Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

**Пермский национальный исследовательский
политехнический университет**

Электротехнический факультет
Кафедра автоматики и телемеханики

УТВЕРЖДАЮ
Проректор по учебной работе
д-р техн. наук, проф.
_____ Н. В. Лобов
«18» ____11____ 2015 г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Безопасность систем баз данных»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основная образовательная программа подготовки специалистов
по специальности: 090303.65 «Информационная безопасность автоматизированных систем»

Специализация специалиста	- 09030307.65 Обеспечение информационной безопасности распределенных информационных систем
Квалификация (степень) выпускника	- специалист
Специальное звание выпускника	- специалист по защите информации
Выпускающая кафедра	«Автоматика и телемеханика»
Форма обучения	очная

Курс: 4,5 Семестр: 8,9

Трудоёмкость:
Кредитов по рабочему учебному плану: 10 ЗЕТ
Часов по рабочему учебному плану: 360 АЧ

Виды контроля:
Зачет: 8 Экзамен: 9

Пермь 2015 г.

Рабочая программа дисциплины «Безопасность систем баз данных» разработана на основании:

- Федерального государственного образовательного стандарта высшего профессионального образования утвержденного приказом Министерства образования и науки Российской Федерации «17» января 2011 г. № 60, по направлению подготовки (специальности) 090303 «Информационная безопасность автоматизированных систем» (квалификация (степень) «специалист»);
- Компетентностной модели (КМ) выпускника ООП по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, утвержденной «24» 06 2013 г.;
- Рабочего учебного плана очной формы обучения по специализации подготовки 090303.07.65 - Обеспечение информационной безопасности распределенных информационных систем, (набор 2011 года), утвержденного «29» августа 2011 г.

Рабочая программа согласована с рабочей программой дисциплин: Введение в специальность, Основы информационной безопасности, Комплексная система защиты информации на предприятии, Управление информационной безопасностью, Программно-аппаратные средства защиты информации.

Разработчик канд. техн. наук _____ Кокоулин А.Н.

Рецензент канд. техн. наук _____ Шабуров А.С.

Рабочая программа рассмотрена и одобрена на заседании кафедры «Автоматика и телемеханика» «14» 01 2015 г., протокол № 14.
Заведующий кафедрой,
«Автоматика и телемеханика»,
д-р. техн. наук, профессор _____ Южаков А.А.

Рабочая программа одобрена методической комиссией электротехнического факультета «25» 06 2015 г., протокол № 8
Председатель методической комиссии
электротехнического факультета,
канд. техн. наук, профессор _____ Гольдштейн А.Л.

СОГЛАСОВАНО
Заведующий выпускающей кафедрой
«Автоматика и телемеханика»
д-р техн. наук, профессор _____ А.А. Южаков

Начальник управления
образовательных программ
канд. техн. наук, доцент _____ Д.С. Репецкий

1. Общие положения

1.1. Цель дисциплины - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности.

В процессе изучения дисциплины студент осваивает части следующих компетенций по направлениям подготовки ВПО:

- Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);
- Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);
- Способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-20).

1.2. Задачи дисциплины:

– изучение основных положений, понятий и категорий международных правовых документов Конституции и нормативно-правовых актов Российской Федерации в области обеспечения информационной безопасности;

– изучение правовых основ и принципов организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны и служб защиты информации на предприятиях;

– ознакомление с политикой безопасности компании в области информационной безопасности;

– ознакомление со стандартами информационной безопасности;

– изучение криптографических методов и алгоритмов шифрования информации;

– изучение алгоритмов аутентификации пользователей;

– приобретение навыков защиты информации в сетях;

– изучение требований к системам защиты информации.

– приобретение умений в разработке проектов нормативных и организационно-распорядительных документов в области обеспечения информационной безопасности и их применении;

– приобретение навыков работы в организации и обеспечении режима секретности, физической защиты объектов, методах организации работы с персоналом и управлению деятельностью служб защиты информации на предприятии.

После изучения дисциплины обучающийся должен демонстрировать следующие результаты:

знать:

- модели данных, систем и процессов защиты информации в автоматизированных системах, критерии оценки защищенности автоматизированных систем;
- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем, средства автоматизации проектирования автоматизированных систем;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

- методы и модели анализа угроз безопасности подсистем автоматизированных систем; методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
- основные меры по защите информации в автоматизированных системах, состав работ по защите информации на стадиях и этапах создания автоматизированных систем, с учетом требований нормативно-технической документации;

уметь:

- разрабатывать модели нарушителей и оценивать угрозы информационной безопасности автоматизированных систем;
- выявлять уязвимости информационно-технологических ресурсов автоматизированных систем;
- определять комплекс мер для обеспечения информационной безопасности автоматизированных систем;
- выполнять работы по эксплуатации компонентов автоматизированных систем на объектах информатизации;

владеть:

- навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
- методами и технологиями проектирования, моделирования, исследования подсистем безопасности автоматизированных систем.

1.3. Предметом освоения дисциплины являются следующие объекты:

- модели данных, систем и процессов защиты информации;
- стандарты оценки защищенности автоматизированных систем;
- критерии оценки защищенности автоматизированных систем;
- угрозы безопасности информации в автоматизированных системах;
- базовая модель угроз безопасности информации;
- модель нарушителя в автоматизированной системе;
- методы и модели оценки угроз безопасности автоматизированных систем;
- стадии и этапы разработки автоматизированных систем;
- средства автоматизации проектирования автоматизированных систем;
- состав работ по защите информации на стадиях и этапах создания автоматизированных систем;
- меры по защите информации в автоматизированных системах;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;

методы, способы и средства обеспечения отказоустойчивости

1.4. Место дисциплины в структуре профессиональной подготовки выпускников

Дисциплина «Безопасность систем баз данных» относится к базовой части цикла профессиональных дисциплин по специальности 090303 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»).

Дисциплина является обязательной при освоении ООП ВПО по указанному направлению и подготовки по специальности.

В таблице 1.3 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций, заявленных в пункте 1.1.

Таблица 1.1 - Дисциплины, направленные на формирование компетенций

Направление (специальность)	**Код компетенции**	**Наименование компетенций**	**Предшествующие дисциплины**	**Последующие дисциплины**
090303.65	ПК-13	Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированных систем	Основы построения инфокоммуникационных систем и сетей Вычислительная техника и информационные технологии	Информационная безопасность в экономике
	ПК-15	Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	Основы построения инфокоммуникационных систем и сетей Защита и обработка конфиденциальных документов	Управление информационной безопасностью
	ПК-20	Способность разрабатывать политики информационной безопасности автоматизированных систем	Основы построения инфокоммуникационных систем и сетей Вычислительная техника и информационные технологии	Защита и обработка конфиденциальных документов Информационная безопасность в банковской системе

2. Требования к результатам освоения учебной дисциплины

Дисциплина обеспечивает формирование части компетенции ПК-13,ПК-15 и ПК-20:

2.1. Дисциплинарная карта компетенции ПК-13

Код ПК-13	**Формулировка компетенции** Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированных систем

Код ПК-13 .С3.Б18	**Формулировка дисциплинарной части компетенции:** Способность разрабатывать модели угроз и нарушителя в подсистемах хранения данных информационных систем в соответствии с требованиями государственных или корпоративных нормативных документов

Требования к компонентному составу части компетенции

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – основные угрозы безопасности информации и модели нарушителя для баз данных; (ПК-13 .С3.Б18.1З) – основные меры по защите информации в автоматизированных системах, в том числе от угроз SQL Injection, XSS, повышение полномочий и атак на программные модули СУБД (ПК-13 .С3.Б18.2З)	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы текущего, рубежного и итогового контроля; собеседование по самостоятельно изученному материалу
умеет: – создавать защищенные приложения, реализующие информационный обмен средствами баз данных; (ПК-13 .С3.Б18.1У) – классифицировать угрозы ИБ, включая НСД, НСК и нарушение доступности; настраивать системубезопасности для обнаружения и парирования типовых угроз (ПК-13 .С3.Б18.2У)	Практические занятия и лабораторные работы; выполнение индивидуального задания по тематике практических занятий и лабораторных работ	Темы индивидуального задания по тематике практических занятий и лабораторных работ
владеет: – методами обнаружения и предотвращения вторжений в информационные системы, использующие базы данных. (ПК-13 .С3.Б18.1В)	Самостоятельная работа по индивидуальному заданию по учебному модулю дисциплины	Те мы индивидуальных заданий по учебному модулю дисциплины

2.2. Дисциплинарная карта компетенции ПК-15

Код ПК-15	**Формулировка унифицированной дисциплинарной компетенции** Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

Код ПК-15 .С3.Б18	**Формулировка дисциплинарной части компетенции:** Способность проектировать и разрабатывать приложения, использующие сетевые базы данных и реализующие основные принципы обеспечения информационной безопасности

Требования к компонентному составу части компетенции

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – модели данных и принципы организации хранения в базах данных; Основы языков программирования БД – SQL; (ПК-15 .С3.Б18.1З) – основные принципы создания безопасных хранимых процедур, триггеров и других объектов с использованием процедурных расширений языка SQL (PL/SQL); (ПК-15 .С3.Б18.2З)	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы текущего, рубежного и итогового контроля; собеседование по самостоятельно изученному материалу
умеет: – реализовывать собственную схему данных средствами языка SQL; реализовывать дискреционную схему разделения доступа к объектам БД; (ПК-15 .С3.Б18.1У)	Практические занятия и лабораторные работы; выполнение индивидуального задания по тематике практических занятий и лабораторных работ	Темы индивидуального задания по тематике практических занятий и лабораторных работ
владеет: – методами и технологиями проектирования, моделирования и программирования безопасных систем хранения данных автоматизированных систем. (ПК-15 .С3.Б18.1В)	Самостоятельная работа по индивидуальному заданию по учебному модулю дисциплины	Те мы индивидуальных заданий по учебному модулю дисциплины

2.3. Дисциплинарная карта компетенции ПК-20

Код ПК-20	**Формулировка унифицированной дисциплинарной компетенции** Способность разрабатывать политики информационной безопасности автоматизированных систем

Код ПК-20 .С3.Б18	**Формулировка дисциплинарной части компетенции:** Способность разрабатывать политики информационной безопасности автоматизированных систем с учетом особенностей операционных систем, баз данных и сетей передачи данных

Требования к компонентному составу части компетенции

Требования к компонентному составу компетенции

Перечень компонентов	Виды учебной работы	Средства оценки
В результате освоения компетенции, студент знает: – методы, способы и содержание этапов разработки безопасной и надежной подсистемы хранения данных автоматизированной системы, включающей защиту от НСД и ведение аудита доступа пользователей; (ПК-20 .С3.Б18.1З) – методы обеспечения доступности данных, включающие журналирование, резервное копирование, кластеризацию и защиту информации от потерь с использованием отказоустойчивых хранилищ; (ПК-20 .С3.Б18.2З)	Лекции Семинарские занятия Самостоятельная работа студентов по изучению теоретического материала	Вопросы текущего, рубежного и итогового контроля; собеседование по самостоятельно изученному материалу
умеет: – проводить аргументированный выбор, рассчитывать характеристики и реализовывать систем резервного копирования; (ПК-20 .С3.Б18.1У) – использовать встроенные средства аудита пользовательских действий для грамотного протоколирования попыток несанкционированного изменения данных и схемы данных; (ПК-20 .С3.Б18.2У)	Практические занятия и лабораторные работы; выполнение индивидуального задания по тематике практических занятий и лабораторных работ	Темы индивидуального задания по тематике практических занятий и лабораторных работ
владеет: – программным обеспечением, реализующим резервное копирование баз данных, экспорт и импорт данных, а также функции аудита баз данных информационных систем. (ПК-20 .С3.Б18.1В)	Самостоятельная работа по индивидуальному заданию по учебному модулю дисциплины	Те мы индивидуальных заданий по учебному модулю дисциплины

3. Объем дисциплины и виды учебной работы

3.1. Структура дисциплины содержит распределение используемых видов аудиторной работы (АРС) и самостоятельной работы студентов (СРС) с указанием трудоемкости и форм представления результатов выполнения видов учебных работ.

3.2. Основными видами аудиторной работы по дисциплине являются:

- лекции (ЛК);
- лабораторные работы (ЛР)
- практические занятия (ПЗ)
- семинарские занятия (СЗ).

3.3. Основными видами самостоятельной работы по дисциплине являются:

- самостоятельное изучение теоретического материала (ИТМ);
- выполнение индивидуальных заданий по тематике лабораторных работ (ИЗЛР) и практических занятий (ИЗПЗ);
- выполнение индивидуального комплексного задания по модулям дисциплины и защита отчета (ИКЗД).

3.4. Структура дисциплины по видам и формам приведена в табл. 3.1.

Таблица 3.1 – Объём и виды учебной работы

№ п/п	Виды учебной работы	Трудоемкость в АЧ			Форма представления результатов
		8	9	Всего	
1	2	3	4	5	6
1	**Аудиторная работа:**	**54**	**108**	**162**	
	– в том числе в интерактивной форме	14	14	28	
	– лекции (Л)	16	32	48	конспект лекций
	– в том числе в интерактивной форме	4	4	8	
	– лабораторные работы	36	36	72	отчет о выполнении
	– практические занятия (ПЗ), семинарские занятия (СЗ)	-	36	36	отчет о выполнении
	– в том числе в интерактивной форме	-	20	20	
2	Контроль самостоятельной работы (КСР)	2	4	6	
3	**Самостоятельная работа студентов (СРС)**	**54**	**108**	**162**	
	Самостоятельное изучение теоретического материала (ИТМ)	20	40	60	отчет по вопросам для текущего и рубежного контроля
	Выполнение индивидуальных заданий по тематике лабораторных работ (ИЗЛР)	10	10	20	отчёт о выполнении
	Выполнение индивидуальных заданий по тематике практических занятий (ИЗПЗ)	-	40	40	отчёт о выполнении
	Выполнение индивидуального комплексного задания по модулям дисциплины (ИКЗД)	24	18	42	отчёт о выполнении
4	Итоговая аттестация по дисциплине:	зачет	36	36	**Экзамен**
3	**Трудоемкость дисциплины, всего:** **в часах (АЧ)** **в зачетных единицах (ЗЕТ)**	**108** **3**	**252** **7**	**360** **10**	

4. Содержание учебной дисциплины

4.1. Модульный тематический план

Общая структура содержания дисциплины представлена тематическим планом, который задает распределение трудоемкостей модулей, разделов и тем содержания по видам аудиторной и самостоятельной работы (табл.4.1).

Таблица 4.1 – Тематический план по модулям учебной дисциплины

Номер учебного модуля	Номер раздела дисциплины	Номер темы дисциплины	Количество часов (очная форма обучения)										Итог.ат	Трудоёмкость АЧ/ЗЕТ
			Аудиторная работа студента (АРС)					Самостоятельная работа студента (СРС)						
			Всего	Лк	ЛР	ПЗ, СЗ	КСР	Всего	ИТМ	ИЗ ПЗ	ИЗ ЛР	ИК ЗД		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1.1	2	2										2
		1.2	2	2				10	10					12
		1.3	4	4				6				6		10
	Всего по модулю:		**8**	8				**16**	10			6		**24**
2	1	1.4	14	2	12			2			2			16
		1.5	15	3	12			14	10		4			29
		1.6	17	3	12		2	22			4	18		39
	Всего по модулю:		**46**	8	36		2	**31**	10		10	18		**84**
Всего по разделу:			**54**	**16**	**36**	**-**	**2**	**54**	**20**		**10**	**24**		**108/3**
3	2	2.1	8	4		4		10	10					14
		2.2	10	6		4		20	10	10				30
		2.3	10	6		4		18		10		8		20
	Всего по модулю:		**28**	16		12		**48**	20	20		**8**		**76**
4	2	2.4	24	4	12	8		10	10		2			**26**
		2.5	26	6	12	8		24	10	10	4			**53**
		2.6	30	6	12	8	4	24		10	4	10		**37**
	Всего по модулю:		**80**	16	36	24	4	**58**	20	20	10	10		**138**
Всего по разделу:			**108**	**32**	**36**	**36**	**4**	**108**	**40**	**40**	**10**	**18**		**216/6**
Итоговая аттестация													**36**	**36/1**
Итого			**162**	**48**	**72**	**36**	**6**	**162**	**60**	**40**	**20**	**42**	**36**	**360/1**

4.2. Содержание разделов и тем учебной дисциплины

Раздел I. Системы хранения и обработки данных современных информационных систем

Модуль 1. Проектирование информационных систем. Реляционные СУБД

АРС: Л - 8 ч.; СРС: ИТМ - 10 ч., ИКЗД - 6 ч.

Тема 1.1. Проектирование информационных управляющих систем

Понятие информационной управляющей системы (ИУС), информационного обеспечения. Этапы развития информационных технологий. Структура ИУС, особенности реализации системы хранения, обработки и представления данных. Информационные потоки в ИУС. Понятие базы данных (БД). Понятие системы управления базами данных (СУБД). Встраиваемые и клиент-серверные СУБД. Жизненный цикл информационной системы. Концептуальное проектирование ИС и ИУС. Современные средства автоматизированного проектирования ИУС. CASE-технологии. ERD-диаграммы. IDEFx-диаграммы.

Тема 1.2. Реляционные БД. Реляционное исчисление.

Реляционные БД. Требования Кодда. Нормализация схемы БД. Основы реляционной алгебры и ее связь с табличным представлением данных. Модульная структура современных реляционных СУБД на примере СУБД Oracle. Доменный тип данных. Первичные и внешние ключи. Внешние и внутренние языки программирования БД. Индексы и ограничения. Многопользовательский режим работы БД. Понятия пользователя и сеанса. Понятие транзакции, конфликта транзакций.

Тема 1.3. SQl - Язык реляционных БД.

Необходимость стандартизации языков управления данными. Переносимость и независимость кода от реализации SQL. Прочие языки управления данными: T-SQL, PL/SQL. Язык определения схемы данных (SDL). Основные типы информационных объектов БД. Таблицы и табличные представления (view). Правила именования таблиц, и атрибутов таблиц. Владельцы таблиц, условия видимости таблиц, табличные пространства. Выделение памяти под пользовательские объектов и тюнинг таблиц. Операторы создания, изменения и удаления таблиц. Язык манипулирования данными (DML). Основные операторы DML: добавление, изменение, выборка и удаление данных. Необходимость использования опции WHERE при выполнении DML. Предикаты и соответствие операций реляционной алгебры операторам DML.

Модуль 2. Методы разграничения доступа и обеспечения безопасности систем управления базами данных

АРС: Л - 8 ч.; ЛР – 36ч. СРС: ИТМ - 10 ч., ИКЗД - 18 ч., ИЗЛР – 10ч.

Тема 1.4. Безопасность информационных систем и баз данных.

Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Права пользователей и виды пользователей СУБД. Системные права и права доступа к пользовательским объектам. Дискреционное и мандатное разграничение доступа. Операторы назначения и удаления прав.

Тема 1.5. Вопросы использования баз данных в клиент-серверных приложениях.

Работа пользователей с БД с использованием языков программирования высокого уровня. Основы клиент-серверного подхода к реализации ИУС. Использование "драйверов БД" для подключения к СУБД из пользовательского приложения. Примеры использования ODBC, ADO, ADO.NET, LINQ и их отличия.

Тема 1.6. Использование PL/SQL для повышения уровня информационной безопасности.
Язык PL/SQL. Преимущества PL/SQL как процедурного языка. Структура блоков PL/SQL. Триггеры. Неименованные блоки. Процедуры и пакеты. Циклы и курсоры в блоках PL/SQL. Возможности использования PL/SQL для создания триггеров и хранимых процедур, обеспечивающих контроль и разграничение доступа к таблицам.

Раздел II. Программные методы обеспечение информационной безопасности и надежности баз данных

Модуль 3. Методы обеспечения безопасности операционных систем и баз данных. АРС: Л - 16 ч; ПЗ (СЗ) - 12 ч. СРС: ИТМ - 20 ч., ИЗПЗ - 20 ч. ИКЗД 8ч.

Тема 2.1. Транзакционный подход к организации доступа к данным.
Сериализация транзакций. Физическая реализация механизмов обработки транзакций на примере сегментов отката. Методы поиска и индексирования данных. Организация доступа к данным в NoSQL-базах данных.
Тема 2.2. Проблемы информационной безопасности БД: SQL Injection, XSS.
Понятие SQL Injection и XSS в распределенных информационных системах. Виды уязвимостей, используемые атаками SQL Injection. Особенности атак на Web-приложения и на клиент-серверные системы. XSS скриптинг. Методы защиты от SQL Injection, XSS.
Тема 2.3. Уязвимости подсистем баз данных.
Виды угроз компонентам СУБД. Атаки на Listener. Атаки с получением и расшифрованием пароля БД. Атаки с использованием стандартных паорлей и иммен пользователей и перебор паролей по словарю. Атаки на Java-машину Oracle. Атаки на клиент-серверные приложения Oracle.

Модуль 4. Обеспечение надежного хранения данных в БД и аудит

АРС: Л - 16 ч; ПЗ (СЗ) - 24 ч., ЛР – 36ч. СРС: ИТМ - 20 ч., ИЗПЗ - 20 ч, ИЗЛР 10ч, ИКЗД 18ч.

Тема 2.4. Безопасность системы хранения баз данных
Виды угроз доступности данным. Логические и физические ошибки данных. Стурктура систем храненеия. Отказоустойчивые системы хранения: технологии RAID,NAS,SAN. Резервное копирование и восстановление данных. Кластеры, Распределенные СУБД. Кластерная и Grid-архитектура на примере Oracle. Подключаемые БД в Oracle. Взаимодействие с сторонними СУБД. Гетерогенные системы БД.
Тема 2.5. Использование режима ARCHIVELOG и ретроспективных запросов.
Недостатки использования резервного копирования и высокая вероятность критической потери данных. Использование журналирования в базах данных. Сегмент откатов. Режим работы СУБД Oracle ARCHIVELOG. Поиск и восстановление несанкционированно измененных данных при использовании обычных методов резервного копирования. Ретроспективные запросы как эффективный инструмент восстановления данных.
Тема 2.6. Использование аудита БД. Системы обнаружения вторжений.
Контроль разграничения доступа пользователей. Контроль нарушения политик ИБ в БД. Аудит в БД. Аудит системных событий. Аудит таблиц. Системы обнаружения вторжений.

4.3 Перечень тем практических занятий (семинаров)

Таблица 4.2 – Темы, практических занятий (ПЗ)

№ п/п	Номер темы	Наименование темы лекционного и практического занятия	Тр., ч
1	1.1	Введение. Вопросы проектирование ИУС. Построение диаграмм IDEFx (ЛК1 - 2 ач)	2
2	1.2	Решение задачи нормализации для выбранной предметной области (ЛК2 - 2 ач)	2
3	1.3	Реляционные БД. Требования Кодда. Основы реляционной алгебры. Язык SQL: DML и SDL (ЛК3 – 4 ач)	4
4	1.4	Принципы разграничения прав пользователей в БД. Табличные пространства. Виды привилегий пользователей: системные и объектные. Операторы SQL GRANT и REVOKE (ЛК4 – 2 ач)	2
5	1.5	Основы построения клиент-серверных приложений, использующих СУБД. Использование ADO.NET (ActiveX Data Object для .NET), LINQ. Встраиваенмые СУБД на примере SQLite. (ЛК5 – 3 ач)	3
6	1.6	Использование PL/SQL программ для повышения уровня информационной безопасности. Триггеры, пакеты процедур. (ЛК6 – 3 ач)	3
7	2.1	Транзакционный подход к организации доступа к данным. Сериализация транзакций. Сегмент откатов. блокировки (захваты) строк и таблиц. (ЛК7 – 4ач)	4
8	2.1	Назначение и способы реализации системы управления транзакциями. Восстановление информации с помощью сегмента откатов (С1 – 4 ач)	4
9	2.2	Проблемы информационной безопасности БД: SQL Injection, XSS скиптинг (ЛК8 – 6ач)	6
10	2.2	Поиск потенциальных уязвимостей в типовых проектах (ПЗ1 - 4 ач)	4
11	2.3	Анализ защищенности служб Oracle. Атаки на Listener. Атаки с получением и расшифрованием пароля, преодоление парольной защиты. Получение доступа к операционной системе. (ЛК9 – 6ач)	6
12	2.3	Безопасная настройка компонентов СУБД. Ограничение доступа процессов СУБД к операционной системе. Настрока безопасности распределенных многозвенных систем (ПЗ2-4ач)	4
13	2.4	Безопасность систем хранения баз данных. Виды, настройка и особенности резервного копирования. отказоустойчивые системы хранения. Распределенные вычисления и кластеры баз данных (ЛК10 – 4 ач)	4
14	2.4	Распределенные СУБД. Грид-технологии. Кластерные технологии. Отказоустойчивые кластеры. Организация Дата-центров (СЗ2-8 ач)	8
15	2.5	Журналирование информации в СУБД. Режимы журналирования.	6

		Восстановление информации в СУБД, использующих журналирование (ЛК11 – 6 ач)	
16	2.5	Режим ARCHIVELOG Oracle. Настройка режима и настройка файлового хранилища для журнала. Ретроспективные запросы. (ПЗ3 – 8 ач)	8
17	2.6	Аудит БД и системы обнаружения вторжений. Контроль нарушения политик ИБ в БД. Виды и назначение аудита системных событий и аудита доступа к пользовательским данным (ЛК12 – 6 ач)	6
18	2.6	Включение аудита системных событий и аудита доступа к таблицам в Oracle. Просмотр отчетности (ПЗ4 – 8ач)	8
		Итого:	84/ 2.3

4.4 Перечень тем лабораторных работ

Таблица 4.3 Темы лабораторных работ

№ УМ	№ темы	№ ЛР	Наименование темы лабораторной работы	Тр., ч
2	1.4	1	CASE-проектирование ИУС по тематике предметной области. Нормализация таблиц. Создание таблиц с помощью операторов SQL. Назначание прав пользователей с использованием SQL.	12
	1.5	2	Написание простейшего приложения, работающего с базой данных с использованием ADO.NET, на языке C#	12
	1.6	3	Создание хранимых процедур, триггеров и пакетов PL/SQL в СУБД. Функции шифрования в СУБД	12
4	2.4	4	Использование виртуального лабораторного стенда EMC для построения и анализа распределенной отказоустойчивой системы хранения данных	12
	2.5	5	Разработка приложений, работающих в режиме транзакций с базой данных. Вызовы хранимых процедур из программ. Использование LINQ в приложениях .NET	12
	2.6	6	Настройка аудита в СУБД. Разработка программ, контролирующих записи в таблицах аудита.	12
			Итого:	**72/2**

4.5 Виды самостоятельной работы студентов

По каждому практическому занятию и лабораторной работе студентам выдается индивидуальное задание, в рамках которого необходимо решить задачу, сформулированную по рассмотренной тематике. Перечень типовых задач приводится в методических указаниях к проведению практических занятий и лабораторных работ.

По комплексному индивидуальному заданию по модулям дисциплины студент должен оформить и защитить отчеты, в которых приводится описание среды реализации, краткие сведения из теории, основные этапы работы, представление результатов выполнения индивидуального задания и выводы.

Собеседование по тематике самостоятельно изученного теоретического материала определяет уровень проработки перечня вопросов, рассматриваемых в рамках соответствующей темы, выделенной на аудиторное или самостоятельное изучение.

Перечень отчетных документов, подготовленных студентом при выполнении индивидуальных видов СРС:

– рефераты РФ1-РФ4

– отчетов по выполнению индивидуального задания по тематике практических занятий – 4 (ИЗПЗ1 – ИЗПЗ4);

– отчетов по выполнению индивидуального задания по тематике лабораторных работ – 6 (ИЗЛР1 – ИЗЛР6);

– отчет по выполнению комплексного индивидуального задания по модулям дисциплины – ИКЗД1, ИКЗД2;

Форма представления результатов изучения – собеседование.

4.5.1. Темы для самостоятельного изучения теоретического материала

Форма представления результатов – рефераты РФ1-РФ4 (по каждому модулю).
Таблица 4.4 – Темы для самостоятельного изучения теоретического материала

Номер темы (раздела) дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	2	3
1.2	ИТМ: Требования Кодда к реляционным базам данных. Операции реляционной алгебры. Эволюция систем управления базами данных	10
1.5	ИТМ: Модели безопасности для СУБД. Вопросы построения защищенных клиент-серверных и многозвенных приложений. Вопросы защиты интеллектуальных информационных систем, использующих OLAP и Data Mining. Использование среды WebGoat для оценки защищенности информационных систем.	10
2.1,2.2	ИТМ: Организация обработки данных в реляционных СУБД и в NoSQL базах данных. Архитектура системы управления транзакциями. Гранулированные блокировки транзакций.	20
2.4,2.5	ИЗМ: Аудит в СУБД различных производителей. Системы обнаружения вторжений. Руткиты для баз данных. Использование сканеров безопасности в составе BackTrack	20
	Итого: в **ч** / в **ЗЕ**	**60/1,8**

4.5.2. Перечень тем для выполнения индивидуального задания по тематике практических занятий (ИЗПЗ)

Таблица 4.5 – темы для выполнения индивидуальных заданий по тематике практических занятий

Номер темы (раздела) дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	2	3
2.2	ИЗПЗ1: Настройка виртуальной машины Virtual PC. Поиск уязвимостей сканерами безопасности. Установка СУБД Oracle XE на подготовленной виртуальной машине. СУБД	10

	Oracle XE: Создание пользователей и задание привилегий.	
2.3	ИЗП32: Защита процесса Listener. Настройка прав доступа пользователей Windows к файлам и ресурсам СУБД	10
2.5	ИЗП33: Настройка автоматического резервного копирования БД. Перенос данных с помощью утилит экспорта/импорта. Подключение к удаленным БД	10
2.6	ИЗП34: Настройка локальной политики безопасности и аудита БД.	10
	Итого: в **ч** / в **ЗЕ**	**40/1,1**

4.5.3. Перечень тем для выполнения индивидуального задания по тематике лабораторных работ (ИЗЛР)

Таблица 4.6 – темы для выполнения индивидуальных заданий по тематике лабораторных работ

Номер темы (раздела) дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	2	3
1.4	ИЗЛР1: Концептуальное проектирование: разработка схемы данных по выбранной индивидуальной предметной области. Построение матрицы доступа. Реализация схемы и матрицы доступа операторами SQL	2
1.5	ИЗЛР2: Создание безопасного подключения приложения к разработанной схеме данных. Авторизация программы в БД. Установка Kali Linux (BackTrack) и сканирование сервера. Использование Armitage для реализации атак на СУБД и приложения.	4
1.6	ИЗЛР3: Разработка хранимых процедур, максимально реализующих бизнес-логику информационной системы. Замена функционала приложения вызовами хранимых процедур	4
2.4	ИЗЛР4: Использование виртуального лабораторного стенда EMC для построения и анализа распределенной отказоустойчивой системы хранения данных по согласованной с преподавателем модели вычислительной сети	2
2.5	ИЗЛР5: Использование LINQPad для работы с коллекциями для LINQ2Object и LINQ2SQL	4
2.6	ИЗЛР6: Oracle Database Firewall – анализ возможностей системы обнаружения вторжений	4
	Итого: в **ч** / в **ЗЕ**	**20/0.6**

4.5.4 Перечень тем индивидуальных комплексных заданий (ИКЗД)

Таблица 4.7 – Типовые темы для выполнения индивидуальных комплексных заданий по модулям дисциплины

Номер темы (раздела) дисциплины	**Вид самостоятельной работы студентов**	**Трудоёмкость, часов**
1	2	3
1.3	ИКЗД1: Концептуальное проектирование ИУС по индивиду-	10

	альн выбранной тематике. CASE-проектирование, диаграммы IDEFx. Реализация схемы данных в БД Oracle	
1.6	ИКЗД2: Настройка прав пользователей в БД. Разработка хранимых процедур и триггеров безопасности.	10
2.3	ИКЗД3: Создание приложения, использующего БД и исследование его безопасности для атак типа SQL Injection.	10
2.6	ИКЗД4: Настройка локальной политики безопасности и аудита БД.	10
	Итого: в **ч** / в **ЗЕ**	**40/1,1**

5 Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

Проведение лабораторных и практических занятий основывается на интерактивной форме взаимодействия преподавателя и студентов между собой. Преподавателем предлагается проблема (ситуация, условия, ограничения, конкретный пример), и путем обсуждения находится решение. Место преподавателя в интерактивных занятиях сводится к направлению деятельности учащихся на достижение целей занятия. Проведение практических занятий основывается на активном применении обучаемыми студентами руководящих документов ФСТЭК России, рекомендаций по применению современных методов и средств защиты информации.

6 Управление и контроль освоения компетенций

6.1 Текущий контроль освоения заданных дисциплинарных компетенций

Текущий контроль освоения дисциплинарных компетенций проводится в следующих формах:

– текущий опрос, текущая проверочная работа для анализа усвоения материала предыдущей лекции;

– оценка работы студента на лекционных, практических занятиях в рамках рейтинговой системы.

6.2 Рубежный и промежуточный контроль освоения заданных дисциплинарных компетенций

Рубежный контроль освоения дисциплинарных компетенций проводится по окончании модулей дисциплины в следующих формах:

– отчет по индивидуальным комплексным заданиям по модулям (модули 1-4);

– отчеты по лабораторным работам (модули 2, 4).

– отчеты по индивидуальным заданиям к практическим занятиям (модули 3,4).

– вопросы для рубежного контроля (модуль 1, 2, 3,4).

6.3 Итоговый контроль освоения заданных дисциплинарных компетенций

1) **Зачёт (8-й семестр)**

2) **Экзамен (9-й семестр)**

Итоговый контроль уровня освоения заданных дисциплинарных компетенции производится в виде зачета (8сем.) и экзамена(9сем.). Допуск к зачету и экзамену по дисциплине предоставляется по итогам проведения рубежного контроля по выполнению всех индивидуальных заданий по модулю, результатам практических и семинарских занятий.

Зачет и экзамен по дисциплине проводится устно по билетам. Билет содержит два теоретических вопроса по программно-аппаратному обеспечению информационной безопасности, в зависимости от раздела изучения дисциплины.

Фонды оценочных средств, включающий типовые задания, задание на контрольную работу, тесты и методы оценки, критерии оценивания, перечень контрольных точек и таблица планирования результатов обучения, контрольные задания к экзаменам, позволяющие оценить результаты освоения данной дисциплины, входит в состав УМКД на правах отдельного документа.

6.4 Виды текущего, рубежного и итогового контроля освоения элементов и частей компетенций

Таблица 6.4. Структура учебной работы студента по видам, формам представления результатов и формам контроля

Коды компонентов ДК	Компоненты ДК	Формулировки компонентов ДК	АРС		СРС		№ Темы
			Форма выполнения	Форма контроля	Форма представления результатов	Форма контроля	
ПК-15 .С3.Б18	Знает:	модели данных и принципы организации хранения в базах данных; Основы языков программирования БД – SQL; (1з)	ЛК1 ЛК2	Текущий, промежут.	ИТМ1	Собеседд., защита	1.1 1.2
		основные принципы создания безопасных хранимых процедур, триггеров и других объектов с использованием процедурных расширений языка SQL (PL/SQL) (2з)	ЛК6, С32	Текущий, промежут.			2.4 1.6
	Умеет:	реализовывать собственную схему данных средствами языка SQL; реализовывать дискреционную схему разделения доступа к объектам БД (1у);	ПЗ4 ЛР1 ЛР2	Рубежный	ИЗЛР1 ИЗЛР2 ИЗПЗ4	Защита	1.4 1.5 2.6
	Владеет:	методами и технологиями проектирования, моделирования и программирования безопасных систем хранения данных автоматизированных систем. (1в).			ИКЗД1 ИКЗД2	Защита	1.3 1.6
ПК-13 .С3.Б18	Знает:	основные угрозы безопасности информации и модели нарушителя для баз данных; (1з);	ЛК4 ЛК10 С32	Текущий, промежут.	ИТМ5	Собеседд. защита	1.4 2.4

		основные меры по защите информации в автоматизированных системах, в том числе от угроз SQL Injection, XSS, повышение полномочий и атак на программные модули СУБД (2з);	ЛК12, ЛК8	Текущий, промежут.	ИТМ4	Собеседование, защита	2.6 2.2
	Умеет:	создавать защищенные приложения, реализующие информационный обмен средствами баз данных; (1у);	ПЗ2 ЛР2 ПЗ1	Рубежный	ИЗПЗ1 ИЗПЗ2	Защита	1.5 2.3 2.2
		классифицировать угрозы ИБ, включая НСД, НСК и нарушение доступности; настраивать системубезопасности для обнаружения и парирования типовых угроз (2у);	ЛР4 ЛР6 ПЗ4	Рубежный	ИЗЛР4 ИЗЛР6 ИЗПЗ4	Защита Защита	2.4 2.6
	Владеет:	методами обнаружения и предотвращения вторжений в информационные системы, использующие базы данных. (1в).			ИКЗДЗ	Защита	2.3
ПК-20 .С3.Б18	Знает:	методы, способы и содержание этапов разработки безопасной и надежной подсистемы хранения данных автоматизированной системы, включающей защиту от НСД и ведение аудита доступа пользователей; (1з);	ЛК7 ЛК9 СЗ1	Текущий, промежут.	ИТМ3	Собеседование, защита	2.1 2.3
		методы обеспечения доступности данных, включающие журналирование, резервное копирование, кластеризацию и защиту информации от потерь с использованием отказоустойчивых хранилищ; (2з);	ЛК11, ЛК10 СЗ2	Текущий, промежут.	ИТМ6 ИТМ5	Собеседование, защита	2.5 2.6
	Умеет:	проводить аргументированный выбор, рассчитывать характеристики и реализовывать систем резервного копирования; (1у);	ПЗ2 ПЗ3 ЛР4	Рубежный	ИЗПЗ2 ИЗЛР3 ИЗЛР4	Защита	2.4 2.5

		использовать встроенные средства аудита пользовательских действий для грамотного протоколирования попыток несанкционированного изменения данных и схемы данных; (2у)	ЛР5 ЛР6 ПЗ4	Рубежный	ИЗЛР5 ИЗЛР6 ИЗПЗ4	Защита	2.5 2.6
	Владеет:	программным обеспечением, реализующим резервное копирование баз данных, экспорт и импорт данных, а также функции аудита баз данных информационных систем (1в).			ИКЗД4	Защита	2.6

7 График учебного процесса по дисциплине

Таблица 7.1 – График учебного процесса по дисциплине (М1-2)

Виды работ	**Распределение часов по учебным неделям**																		Итого, ч
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Раздел:	**Р1**																		
Лекции	2		2		2		2			2		2		2		2			**16**
Практические, семинарские занятия (ПЗ, СЗ)																			
Самост. изучение теоретического материала		2	2		2	2	2	2			2	2	2		2	2	2		**20**
Лабораторные работы (ЛР)										4	4	4	4	4	4	4	4	4	**36**
Вып. индив. задания по модулям (ИКЗД)							3	3				6			6			6	**24**
КСР																	2		**2**
Модуль:	**1**						**2**						**3**						
Контр. тестирование						+					+							+	
Дисциплин. контроль																			**зачет.**

Продолжение таблицы 7.1 – График учебного процесса по дисциплине (М3-4)

Виды работ	**Распределение часов по учебным неделям**																		Итого, ч
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	
Раздел:	**Р2**																		
Лекции	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	**32**
Практические, семинарские занятия (ПЗ, СЗ)		2	2		2	2		2	2		4	4		4	4		4	4	**36**
Самост. изучение теоретического материала		4	4		4	4		4			4	4		4	4		4		**40**
Лабораторные										4	4	4	4	4	4	4	4	4	**36**

работы (ЛР)																			
Вып. индив. задания по модулям(ИКЗД)							4	4							5	5			**18**
КСР									2								2		**4**
Модуль:	**1**						**2**						**3**						
Контр. тес-тирование						+					+							+	
Дисциплин. контроль																			**Экз.**

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Карта обеспеченности дисциплины учебно-методической литературой

Безопасность систем баз данных	*Профессиональный цикл*	
полное название дисциплины	[x] основная [ ] по выбору студента	[x] базовая часть цикла [ ] вариативная часть цикла

09030307.65	**«Информационная безопасность автоматизированных систем»,** специализация «Обеспечение информационной безопасности распределенных информационных систем»
код направления / специальности	*полное название направления/ специальности*

КОБ/КОБ	Уровень подготовки	Форма обучения
	[x] специалист [ ] бакалавр [ ] магистр	[x] очная [ ] заочная [ ] очно-заочная

2015 семестр (ы) 8,9 количество групп **1**
количество студентов **20**

Кокоулин Андрей Николаевич, доцент,
электротехнический факультет,
кафедра АТ, телефон: 239-18-16.

СПИСОК ИЗДАНИЙ

№	Библиографическое описание	Количество экземпляров в библиотеке
1	2	3
	1. Основная литература	
1	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин.— М.: ФОРУМ: ИНФРА-М, 2008,2009.— 415 с.	12
2	Голенищев Э.П. Информационное обеспечение систем управления: учеб. пособие для вузов – Ростов-на-Дону : Феникс, 2010. – 315 с. : ил..	5
3	Громов Ю.Ю. Информационная безопасность и защита информации : учебное пособие для вузов / Ю. Ю. Громов [и др.] .— Старый Оскол : ТНТ, 2010 .— 383 с. : ил	5
4	Клейменов С.А. Администрирование в информационных системах : учебное пособие для вузов / С.А. Клейменов, В.П. Мельников, А.М. Петраков ; Под ред. В.П. Мельникова.— М. : Академия, 2008. — 271 с.	5
	2. Дополнительная литература	
	2.1. Учебные и научные издания	
1	Бабаш А.В. Информационная безопасность. Лабораторный практикум : учебное пособие для вузов / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников .— Москва : КНОРУС, 2012 .— 131 с., 8,5 усл. печ. л. : ил. + CD-ROM .	2
2	Т.Кайт. Oracle для профессионалов : пер. с англ. / Том Кайт. Кн. 1: Архитектура и основные особенности .— 2-е изд. — 2004 .— 662 с	3
3	Т.Кайт. Oracle для профессионалов / Том Кайт Кн.2: Расширение возможностей и защита .— 2-е изд. — 2004 .— 831 с	3

Основные данные об обеспеченности на _____

(дата составления рабочей программы)

Основная литература [x] обеспечена [ ] не обеспечена

Дополнительная литература [x] обеспечена [ ] не обеспечена

Зав. отделом комплектования научной библиотеки _____ Н. В. Тюрикова

Текущие данные об обеспеченности на _____

(дата контроля литературы)

Основная литература [ ] обеспечена [ ] не обеспечена

Дополнительная литература [ ] обеспечена [ ] не обеспечена

Зав. отделом комплектования научной библиотеки _____ Н.В. Тюрикова

Карта книго-обеспеченности в библиотеку сдана

8.2 Компьютерные обучающие и контролирующие программы

Таблица 8.1 – Используемые компьютерные обучающие программы

№ п/п	Вид учебного занятия	Наименование программного продукта	Рег. номер	Назначение
1	2	3	4	5
1	ПЗ, СЗ	Базы данных правовой информации, информационно-справочные и поисковые системы – Деловая пресса - www. businesspress.ru; – Гарант - www. garant.ru; – Информационно-справочная система «Консультант Плюс».	б/н	Получение правовой информации

8.3 Программные инструментальные средства

Не предусмотрены

8.4 Аудио- и видео-пособия

Не предусмотрены

9 Материально-техническое обеспечение дисциплины

9.1 Специализированные лаборатории и классы

Таблица 9.1 – Специализированные лаборатории и классы

№ п.п.	Помещения			Площадь, $м^2$	Количество посадочных мест
	Название	Принадлежность (кафедра)	Номер аудитории		
1	Дисплейный класс	Кафедра АТ	321 корп. А	34	18

9.2 Основное учебное оборудование

Таблица 9.2 – Учебное оборудование

№ п.п.	Наименование и марка оборудования (стенда, макета, плаката)	Кол-во, ед.	Форма приобретения / владения (собственность, оперативное управление, аренда и т.п.)	Номер аудитории
1	ПК Intel Pentium Dual CPU 2000 МГц	12	Оперативное управление	321 корп. А

Лист регистрации изменений

№ п.п.	Содержание изменения	Дата, номер протокола заседания кафедры
1.		
2.		
3.		
4.		
5.		

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**
Электротехнический факультет
Кафедра «Автоматика и телемеханика»

УТВЕРЖДАЮ
Заведующий кафедрой
«Автоматика и телемеханика»
д-р техн. наук, проф.
_____ А.А. Южаков
Протокол заседания кафедры АТ
от «16» января 2017 г. № 18

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
«Безопасность систем баз данных»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Специальность:	10.05.03 Информационная безопасность автоматизированных систем
Специализация:	Обеспечение информационной безопасности распределенных информационных систем
Квалификация выпускника:	специалист
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	очная

Курсы: 4,5 Семестры: 8,9

Трудоемкость:

Кредитов по рабочему учебному плану (БУП): **10**
Часов по рабочему учебному плану (БУП): **360**

Виды контроля:

Экзамен: **- 9** Зачет: **- 8** Курсовой проект: **- нет** Курсовая работа: **- нет**

Пермь 2017 г.

Рабочая программа дисциплины «Безопасность систем баз данных» разработана на основании:

- Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от «01» декабря 2016 г. № 1509;
- Компетентностной модели выпускника образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденной «24» июня 2013 г. (с изменениями, в связи с переходом на ФГОС ВО);
- Базового учебного плана очной формы обучения образовательной программы высшего образования – программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации «Обеспечение информационной безопасности распределенных информационных систем», утвержденного «22» декабря 2016 г.

Рабочая программа согласована с рабочими программами дисциплин, участвующих в формировании компетенций и их составляющих, приобретение которых является целью данной дисциплины:

Основы построения инфокоммуникационных систем и сетей, Научно-исследовательская работа студента, Метрология, стандартизация и сертификация базового учебного плана образовательной программы высшего образования - программы по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализации Обеспечение информационной безопасности распределенных информационных систем.

Лист регистрации изменений

№ п.п	Содержание изменения	Дата, номер протокола заседания кафедры. Подпись заведующего кафедрой
1.	Содержание стр. 1, кроме абзацев 6-9, изложить в редакции, приведенной на стр. 1а.	Протокол заседания кафедры АТ от «16 » января 2017 г. № 18 Зав. кафедрой АТ д-р техн. наук, проф. _____ А.А. Южаков
	Содержание стр. 2 (абзацы 1-5) изложить в редакции, приведенной на стр. 2а.	
	Изменения шифров и формулировок компетенций (стр. 3- 5, 7-9,) внесены на основании перехода на ФГОС ВО: **по специальности 10.05.03, утвержденный приказом Министерства образования и науки РФ от 01.12.2016 г. № 1509, и обновления базового учебного плана подготовки по специальности 10.05.03, утвержденного 22.16.2016 г.:** - профессиональную компетенцию ПК-13 считать профессиональную компетенцией ПК-5 с формулировкой: «Способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-13.С3.Б18 на ПК-5.Б1.Б.36; - профессиональную компетенцию ПК-15 считать профессиональной компетенцией ПК-4 с формулировкой «Способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-15.С3.Б18 на ПК-9.Б1.Б.36; - профессиональную компетенцию ПК-20 считать профессиональной компетенцией ПСК-7.4 с формулировкой «Способность разрабатывать политики информационной безопасности автоматизированных систем»; - изменить шифр дисциплинарной компетенции с ПК-20.С3.Б18 на ПСК-7.4.Б1.Б.36;	
	Наименование раздела 1.4 «Место учебной дисциплины в структуре профессиональной подготовки выпускников» изложить в следующей редакции: «Место учебной дисциплины в структуре образовательной программы».	
	В первом абзаце раздела 1.4 заменить слова «цикла профессиональных дисциплин» на «блока 1. Дисциплины (модули)». Шифр названия направления и специальности читать в новой редакции.	
	Наименование раздела 2 «Требования к результатам освоения учебной дисциплины» изложить в следующей редакции: «Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы».	

	Раздел 3 «Структура учебной дисциплины по видам и формам учебной работы» дополнить новым абзацем следующего содержания: «Объем дисциплины в зачетных единицах составляет 10 ЗЕ. Количество часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся указано в таблице 3.1.».	
	В табл. 3.1.: а) строку п. 1 дополнить словами «(контактная работа)»; б) строку п. 3 изложить в следующей редакции: «Итоговый контроль (промежуточная аттестация обучающихся) по дисциплине:».	
	В табл. 4.1.: а) в строке п. 1 «Количество часов (очная форма обучения)» дополнить словами «и виды занятий»; б) «Итоговая аттестация» заменить на «Итоговый контроль (промежуточная аттестация).	
	В раздел 4.5 «Распределение тем по видам самостоятельной работы» добавить параграф с наименованием «Методические указания для обучающихся по изучению дисциплины» следующего содержания: «При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации: 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу. 4. Изучение дисциплины осуществляется в течение одного семестра, график изучения дисциплины приводится п. 7. 5. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.»	
	Наименование раздела 6 изложить в следующей редакции: «Фонд оценочных средств дисциплины».	
	Наименование параграфа 6.1 изложить в редакции «Текущий и рубежный контроль освоения заданных дисциплинарных частей компетенций».	
	В параграф 6.1 добавить первый абзац следующего содержания: «Текущий контроль осуществляется путем устного опроса во время аудиторных занятий».	
	Наименование раздела 8 Учебно-методическое и информационное обеспечение дисциплины» изложить в следующей редакции: «Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине».	
	Изменить название раздела «Список изданий» на «8.2. Пере-	

	чень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».	
	Добавить в таблицу 8.1 строку «2.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины».	
	Дополнить п. 2.5 таблицы строками: **Электронная библиотека** Научной библиотеки Пермского национального исследовательского политехнического университета [Электронный ресурс: полнотекстовая база данных электрон. документов, изданных в Изд-ве ПНИПУ]. – Электрон. дан. (1 912 записей). – Пермь, 2014. – Режим доступа: http://elib.pstu.ru/. – Загл. с экрана. **Лань** [Электронный ресурс: электрон. -библ. система: полнотекстовая база данных электрон. документов по гуманит., естеств., и техн. наукам] / Изд-во «Лань». – Санкт-Петербург: Лань, 2010- . – Режим доступа: http://e.lanbook.com/. – Загл. с экрана. **Консультант Плюс** [Электронный ресурс : справочная правовая система : документы и комментарии : универсал. информ. ресурс]. – Версия Проф, сетевая. – Москва, 1992. – Режим доступа: Компьютер. сеть Науч. б-ки Перм. нац. исслед. политехн. ун-та, свободный.».	
	Раздел 8.2 «Компьютерные обучающие и контролирующие программы» считать разделом 8.3 и наименование изложить в следующей редакции: «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине».	
	Раздел 8.3 «Программные инструментальные средства» считать разделом 8.4 «Перечень программного обеспечения, в том числе компьютерные обучающие и контролирующие программы».	
	Раздел 8.4 «Аудио- и видео-пособия» считать разделом 8.5.	
	Наименование раздела 9 изложить в следующей редакции: «Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине».	
2.		
3.		