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

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Организация защиты объектов критической информационной инфраструктуры

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **1**
Семестр: **2**
Учебный план набора 2021 года

Распределение рабочего времени

№	Виды учебной деятельности	2 семестр	Всего	Единицы
1	Лекции	16	16	часов
2	Практические занятия	32	32	часов
3	Всего аудиторных занятий	48	48	часов
4	Самостоятельная работа	132	132	часов
5	Всего (без экзамена)	180	180	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Экзамен: 2 семестр

Томск

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) 10.04.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. КИБЭВС _____ Е. М. Давыдова

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

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

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ Е. Ю. Костюченко

1. Цели и задачи дисциплины

1.1. Цели дисциплины

формирование компетенций, необходимых специалистам, для обеспечения безопасности значимых объектов критической инфраструктуры

1.2. Задачи дисциплины

– выделение объектов, угроз, определение способов и средств защиты объектов критической инфраструктуры.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Организация защиты объектов критической информационной инфраструктуры» (Б1.В.3) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Технологии обеспечения информационной безопасности.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты, Управление компьютерными инцидентами.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-1 способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

– ПК-14 способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

– ПК-16 способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** технологии обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России организационно-распорядительные документы, бизнес-планы техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасности

– **уметь** организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России; разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности анализировать направления развития информационных (телекоммуникационных) технологий.

– **владеть** способностью организовать работу способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности способностью прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты способностью

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Аудиторные занятия (всего)	48	48

Лекции	16	16
Практические занятия	32	32
Самостоятельная работа (всего)	132	132
Проработка лекционного материала	5	5
Подготовка к практическим занятиям, семинарам	127	127
Всего (без экзамена)	180	180
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

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 Понятие критической информационной инфраструктуры	2	2	5	9	ПК-1
2 Правовое обеспечение критической информационной инфраструктуры	4	4	21	29	ПК-14
3 Категории объектов критической информационной инфраструктуры	2	8	35	45	ПК-1, ПК-14, ПК-16
4 Технические и организационные меры безопасности значимых объектов	4	6	17	27	ПК-1, ПК-14, ПК-16
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	2	8	13	23	ПК-14, ПК-16
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	2	4	41	47	ПК-14, ПК-16
Итого за семестр	16	32	132	180	
Итого	16	32	132	180	

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 Понятие критической	Термины и определения, понятие критической информационной инфраструктуры	2	ПК-1

информационной инфраструктуры	(КИИ), объекты КИИ		
	Итого	2	
2 Правовое обеспечение критической информационной инфраструктуры	Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ.Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ	4	ПК-14
	Итого	4	
3 Категории объектов критической информационной инфраструктуры	Классификация АСУТП. Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах.ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ.	2	ПК-1, ПК-16
	Итого	2	
4 Технические и организационные меры безопасности значимых объектов	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.Анализ угроз и разработка модели угроз.Проектирование системы безопасности значимого объекта КИИ.Разработка рабочей и эксплуатационной документации.	4	ПК-14, ПК-16
	Итого	4	
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.	2	ПК-14, ПК-16
	Итого	2	
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	Организационно-распорядительные документыпо безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ	2	ПК-16
	Итого	2	
Итого за семестр		16	

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	6
Предшествующие дисциплины						
1 Технологии обеспечения информационной безопасности	+			+	+	+
Последующие дисциплины						
1 Защита выпускной квалификационной работы, включая подготовку к защите и процедуру защиты	+	+	+	+	+	+
2 Управление компьютерными инцидентами		+	+	+	+	+

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.	
ПК-1	+	+	+	Собеседование, Опрос на занятиях, Тест
ПК-14	+	+	+	Собеседование, Тест
ПК-16	+	+	+	Собеседование, Тест

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 Понятие критической информационной инфраструктуры	Термины и определения, понятие критической информационной инфраструктуры (КИИ), объекты КИИ	2	ПК-1
	Итого	2	
2 Правовое обеспечение критической информационной инфраструктуры	Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ.Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ.Постановление от 8 февраля 2018 года №127. О порядке категорирования объектов критической информаци-	4	ПК-14

	онной инфраструктуры. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»		
	Итого	4	
3 Категории объектов критической информационной инфраструктуры	Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31.Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах.ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ.	8	ПК-1, ПК-14
	Итого	8	
4 Технические и организационные меры безопасности значимых объектов	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.Анализ угроз и разработка модели угроз.Проектирование системы безопасности значимого объекта КИИ.Разработка рабочей и эксплуатационной документации.Приказ № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»	6	ПК-1, ПК-14, ПК-16
	Итого	6	
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.	8	ПК-14, ПК-16
	Итого	8	
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ	4	ПК-14, ПК-16
	Итого	4	
Итого за семестр		32	

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 Понятие критической информационной инфраструктуры	Подготовка к практическим занятиям, семинарам	4	ПК-1	Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Итого	5		
2 Правовое обеспечение критической информационной инфраструктуры	Подготовка к практическим занятиям, семинарам	20	ПК-14	Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	21		
3 Категории объектов критической информационной инфраструктуры	Подготовка к практическим занятиям, семинарам	34	ПК-1, ПК-14, ПК-16	Собеседование, Тест
	Проработка лекционного материала	1		
	Итого	35		
4 Технические и организационные меры безопасности значимых объектов	Подготовка к практическим занятиям, семинарам	16	ПК-14, ПК-16	Тест
	Проработка лекционного материала	1		
	Итого	17		
5 Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры	Подготовка к практическим занятиям, семинарам	13	ПК-14, ПК-16	Собеседование, Тест
	Проработка лекционного материала	0		
	Итого	13		
6 Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	Подготовка к практическим занятиям, семинарам	40	ПК-14, ПК-16	Тест
	Проработка лекционного материала	1		
	Итого	41		
Итого за семестр		132		
	Подготовка и сдача эк-	36		Экзамен

	замена			
Итого		168		

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				
Опрос на занятиях	10	5	10	25
Собеседование	5	5	5	15
Тест	10	10	10	30
Итого максимум за период	25	20	25	70
Экзамен				30
Нарастающим итогом	25	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. Основы Информационной безопасности / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А., - Из-во Горячая линия "Телеком", - 2011г., 558 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/reader/book/111016/#1 (дата обращения: 29.06.2020).

12.2. Дополнительная литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: http://ivo.garant.ru/#/document/71730198/paragraph/1:0 (дата обращения: 29.06.2020).
2. № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_291398/ (дата обращения: 29.06.2020).
3. № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»; [Электронный ресурс]: — Режим доступа: https://rg.ru/2018/02/13/fstek-prikaz-227-site-dok.html (дата обращения: 29.06.2020).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Зайцев, Александр Петрович. Технические средства и методы защиты информации : Лабораторный практикум: Учебное пособие. - Томск : В-Спектр , 2007. - 119[1] с. (наличие в библиотеке ТУСУР - 65 экз.)

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 http://www.garant.ru/
2. КонсультантПлюс http://www.consultant.ru/

12.5. Периодические издания

1. Информационная безопасность

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 ил-

люстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:

- Моноблок Asus V222GAK-BA021D: IntelJ5005/ DDR44G / 500Gb/ WiFi / мышь/ клавиатура (10шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security

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 инва-

лидностью.

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:

14.1.1. Тестовые задания

ПК1 способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК14 способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

ПК16 способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности.

1. Какое из определений информационных технологий верно
- процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных;
- ресурсы, необходимые для сбора, обработки, хранения и распространения информации;
-все перечисленное.

2.Безопасность информации
- состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;
- состояние при котором невозможно изменить информацию;
- состояние обеспечивающее целостность и защищенность информации;
- состояние при котором злоумышленник не может получить информацию.

3.Безопасность критической информационной инфраструктуры
- состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;
- состояние защищенности, при котором обеспечены конфиденциальность, доступность и целостность информации;
- состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование
- состояние обеспечивающее целостность и защищенность информации.

4.Доступ к информации
- возможность получения информации и ее использования;
- состояние доступности;
- возможность проводить сбор, обработку и передачу информации
- Возможность изменения информации

5.Значимый объект критической информационной инфраструктуры
- объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

- объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;

-информационно-телекоммуникационная сеть;

- автоматизированная система управления субъекта критической информационной инфраструктуры.

6.Объект критической информационной инфраструктуры

- информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационной инфраструктуры;

- автоматизированная система управления субъекта критической информационной инфраструктуры;

- объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;

- который включен в реестр значимых объектов критической информационной инфраструктуры.

7.Субъекты критической информационной инфраструктуры

- государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы;

- информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности,

- российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;

- все выше перечисленное.

8.Какой закон регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

- Федеральный закон от 26.07.2017 № 187ФЗ;
- Приказ ФСБ России от 19.06.2019 № 281;
- Приказ ФСТЭК России от 25 декабря 2017 г. № 239;
- Постановление Правительства РФ от 8 февраля 2018 г. № 127.

9.Компьютерный инцидент

- любое реальное или предполагаемое событие имеющее отношение к безопасности компьютерной системы или компьютерной сети;
- атака на компьютерную систему;
- изменение системы безопасности компьютерной сети;
- событие изменяющее компьютерную систему.

10 Под ? понимается установление соответствия объекта КИИ

критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

- категорированием;
- идентификацией;
- установлением значимости;
- обеспечением безопасности.

14.1.2. Экзаменационные вопросы

1. Состав технических мер по защите КИИ согласно приказу №239 ФСТЭК
2. Состав организационных мер по защите КИИ согласно приказу №239 ФСТЭК
3. Основные законы в сфере безопасности КИИ
4. Перечислите потенциальные сферы объектов КИИ, кратко охарактеризуйте их
5. Как определяются категории значимости объектов КИИ

6. Основные регуляторы объектов КИИ, их функции
7. Какая информация включается в реестр КИИ
8. Основные требования и последовательность реализаций требований к ИБ объекта КИИ
9. Классификация угроз безопасности объектов КИИ
10. Состав системы безопасности значимых объектов
11. Требования к средствам системы безопасности объектов КИИ

14.1.3. Вопросы на собеседование

1. Сетевые средства ИнфоТеКС для защиты АСУ КИИ
2. Средства VipNet Coordinator IG

14.1.4. Темы опросов на занятиях

1. Классификация АСУТП: требования, параметры, сроки. Категорирование объектов критической информационной инфраструктуры
2. Разработка модели угроз
3. Выбор мер защиты объектов информатизации

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.