МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. В. Сенченко
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **1**
Семестр: **2**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	2 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	10	10	часов
3	Всего аудиторных занятий	38	38	часов
4	Самостоятельная работа	70	70	часов
5	Всего (без экзамена)	108	108	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 2 семестр

Томск

Согласована на портале № 50824

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. КИБЭВС _____ А. А. Конев

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. Ю. Якимук

Согласована на портале № 50824

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Основы информационной безопасности» является освоение базовой терминологии в области информационной безопасности (ИБ), понимание принципов выявления угроз и защиты от них.

1.2. Задачи дисциплины

- получение студентами знания базовой терминологии и состава нормативно-правовой документации в области ИБ;
- получение студентами знаний о классификации защищаемой информации по видам тайн и степеням конфиденциальности;
- получение студентами знаний о классификации угроз ИБ;
- получение студентами умений по составлению перечня угроз ИБ;
- получение студентами знаний об основных методах защиты информации.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» (Б1.Б1.04.01) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Введение в специальность, Системный анализ.

Последующими дисциплинами являются: Безопасность сетей ЭВМ, Безопасность систем баз данных, Криптографические методы защиты информации, Нормативное обеспечение защиты информации, Организационное и правовое обеспечение информационной безопасности, Основы управления информационной безопасностью, Прикладная криптография.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОК-5 способностью 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 ;
- ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ;
- ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности ;

В результате изучения дисциплины обучающийся должен:

- **знать** сущность и понятие информации, информационной безопасности и характеристику ее составляющих; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; основные понятия, связанные с обеспечением информационной безопасности личности, общества и государства.
- **уметь** классифицировать угрозы информационной безопасности.
- **владеть** терминологией в области обеспечения ИБ.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры

Согласована на портале № 50824

		2 семестр
Аудиторные занятия (всего)	38	38
Лекции	28	28
Практические занятия	10	10
Самостоятельная работа (всего)	70	70
Проработка лекционного материала	8	8
Самостоятельное изучение тем (вопросов) теоретической части курса	22	22
Подготовка к практическим занятиям, семинарам	40	40
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр					
1 Классификация защищаемой информации	2	4	25	31	ОПК-7, ПК-9
2 Угрозы информационной безопасности	4	4	15	23	ОПК-7
3 Система защиты информации	2	2	11	15	ОПК-7, ПК-9
4 Направления обеспечения информационной безопасности	16	0	18	34	ОК-5, ПК-9
5 Кибертерроризм и кибербезопасность.	4	0	1	5	ОК-5
Итого за семестр	28	10	70	108	
Итого	28	10	70	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
2 семестр			
1 Классификация защищаемой информации	Информация как объект защиты. Свойства информации, обеспечиваемые при её защите. Виды защищаемой информации.	2	ОПК-7
	Итого	2	
2 Угрозы	Понятие «Угроза информационной без-	4	ОПК-7

Согласована на портале № 50824

информационной безопасности	опасности». Классификация угроз. Способы реализации угроз.		
	Итого	4	
3 Система защиты информации	Понятие «Система защиты информации». Направления защиты информации. Понятие «Уязвимость». Угрозы системе защиты информации.	2	ОПК-7
	Итого	2	
4 Направления обеспечения информационной безопасности	Основные нормативно-правовые документы и принципы обеспечения защиты информации в области правового, технического, программно-аппаратного, криптографического и организационного направлений защиты информации.	16	ОК-5, ПК-9
	Итого	16	
5 Кибертерроризм и кибербезопасность.	Отличительные особенности и классификация кибертерроризма. Международное и российское законодательство в области обеспечения кибербезопасности.	4	ОК-5
	Итого	4	
Итого за семестр		28	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин				
	1	2	3	4	5
Предшествующие дисциплины					
1 Введение в специальность	+				
2 Системный анализ	+				
Последующие дисциплины					
1 Безопасность сетей ЭВМ		+	+	+	
2 Безопасность систем баз данных		+	+	+	
3 Криптографические методы защиты информации		+	+	+	
4 Нормативное обеспечение защиты информации				+	
5 Организационное и правовое обеспечение информационной безопасности		+	+	+	
6 Основы управления информационной безопасностью				+	
7 Прикладная криптография				+	

Согласована на портале № 50824

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ОК-5	+		+	Экзамен, Тест
ОПК-7	+	+	+	Экзамен, Тест, Отчет по практическому занятию
ПК-9	+	+	+	Экзамен, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
2 семестр			
1 Классификация защищаемой информации	Построение модели объекта защиты.	4	ОПК-7
	Итого	4	
2 Угрозы информационной безопасности	Моделирование угроз информационной безопасности.	4	ОПК-7
	Итого	4	
3 Система защиты информации	Определение мер защиты информации	2	ПК-9
	Итого	2	
Итого за семестр		10	

Согласована на портале № 50824

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
2 семестр				
1 Классификация защищаемой информации	Подготовка к практическим занятиям, семинарам	20	ОПК-7, ПК-9	Отчет по практическому занятию, Тест, Экзамен
	Самостоятельное изучение тем (вопросов) теоретической части курса	4		
	Проработка лекционного материала	1		
	Итого	25		
2 Угрозы информационной безопасности	Подготовка к практическим занятиям, семинарам	10	ОПК-7	Отчет по практическому занятию, Тест, Экзамен
	Самостоятельное изучение тем (вопросов) теоретической части курса	4		
	Проработка лекционного материала	1		
	Итого	15		
3 Система защиты информации	Подготовка к практическим занятиям, семинарам	10	ПК-9, ОПК-7	Отчет по практическому занятию, Тест
	Проработка лекционного материала	1		
	Итого	11		
4 Направления обеспечения информационной безопасности	Самостоятельное изучение тем (вопросов) теоретической части курса	14	ОК-5, ПК-9	Тест, Экзамен
	Проработка лекционного материала	4		
	Итого	18		
5 Кибертерроризм и кибербезопасность.	Проработка лекционного материала	1	ОК-5	Тест
	Итого	1		
Итого за семестр		70		
	Подготовка и сдача экзамена	36		Экзамен
Итого		106		

Согласована на портале № 50824

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
2 семестр				
Отчет по практическому занятию		30	20	50
Тест	10	5	5	20
Итого максимум за период	10	35	25	70
Экзамен				30
Нарастающим итогом	10	45	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Петренко, В. И. Теоретические основы защиты информации [Электронный ресурс]: учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный //

Согласована на портале № 50824

Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/155247 (дата обращения: 03.05.2021).

2. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. — Текст : электронный // Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/111016 (дата обращения: 03.05.2021).

12.2. Дополнительная литература

1. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 03.05.2021).

2. Р 50.1.028-2001. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования [Электронный ресурс]: — Режим доступа: https://standartgost.ru/g/%D0%A0_50.1.028-2001 (дата обращения: 03.05.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А. Основы информационной безопасности [Электронный ресурс]: Методические указания к практическим занятиям и самостоятельной работе. - Томск, 2020. - 9 с. — Режим доступа: https://disk.fb.tusur.ru/oib/practice.pdf (дата обращения: 03.05.2021).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. ГАРАНТ
2. КонсультантПлюс
3. При изучении дисциплины рекомендуется обращаться к базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

Согласована на портале № 50824

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Учебная аудитория

учебная аудитория для проведения занятий практического типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 403 ауд.

Описание имеющегося оборудования:

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение не требуется.

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

Согласована на портале № 50824

14.1.1. Тестовые задания

Что является объектом защиты информации?

а) Информация

б) Носитель информации

в) Информационный процесс

г) Все вышеперечисленное

Состоянием информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право, называется:

а) Доступность

б) Целостность

в) Конфиденциальность

г) Неотказуемость

Вид защиты информации, основанный на защите информации правовыми методами и включающий в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением – это:

а) Правовая защита информации

б) Техническая защита информации

в) Криптографическая защита информации

г) Физическая защита информации

14.1.2. Экзаменационные вопросы

1. Типы объектов защиты информации и их определения.
2. Свойства информации, обеспечиваемые при её защите.
3. Категории доступа к информации. Степени секретности сведений, составляющих государственную тайну.
4. Виды информации, относящейся к сведениям конфиденциального характера.
5. Понятие «нарушение информационной безопасности». Примеры атак на информационные системы.
6. Понятие «угроза информационной безопасности». Формы представления информации.
7. Угрозы конфиденциальности информации, представленной в различных формах.
8. Угрозы целостности информации, представленной в различных формах.
9. Угрозы доступности информации, представленной в различных формах.
10. Способы реализации угроз, направленных на акустическую информацию.
11. Способы реализации угроз, направленных на видовую информацию.
12. Способы реализации угроз информации, представленной в виде сигналов.
13. Способы реализации угроз, направленных на компьютерную информацию.
14. Понятие «обеспечение информационной безопасности организации». Примеры методов и средств защиты информации.
15. Понятие «система защиты информации». Направления защиты информации.
16. Элементы информационной системы, являющиеся объектами защиты.
17. Угрозы конфиденциальности и целостности, направленные на автоматизированные информационные системы.
18. Угрозы конфиденциальности и целостности, направленные на персонал организации.
19. Способы реализации угроз, направленных на автоматизированные информационные системы и системы защиты информации.
20. Понятие «Уязвимость». Причины возникновения уязвимостей.
21. Законодательные акты, регламентирующие работу со сведениями, составляющими государственную тайну.
22. Законодательные акты, регламентирующие работу с персональными данными.
23. Законодательные акты, регламентирующие работу со сведениями, составляющими служебную и коммерческую тайну.
24. Основные функции ФСБ России в области обеспечения информационной безопасности.
25. Основные функции ФСТЭК России в области обеспечения информационной безопасности.

Согласована на портале № 50824

26. Правовые документы, устанавливающие ответственность за компьютерные преступления.

27. Правовые документы, устанавливающие ответственность за разглашение сведений ограниченного доступа.

28. Правовые документы, устанавливающие ответственность за разглашение персональных данных.

29. Задачи организационной защиты информации.

30. Стандарты семейства ISO 27000.

31. Этапы анализа объектов защиты.

32. Основные нормативные документы, регламентирующие обеспечение информационной безопасности в организации.

33. Основные определения в области технической защиты информации.

34. Примеры технических и инженерно-технических средств защиты информации.

35. Виды лицензируемой деятельности по технической защите конфиденциальной информации.

36. Виды лицензируемой деятельности по разработке и производству средств защиты конфиденциальной информации.

37. Нормативные документы, регламентирующие сертификацию средств защиты информации.

38. Виды средств защиты информации, подлежащих сертификации в системе сертификации СЗИ-ГТ.

39. Законы и стандарты в области криптографической защиты информации.

40. Основные определения в области криптографической защиты информации.

41. Сферы применения симметричного и асимметричного шифрования.

42. Примеры криптографических средств защиты информации.

43. Виды лицензируемой деятельности по криптографической защите информации.

44. Требования по сертификации криптографических средств защиты информации.

45. Нормативные документы ФСБ России по защите персональных данных.

46. Методы программно-аппаратной защиты информации.

47. Примеры средств программно-аппаратной защиты информации.

48. Виды сертификатов соответствия средств защиты информации.

49. Нормативные документы ФСТЭК России по сертификации автоматизированных систем и средств вычислительной техники.

50. Нормативные документы ФСТЭК России по защите персональных данных.

51. Нормативные документы ФСТЭК России по сертификации средств защиты информации на основе профилей защиты.

52. Требования ФСТЭК России по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

53. Требования ФСТЭК России по обеспечению безопасности государственных информационных систем.

54. Требования ФСТЭК России по обеспечению безопасности систем критической информационной инфраструктуры.

55. Требования ФСТЭК России по обеспечению безопасности АСУТП.

56. Понятие «кибертерроризм». Основные внешние факторы, способствующие распространению терроризма.

57. Способы использования информационных технологий террористическими группами.

58. Классификация информационного терроризма.

59. Задачи по защите от кибертерроризма.

60. Понятие кибербезопасности в ISO/IEC 27032:2012.

14.1.3. Вопросы для подготовки к практическим занятиям, семинарам

Построение модели объекта защиты.

Моделирование угроз информационной безопасности.

Определение мер защиты информации

Согласована на портале № 50824

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 50824