

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра вычислительной техники
Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ

к.т.н. Рева И. Л.

“ ____ ” _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Построение защищенных компьютерных сетей

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская
программа: Кибербезопасность информационных систем

Курс: 1 2, семестры : 2 3

Факультет автоматики и вычислительной техники,

		Семестр	
№	Вид деятельности	2	3
1	Всего зачетных единиц (кредитов)	2	3
2	Всего часов	72	108
3	Всего занятий в контактной форме, час.	42	27
4	Лекции, час.	18	0
5	Практические занятия, час.	18	18
6	Лабораторные занятия, час.	0	0
7	из них в активной и интерактивной форме, час.	8	0
8	Аттестация, час.	2	2
9	Консультации, час.	4	7
10	Самостоятельная работа, час.	30	81
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ	КП
12	Вид аттестации	3	Э

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 09.04.01 Информатика и вычислительная техника

ФГОС введен в действие приказом №1420 от 30.10.2014 г. , дата утверждения: 25.11.2014 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 09.04.01 Информатика и вычислительная техника

Рабочая программа обсуждена на заседании кафедры

ВТ, протокол заседания кафедры №6 от 20.06.2017

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматизации и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.ф.-м.н. Котов Ю. А.

Заведующий кафедрой:

доцент, к.т.н. Якименко А. А.

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

доцент Якименко А. А.

1. Внешние требования

Таблица 1.1

Компетенция ФГОС: ОК.7 способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности; в части следующих результатов обучения:
у1. осваивать новые программные средства для профессиональной деятельности
Компетенция ФГОС: ОПК.3 способность анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности; в части следующих результатов обучения:
з1. знать современный отечественный и зарубежный опыт в профессиональной деятельности
Компетенция ФГОС: ПК.19 способность к применению современных технологий разработки программных комплексов с использованием CASE-средств, контролировать качество разрабатываемых программных продуктов; в части следующих результатов обучения:
з1. знать принципы построения архитектуры программного обеспечения и виды архитектур программного обеспечения
Компетенция НГТУ: ПК.20.В способность управлять средой функционирования объектов профессиональной деятельности; в части следующих результатов обучения:
з1. методы и средства обеспечения информационной безопасности компьютерных систем
у1. использовать специализированные программные средства при решении профессиональных задач

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
<i>Построение защищенных компьютерных сетей</i>	
ОПК.3.з1 знать современный отечественный и зарубежный опыт в профессиональной деятельности	
1.з1. знать современный отечественный и зарубежный опыт в профессиональной деятельности	Лекции; Практические занятия; Самостоятельная работа
ОК.7.у1 осваивать новые программные средства для профессиональной деятельности	
2.осваивать новые программные средства для профессиональной деятельности	Лекции; Практические занятия; Самостоятельная работа
ПК.19.з1 знать принципы построения архитектуры программного обеспечения и виды архитектур программного обеспечения	
3.з1. знать принципы построения архитектуры программного обеспечения и виды архитектур программного обеспечения	Лекции; Практические занятия; Самостоятельная работа
ПК.20.В.з1 методы и средства обеспечения информационной безопасности компьютерных систем	
4.методы и средства обеспечения информационной безопасности компьютерных систем	Лекции; Практические занятия; Самостоятельная работа
ПК.20.В.у1 использовать специализированные программные средства при решении профессиональных задач	
5.использовать специализированные программные средства при решении профессиональных задач	Лекции; Практические занятия; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 2			
Дидактическая единица: Защита систем			

1. Классификация компьютерных сетей.	0	2	1, 2, 3, 4, 5
2. Функциональная иерархическая модель информационных сетей.	0	2	1, 2, 3, 4, 5
3. Общая характеристика распределенной операционной системы.	0	2	1, 2, 3, 4, 5
4. Функции и основные характеристики корпоративных сетей.	0	2	1, 2, 3, 4, 5
5. Типовая структура корпоративной компьютерной сети.	0	2	1, 2, 3, 4, 5
6. Фазы процесса связи удаленных объектов	0	2	1, 2, 3, 4, 5
7. Классификация сетевых угроз и атак.	0	2	1, 2, 3, 4, 5
8. Рекомендации по построению систем защиты.	0	2	1, 2, 3, 4, 5
9. Межсетевые экраны (МЭ) с фильтрацией пакетов.	0	2	1, 2, 3, 4, 5

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 2				
Дидактическая единица: Защита систем				
1. Межсетевые экраны уровня приложений	0	2	1, 2, 3, 4, 5	практика
2. Шлюзы уровня соединений.	1	2	1, 2, 3, 4, 5	практика
3. МЭ с адаптивной проверкой пакетов	1	2	1, 2, 3, 4, 5	практика
4. Способы НСД к информации	1	2	1, 2, 3, 4, 5	практика
5. Методы и средства защиты от НСД в сети	1	2	1, 2, 3, 4, 5	практика
6. Аутентификация пользователей	1	2	1, 2, 3, 4, 5	практика
7. Основные особенности сетевой аутентификации	1	2	1, 2, 3, 4, 5	практика
8. Простой метод запрос-ответ	1	2	1, 2, 3, 4, 5	практика
9. Аутентификация в протоколе SMB	1	2	1, 2, 3, 4, 5	практика
Семестр: 3				
Дидактическая единица: Средства информационной защиты				
10. Разграничение доступа пользователей к ресурсам АС	0	2	1, 2, 3, 4, 5	практика
11. Криптографические сетевые протоколы	0	2	1, 2, 3, 4, 5	практика
12. Протокол IPSec	0	2	1, 2, 3, 4, 5	практика
13. Протокол TLS.	0	2	1, 2, 3, 4, 5	практика

14. Стандарт SET	0	2	1, 2, 3, 4, 5	практика
15. Управление ключами	0	2	1, 2, 3, 4, 5	практика
16. KDC.	0	2	1, 2, 3, 4, 5	практика
17. . Система распределенной аутентификации Kerberos	0	2	1, 2, 3, 4, 5	практика
18. Стандарты безопасности вычислительных сетей и их компонентов	0	2	1, 2, 3, 4, 5	практика

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 2				
1	РГЗ	1, 2, 3, 4, 5	30	4
: Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007				
Семестр: 3				
1	Курсовой проект	1, 2, 3, 4, 5	81	7
: Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	Личный типовой сайт; Портал НГТУ; Среда электронного обучения НГТУ
Консультирование	Портал НГТУ; Среда электронного обучения НГТУ
Контроль	Портал НГТУ; Среда электронного обучения НГТУ
Размещение учебных материалов	Портал НГТУ; Среда электронного обучения НГТУ; ЭБС

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Максимальный балл
Семестр: 2	

<i>Практические занятия:</i>	40
<i>РГЗ:</i>	40
<i>Зачет:</i>	20
Семестр: 3	
<i>Практические занятия:</i>	30
<i>Курсовой проект:</i>	30
<i>Экзамен:</i>	40

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля			
		Защита РГЗ	Защита КП/КР	Зачет	Экзамен
ОК.7	у1. осваивать новые программные средства для профессиональной деятельности	+	+	+	+
ОПК.3	з1. знать современный отечественный и зарубежный опыт в профессиональной деятельности	+	+	+	
ПК.19	з1. знать принципы построения архитектуры программного обеспечения и виды архитектур программного обеспечения	+	+	+	
	ПК.20.В з1. методы и средства обеспечения информационной безопасности компьютерных систем	+	+	+	
	ПК.20.В у1. использовать специализированные программные средства при решении профессиональных задач	+	+	+	

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Проскурин В. Г. Защита программ и данных : [учебное пособие для вузов по специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем"] / В. Г. Проскурин. - М., 2011. - 198, [1] с.
2. Абденов А. Ж. Методика оценки риска для информационных систем на основе экспертных оценок : учебное пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель ; Новосиб. гос. техн. ун-т. - Новосибирск, 2014. - 69, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000213163

Дополнительная литература

1. ГОСТ Р 53113.2-2009. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 2 / Федер. агентство по техн. регулированию и метрологии. - М., 2010. - IV, 7 [1] с. : ил.
2. Тарасюк М. В. Защищенные информационные технологии. Проектирование и применение / М. В. Тарасюк. - Москва, 2004. - 191 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : <http://elibrary.nstu.ru/>
2. ЭБС «Издательство Лань» : <https://e.lanbook.com/>
3. ЭБС IPRbooks : <http://www.iprbookshop.ru/>

4. ЭБС "Znanium.com" : <http://znanium.com/>

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007

8.2 Специализированное программное обеспечение

1 Microsoft Windows

2 Microsoft Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Используется при проведении лекций

1. Обобщенная структура фонда оценочных средств учебной дисциплины

Обобщенная структура фонда оценочных средств по дисциплине **Построение защищенных компьютерных сетей** приведена в Таблице.

Таблица

Формируемые компетенции	Показатели сформированности компетенций (знания, умения, навыки)	Темы	Этапы оценки компетенций	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	Промежуточная аттестация (экзамен, зачет)
ОК.7 способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности	у1. осваивать новые программные средства для профессиональной деятельности	. Система распределенной аутентификации Kerberos KDC. Аутентификация в протоколе SMB Аутентификация пользователей Классификация компьютерных сетей. Классификация сетевых угроз и атак. Криптографические сетевые протоколы Межсетевые экраны (МЭ) с фильтрацией пакетов. Межсетевые экраны уровня приложений Методы и средства защиты от НСД в сети МЭ с адаптивной проверкой пакетов Общая характеристика распределенной операционной системы. Основные особенности сетевой аутентификации Простой метод запрос-ответ Протокол IPSec Протокол TLS. Разграничение доступа пользователей к ресурсам АС Рекомендации по построению систем защиты. Способы НСД к информации Стандарт SET Стандарты безопасности вычислительных сетей и их компонентов Типовая структура корпоративной компьютерной сети. Управление ключами Фазы процесса связи удаленных объектов Функции и основные характеристики корпоративных сетей. Функциональная иерархическая модель информационных сетей. Шлюзы уровня соединений.	Курсовой проект РГЗ, разделы 1	Зачет Экзамен, вопросы 1-9
ОПК.3 способность анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и	з1. знать современный отечественный и зарубежный опыт в профессиональной деятельности	Аутентификация в протоколе SMB Аутентификация пользователей Классификация компьютерных сетей. Классификация сетевых угроз и атак. Межсетевые экраны (МЭ) с фильтрацией пакетов. Межсетевые экраны уровня приложений Методы и средства защиты от НСД в	Курсовой проект РГЗ, разделы 1-2	Зачет, вопросы 10-15

профессиональной мобильности		сети МЭ с адаптивной проверкой пакетов Общая характеристика распределенной операционной системы. Основные особенности сетевой аутентификации Простой метод запрос-ответ Рекомендации по построению систем защиты. Способы НСД к информации Типовая структура корпоративной компьютерной сети. Фазы процесса связи удаленных объектов Функции и основные характеристики корпоративных сетей. Функциональная иерархическая модель информационных сетей. Шлюзы уровня соединений.		
ПК.19/ПТ способность к применению современных технологий разработки программных комплексов с использованием CASE-средств, контролировать качество разрабатываемых программных продуктов	з1. знать принципы построения архитектуры программного обеспечения и виды архитектур программного обеспечения	Аутентификация в протоколе SMB Аутентификация пользователей Классификация компьютерных сетей. Классификация сетевых угроз и атак. Межсетевые экраны (МЭ) с фильтрацией пакетов. Межсетевые экраны уровня приложений Методы и средства защиты от НСД в сети МЭ с адаптивной проверкой пакетов Общая характеристика распределенной операционной системы. Основные особенности сетевой аутентификации Простой метод запрос-ответ Рекомендации по построению систем защиты. Способы НСД к информации Типовая структура корпоративной компьютерной сети. Фазы процесса связи удаленных объектов Функции и основные характеристики корпоративных сетей. Функциональная иерархическая модель информационных сетей. Шлюзы уровня соединений.	Курсовой проект РГЗ, разделы 1-3	Зачет, вопросы 16-23
ПК.20.В способность управлять средой функционирования объектов профессиональной деятельности	з1. методы и средства обеспечения информационной безопасности компьютерных систем	Аутентификация в протоколе SMB Аутентификация пользователей Классификация компьютерных сетей. Классификация сетевых угроз и атак. Межсетевые экраны (МЭ) с фильтрацией пакетов. Межсетевые экраны уровня приложений Методы и средства защиты от НСД в сети МЭ с адаптивной проверкой пакетов Общая характеристика распределенной операционной системы. Основные особенности сетевой	Курсовой проект РГЗ, разделы 4	Зачет, вопросы 24-31

		аутентификации Простой метод запрос-ответ Рекомендации по построению систем защиты. Способы НСД к информации Типовая структура корпоративной компьютерной сети. Фазы процесса связи удаленных объектов Функции и основные характеристики корпоративных сетей. Функциональная иерархическая модель информационных сетей. Шлюзы уровня соединений.		
ПК.20.В	у1. использовать специализированные программные средства при решении профессиональных задач	Аутентификация в протоколе SMB Аутентификация пользователей Классификация компьютерных сетей. Классификация сетевых угроз и атак. Межсетевые экраны (МЭ) с фильтрацией пакетов. Межсетевые экраны уровня приложений Методы и средства защиты от НСД в сети МЭ с адаптивной проверкой пакетов Общая характеристика распределенной операционной системы. Основные особенности сетевой аутентификации Простой метод запрос-ответ Рекомендации по построению систем защиты. Способы НСД к информации Типовая структура корпоративной компьютерной сети. Фазы процесса связи удаленных объектов Функции и основные характеристики корпоративных сетей. Функциональная иерархическая модель информационных сетей. Шлюзы уровня соединений.	Курсовой проект РГЗ, разделы 1-4	Зачет, вопросы 32-45

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 2 семестре - в форме зачета, в 3 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОК.7, ОПК.3, ПК.19/ПТ, ПК.20.В.

Зачет проводится в устной форме, по билетам (тестам).

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 3 семестре обязательным этапом текущей аттестации является курсовой проект. Требования к выполнению курсового проекта, состав и правила оценки сформулированы в паспорте курсового проекта.

В 2 семестре обязательным этапом текущей аттестации является расчетно-графическое задание

(работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОК.7, ОПК.3, ПК.19/ПТ, ПК.20.В, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Паспорт зачета

по дисциплине «Проектирование защищенных компьютерных сетей», 2 семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-20, второй вопрос из диапазона вопросов 21-40 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____

к зачету по дисциплине «Проектирование защищенных компьютерных сетей»

1. Авторизация доступа к отношениям и их полям.
2. Распределенные базы данных в сетях ЭВМ.

Утверждаю: зав. кафедрой _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на зачетный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *5 баллов*.
- Ответ на зачетный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает не принципиальные ошибки, например, вычислительные, оценка составляет *10 баллов*.
- Ответ на зачетный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить

качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *_15_ баллов*.

- Ответ на зачетный билет билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет *_20_ баллов*.

3. Шкала оценки

В общей оценке по дисциплине зачетные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Вопросы к зачету по дисциплине «Проектирование защищенных компьютерных сетей»

1. Реляционная, иерархическая и сетевая модели.
2. Распределенные базы данных в сетях ЭВМ.
3. Файловые системы.
4. Структуры файлов.
5. Именованное файлов.
6. Защита файлов.
7. Режим многопользовательского доступа.
8. Области применения файлов
9. Общая характеристика, назначение и возможности систем управления базами данных.
10. Основные функции СУБД.
11. Непосредственное управление данными во внешней памяти.
12. Управление буферами оперативной памяти.
13. Управление транзакциями.
14. Журнализация.
15. Поддержка языков БД.
16. Типовая организация современной СУБД.
17. Языковые средства СУБД для различных моделей данных.
18. Языковые средства манипулирования данными в реляционных СУБД.
19. Языковые средства описания данных реляционных СУБД; SEQUEL/SQL СУБД System R.
20. Запросы и операторы манипулирования данными.
21. Операторы определения и манипулирования схемой БД.
22. Определения ограничений целостности и триггеров.
23. Представления базы данных.
24. Особенности языковых средств управления и обеспечения безопасности данных в реляционных СУБД.
25. Определение управляющих структур.
26. Авторизация доступа к отношениям и их полям.
27. Точки сохранения и откаты транзакции.
28. Встроенный SQL .
29. Динамический SQL.
30. Язык SQL в коммерческих реализациях.
31. Стандартизация SQL.
32. Оптимизация производительности и характеристик доступа к базам данных.
33. Средства идентификации и аутентификации объектов баз данных.

34. Языковые средства разграничения доступа.
35. концепция и реализация механизма ролей.
36. организация аудита событий в системах баз данных.
37. Средства контроля целостности информации,
38. Организация взаимодействия СУБД и базовой ОС.
39. Журнализация, средства создания резервных копии и восстановления баз данных.
40. Технологии удаленного доступа к системам баз данных, тиражирование и синхронизация в распределенных системах баз данных.

Паспорт расчетно-графического задания (работы)

по дисциплине «Проектирование защищенных компьютерных сетей», 2 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны рассчитать параметры элементов защиты информационной системы.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ объекта, выбрать и обосновать способы НСД, разработать процедуру НСД, выбрать программные средства.

Обязательные структурные части РГЗ: постановка задачи, описание уязвимости, процедуры НСД..

Оцениваемые позиции: полнота анализа уязвимости и оригинальность НСД.:

2. Критерии оценки

- Работа считается **не выполненной**, если выполнены не все части РГЗ(Р), отсутствует анализ объекта, не обоснованы способы НСД, программные средства не выбраны или не соответствуют современным требованиям, оценка составляет __10__ баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, программные средства не соответствуют современным требованиям, оценка составляет __20__ баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования уязвимости обоснованы, процедуры НСД разработаны, но не оптимизированы, программные средства выбраны без достаточного обоснования, оценка составляет __30__ баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры уязвимости обоснованы, процедуры НСД разработаны и реализованы, выбор программных средств обоснован, оценка составляет __40__ баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

Обход пароля учетной записи Windows с помощью программы Kon Boot
Вскрытие пароля учетной записи Windows с помощью программы Ophcrack
Повышение прав пользователя Windows с использованием системного реестра
Блокирование сайтов и обход системы блокировки в ОС Windows
Блокирование USB портов и обход блокировки в ОС Windows
Сброс пароля администратора ОС Windows и создание нового администратора без использования дополнительных программ

Включение изначально скрытой учётной записи «Администратор» в ОС Windows
Вскрытие пароля локального администратора компьютера под управлением ОС Windows7
Изменение прав пользователя в ОС Windows
Сброс пароля администратора в ОС Windows и создание нового администратора
Получение логина и пароля удаленного компьютера
Перехват логина и пароля по протоколу Telnet в локальной сети
Организация скрытого входа в ОС Windows (подмена процессов)
Получение несанкционированного доступа в ОС Windows

Паспорт экзамена

по дисциплине «Проектирование защищенных компьютерных сетей», 3 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-20, второй вопрос из диапазона вопросов 21-45 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____

к экзамену по дисциплине «Проектирование защищенных компьютерных сетей»

1. Классификация сетевых угроз и атак.
2. Управление ключами.

Утверждаю: зав. кафедрой _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет 10 баллов.
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет 20 баллов.
- Ответ на экзаменационный билет билета засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику

процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет 30 баллов.

- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет 40 баллов.

3. Шкала оценки

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Вопросы к экзамену по дисциплине «Проектирование защищенных компьютерных сетей»

1. Классификация компьютерных сетей.
2. Функциональная иерархическая модель информационных сетей.
3. Общая характеристика распределенной операционной системы.
4. Функции и основные характеристики корпоративных сетей.
5. Типовая структура корпоративной компьютерной сети.
6. Фазы процесса связи удаленных объектов.
7. Классификация сетевых угроз и атак.
8. Рекомендации по построению систем защиты.
9. Межсетевые экраны (МЭ) с фильтрацией пакетов.
10. Межсетевые экраны уровня приложений.
11. Шлюзы уровня соединений.
12. МЭ с адаптивной проверкой пакетов (или МЭ с запоминанием состояния пакетов).
13. Способы НСД к информации.
14. Методы и средства защиты от НСД в сети.
15. Аутентификация пользователей.
16. Основные особенности сетевой аутентификации.
17. Простой метод запрос-ответ.
18. Аутентификация в протоколе SMB (Server Message Block – блок сообщений сервера).
19. Разграничение доступа пользователей к ресурсам АС.
20. Криптографические сетевые протоколы.
21. Протокол IPSec.
22. Протокол TLS.
23. Стандарт SET.
24. Управление ключами.
25. KDC.
26. Система распределенной аутентификации Kerberos.
27. Стандарты безопасности вычислительных сетей и их компонентов.
28. Классификация СВТ по уровню защищенности от НСД.
29. Классификация автоматизированных систем по уровню защищенности от НСД.
30. Межсетевые экраны. Показатели защищенности от НСД к информации.
31. Базовые протоколы семейства TCP/IP.
32. Прикладной уровень TCP/IP.
33. Транспортный уровень TCP/IP.
34. Межсетевой уровень TCP/IP.

35. Уровень доступа к сети.
36. Прикладные протоколы и службы (WWW, электронная почта, передача файлов).
37. Виртуальные частные сети.
38. Построение VPN на базе сетевой операционной системы.
39. Построение VPN на базе маршрутизаторов.
40. Построение VPN на базе межсетевых экранов.
41. Вопросы безопасности базовых протоколов TCP/IP.
42. Перехват данных, имперсонация, отказ в обслуживании.
43. Несанкционированное подключение к сети.
44. Несанкционированный обмен данными.
45. Безопасность WWW, электронной почты, Java.

Паспорт курсового проекта

по дисциплине «Проектирование защищенных компьютерных сетей», 3 семестр

1. Методика оценки.

Задание: Элементы защиты в БД MS Access или другой БД.

Структура: 1. Цель работы. 2. Постановка задачи (заданный вариант БД).

3. Результаты выполнения. 4. Заключение. 5. Список литературы.

Этапы выполнения и защиты: в соответствии со структурой

Оцениваемые позиции: работа в целом.

Критерии оценки.

- работа считается **не выполненной**, если оценка составляет менее 50 баллов.
- работа считается выполненной **на пороговом** уровне, если оценка составляет 50-72 баллов.
- работа считается выполненной **на базовом** уровне, если оценка составляет 73-88 баллов.
- работа считается выполненной **на продвинутом** уровне, если оценка составляет более 88 баллов

2. Шкала оценки.

В общей оценке по дисциплине баллы за работы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

3. Примерный перечень тем курсового проекта (работы).

1. Элементы защиты в БД MS Access данных текстового анализа.
2. Элементы защиты в БД MS Access текстовых данных.
3. Элементы защиты в БД MS Access криптографических ключей.
4. Защита БД текстовых данных в MS SQL.
5. Защита БД данных текстового анализа в MS SQL.
6. Защита БД криптографических ключей в MS SQL.

4. Перечень вопросов к защите курсового проекта (работы).

1. Основные требования к защите и безопасности БД.
2. Системы защиты универсальных БД и их недостатки.
3. Средства и методы защиты БД.
4. Защита БД в сетях.
5. Связь безопасности БД и политики методов доступа.
6. Идентификация и аутентификация при защите БД.
7. Криптографические методы в защите БД.
8. Система защиты БД MS Access
9. Система защиты MS SQL.
10. Система защиты Oracle.