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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

зав.кафедрой, д.т.н.,проф.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)

(подпись)
«20» февраля 2026 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/ специализации	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.кафедрой, д.т.н.,проф. (должность, уч. степень, звание) — 20.02.26 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф. (уч. степень, звание) — 20.02.26 (подпись, дата) — С.В. Беззатеев (инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н. (должность, уч. степень, звание) — 20.02.26 (подпись, дата) — Н.В. Решетникова (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/специализации «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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-10 «Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации»

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 экзамена (4 семестр).

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-7 Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа	ПК-7.З.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.З.3 знать формальные модели управления доступом
Профессиональные компетенции	ПК-10 Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации	ПК-10.З.1 знать источники и классификацию угроз информационной безопасности ПК-10.У.2 уметь классифицировать защищаемую информацию по видам тайны и степени конфиденциальности ПК-10.В.2 владеть навыками организации процесса разработки моделей угроз и моделей нарушителя безопасности компьютерных систем

2. Место дисциплины в структуре ОП

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

- 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
		№4
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	34	34
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	38	38
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Экз.,	Экз.,

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 спецификаций в области информационной безопасности	1				2
Раздел 2: "Общие критерии", часть 1. Основные идеи	1	8			2
Раздел 3: "Общие критерии", часть 2. Функциональные требования безопасности	1				2

Раздел 4: "Общие критерии", часть 3. Требования доверия безопасности	1				2
Раздел 5: Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности	1	10			2
Раздел 6: Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности	1				2
Раздел 7: Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности	1				2
Раздел 8: Рекомендации семейства X.500 84	1				2
Раздел 9: Спецификации Internet-сообщества IPsec	1	8			2
Раздел 10: Спецификация Internet-сообщества TLS	1				2
Раздел 11. Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности"	1				2
Раздел 12. Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия"	1				2
Раздел 13. Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности"	1				2
Раздел 14. Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг"	1				4
Раздел 15. Британский стандарт BS 7799	1	4			4
Раздел 16. Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	1	4			2
Раздел 17. Заключение	1				2
Итого в семестре:	17	34			38
Итого	17	34	0	0	38

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1: Обзор наиболее важных стандартов и спецификаций в области информационной безопасности Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности Краткие сведения о стандартах и спецификациях, не являющихся

	предметом данного курса. Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций
2	Раздел 2: "Общие критерии", часть 1. Основные идеи История создания и текущий статус "Общих критериев" Основные понятия и идеи "Общих критериев" Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий"
3	Раздел 3: "Общие критерии", часть 2. Функциональные требования безопасности Классификация функциональных требований безопасности Классы функциональных требований, описывающие элементарные сервисы безопасности Классы функциональных требований, описывающие производные сервисы безопасности Защита данных пользователя Защита функций безопасности объекта оценки Классы функциональных требований, играющие инфраструктурную роль
4	Раздел 4: "Общие критерии", часть 3. Требования доверия безопасности Основные понятия и классификация требований доверия безопасности Оценка профилей защиты и заданий по безопасности Требования доверия к этапу разработки Требования к этапу получения, представления и анализа результатов разработки Требования к поставке и эксплуатации, поддержка доверия Оценочные уровни доверия безопасности
5	Раздел 5: Профили защиты, разработанные на основе "Общих критериев". Часть 1. Общие требования к сервисам безопасности Общие положения Общие предположения безопасности Общие угрозы безопасности Общие элементы политики и цели безопасности Общие функциональные требования Общие требования доверия безопасности
6	Раздел 6: Профили защиты, разработанные на основе "Общих критериев". Часть 2. Частные требования к сервисам безопасности Биометрическая идентификация и аутентификация Требования к произвольному (дискреционному) управлению доступом Требования к принудительному (мандатному) управлению доступом Ролевое управление доступом Межсетевое экранирование Системы активного аудита Анонимизаторы Анализ защищенности
7	Раздел 7: Профили защиты, разработанные на основе "Общих критериев". Часть 3. Частные требования к комбинациям и приложениям сервисов безопасности Операционные системы Виртуальные частные сети Виртуальные локальные сети Смарт-карты

	Некоторые выводы
8	Раздел 8: Рекомендации семейства X.500 84 Основные понятия и идеи рекомендаций семейства X.500 Каркас сертификатов открытых ключей Каркас сертификатов атрибутов Простая и сильная аутентификация
9	Раздел 9: Спецификации Internet-сообщества IPsec Архитектура средств безопасности IP-уровня Контексты безопасности и управление ключами Протокольные контексты и политика безопасности Обеспечение аутентичности IP-пакетов Обеспечение конфиденциальности сетевого трафика
10	Раздел 10: Спецификация Internet-сообщества TLS Основные идеи и понятия протокола TLS Протокол передачи записей Протокол установления соединений и ассоциированные протоколы Применение протокола HTTP над TLS
11	Раздел 11. Спецификация Internet-сообщества "Обобщенный прикладной программный интерфейс службы безопасности" Введение Основные понятия Функции для работы с удостоверениями Создание и уничтожение контекстов безопасности Защита сообщений Логика работы пользователей интерфейса безопасности Представление некоторых объектов интерфейса безопасности в среде языка C
12	Раздел 12. Спецификация Internet-сообщества "Руководство по информационной безопасности предприятия" Основные понятия Проблемы, с которыми может столкнуться организация Основы предлагаемого подхода Общие принципы выработки официальной политики предприятия в области информационной безопасности Анализ рисков, идентификация активов и угроз Регламентация использования ресурсов Реагирование на нарушения политики безопасности (административный уровень) Подход к выработке процедур для предупреждения нарушений безопасности Выбор регуляторов для практичной защиты Ресурсы для предупреждения нарушений безопасности Реагирование на нарушения безопасности (процедурный уровень)
13	Раздел 13. Спецификация Internet-сообщества "Как реагировать на нарушения информационной безопасности" Основные понятия Взаимодействие между группой реагирования, опекаемым сообществом и другими группами Порядок публикации правил и процедур деятельности групп реагирования Описание правил группы реагирования Описание услуг группы реагирования

14	Раздел 14. Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг" Общие положения Роль поставщика Internet-услуг в реагировании на нарушения безопасности Меры по защите Internet-сообщества Маршрутизация, фильтрация и ограничение вещания Защита системной инфраструктуры Размещение Web-серверов Возможные вопросы к поставщику Internet-услуг
15	Раздел 15. Британский стандарт BS 7799 Обзор стандарта BS 7799 Регуляторы безопасности и реализуемые ими цели. Часть 1. Регуляторы общего характера Регуляторы безопасности и реализуемые ими цели. Часть 2. Регуляторы технического характера Регуляторы безопасности и реализуемые ими цели. Часть 3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия Четырехфазная модель процесса управления информационной безопасностью
16	Раздел 16. Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей" 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.
17	Раздел 17. Заключение Основные идеи курса 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

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	8		2
2	Профили защиты	семинар	10		5
3	Спецификации	семинар	8		9

	Internet-сообщества				
4	Британский стандарт BS 7799	семинар	4		15
5	Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	семинар	4		16
Всего			34		

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. Выполнение курсового проекта/ 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 4, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	9	9
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	9	9
Всего:	38	38

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

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

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
	http://e.lanbook.com/books/element.php?pl1_id=5117 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
	http://e.lanbook.com/books/element.php?pl1_id=2713 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
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП

	«Интегрированная среда обучения» в течение учебного семестра

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
1	Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» (https://pro.guap.ru/) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке https://guap.ru/it/system/iso
2	Официальный сайт образовательной организации в сети «Интернет» (https://guap.ru/), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23)
3	LibreOffice 5 (Лицензия LGPLv3)

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
1	ЭБС Znanium (https://znanium.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
2	ЭБС «Лань» (https://e.lanbook.com/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
3	Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru), доступ через личный кабинет читателя библиотеки ГУАП

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Мультимедийная лекционная аудитория: Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; набор демонстрационного оборудования. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по точке доступа Wi-Fi.	
2	Лаборатория компьютерного моделирования:	52-46, 52-44 (ул.

	– специализированная мебель; – технические средства обучения, служащие для представления учебной информации; панель интерактивная/телевизор; Лабораторное оборудование: ПЭВМ – «Место рабочее автоматизированное» – 13 шт. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети.	Большая Морская, д.67, лит. А)
3	Помещение для самостоятельной работы, Интернет-класс. Специализированная мебель, возможность подключения к сети «Интернет» и доступ в электронную информационно-образовательную среду организации. 10 ПК, Принтер лазерный HPLJP4515n, Принтер HP LaserJetEnterprise 600 M602dn.	14-34 (ул. Большая Морская, д.67, лит. А)
4	Помещение для самостоятельной работы обучающихся - Читальный зал библиотеки ГУАП: специализированная мебель; персональные компьютеры – 10 шт., обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi, а также к электронно-библиотечным системам, реферативной базе данных Scopus; копировальный аппарат Kyocera KM2035	22-19 (ул. Большая Морская, д.67, лит. А)

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты*; Задачи; Тесты.

Примечание: *экзаменационные билеты формируются на основе вопросов и задач таблицы 15.

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»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– правильно выполнил от 90% до 100% тестовых заданий**.
«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. – правильно выполнил от 70% до 89% тестовых заданий**.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий**.

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	Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса. Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций История создания и текущий статус "Общих критериев" Основные понятия и идеи "Общих критериев" Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий" Классификация функциональных требований безопасности Классы функциональных требований, описывающие	ПК-7.З.1

	элементарные сервисы безопасности Классы функциональных требований, описывающие производные сервисы безопасности Защита данных пользователя Защита функций безопасности объекта оценки Классы функциональных требований, играющие инфраструктурную роль Основные понятия и классификация требований доверия безопасности Оценка профилей защиты и заданий по безопасности Требования доверия к этапу разработки Требования к этапу получения, представления и анализа результатов разработки Требования к поставке и эксплуатации, поддержка доверия Оценочные уровни доверия безопасности Общие требования к сервисам безопасности Общие предположения безопасности Общие угрозы безопасности Общие элементы политики и цели безопасности Общие функциональные требования Общие требования доверия безопасности Биометрическая идентификация и аутентификация Требования к произвольному (дискреционному) управлению доступом Требования к принудительному (мандатному) управлению доступом Ролевое управление доступом Межсетевое экранирование Системы активного аудита Анонимизаторы Анализ защищенности Частные требования к комбинациям и приложениям сервисов безопасности Операционные системы Виртуальные частные сети Виртуальные локальные сети Смарт-карты Некоторые выводы Основные понятия и идеи рекомендаций семейства X.500 Каркас сертификатов открытых ключей	
2	Каркас сертификатов атрибутов Простая и сильная аутентификация Архитектура средств безопасности IP-уровня Контексты безопасности и управление ключами Протокольные контексты и политика безопасности Обеспечение аутентичности IP-пакетов Обеспечение конфиденциальности сетевого трафика Основные идеи и понятия протокола TLS Протокол передачи записей Протокол установления соединений и ассоциированные протоколы	ПК-9.З.3

	Применение протокола HTTP над TLS программный интерфейс службы безопасности" Введение Основные понятия Функции для работы с удостоверениями Создание и уничтожение контекстов безопасности Защита сообщений Логика работы пользователей интерфейса безопасности Представление некоторых объектов интерфейса безопасности в среде языка C Проблемы, с которыми может столкнуться организация Основы предлагаемого подхода Общие принципы выработки официальной политики предприятия в области информационной безопасности Анализ рисков, идентификация активов и угроз Регламентация использования ресурсов	
3	Реагирование на нарушения политики безопасности (административный уровень) Подход к выработке процедур для предупреждения нарушений безопасности Выбор регуляторов для практичной защиты Ресурсы для предупреждения нарушений безопасности Реагирование на нарушения безопасности (процедурный уровень) Взаимодействие между группой реагирования, опекаемым сообществом и другими группами Порядок публикации правил и процедур деятельности групп реагирования Описание правил группы реагирования Описание услуг группы реагирования Роль поставщика Internet-услуг в реагировании на нарушения безопасности Меры по защите Internet-сообщества Маршрутизация, фильтрация и ограничение вещания Защита системной инфраструктуры Размещение Web-серверов Возможные вопросы к поставщику Internet-услуг Обзор стандарта BS 7799	ПК-10.З.1
4	Регуляторы безопасности и реализуемые ими цели. Часть 1. Регуляторы общего характера Регуляторы безопасности и реализуемые ими цели. Часть 2. Регуляторы технического характера Регуляторы безопасности и реализуемые ими цели. Часть 3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия Четырехфазная модель процесса управления информационной безопасностью Основные понятия и идеи стандарта FIPS 140-2 169	ПК-10.У.2
5	Требования безопасности. Часть 1. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация Требования безопасности. Часть 2. Модель в виде конечного автомата, физическая безопасность	ПК-10.В.2

	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	

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 выполнения курсового проекта/ курсовой работы представлены в таблице 17.

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

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

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

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	**Вопрос 1** Какой стандарт описывает систему менеджмента информационной безопасности (СМИБ)? 1. ГОСТ Р ИСО/МЭК 27001 2. ГОСТ Р ИСО 9001 3. ГОСТ Р ИСО/МЭК 27002 4. ГОСТ Р 50922 *Правильный ответ: 1* **Вопрос 2** Что представляет собой стандарт ГОСТ Р ИСО/МЭК 27002? 1. Требования к сертификации аудиторов 2. Свод норм и правил практического управления информационной безопасностью 3. Спецификацию для создания криптографических систем 4. Руководство по физической охране объектов *Правильный ответ: 2* **Вопрос 3** Какой международный стандарт является базовым для оценки безопасности информационных технологий (Common Criteria)? 1. ISO/IEC 15408 2. ISO/IEC 27005 3. ISO/IEC 27031	ПК-7.З.1

	4. ISO/IEC 20000 *Правильный ответ: 1*	
2	**Вопрос 4** Какая серия стандартов ГОСТ Р в России определяет основные термины и определения в области защиты информации? 1. ГОСТ Р 50922 2. ГОСТ Р 51275 3. ГОСТ Р 53114 4. Все перечисленные *Правильный ответ: 4* **Вопрос 5** Что означает аббревиатура СМИБ в контексте стандартов ИБ? 1. Система мониторинга и блокировок 2. Система менеджмента информационной безопасности 3. Сетевой модуль информационной безопасности 4. Стандарт межсетевого взаимодействия бизнеса *Правильный ответ: 2* **Вопрос 6** Какой стандарт регламентирует менеджмент риска информационной безопасности? 1. ГОСТ Р ИСО/МЭК 27005 2. ГОСТ Р ИСО/МЭК 27033 3. ГОСТ Р ИСО/МЭК 27035 4. ГОСТ Р ИСО 22301 *Правильный ответ: 1*	ПК-9.З.3
3	**Вопрос 7** Какой стандарт устанавливает требования к обеспечению непрерывности бизнеса? 1. ГОСТ Р ИСО 22301 2. ГОСТ Р ИСО/МЭК 27001 3. ГОСТ Р ИСО/МЭК 27018 4. ГОСТ Р 57580.1 *Правильный ответ: 1* **Вопрос 8** Какая серия стандартов посвящена безопасности облачных вычислений и защите персональных данных в облаках? 1. ИСО/МЭК 27017 и 27018 2. ИСО/МЭК 27001 и 27002 3. ИСО/МЭК 15408 4. ИСО/МЭК 27033 *Правильный ответ: 1* **Вопрос 9** Что регулирует комплекс стандартов ГОСТ Р 57580 в Российской Федерации? 1. Безопасность финансовых (банковских) операций 2. Защиту государственной тайны 3. Криптографическую защиту информации 4. Пожарную безопасность дата-центров *Правильный ответ: 1*	ПК-10.З.1
4	**Вопрос 10** Какой международный стандарт определяет руководящие принципы аудита систем менеджмента?	ПК-10.У.2

	1. ИСО 19011 2. ИСО 9000 3. ИСО/МЭК 27006 4. ИСО/МЭК 27007 *Правильный ответ: 1* **Вопрос 11** Что такое «профиль защиты» (Protection Profile) в соответствии с ISO/IEC 15408? 1. Совокупность правил доступа пользователей 2. Документ, содержащий реализацию конкретной СЗИ 3. Совокупность требований безопасности для определенного класса ИТ-продуктов 4. Паспорт технической укрепленности помещения *Правильный ответ: 3* **Вопрос 12** Какой этап не входит в цикл управления рисками по стандартам ИСО/МЭК 27005? 1. Идентификация рисков 2. Анализ и оценка рисков 3. Физическая ликвидация оборудования 4. Обработка рисков *Правильный ответ: 3*	
5	**Вопрос 13** Какой стандарт описывает методы и средства обеспечения сетевой безопасности? 1. ГОСТ Р ИСО/МЭК 27033 2. ГОСТ Р ИСО/МЭК 27037 3. ГОСТ Р ИСО/МЭК 27040 4. ГОСТ Р 56939 *Правильный ответ: 1* **Вопрос 14** Что является главным объектом защиты по стандарту PCI DSS? 1. Данные владельцев банковских карт 2. Персональные данные медицинских работников 3. Сведения, составляющие государственную тайну 4. Государственные информационные системы *Правильный ответ: 1* **Вопрос 15** Какой стандарт регламентирует менеджмент инцидентов информационной безопасности? 1. ГОСТ Р ИСО/МЭК 27035 2. ГОСТ Р ИСО/МЭК 27001 3. ГОСТ Р ИСО/МЭК 27042 4. ГОСТ Р 50922 *Правильный ответ: 1*	ПК-10.В.2

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

11.1. Методические указания для обучающихся по освоению лекционного материала *(если предусмотрено учебным планом по данной дисциплине).*

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 обучающимися 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:

Структура лекционного материала по дисциплине «Стандарты информационной безопасности» включает введение в техническое регулирование, обзор международных (ISO/IEC 27000), национальных ГОСТ Р, нормативных требований регуляторов (ФСТЭК, ФСБ), а также методологии построения систем управления информационной безопасностью (СУИБ) и аудита.

Введение и теоретические основы

– Цели, задачи и предмет дисциплины.

– Понятие стандарта ИБ, роль и место стандартизации в управлении рисками.

– Классификация стандартов (международные, национальные, отраслевые, корпоративные).

Международные стандарты ИБ

– Семейство стандартов ISO/IEC 27000 (ISO/IEC 27001 — требования к СУИБ, ISO/IEC 27002 — свод норм и правил).

– Стандарты непрерывности бизнеса (ISO 22301) и управления IT-услугами (ISO/IEC 20000).

– Зарубежные фреймворки и методологии (NIST SP 800-53, COBIT, ITIL).

Национальная и нормативно-правовая база

– Российские стандарты серии ГОСТ Р ИСО/МЭК 27000.
– Требования и руководящие документы ФСТЭК России по защите информации.
– Криптографические стандарты и требования ФСБ России.
– Федеральное законодательство в сфере информации (ФЗ-149, ФЗ-152 о персональных данных).

Оценка соответствия, аудит и управление риском

– Методы анализа и оценки рисков по стандартам (ISO/IEC 27005).
– Порядок проведения аудита информационной безопасности по стандартам.
– Процедуры сертификации и аттестации систем защиты.

11.2. 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 обучающемся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающемся 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

11.3. 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.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему 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 обучающихсяявляются:

– учебно-методический материал по дисциплине;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль включает следующие формы:

– Устный опрос (коллоквиум, собеседование)

– Письменные работы (тестирование)

– Лабораторные работы

– Проектная деятельность (рефераты, доклады, презентации)

Критерии оценивания

Оценка выставляется на основе демонстрации обучающимся следующих компетенций:

– Оценка «Отлично» (высокий уровень): глубокое знание материала, логичное изложение, умение решать нестандартные задачи, аргументированные ответы.

– Оценка «Хорошо» (продвинутый уровень): твердое знание материала, грамотное изложение, выполнение практических заданий без принципиальных ошибок, небольшие неточности при ответах.

– Оценка «Удовлетворительно» (пороговый уровень): знание базовых положений, затруднения при самостоятельном анализе, наличие ошибок в вычислениях или логике, неуверенные ответы.

– Оценка «Неудовлетворительно» (критический уровень): отсутствие базовых знаний, невыполнение обязательных практических заданий, отказ от ответа.

Порядок ликвидации задолженностей

– Обучающийся обязан проходить все формы контроля в установленные сроки.

– В случае пропуска по уважительной причине (болезнь, подтвержденная справкой), сроки прохождения переносятся.

– При неудовлетворительной оценке или неуважительном пропуске обучающийся обязан отработать задолженность в часы консультаций преподавателя до начала сессии.

11.5. 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».

Порядок проведения аттестации:

1. Допуск к аттестации. Студент обязан выполнить все практические, лабораторные и курсовые работы. Все текущие контроли должны быть сданы в срок.
2. Подготовка к контролю. Преподаватели выдают перечень вопросов и заданий. Кафедра организует консультации перед экзаменом.
3. Проведение испытания. Аттестация проходит по утвержденному расписанию сессии. Билет содержит теоретические вопросы и практические задачи.
4. Выставление отметки. Преподаватель оценивает ответ сразу после экзамена.

Критерии выставления оценок на экзамене определяются уровнем усвоения материала, глубиной знаний и умением применять их на практике. При этом используется классическая четырехбалльная система отчетов.

Расшифровка экзаменационных оценок

– «Отлично» (5). Студент демонстрирует глубокое и полное знание материала. Свободно владеет терминологией, логично излагает ответ, не допускает ошибок. Легко решает сложные практические задачи и связывает теорию с практикой.

– «Хорошо» (4). Студент твердо знает материал и грамотно его излагает. Ответ правильный по существу, но могут быть мелкие неточности или пропуски. Практические задания выполняются уверенно, но с незначительными недочетами.

– «Удовлетворительно» (3). Студент знает только основной материал, путается в деталях и терминах. Ответ поверхностный, нарушена логика изложения. Практические задачи вызывают серьезные затруднения и решаются только с помощью наводящих вопросов преподавателя.

– «Неудовлетворительно» (2). Студент имеет грубые пробелы в базовых знаниях. Не может ответить на основные вопросы и не справляется с практическими заданиями. Оценка означает, что курс не освоен, и ведет к академической задолженности.

Сравнение оценок по ключевым критериям

Оценка	Понимание теории	Практические навыки	Самостоятельность
Отлично	Полное, системное	Безошибочное выполнение	Полная самостоятельность
Хорошо	Твердое, без грубых ошибок	Выполнение с мелкими недочетами	Высокая самостоятельность
Удовлетворительно	Поверхностное, фрагментарное	Выполнение с подсказками	Требуется помощь
Неудовлетворительно	Отсутствует	Задания не выполнены	Не справляется

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