МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ 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 2016 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.

Зачёт: 7 семестр

Томск

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

Предшествующими дисциплинами, формирующими начальные знания, являются: Разработка методов обеспечения безопасности информационных технологий (ГПО-2).

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; - навыками разработки политик безопасности для катастрофоустойчивых ИТС ВД.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
7 семестр
1 Системотехника катастрофоустойчивых автоматизированных систем
2 Методы обеспечения катастрофоустойчивости автоматизированных систем
3 Средства и практические решения по обеспечению катастрофоустойчивости автоматизированных систем
4 Организация функционирования катстрофоустойчивых автоматизированных систем