МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Катастрофоустойчивость автоматизированных банковских систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Всего аудиторных занятий	46	46	часов
4	Из них в интерактивной форме	16	16	часов
5	Самостоятельная работа	26	26	часов
6	Всего (без экзамена)	72	72	часов
7	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Зачет: 7 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «15» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:
Доцент каф. КИБЭВС _____ Е. И. Губин

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф.
КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент каф. КИБЭВС _____ А. А. Конев

Доцент каф. КИБЭВС _____ К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины "Катастрофоустойчивость автоматизированных банковских систем" является изучение технологий, методов и средств построения катастрофоустойчивых информационно-телекоммуникационных систем (ИТС) высокой доступности (ВД), связанных с проектированием и созданием катастрофоустойчивых коллективных центров обработки информации (КЦОИ) и телекоммуникационных средств при обеспечении необходимого уровня информационной безопасности.

1.2. Задачи дисциплины

- -сбор, обработка, анализ и систематизация научно-технической
- информации, отечественного и зарубежного опыта по проблемам безопасности автоматизированных банковских систем;
- -подготовка научно-технических отчетов, обзоров, публикаций по
- результатам выполненных исследований;
- -моделирование и исследование защищенных автоматизированных банковских систем,
- анализ их уязвимостей и эффективности средств и способов защиты;
- -анализ безопасности информационных технологий, реализуемых в
- автоматизированных банковских системах;

2. Место дисциплины в структуре ОПОП

Дисциплина «Катастрофоустойчивость автоматизированных банковских систем» (Б1.Б.32.2) относится к блоку 1 (базовая часть).

Последующими дисциплинами являются: Защита информации в банковских системах.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПСК-5.5 способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;
- ПСК-5.1 способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;

В результате изучения дисциплины обучающийся должен:

- **знать** -основные принципы построения катастрофоустойчивых ИТС ВД; -подходы к централизации катастрофоустойчивых ИТС ВД. -принципы работы средств обеспечения катастрофоустойчивости ИТС ВД; -основы оптимизации средств построения катастрофоустойчивых ИТС ВД; -основные методы и средства реализации катастрофоустойчивых ИТС ВД; -о политиках безопасности и мерах защиты в катастрофоустойчивых ИТС ВД; -о комплексном подходе к построению катастрофоустойчивых ИТС ВД.
- **уметь** -проектировать катастрофоустойчивые ИТС ВД; -определять и рациональные пути построения катастрофоустойчивых ИТС ВД ; -строить модель нарушителя ИБ для катастрофоустойчивых ИТС ВД; - выявлять условия необходимости построения катастрофоустойчивых ИТС ВД; -формировать организационно-распорядительное обеспечение катастрофоустойчивых ИТС ВД ; -применять стандартные решения для защиты информации в катастрофоустойчивых ИТС ВД и квалифицированно оценивать их качество; -используя современные методы и средства, разрабатывать и оценивать варианты построения катастрофоустойчивых ИТС ВД; -реализовывать системы защиты информации в катастрофоустойчивых ИТС ВД в соответствии со стандартами по оценке защищенных систем; -применять комплексный подход к обеспечению информационной безопасности в катастрофоустойчивых ИТС ВД; - проектировать и реализовывать комплексную систему управления катастрофоустойчивыми ИТС ВД; -осуществлять мониторинг и аудит безопасности катастрофоустойчивых ИТС ВД; - осуществлять администрирование катастрофоустойчивых ИТС ВД; -осуществлять управление ИБ в катастрофоустойчивых ИТС ВД.
- **владеть** -терминологией и системным подходом построения катастрофоустойчивых ИТС ВД; -навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых ИТС ВД; - навыка-

ми разработки политик безопасности для катастрофоустойчивых ИТС ВД.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	46	46
Лекции	28	28
Практические занятия	18	18
Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	26	26
Проработка лекционного материала	4	4
Подготовка к практическим занятиям, семинарам	22	22
Всего (без экзамена)	72	72
Общая трудоемкость, ч	72	72
Зачетные Единицы	2.0	2.0

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
7 семестр					
1 Системотехника катастрофоустойчивых автоматизированных систем	6	4	5	15	ПСК-5.1, ПСК-5.5
2 Методы обеспечения катастрофоустойчивости автоматизированных систем	6	4	7	17	ПСК-5.1, ПСК-5.5
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	8	4	7	19	ПСК-5.1, ПСК-5.5
4 Организация функционирования катстрофоустойчивых автоматизированных систем	8	6	7	21	ПСК-5.1, ПСК-5.5
Итого за семестр	28	18	26	72	
Итого	28	18	26	72	

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
7 семестр			
1 Системотехника катастрофоустойчивых автоматизированных систем	Общие положения Основные системотехнические принципы построения информационно-телекоммуникационной системы (ИТС). Проблемы традиционного системотехнического подхода к реализации ИТС. Условия возврата к централизованной обработке Подходы к созданию системы территориальнораспределенной обработки информации (СТРОИ) на основе центров обработки информации коллективного пользования (ЦОИ КП)	6	ПСК-5.1, ПСК-5.5
	Итого	6	
2 Методы обеспечения катастрофоустойчивост и автоматизированных систем	Активное резервирование и режимы функционирования ЦОИ КП в составе катастрофоустойчивой СТРОИ Выбор рациональных решений по организации средств восстановления ЦОИ ИТС после отказов и катастроф Оптимизация средств восстановления после отказов Поиск рациональных решений построения средств восстановления после катастроф	6	ПСК-5.1, ПСК-5.5
	Итого	6	
3 Средства и практические решения по обеспечению катастрофоустойчивост и автоматизированных систем	Практические решения построения средств восстановления после катастроф Основы обеспечения информационной безопасности в катастрофоустойчивых КЦОИ Требования к системно-техническим решениям по обеспечению комплексной защиты информации в КЦОИ	8	ПСК-5.1, ПСК-5.5
	Итого	8	
4 Организация функционирования катстрофоустойчивых автоматизированных систем	Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам КЦОИ в особых режимах его функционирования Типовой сценарий переноса обработки в случае частичного или полного выхода из строя КЦОИ Пример системотехнического решения по построению КЦОИ на основе zSeries	8	ПСК-5.1, ПСК-5.5
	Итого	8	
Итого за семестр		28	

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

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

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин			
	1	2	3	4
Последующие дисциплины				
1 Защита информации в банковских системах	+	+	+	+

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.	
ПСК-5.5	+	+	+	Конспект самоподготовки, Опрос на занятиях, Тест, Отчет по практическому занятию
ПСК-5.1	+	+	+	Конспект самоподготовки, Опрос на занятиях, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий приведены в таблице 6.1.

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные практические занятия, ч	Интерактивные лекции, ч	Всего, ч
7 семестр			
IT-методы		6	6
Работа в команде	4		4
Case-study (метод конкретных ситуаций)	4	2	6
Итого за семестр:	8	8	16
Итого	8	8	16

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
7 семестр			

1 Системотехника катастрофоустойчивых автоматизированных систем	Системотехника катастрофоустойчивых автоматизированных систем	4	ПСК-5.1, ПСК-5.5
	Итого	4	
2 Методы обеспечения катастрофоустойчивости автоматизированных систем	Методы обеспечения катастрофоустойчивости автоматизированных систем	4	ПСК-5.1, ПСК-5.5
	Итого	4	
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	4	ПСК-5.1, ПСК-5.5
	Итого	4	
4 Организация функционирования катстрофоустойчивых автоматизированных систем	Организация функционирования катастрофоустойчивых автоматизированных систем	6	ПСК-5.1, ПСК-5.5
	Итого	6	
Итого за семестр		18	

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
7 семестр				
1 Системотехника катастрофоустойчивых автоматизированных систем	Подготовка к практическим занятиям, семинарам	4	ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Итого	5		
2 Методы обеспечения катастрофоустойчивости автоматизированных систем	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Итого	7		
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		

систем	Итого	7		
4 Организация функционирования катстрофоустойчивых автоматизированных систем	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по практическому занятию
	Проработка лекционного материала	1		
	Итого	7		
Итого за семестр		26		
Итого		26		

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
7 семестр				
Конспект самоподготовки	5	5	5	15
Опрос на занятиях	12	12	12	36
Отчет по практическому занятию	15	17	17	49
Итого максимум за период	32	34	34	100
Нарастающим итогом	32	66	100	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. Малафеев, С.И. Надежность технических систем. Примеры и задачи [Электронный ресурс] : учебное пособие / С.И. Малафеев, А.И. Копейкин. — Санкт-Петербург : Лань, 2016. — 316 с. - ISBN 978-5-8114-1268-6. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/87584#authors (дата обращения: 02.07.2018).

2. Дорохов, А.Н. Обеспечение надежности сложных технических систем [Электронный ресурс] : учебник / А.Н. Дорохов, В.А. Керножицкий, А.Н. Миронов, О.Л. Шестопалова. — Санкт-Петербург : Лань, 2017. — 352 с. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/93594 (дата обращения: 02.07.2018).

12.2. Дополнительная литература

1. Информационные технологии и системы: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 352 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0376-6. [Электронный ресурс] - Режим доступа: http://znanium.com/catalog/product/374014 (дата обращения: 02.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Теория надежности: Методические указания для проведения практических занятий / Козлов В. Г. - 2012. 5 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1272 (дата обращения: 02.07.2018).

2. Теория надежности для специальности 210201: Методические указания по практическим занятиям и самостоятельной работе студентов / Козлов В. Г. - 2012. 20 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1716 (дата обращения: 02.07.2018).

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. 1. Компьютерная справочная правовая система КонсультантПлюс;
2. 2. Справочно-правовая система по законодательству Российской Федерации Гарант;
3. 3. Образовательный портал университета – http://www.lib.tusur.ru.
4. 4. Научная электронная библиотека – http://www.elibrary.ru

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

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле

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

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Компьютеры класса не ниже GigaByte GA-F2A68HM-DS2 rev1.0 (RTL) / AMD A4-6300 / DDR-III DIMM 8Gb / SVGARadeon HD 8370D / HDD 1Tb Gb SATA-III Seagate (10 шт.);
- Обучающий стенд локальные компьютерные сети Microtik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 (3 шт.);
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 (2 шт.);
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 (2 шт.);
- Маршрутизатор Cisco C881-V-K9 (2 шт.);
- Маршрутизатор Check Point CPAP-SG1200R-NGFW (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– Microsoft Windows 10

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:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– Microsoft SQL Server 2014
– Microsoft Windows 10

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

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

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

Состав оборудования:

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

Перечень программного обеспечения:

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

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

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

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

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

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

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

14.1.1. Тестовые задания

Комплекс аппаратных средств, предназначенных для работы информационной системы называется _____ обеспечением ИС.

1. материальным
2. организационным
3. техническим
4. экономическим

На стадии эксплуатации АБС НЕ должны быть определены, выполняться и регистрироваться процедуры:

1. контроля отсутствия уязвимостей в оборудовании и программном обеспечении

АБС;выпуск продукции, удовлетворяющей потребностям человека или системы

2. контроля за персоналом;

3. контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер.

В организации БС РФ должна быть организована эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей на:

1. рабочих станциях;

2. серверном оборудовании, в том числе серверах электронной почты;

3. технических средствах межсетевого экранирования;

4. все вышеперечисленные варианты ответа.

План обеспечения непрерывности бизнеса и его восстановления

после возможного прерывания должен содержать:

1. комплекс информационных ресурсов и методик;

2. комплект приборов для устранения неполадок;

3. инструкции и порядок действий работников организации БС РФ по восстановлению бизнеса.

Что входит в число задач, решаемых в ходе проведения анализа информационной безопасности объектов на соответствие требованиям стандартов в области информационной безопасности?

1. сбор и анализ данных об организационной и функциональной структуре информационной системы компании

2. анализ существующей политики обеспечения информационной безопасности

3. построение модели нарушителей информационной безопасности

4. все выше перечисленное

Для какого вида отказоустойчивости верно следующее предложение: система продолжает работать в случае отказов отдельных ее элементов без существенной потери функциональных свойств.

1. нулевая

2. частичная

3. полная

4. фрагментарная

Исходя из каких критериев происходит категорирование объектов критической информационной инфраструктуры?

1. социальная значимость

2. политическая значимость

3. экономическая значимость

4. все выше перечисленное

Что позволяет выявить аудит информационной безопасности?

1. оценить текущую безопасность функционирования корпоративной информационной системы

2. оценить и спрогнозировать риски, а также управлять их влиянием на бизнес процессы компании;

3. корректно и обоснованно подойти к вопросу обеспечения безопасности информационных активов компании

4. все выше перечисленное

Что характерно для низкого уровня политики информационной безопасности?

1. политика информационной безопасности служит для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности;

2. политика информационной безопасности определяет отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации.

3. Политика безопасности относится к отдельным элементам информационных систем и участкам обработки и хранения информации и описывают конкретные процедуры и документы, связанные с обеспечением информационной безопасности.

4. политика информационной безопасности является средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.

Какой из перечисленных видов нарушителей имеет наибольший потенциал?

1. Конкурирующие организации
2. Специальные службы иностранных государств
3. Лица, обеспечивающие функционирование информационных систем
4. Экстремистские группировки

Выявление критически важных функций организации; идентификация ресурсов, необходимых для выполнения критически важных функций; определение перечня возможных аварий; разработка стратегии; подготовка к реализации выбранной стратегии – это?

1. Активный аудит (оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения), служит для обнаружения и отражения атак.
2. Пассивный аудит
3. Процесс планирования восстановительных работ
4. Предупреждение или обнаружение атак

Что, согласно ГОСТ Р ИСО/МЭК 27031-2012 не является ключевым принципом ГИКТОНБ (готовность ИКТ к обеспечению непрерывности бизнеса):

1. предупреждение инцидентов
2. обнаружение инцидентов
3. планирование
4. реагирование

Согласно СТО БР ИББС-1.0-2014 группы процессов СМИБ организации БС РФ следует организовывать в виде циклической модели «Деминга», а именно:

1. планирование — проверка — реализация — совершенствование — планирование;
2. планирование — проверка — реализация— планирование— совершенствование;
3. планирование — реализация — проверка — совершенствование — планирование;
4. планирование — реализация — проверка — планирование — совершенствование.

Регламентацией называют методы защиты ИС:

1. побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм;
2. метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации);
3. создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени;
4. метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

7. Что, согласно СТО БР ИББС-1.0-2014 не входит в общие стадии модели ЖЦ АБС?

1. разработка технических заданий;
2. приемка и ввод в действие;
3. разработка инструкций;
4. эксплуатация

Под катастрофоустойчивостью АБС подразумевается:

1. способность не подвергаться техногенным воздействиям;
2. способность восстанавливать необходимую документацию, после техногенных катастроф;
3. способность к восстановлению работы приложений и данных за минимально короткий период времени после катастрофы.

На основании каких нормативных документов производится внедрение системы защиты ИС?

1. ГОСТ 34.601;
2. ГОСТ Р 51583
3. ГОСТ Р 51624;

4. ГОСТ 34.603.

Кто согласно СТО БР ИББС-1.0-2014 обладает наибольшими возможностями для нанесения ущерба организации БС РФ:

1. вредоносное ПО;
2. стихийные бедствия;
3. персонал.

Какие нормативные документы регламентируют создание ТЗ на защиту информации в ИС?

1. Приказ ФСТЭК России от 14.03.2014 г. №31;
2. Приказ ФСТЭК России от 11.02.2013 №17;
3. (ГОСТ 34.601, ГОСТ Р 51583);
4. 149-ФЗ «Об информации, ИТ и о ЗИ».

Назовите уровни обеспечения информационной безопасности ИС:

1. Инициация. Закупка. Установка. Эксплуатация;
2. Техническое задание, Рабочий проект, Внедрение, Эксплуатация;
3. Законодательный, административный, процедурный, программно-технический;
4. Организационный; Технологический; Процедурный; Технический.

В рамках банковских платежных технологических процессов в качестве активов, защищаемых в первую очередь, следует рассматривать:

1. банковский платежный технологический процесс;
2. платежную информацию;
3. Всё из вышеперечисленного;
4. Ничего из вышеперечисленного

14.1.2. Темы опросов на занятиях

Общие положения Основные системотехнические принципы построения информационно-телекоммуникационной системы (ИТС). Проблемы традиционного системотехнического подхода к реализации ИТС. Условия возврата к централизованной обработке Подходы к созданию системы территориальнораспределенной обработки информации (СТРОИ) на основе центров обработки информации коллективного пользования (ЦОИ КП)

Активное резервирование и режимы функционирования ЦОИ КП в составе катастрофоустойчивой СТРОИ Выбор рациональных решений по организации средств восстановления ЦОИ ИТС после отказов и катастроф Оптимизация средств восстановления после отказов Поиск рациональных решений построения средств восстановления после катастроф

Практические решения построения средств восстановления после катастроф Основы обеспечения информационной безопасности в катастрофоустойчивых КЦОИ Требования к системно-техническим решениям по обеспечению комплексной защиты информации в КЦОИ

Организационно-технические решения по обеспечению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам КЦОИ в особых режимах его функционирования Типовой сценарий переноса обработки в случае частичного или полного выхода из строя КЦОИ Пример системотехнического решения по построению КЦОИ на основе zSeries

14.1.3. Вопросы на самоподготовку

1. Специфика защиты ресурсов открытых ИС.
2. Модели угроз и нарушителей ИБ
3. Политика ИБ для открытых ИС
4. Удаленные атаки на сети
5. Средства защиты открытых ИС

14.1.4. Вопросы для подготовки к практическим занятиям, семинарам

Системотехника катастрофоустойчивых автоматизированных систем

Методы обеспечения катастрофоустойчивости автоматизированных систем

Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем

Организация функционирования катастрофоустойчивых автоматизированных систем

14.1.5. Зачёт

1.Основные системотехнические принципы построения информационно-телекоммуникаци-

онной системы (ИТС).

2. Проблемы традиционного системотехнического подхода к реализации ИТС.

3. Условия возврата к централизованной обработке.

4. Подходы к созданию системы территориально-распределенной обработки информации (СТРОИ) на основе центров обработки информации коллективного пользования (ЦОИ КП)

5. Методы обеспечения катастрофоустойчивости автоматизированных систем

6.Активное резервирование и режимы функционирования ЦОИ КП в составе катастрофоустойчивой СТРОИ

7. Выбор рациональных решений по организации средств восстановления ЦОИ ИТС после отказов и катастроф

8. Оптимизация средств восстановления после отказов

9. Поиск рациональных решений построения средств восстановления после катастроф.

10.. Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем

11. Практические решения построения средств восстановления после катастроф Основы обеспечения информационной безопасности в катастрофоустойчивых КЦОИ

12. Требования к системно-техническим решениям по обеспечению комплексной защиты информации в КЦОИ

13. Организация функционирования катастрофоустойчивых автоматизированных систем

печению защиты от несанкционированного доступа со стороны обслуживающего персонала к ресурсам КЦОИ в особых режимах его функционирования

14. Типовой сценарий переноса обработки в случае частичного или полного выхода из строя КЦОИ

15 .Пример системотехнического решения по построению КЦОИ на основе zSeries

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.