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
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Стандарты информационной безопасности»
(Название дисциплины)

Код направления	10.05.03
Наименование направления/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Обеспечение информационной безопасности распределенных информационных систем
Форма обучения	очная

Санкт-Петербург– 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц.,к.э.н.,доц.	24.06.21	Т.Н. Елина
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34
«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34

проф.,д.т.н.,доц.	«24» июня 2021 г	С.В. Беззатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.03(07)

доц.,к.т.н.,доц.	24.06.21	В.А. Мыльников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц.,к.э.н.,доц.	24.06.21	Г.С. Армашова-Тельник
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Стандарты информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по специальности «10.05.03 «Информационная безопасность автоматизированных систем» направленность «Обеспечение информационной безопасности распределенных информационных систем». Дисциплина реализуется кафедрой №54.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-5 «способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»;

общепрофессиональных компетенций:

ОПК-6 «способность применять нормативные правовые акты в профессиональной деятельности»;

профессиональных компетенций:

ПК-7 «способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ»,

ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы».

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-5 «способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»:

знать – роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности

уметь – осуществлять защиту данных пользователя в соответствии со стандартами информационной безопасности

владеть навыками – применения существующих стандартов информационной безопасности при разработке информационных систем

иметь опыт деятельности – по оценке информационных систем по требованиям стандартов информационной безопасности;

ОПК-6 «способность применять нормативные правовые акты в профессиональной деятельности»:

знать – основные понятия и идеи общей методологии оценки безопасности информационных технологий

уметь – применять стандарты информационной безопасности в профессиональной деятельности

владеть навыками – анализа существующих стандартов информационной безопасности;

иметь опыт деятельности – по составлению шаблонов нормативных регламентирующих документов;

ПК-7 «способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ»:

знать – классификацию функциональных требований безопасности

уметь – разрабатывать научно-техническую документацию;

владеть навыками – подготовки обзоров существующих стандартов информационной безопасности;

иметь опыт деятельности – по подготовке рефератов по стандартам информационной безопасности

ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»:

знать – требования доверия к этапу разработки автоматизированной системы

уметь – согласовывать политику безопасности автоматизированной системы со стандартами информационной безопасности

владеть навыками – разработки политики информационной безопасности автоматизированной системы

иметь опыт деятельности – по поиску стандартов информационной безопасности автоматизированной системы.

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 дисциплины в ЗЕ/академ. час

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

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№5
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	8	8
Аудиторные занятия, всего час., ***В том числе***	51	51
лекции (Л), (час)	34	34
Практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)		
Самостоятельная работа, всего	57	57
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Зачет	Зачет

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

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

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 5					
Раздел 1: Обзор наиболее важных стандартов и спецификаций в области информационной безопасности	2				2
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	2	2			4

7799					
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

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1: 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 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	ра ди л
	Семестр 5				
1	Общие критерии	семинар	4		
2	Профили защиты	семинар	5		
3	Спецификации Internet-сообщества	семинар	4	4	
4	Британский стандарт BS 7799	семинар	2		
5	Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей"	семинар	2	4	
		Всего:	17	8	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Учебным планом не предусмотрено			
	Всего:		

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час
1	2	3
Самостоятельная работа, всего	57	57
изучение теоретического материала дисциплины (ТО)	50	0
курсовое проектирование (КП, КР)		
расчетно-графические задания (РГЗ)		
выполнение реферата (Р)		
Подготовка к текущему контролю (ТК)	7	7
домашнее задание (ДЗ)		
контрольные работы заочников (КРЗ)		

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

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

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.065	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.	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.65 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 ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

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

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

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

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

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

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

Состав материально-технической базы представлен в таблице 12.

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. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Зачет	Список вопросов

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОК-5 «способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики»	
1	Введение в специальность
3	Информационные технологии
5	Теория информации
5	Стандарты информационной безопасности
9	Основы управленческой деятельности
9	Управление информационной безопасностью

9	Организационное и правовое обеспечение информационной безопасности
10	Информационная безопасность распределенных информационных систем
ОПК-6 «способность применять нормативные правовые акты в профессиональной деятельности»	
5	Стандарты информационной безопасности
5	Метрология
5	Микропроцессорная техника
6	Теория информационной безопасности
9	Организационное и правовое обеспечение информационной безопасности
ПК-7 «способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ»	
5	Стандарты информационной безопасности
6	Базы данных
6	Сети и системы передачи информации
7	Методы и средства проектирования информационных систем
7	Базы данных
8	Разработка и эксплуатация защищенных автоматизированных систем
8	Методы и средства проектирования информационных систем
9	Проектирование безопасных информационных систем
9	Разработка и эксплуатация защищенных автоматизированных систем
ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»	
4	Основы информационной безопасности
5	Стандарты информационной безопасности
7	Безопасность операционных систем
7	Безопасность систем баз данных
7	Безопасность сетей ЭВМ
9	Защита информации в сенсорных сетях

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	

$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \le К \le 84$	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \le К \le 69$	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$К \le 54$	«неудовлетво рительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

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

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	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 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 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 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 С 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) 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 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 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

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

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

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

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	не предусмотрено

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

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	• Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации. • ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство. • ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. • 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. • ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. • ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. • 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. • ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005. • ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005. • ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты. • Стандарт Банка России СТО БР ИББС-1.0-2014 - Стандарт Банка России:

	«Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». • PCI DSS (Payment Card Industry Data Security Standard) - Стандарт безопасности данных индустрии платёжных карт

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению 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.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

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

Структура предоставления лекционного материала:

Раздел 1: Обзор наиболее важных стандартов и спецификаций в области информационной безопасности

Раздел 2: "Общие критерии", часть 1. Основные идеи

Раздел 3: "Общие критерии", часть 2. Функциональные требования безопасности

Раздел 4: "Общие критерии", часть 3. Требования доверия безопасности

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

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 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.

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