МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Катастрофоустойчивость автоматизированных банковских систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **5**
Семестр: **9**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	56	56	часов
4	Из них в интерактивной форме	16	16	часов
5	Самостоятельная работа	52	52	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 9 семестр

Томск 2017

Согласована на портале № 16394

Рассмотрена и одобрена на заседании кафедры
протокол № 2 от «28» 2 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа 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 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчики:

Доцент, кандидат физико-математических наук каф. КИБЭВС _____ Губин Е. И.

Заведующий обеспечивающей каф. КИБЭВС _____ Шелупанов А. А.

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ _____ Давыдова Е. М.

Заведующий выпускающей каф. КИБЭВС _____ Шелупанов А. А.

Эксперты:

Доцент, кандидат технических наук каф. КИБЭВС _____ Конев А. А.

Согласована на портале № 16394

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.33.3) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: 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 студент 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.

Согласована на портале № 16394

– **владеть** -терминологией и системным подходом построения катастрофоустойчивых ИТС ВД; -навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых ИТС ВД; -навыками разработки политик безопасности для катастрофоустойчивых ИТС ВД.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Аудиторные занятия (всего)	56	56
Лекции	28	28
Практические занятия	28	28
Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	52	52
Проработка лекционного материала	28	28
Подготовка к практическим занятиям, семинарам	24	24
Всего (без экзамена)	108	108
Общая трудоемкость ч	108	108
Зачетные Единицы	3.0	3.0

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	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
9 семестр					
1 Системотехника катастрофоустойчивых автоматизированных систем	6	8	13	27	ПСК-5.1, ПСК-5.5
2 Методы обеспечения катастрофоустойчивости автоматизированных систем	6	8	13	27	ПСК-5.1, ПСК-5.5
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	8	6	13	27	ПСК-5.1, ПСК-5.5
4 Организация функционирования катстрофоустойчивых автоматизированных систем	8	6	13	27	ПСК-5.1, ПСК-5.5
Итого за семестр	28	28	52	108	

Согласована на портале № 16394

Итого	28	28	52	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
9 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 катастрофоустойчивости 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 катастрофоустойчивости 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	8	ПСК-5.1, ПСК-5.5

Согласована на портале № 16394

	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		
	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
Предшествующие 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 и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ПСК-5.5	+	+	+	Конспект самоподготовки, Опрос на занятиях, Отчет по практике
ПСК-5.1	+	+	+	Конспект самоподготовки, Опрос на занятиях, Отчет по практике

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
9 семестр			

Согласована на портале № 16394

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
9 семестр			
1 Системотехника катастрофоустойчивых автоматизированных систем	Системотехника катастрофоустойчивых автоматизированных систем	8	ПСК-5.1, ПСК-5.5
	Итого	8	
2 Методы обеспечения катастрофоустойчивости автоматизированных систем	Методы обеспечения катастрофоустойчивости автоматизированных систем	8	ПСК-5.1, ПСК-5.5
	Итого	8	
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	6	ПСК-5.1, ПСК-5.5
	Итого	6	
4 Организация функционирования катстрофоустойчивых автоматизированных систем	Организация функционирования катастрофоустойчивых автоматизированных систем	6	ПСК-5.1, ПСК-5.5
	Итого	6	
Итого за семестр		28	

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
9 семестр				

Согласована на портале № 16394

1 Системотехника катастрофоустойчивых автоматизированных систем	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по практике
	Проработка лекционного материала	7		
	Итого	13		
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 практике
	Проработка лекционного материала	7		
	Итого	13		
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем	Подготовка к практическим занятиям, семинарам	6	ПСК-5.1, ПСК-5.5	Конспект самоподготовки, Опрос на занятиях, Отчет по практике
	Проработка лекционного материала	7		
	Итого	13		
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 практике
	Проработка лекционного материала	7		
	Итого	13		
Итого за семестр		52		
Итого		52		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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
9 семестр				
Конспект самоподготовки	5	5	5	15
Опрос на занятиях	12	12	12	36
Отчет по практике	15	17	17	49
Итого максимум за период	32	34	34	100
Нарастающим итогом	32	66	100	100

Согласована на портале № 16394

11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

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

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Основы информационных технологий: Учебное пособие / Исакова А. И. - 2016. 206 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6484, дата обращения: 28.02.2017.

2. Организационное обеспечение информационной безопасности : учебник для вузов / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188, [4] с. - (Высшее профессиональное образование. Информационная безопасность) (Учебник). - Библиогр.: с. 185. - ISBN 978-5-7695-4272-5 (наличие в библиотеке ТУСУР - 1 экз.)

12.2. Дополнительная литература

1. Разработка правил информационной безопасности : пер. с англ. / С. Бармен ; пер.: И. В. Чайка, В. И. Яковлев. - М. : Вильямс, 2002. - 207, [1] с. : ил., портр. - Предм. указ.: с. 206-207. - ISBN 5-8459-0323-8 (наличие в библиотеке ТУСУР - 1 экз.)

2. Финансовые рынки: Учебное пособие / Цибульникова В. Ю. - 2011. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/3849, дата обращения: 28.02.2017.

3. Предметно-ориентированные экономические информационные системы: Учебное пособие / Исакова А. И. - 2016. 239 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6542, дата обращения: 28.02.2017.

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2506, дата обращения:

Согласована на портале № 16394

28.02.2017.

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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. Ресурсы сети Интернет

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. http://www.lib.tusur.ru – образовательный портал университета;
2. http://www.elibrary.ru – научная электронная библиотека.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Мультимедийная лекционная аудитория. Дисплейный класс с локальной вычислительной сетью. Интерактивная доска с лицензионным программным обеспечением и мультимедиапроектором.

13.1.2. Материально-техническое обеспечение для практических занятий

Мультимедийная лекционная аудитория. Дисплейный класс с локальной вычислительной сетью. Интерактивная доска с лицензионным программным обеспечением и мультимедиапроектором.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Мультимедийная лекционная аудитория. Дисплейный класс с локальной вычислительной сетью. Интерактивная доска с лицензионным программным обеспечением и мультимедиапроектором.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного

Согласована на портале № 16394

аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 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;

Согласована на портале № 16394

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 16394

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Катастрофоустойчивость автоматизированных банковских систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **5**
Семестр: **9**

Учебный план набора 2012 года

Разработчики:

- Доцент, кандидат физико-математических наук каф. КИБЭВС Губин Е. И.

Зачет: 9 семестр

Томск 2017

Согласована на портале № 16394

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования 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	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. ; Должен 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
ПСК-5.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем	

Согласована на портале № 16394

		управления катастрофоустойчивыми ИТС ВД; -осуществлять мониторинг и аудит безопасности катастрофоустойчивых ИТС ВД; - осуществлять администрирование катастрофоустойчивых ИТС ВД; -осуществлять управление ИБ в катастрофоустойчивых ИТС ВД.; Должен владеть -терминологией и системным подходом построения катастрофоустойчивых ИТС ВД; -навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых ИТС ВД; - навыками разработки политик безопасности для катастрофоустойчивых ИТС ВД. ;

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПСК-5.5

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.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	-основные принципы построения катастрофоустойчивых	-проектировать катастрофоустойчивые ИТС ВД; -определять и	-терминологией и системным подходом построения

Согласована на портале № 16394

	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.	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	катастрофоустойчивых ИТС ВД; -навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых ИТС ВД; - навыками разработки политик безопасности для катастрофоустойчивых ИТС ВД.

Согласована на портале № 16394

		ИТС ВД; -осуществлять управление ИБ в катастрофоустойчивых ИТС ВД.	
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Зачет;	• Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Зачет;	• Отчет по практике; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в с пониманием границ применимости;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	• Контролирует работу, проводит оценку, совершенствует действия работы.;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования.;	• Берет ответственность за завершения задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем.;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями.;	• Обладает основными умениями, требуемыми для выполнения простых задач.;	• Работает при прямом наблюдении.;

2.2 Компетенция ПСК-5.1

ПСК-5.1: способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть

Согласована на портале № 16394

Содержание этапов	-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.	-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	-терминологией и системным подходом построения катастрофоустойчивых ИТС ВД; -навыками анализа угроз ИБ и уязвимостей в катастрофоустойчивых ИТС ВД; - навыками разработки политик безопасности для катастрофоустойчивых ИТС ВД.

Согласована на портале № 16394

		ИТС ВД; - осуществлять администрирование катастрофоустойчивых ИТС ВД; -осуществлять управление ИБ в катастрофоустойчивых ИТС ВД.	
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Зачет;	• Опрос на занятиях; • Конспект самоподготовки; • Отчет по практике; • Зачет;	• Отчет по практике; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Обладает фактическими и теоретическими знаниями в пределах изучаемой области в с пониманием границ применимости;	• Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем.;	• Контролирует работу, проводит оценку, совершенствует действия работы.;
Хорошо (базовый уровень)	• Знает факты, принципы, процессы, общие понятия в пределах изучаемой области.;	• Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования.;	• Берет ответственность за завершения задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем.;
Удовлетворительно (пороговый уровень)	• Обладает базовыми общими знаниями.;	• Обладает основными умениями, требуемыми для выполнения простых задач.;	• Работает при прямом наблюдении.;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

Согласована на портале № 16394

3.1 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

3.2 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

3.3 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

3.4 Зачёт

– 1.Основные системотехнические принципы построения информационно-телекоммуникационной 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

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций,

Согласована на портале № 16394

согласно п. 12 рабочей программы.

4.1. Основная литература

1. Основы информационных технологий: Учебное пособие / Исакова А. И. - 2016. 206 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6484, свободный.
2. Организационное обеспечение информационной безопасности : учебник для вузов / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188, [4] с. - (Высшее профессиональное образование. Информационная безопасность) (Учебник). - Библиогр.: с. 185. - ISBN 978-5-7695-4272-5 (наличие в библиотеке ТУСУР - 1 экз.)

4.2. Дополнительная литература

1. Разработка правил информационной безопасности : пер. с англ. / С. Бармен ; пер.: И. В. Чайка, В. И. Яковлев. - М. : Вильямс, 2002. - 207, [1] с. : ил., портр. - Предм. указ.: с. 206-207. - ISBN 5-8459-0323-8 (наличие в библиотеке ТУСУР - 1 экз.)
2. Финансовые рынки: Учебное пособие / Цибульникова В. Ю. - 2011. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/3849, свободный.
3. Предметно-ориентированные экономические информационные системы: Учебное пособие / Исакова А. И. - 2016. 239 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6542, свободный.

4.3. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности: Методические указания по практическим занятиям и самостоятельной работе / Семенов Э. В. - 2012. 13 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2506, свободный.

4.4. Ресурсы сети Интернет

4.4. Базы данных, информационно справочные и поисковые системы

1. http://www.lib.tusur.ru – образовательный портал университета;
2. http://www.elibrary.ru – научная электронная библиотека.

Согласована на портале № 16394