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

Обеспечение устойчивости телекоммуникационных систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	20	20	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: 10 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 18.12.2019
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 51386

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) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

И.о. зав. каф. каф. БИС _____ Е. Ю. Костюченко

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. БИС _____ Е. Ю. Костюченко

Эксперты:

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

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

Согласована на портале № 51386

1. Цели и задачи дисциплины

1.1. Цели дисциплины

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

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

2. Место дисциплины в структуре ОПОП

Дисциплина «Обеспечение устойчивости телекоммуникационных систем» (Б1.Б.09.05) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности, Проектирование защищенных телекоммуникационных систем.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-5 способностью проектировать защищённые телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов;
- ПК-7 способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования;

В результате изучения дисциплины обучающийся должен:

- **знать** условия функционирования интегрированной информационно-телекоммуникационной сети
- **уметь** проводить оценку стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть
- **владеть** навыками синтеза системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства

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
		10 семестр
Аудиторные занятия (всего)	38	38
Лекции	18	18

Согласована на портале № 51386

Практические занятия	20	20
Самостоятельная работа (всего)	70	70
Проработка лекционного материала	5	5
Подготовка к практическим занятиям, семинарам	65	65
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
10 семестр					
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	4	4	20	28	ПК-5, ПК-7
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	6	6	18	30	ПК-5, ПК-7
3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	4	6	17	27	ПК-5, ПК-7
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	4	4	15	23	ПК-5, ПК-7
Итого за семестр	18	20	70	108	
Итого	18	20	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
10 семестр			
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях	Структура и задачи сил кибероперацій вооруженных сил США. Функциональная модель информационно-телекоммуникационной сети	4	ПК-5, ПК-7
	Итого	4	

Согласована на портале № 51386

информационного противоборства			
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	ПК-5, ПК-7
	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 воздействия эквивалентных компьютерных атак	4	ПК-5, ПК-7
	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 информационнотелекоммуникационной сети от компьютерных атак. Методика синтеза системы защиты информационнотелекоммуникационной сети в условиях информационного противоборства	4	ПК-5, ПК-7
	Итого	4	
Итого за семестр		18	

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
Предшествующие дисциплины				
1 Основы информационной безопасности	+	+	+	+
2 Проектирование защищенных телекоммуникационных систем	+	+	+	+

Согласована на портале № 51386

Последующие дисциплины				
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+
2 Преддипломная практика	+	+	+	+

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-5	+	+	+	Опрос на занятиях, Тест
ПК-7	+	+	+	Опрос на занятиях, 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
10 семестр			
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	Обсуждение и практическое применение изученных на лекции приемов.	4	ПК-5, ПК-7
	Итого	4	
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	Обсуждение и практическое применение изученных на лекции приемов.	6	ПК-5, ПК-7
	Итого	6	
3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	Обсуждение и практическое применение изученных на лекции приемов.	6	ПК-5, ПК-7
	Итого	6	
4 Синтез системы защиты	Обсуждение и практическое применение изученных на лекции приемов.	4	ПК-5, ПК-7

Согласована на портале № 51386

информационно-телекоммуникационной сети в условиях информационного противоборства	Итого	4	
Итого за семестр		20	

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
10 семестр				
1 Анализ условий функционирования интегрированной информационно-телекоммуникационной сети в условиях информационного противоборства	Подготовка к практическим занятиям, семинарам	19	ПК-5, ПК-7	Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Итого	20		
2 Оценка стратегии комплексного информационного воздействия на информационно-телекоммуникационную сеть	Подготовка к практическим занятиям, семинарам	16	ПК-5, ПК-7	Опрос на занятиях, Тест
	Проработка лекционного материала	2		
	Итого	18		
3 Устойчивость информационно-телекоммуникационной сети в условиях информационного противоборства	Подготовка к практическим занятиям, семинарам	16	ПК-5, ПК-7	Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Итого	17		
4 Синтез системы защиты информационно-телекоммуникационной сети в условиях информационного противоборства	Подготовка к практическим занятиям, семинарам	14	ПК-5, ПК-7	Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Итого	15		
Итого за семестр		70		
	Подготовка и сдача экзамена	36		Экзамен
Итого		106		

Согласована на портале № 51386

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
10 семестр				
Опрос на занятиях	20	20	20	60
Тест			10	10
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	40	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. 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. — Текст : электрон-

Согласована на портале № 51386

ный // ЭБС Юрайт [сайт]. — Режим доступа: https://urait.ru/bcode/473348 (дата обращения: 11.06.2021).

12.2. Дополнительная литература

1. Основы информационной безопасности [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2007. 201 с. — Режим доступа: https://edu.tusur.ru/publications/1024 (дата обращения: 11.06.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности [Электронный ресурс]: Учебное пособие для практических и семинарских занятий / А. М. Голиков - 2007. 154 с. — Режим доступа: https://edu.tusur.ru/publications/1017 (дата обращения: 11.06.2021).
2. Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. Информационная безопасность и защита информации [Электронный ресурс]: Практикум // Издательство Государственный университет «Дубна» // ISBN 978-5-89847-608-3 // 2020 // 85 с. — Режим доступа: https://e.lanbook.com/book/154490 (дата обращения: 11.06.2021).

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. https://lib.tusur.ru/
2. https://edu.tusur.ru/
3. Рекомендуется использовать информационные, справочные и нормативные базы данных 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.

13.1.2. 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.

Согласована на портале № 51386

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры: AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb/ мышь/ клавиатура/ монитор (15шт.);
- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– VirtualBox

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.

Согласована на портале № 51386

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

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

Согласована на портале № 51386

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?

Согласована на портале № 51386

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

Согласована на портале № 51386

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

Стихийные бедствия

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

14.1.2. Экзаменационные вопросы

Структура и задачи сил кибероперациий вооруженных сил США.

Функциональная модель информационно-телекоммуникационной сети

Особенности организации компьютерных атак.

Применение метода анализа иерархий для оценки опасности компьютерных атак на информационно-телекоммуникационную сеть.

Методика оценки стратегии информационного воздействия на ИТКС

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 воз-

Согласована на портале № 51386

действия.

Вероятностно-временные характеристики последовательностей воздействия эквивалентных компьютерных атак

Направления повышения защищённости информационнотелекоммуникационной сети в условиях информационного противоборства.

Оценка эффективности средств защиты информационнотелекоммуникационной сети от компьютерных атак.

Методика синтеза системы защиты информационнотелекоммуникационной сети в условиях информационного противоборства

14.1.3. Темы опросов на занятиях

Структура и задачи сил кибероперацій вооруженных сил США. Функциональная модель информационно-телекоммуникационной сети

Особенности организации компьютерных атак. Применение метода анализа иерархий для оценки опасности компьютерных атак на информационно-телекоммуникационную сеть. Методика оценки стратегии информационного воздействия на ИТКС

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 воздействия эквивалентных компьютерных атак

Направления повышения защищённости информационнотелекоммуникационной сети в условиях информационного противоборства. Оценка эффективности средств защиты информационнотелекоммуникационной сети от компьютерных атак. Методика синтеза системы защиты информационнотелекоммуникационной сети в условиях информационного противоборства

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;

Согласована на портале № 51386

– 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 № 51386