование</p> <p>Системы активного аудита</p> <p>Анонимизаторы</p> <p>Анализ защищенности</p>
7	<p>Раздел 7: Профили защиты, разработанные на основе "Общих</p>

	<p>критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности</p> <p>Операционные системы</p> <p>Виртуальные частные сети</p> <p>Виртуальные локальные сети</p> <p>Смарт-карты</p> <p>Некоторые выводы</p>
<b>8</b>	<p>Раздел 8: Рекомендации семейства X.500 84</p> <p>Основные понятия и идеи рекомендаций семейства X.500</p> <p>Каркас сертификатов открытых ключей</p> <p>Каркас сертификатов атрибутов</p> <p>Простая и сильная аутентификация</p>
<b>9</b>	<p>Раздел 9: Спецификации Internet-сообщества IPsec</p> <p>Архитектура средств безопасности IP-уровня</p> <p>Контексты безопасности и управление ключами</p> <p>Протокольные контексты и политика безопасности</p> <p>Обеспечение аутентичности IP-пакетов</p> <p>Обеспечение конфиденциальности сетевого трафика</p>
<b>10</b>	<p>Раздел 10: Спецификация Internet-сообщества TLS</p> <p>Основные идеи и понятия протокола TLS</p> <p>Протокол передачи записей</p> <p>Протокол установления соединений и ассоциированные протоколы</p> <p>Применение протокола HTTP над TLS</p>
<b>11</b>	<p>Раздел 11. Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности"</p> <p>Введение</p> <p>Основные понятия</p> <p>Функции для работы с удостоверениями</p> <p>Создание и уничтожение контекстов безопасности</p> <p>Защита сообщений</p> <p>Логика работы пользователей интерфейса безопасности</p> <p>Представление некоторых объектов интерфейса безопасности в среде языка C</p>
<b>12</b>	<p>Раздел 12. Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия"</p> <p>Основные понятия</p> <p>Проблемы, с которыми может столкнуться организация</p> <p>Основы предлагаемого подхода</p> <p>Общие принципы выработки официальной политики предприятия в области информационной безопасности</p> <p>Анализ рисков, идентификация активов и угроз</p> <p>Регламентация использования ресурсов</p> <p>Реагирование на нарушения политики безопасности (административный уровень)</p> <p>Подход к выработке процедур для предупреждения нарушений безопасности</p> <p>Выбор регуляторов для практической защиты</p> <p>Ресурсы для предупреждения нарушений безопасности</p> <p>Реагирование на нарушения безопасности (процедурный уровень)</p>
<b>13</b>	<p>Раздел 13. Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности"</p> <p>Основные понятия</p>

	<p>Взаимодействие между группой реагирования, опекаемым сообществом и другими группами</p> <p>Порядок публикации правил и процедур деятельности групп реагирования</p> <p>Описание правил группы реагирования</p> <p>Описание услуг группы реагирования</p>
<b>14</b>	<p>Раздел 14. Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"</p> <p>Общие положения</p> <p>Роль поставщика Internet-услуг в реагировании на нарушения безопасности</p> <p>Меры по защите Internet-сообщества</p> <p>Маршрутизация, фильтрация и ограничение вещания</p> <p>Защита системной инфраструктуры</p> <p>Размещение Web-серверов</p> <p>Возможные вопросы к поставщику Internet-услуг</p>
<b>15</b>	<p>Раздел 15. Британский стандарт BS 7799</p> <p>Обзор стандарта BS 7799</p> <p>Регуляторы безопасности и реализуемые ими цели. Часть 1. Регуляторы общего характера</p> <p>Регуляторы безопасности и реализуемые ими цели. Часть 2. Регуляторы технического характера</p> <p>Регуляторы безопасности и реализуемые ими цели. Часть 3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия</p> <p>Четырехфазная модель процесса управления информационной безопасностью</p>
<b>16</b>	<p>Раздел 16. Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"</p> <p>Основные понятия и идеи стандарта FIPS 140-2 169</p> <p>Требования безопасности. Часть 1. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация</p> <p>Требования безопасности. Часть 2. Модель в виде конечного автомата, физическая безопасность</p> <p>Требования безопасности. Часть 3. Эксплуатационное окружение, управление криптографическими ключами</p> <p>Требования безопасности. Часть 4. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.</p>
<b>17</b>	<p>Раздел 17. Заключение</p> <p>Основные идеи курса</p> <p>Общие критерии" и профили защиты на их основе</p> <p>Спецификации Internet-сообщества для программно-технического уровня ИБ</p> <p>Спецификации Internet-сообщества для административного и процедурного уровней ИБ</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 5					
1	Общие критерии	семинар	4		2
2	Профили защиты	семинар	5		5
3	Спецификации Internet-сообщества	семинар	4		9
4	Британский стандарт BS 7799	семинар	2		15
5	Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	семинар	2		16
Всего			17		

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

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

Учебным планом не предусмотрено

#### 4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	40	40
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю	1010	

успеваемости (ТКУ)		
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	7	7
Всего:	57	57

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)
004.065	Фуфаев Э.В. Базы данных: учебное пособие Э.- М: Академия, 2008.	60
004.6(075)	Галанина В.А. Базы данных: введение в теорию реляционных баз данных. – СПб:ГОУ ВПО «СПбГУАП»,2008	64
004.4(075)Ф 96	Пакеты прикладных программ: учебное пособие для учреждений СПО/ Э. В. Фуфаев, Л. И. Фуфаева. - 4-е изд., стер.. - М.: Академия, 2008. - 352 с	60
	<a href="http://e.lanbook.com/books/element.php?pl1_id=5117">http://e.lanbook.com/books/element.php?pl1_id=5117</a> Беленькая, М.Н. Администрирование в информационных системах. [Электронный ресурс] : учебное пособие / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. — Электрон. дан. — М. : Горячая линия-Телеком, 2011. — 400 с.	
004.65 Д44	Диго, С.М. Базы данных: проектирование и использование: учебник.-М.: Финансы и статистика,2005.	10
681.518(075) П 33	Пирогов В.Ю. Информационные системы и базы данных: организация и проектирование. – СПб:БХВ –Петербург,2009.	15
	<a href="http://e.lanbook.com/books/element.php?pl1_id=2713">http://e.lanbook.com/books/element.php?pl1_id=2713</a> Зинченко, Л.А. Бионические информационные системы и их практические применения [Электронный ресурс] : / Л.А. Зинченко, В.М. Курейчика, В.Г. Редько. — Электрон. дан. — М. : Физматлит, 2011. — 286 с.	
004.007(075) М 69	Архитектура вычислительных систем: учебное пособие/ В. Г. Хорошевский. - 2-е изд., перераб. и доп.. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2008.	10

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

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

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

URL адрес	Наименование
<a href="http://www.intuit.ru">http://www.intuit.ru</a>	Национальный открытый университет ИНТУИТ
<a href="http://citforum.ru/security/articles/">http://citforum.ru/security/articles/</a>	Информационная безопасность - статьи, обзоры, книги
<a href="http://www.intuit.ru/studies/courses/3499/741/info">http://www.intuit.ru/studies/courses/3499/741/info</a>	Технопарк Mail.ru Group: Базы данных

## 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	Мультимедийная лекционная аудитория	

## 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
Зачет	Список вопросов; Тесты; Задачи.

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

Таблица 14 – Критерии оценки уровня сформированности компетенций

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

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

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

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

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код
-------	---	-----

		индикатора
1	<p>Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности</p> <p>Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса.</p> <p>Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций</p> <p>История создания и текущий статус "Общих критериев"</p> <p>Основные понятия и идеи "Общих критериев"</p> <p>Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий"</p> <p>Классификация функциональных требований безопасности</p> <p>Классы функциональных требований, описывающие элементарные сервисы безопасности</p> <p>Классы функциональных требований, описывающие производные сервисы безопасности</p> <p>Защита данных пользователя</p> <p>Защита функций безопасности объекта оценки</p> <p>Классы функциональных требований, играющие инфраструктурную роль</p> <p>Основные понятия и классификация требований доверия безопасности</p> <p>Оценка профилей защиты и заданий по безопасности</p> <p>Требования доверия к этапу разработки</p> <p>Требования к этапу получения, представления и анализа результатов разработки</p> <p>Требования к поставке и эксплуатации, поддержка доверия</p> <p>Оценочные уровни доверия безопасности</p> <p>Общие требования к сервисам безопасности</p> <p>Общие предположения безопасности</p> <p>Общие угрозы безопасности</p> <p>Общие элементы политики и цели безопасности</p> <p>Общие функциональные требования</p> <p>Общие требования доверия безопасности</p> <p>Биометрическая идентификация и аутентификация</p> <p>Требования к произвольному (дискреционному) управлению доступом</p> <p>Требования к принудительному (мандатному) управлению доступом</p> <p>Ролевое управление доступом</p> <p>Межсетевое экранирование</p> <p>Системы активного аудита</p> <p>Анонимизаторы</p> <p>Анализ защищенности</p> <p>Частные требования к комбинациям и приложениям сервисов безопасности</p> <p>Операционные системы</p> <p>Виртуальные частные сети</p> <p>Виртуальные локальные сети</p> <p>Смарт-карты</p> <p>Некоторые выводы</p>	ПК-4.В.1

	<p>Основные понятия и идеи рекомендаций семейства X.500</p> <p>Каркас сертификатов открытых ключей</p>	
2	<p>Каркас сертификатов атрибутов</p> <p>Простая и сильная аутентификация</p> <p>Архитектура средств безопасности IP-уровня</p> <p>Контексты безопасности и управление ключами</p> <p>Протокольные контексты и политика безопасности</p> <p>Обеспечение аутентичности IP-пакетов</p> <p>Обеспечение конфиденциальности сетевого трафика</p> <p>Основные идеи и понятия протокола TLS</p> <p>Протокол передачи записей</p> <p>Протокол установления соединений и ассоциированные протоколы</p> <p>Применение протокола HTTP над TLS</p> <p>программный интерфейс службы безопасности"</p> <p>Введение</p> <p>Основные понятия</p> <p>Функции для работы с удостоверениями</p> <p>Создание и уничтожение контекстов безопасности</p> <p>Защита сообщений</p> <p>Логика работы пользователей интерфейса безопасности</p> <p>Представление некоторых объектов интерфейса безопасности в среде языка C</p> <p>Проблемы, с которыми может столкнуться организация</p> <p>Основы предлагаемого подхода</p> <p>Общие принципы выработки официальной политики предприятия в области информационной безопасности</p> <p>Анализ рисков, идентификация активов и угроз</p> <p>Регламентация использования ресурсов</p>	ПК-7.3.1
3	<p>Реагирование на нарушения политики безопасности (административный уровень)</p> <p>Подход к выработке процедур для предупреждения нарушений безопасности</p> <p>Выбор регуляторов для практической защиты</p> <p>Ресурсы для предупреждения нарушений безопасности</p> <p>Реагирование на нарушения безопасности (процедурный уровень)</p> <p>Взаимодействие между группой реагирования, опекаемым сообществом и другими группами</p> <p>Порядок публикации правил и процедур деятельности групп реагирования</p> <p>Описание правил группы реагирования</p> <p>Описание услуг группы реагирования</p> <p>Роль поставщика Internet-услуг в реагировании на нарушения безопасности</p> <p>Меры по защите Internet-сообщества</p> <p>Маршрутизация, фильтрация и ограничение вещания</p> <p>Защита системной инфраструктуры</p> <p>Размещение Web-серверов</p> <p>Возможные вопросы к поставщику Internet-услуг</p> <p>Обзор стандарта BS 7799</p>	ПК-9.3.3
4	<p>Регуляторы безопасности и реализуемые ими цели. Часть</p>	ПК-11.У.2

	<p>1. Регуляторы общего характера Регуляторы безопасности и реализуемые ими цели. Часть 2.</p> <p>2. Регуляторы технического характера Регуляторы безопасности и реализуемые ими цели. Часть 3.</p> <p>3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия Четырехфазная модель процесса управления информационной безопасностью Основные понятия и идеи стандарта FIPS 140-2 169 Требования безопасности. Часть 1. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация Требования безопасности. Часть 2. Модель в виде конечного автомата, физическая безопасность Требования безопасности. Часть 3. Эксплуатационное окружение, управление криптографическими ключами Требования безопасности. Часть 4. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации. Общие критерии" и профили защиты на их основе Спецификации Internet-сообщества для программно-технического уровня ИБ Спецификации Internet-сообщества для административного и процедурного уровней ИБ</p>	
--	---	--

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

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

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

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

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	<ul style="list-style-type: none"> <li>• Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.</li> <li>• ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.</li> <li>• ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.</li> <li>• ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.</li> <li>• ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности.</li> </ul>	

	<p>Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.</p> <ul style="list-style-type: none"> <li>• ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности.</li> </ul> <p>Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.</p> <ul style="list-style-type: none"> <li>• ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.</li> <li>• ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.</li> <li>• ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.</li> <li>• ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.</li> <li>• Стандарт Банка России СТО БР ИББС-1.0-2014 - Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».</li> <li>• PCI DSS (Payment Card Industry Data Security Standard) - Стандарт безопасности данных индустрии платёжных карт</li> </ul>	
--	--	--

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.

#### **Методические указания для обучающихся по участию в семинарах**

Семинар – один из наиболее сложных и в то же время плодотворных видов (форм) вузовского обучения и воспитания. В условиях высшей школы семинар – один из видов практических занятий, проводимых под руководством преподавателя, ведущего научные исследования по тематике семинара и являющегося знатоком данной проблемы или отрасли научного знания. Семинар предназначается для углубленного изучения



дисциплины и овладения методологией применительно к особенностям изучаемой отрасли науки. При изучении дисциплины семинар является не просто видом практических занятий, а, наряду с лекцией, основной формой учебного процесса.

Основной целью для обучающегося является систематизация и обобщение знаний по изучаемой теме, разделу, формирование умения работать с дополнительными источниками информации, сопоставлять и сравнивать точки зрения, конспектировать прочитанное, высказывать свою точку зрения и т.п. В соответствии с ведущей дидактической целью содержанием семинарских занятий являются узловые, наиболее трудные для понимания и усвоения темы, разделы дисциплины. Спецификой данной формы занятий является совместная работа преподавателя и обучающегося над решением поставленной проблемы, а поиск верного ответа строится на основе чередования индивидуальной и коллективной деятельности.

При подготовке к семинарскому занятию по теме прослушанной лекции необходимо ознакомиться с планом его проведения, с литературой и научными публикациями по теме семинара.

### **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**

На практических занятиях под руководством преподавателя, решают практические задачи.

При проведении практических занятиях применяются следующие интерактивные методы обучения:

- метод «мозгового штурма»: метод представляет собой разновидность групповой дискуссии, которая характеризуется сбором всех вариантов решений, гипотез и предложений, рожденных в процессе осмысления какой-либо проблемы, их последующим анализом с точки зрения перспективы дальнейшего использования или реализации на практике;

-«снежный ком»: цель наработка и согласование мнений всех членов группы. При использовании этой техники в активное обсуждение включаются практически все студенты.

### **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