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

ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Управление безопасностью телекоммуникационных систем и сетей**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра безопасности информационных систем (БИС)**
Курс: **5**
Семестр: **10**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	10 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Практические занятия	20	20	часов
в т.ч. в форме практической подготовки	6	6	часов
Самостоятельная работа	70	70	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	10

Томск

1. Общие положения

1.1. Цели дисциплины

1. Построение прогнозов распределения компьютерных атак по элементам, с учётом места и роли элементов в информационно-телекоммуникационной сети, а также определить показатели, характеризующие устойчивость сети в условиях воздействия компьютерных атак и требования системе защиты.

1.2. Задачи дисциплины

1. изучить анализ условий функционирования интегрированной информационно-телекоммуникационной сети.
2. изучить оценку стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть.
3. проанализировать понятие устойчивости информационно-телекоммуникационной сети в условиях информационного противоборства.
4. рассмотреть синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специализации (major).
Индекс дисциплины: Б1.О.05.05.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

ОПК-9.1. Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей	ОПК-9.1.1. Знает стандарты, руководящие и методические документы в области защиты информации в телекоммуникационных системах и сетях	Знает стандарты, руководящие и методические документы в области защиты информации в телекоммуникационных системах и сетях
	ОПК-9.1.2. Умеет определять угрозы, реализация которых может привести к нарушению безопасности и корректности функционирования телекоммуникационных систем и сетей, выполнять анализ безопасности и составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей	Умеет определять угрозы, реализация которых может привести к нарушению безопасности и корректности функционирования телекоммуникационных систем и сетей, выполнять анализ безопасности и составлять отчеты по результатам проверок защищенности телекоммуникационных систем и сетей
	ОПК-9.1.3. Владеет навыками оценки рисков, связанных с осуществлением угроз безопасности телекоммуникационных систем и сетей	Владеет навыками оценки рисков, связанных с осуществлением угроз безопасности телекоммуникационных систем и сетей
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	38	38
Лекционные занятия	18	18
Практические занятия	20	20
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	70	70
Подготовка к зачету	35	35
Подготовка к тестированию	35	35
Общая трудоемкость (в часах)	108	108

Общая трудоемкость (в з.е.)	3	3

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр					
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	4	4	20	28	ОПК-9.1
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	6	6	20	32	ОПК-9.1
3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	4	6	20	30	ОПК-9.1
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	4	4	10	18	ОПК-9.1
Итого за семестр	18	20	70	108	
Итого	18	20	70	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
10 семестр			
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	Структура и задачи сил кибероперацій вооруженных сил США. Функциональная модель информационно-телекоммуникационной сети	4	ОПК-9.1
	Итого	4	
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	Особенности организации компьютерных атак. Применение метода анализа иерархий для оценки опасности компьютерных атак на информационно-телекоммуникационную сеть. Методика оценки стратегии информационного воздействия на ИТКС	6	ОПК-9.1
	Итого	6	

3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	Методика оценки устойчивости в условиях информационного противоборства. Вероятностно-временные характеристики компьютерных атак на элементы ИТКС. Вероятностно-временные характеристики эквивалентных компьютерных атак. Вероятностно-временные характеристики эквивалентных компьютерных атак по виду воздействия. Вероятностно-временные характеристики последовательностей воз-действия эквивалентных компьютерных атак	4	ОПК-9.1
	Итого	4	
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	Направления повышения защищённости информационнотелекоммуникационной сети в условиях информационного противоборства. Оценка эффективности средств защиты информационнотелеком-муникационной сети от компьютерных атак. Методика синтеза системы защиты информационнотелекоммуникационной сети в условиях информационного противоборства	4	ОПК-9.1
	Итого	4	
Итого за семестр		18	
Итого		18	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	Обсуждение и практическое применение изученных на лекции приемов.	4	ОПК-9.1
	Итого	4	
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	Обсуждение и практическое применение изученных на лекции приемов.	6	ОПК-9.1
	Итого	6	

3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	Обсуждение и практическое применение изученных на лекции приемов.	6	ОПК-9.1
	Итого	6	
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	Обсуждение и практическое применение изученных на лекции приемов.	4	ОПК-9.1
	Итого	4	
Итого за семестр		20	
Итого		20	

5.4. Лабораторные занятия

Не предусмотрено учебным планом

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	Подготовка к зачету	10	ОПК-9.1	Зачёт
	Подготовка к тестированию	10	ОПК-9.1	Тестирование
	Итого	20		
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	Подготовка к зачету	10	ОПК-9.1	Зачёт
	Подготовка к тестированию	10	ОПК-9.1	Тестирование
	Итого	20		
3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	Подготовка к зачету	10	ОПК-9.1	Зачёт
	Подготовка к тестированию	10	ОПК-9.1	Тестирование
	Итого	20		
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	Подготовка к зачету	5	ОПК-9.1	Зачёт
	Подготовка к тестированию	5	ОПК-9.1	Тестирование
	Итого	10		
Итого за семестр		70		
Итого		70		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Прак. зан.	Сам. раб.	
ОПК-9.1	+	+	+	Зачёт, Тестирование

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	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
10 семестр				
Зачёт	0	0	30	30
Тестирование	20	20	30	70
Итого максимум за период	20	20	60	100
Нарастающим итогом	20	40	100	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения [Электронный ресурс]: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/473348.

7.2. Дополнительная литература

1. Основы информационной безопасности: Учебное пособие / А. М. Голиков - 2007. 201 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1024.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / А. М. Голиков - 2007. 154 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/1017.

7.3.2. 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.

7.4. Современные профессиональные базы данных и информационные справочные системы

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

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;

- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- Microsoft Windows 10;
- VirtualBox;

8.3. 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.

Описание имеющегося оборудования:
- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. 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 зрения** 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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	ОПК-9.1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	ОПК-9.1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	ОПК-9.1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	ОПК-9.1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков

5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?
   Группы пользователей и права доступа
   Пользователи и группы
   Сервер и рабочая станция
   Риски и контрмеры
2. По каким угрозам в системе ГРИФ не оценивается ущерб?
   Конфиденциальности
   Целостности
   Достоверность
   Доступность
3. Какой категории угроз не представлено в системе ГРИФ?
   Физические угрозы человека
   Угрозы персонала
   Системные ошибки
   Физические угрозы
4. Какого типа экономического ущерба не существует?
   Долговременный экономический ущерб
   Кратковременный экономический ущерб
   Отсроченный экономический ущерб
   Немедленный экономический ущерб
5. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «нарушение бизнес-деятельности»?

Кратковременный экономический ущерб
Отсроченный экономический ущерб
Немедленный экономический ущерб
Долговременный экономический ущерб

6. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?
Не повлияет
Приравняет к нулю
Вызовет уменьшение
Вызовет рост
7. Какая из перечисленных выполняемых проверок не входит в перечень обязательных действий, входящих в руководство по реализации средств управления против злонамеренного кода?
Проверка любых файлов на электронном или оптическом носителе, а также файлов, полученных по сетям, на наличие злонамеренного кода перед использованием
Проверка web-страниц на наличие злонамеренного кода
Проверка обновлений средства управления против злонамеренного кода
Проверка приложений к электронным письмам и загрузок на наличие злонамеренного кода перед использованием
8. По какой причине для класса группы авторизованных интернет-пользователей в системе ГРИФ не предлагается никаких средств защиты рабочего места?
Для данной группы характерна минимальная вероятность реализации угрозы
Для группы по умолчанию выбран набор средств защиты рабочего места
Для группы неизвестно, откуда будет осуществляться доступ
Для группы неизвестна степень влияния на систему
9. Какие данные нельзя указать при задании контрмер в системе ГРИФ?
Стоимость внедрения
Возможное снижение затрат на ИБ
Срок внедрения контрмеры
Название для отчета
10. Какие параметры нельзя включить в состав отчета по проекту в системе КОНДОР?
Выполненные требования
Невыполненные требования
Риски
Контрмеры
11. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «подрыв репутации»?
Кратковременный экономический ущерб
Отсроченный экономический ущерб
Долговременный экономический ущерб
Немедленный экономический ущерб
12. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «снижение розничных продаж»?
Отсроченный экономический ущерб
Немедленный экономический ущерб
Кратковременный экономический ущерб
Долговременный экономический ущерб
13. Какой информации не содержится в отчете по периоду, формируемом системой КОНДОР?
Количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита
Уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита
Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
Затраты на контрмеры в целом по системе для выбранного периода аудита
14. Чему по умолчанию равны вероятность в течение года и критичность реализации для

только что созданной угрозы?
25 %
15 %
10 %
0 %

15. Какой информации не содержится в отчете по проекту, формируемом системой КОНДОР?
Изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
Изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
Текст выполненных требований по каждому разделу
Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
16. Какое количество мер защиты содержит в себе «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0»?
32
33
34
35
17. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР ИББС-1.2?
Диаграмма Ганта
Гистограмма
Круговая диаграмма
Срез структуры
18. Что понимается под базовым временем простоя ресурсов?
Время необходимое на обработку информации после запроса
Время отклика системы на запрос
Время, в течение которого доступ к информации ресурса невозможен
Время, в течение которого система загружает необходимые для работы службы
19. Фактором, значимым для использования уязвимости не является?
Время, затрачиваемое на идентификацию уязвимости
Техническая компетентность специалиста
Программное средство, требуемое для анализа
Знание проекта и функционирования объекта
20. Что понимается под эффективностью средства защиты информации?
Показатель быстродействия системы в условиях использования средств защиты информации
Коэффициент снижения уровня риска по отношению к первоначальному уровню
Степень влияния на защищенность информации и рабочего места группы пользователей
Субъективная оценка экспертами корректности функционирования средства защиты информации
21. Что понимается под базовой вероятностью конфиденциальности?
Вероятность огласки информации минимального уровня конфиденциальности в системе
Минимальная вероятность реализации угрозы
Максимальная вероятность реализации угрозы
Вероятность огласки информации максимального уровня конфиденциальности в системе
22. Какой тип внутренних нарушителей наиболее подвержен социальной инженерии?
Подрабатывающий
Внедренный
Манипулируемый
Нелояльный
23. К внешним чрезвычайным ситуациям не относятся?
Стихийные бедствия
Преступные действия
Техногенные аварии и сбои

Диверсии

24. Что не входит перечень того, что для любой организации, серьезно относящейся к информационной безопасности, важно применять в структурном и плановом подходе ГОСТ Р ИСО/МЭК ТО 18044-2007?
    Обнаружение, оповещение об инцидентах информационной безопасности и их оценка
    Реагирование на инциденты информационной безопасности, включая активацию защитных мер для предотвращения, уменьшения последствий и (или) восстановление после негативных воздействий
    Предотвращение инцидентов информационной безопасности
    Извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к менеджменту инцидентов информационной безопасности
25. Что понимается под инцидентом информационной безопасности?
    Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости
    Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности
    Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности
    Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов
26. К какому варианту неработоспособности относится болезнь сотрудника?
    Полное прекращение выполнения сотрудником своих обязанностей
    Опасность для жизни персонала
    Прекращение выполнения сотрудником рутинных операций
    Саботаж
27. К какой группе внешних чрезвычайных ситуаций относится скупка контрольного пакета акций?
    Общественные
    Правовые
    Экономические
    Экстренные
28. Какому из перечисленных типов внутренних нарушителей характерна постановка задачи извне?
    Халатный
    Манипулируемый
    Подрабатывающий
    Обиженный
29. Что понимается под характеристиками группы пользователей?
    Состав группы пользователей
    Название группы пользователей
    Вид доступа группы пользователей
    Описание группы пользователей
30. Какая статья расходов не входит в расходы на информационную безопасность?
    Затраты на приобретение систем защиты информации
    Затраты на управление системой защиты информации
    Затраты на разработку политики безопасности
    Затраты на обучение персонала
31. Что произойдет, если задать пороговое значение риска в 50% в системе КОНДОР?
    Будут отображены все положения стандартов, риски для которых ниже 50%
    Будут отображены все положения стандартов, риски для которых выше 50%
    Будут отображены только критичные положения стандартов, которые не выполнены
    Будут отображены только критичные положения стандартов, которые выполнены

9.1.2. Перечень вопросов для зачета

1. Структура и задачи сил кибероперацій вооруженных сил США.
2. Функциональная модель информационно-телекоммуникационной сети
3. Особенности организации компьютерных атак.
4. Применение метода анализа иерархий для оценки опасности компьютерных атак на информационно-телекоммуникационную сеть.
5. Методика оценки стратегии информационного воздействия на ИТКС
6. Методика оценки устойчивости в условиях информационного противоборства.
7. Вероятностно-временные характеристики компьютерных атак на элементы ИТКС.
8. Вероятностно-временные характеристики эквивалентных компьютерных атак.
9. Вероятностно-временные характеристики эквивалентных компьютерных атак по виду воздействия.
10. Вероятностно-временные характеристики последовательностей воздействия эквивалентных компьютерных атак
11. Направления повышения защищённости информационнотелекоммуникационной сети в условиях информационного противоборства.
12. Оценка эффективности средств защиты информационнотелекоммуникационной сети от компьютерных атак.
13. Методика синтеза системы защиты информационнотелекоммуникационной сети в условиях информационного противоборства

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. 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 9.2.

Таблица 9.2 – 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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 11 от «14» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	Е.Ю. Костюченко	Разработано, c6235dfe-234a-4234-88f9-e1597aac6463
Старший преподаватель, каф. КИБЭВС	А.И. Гуляев	Разработано, 9c396fa5-5881-4fe2-a7b2-3bea6e1a618f