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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность информационных систем персональных данных

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 4, семестр : 8

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	94
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	36
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	20
10	Самостоятельная работа, час.	86
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

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

Программу разработал:

доцент, к.т.н. Зырянов С. А.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.13 способность участвовать в проектировании средств защиты информации автоматизированной системы; *в части следующих результатов обучения*:**
з2. знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации
***Компетенция ФГОС*: ПК.22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации; *в части следующих результатов обучения*:**
з1. знать правила формирования политики информационной безопасности организации
у2. уметь участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
***Компетенция ФГОС*: ПК.23 способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа; *в части следующих результатов обучения*:**
у3. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем
***Компетенция ФГОС*: ПК.24 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; *в части следующих результатов обучения*:**
у1. уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем
***Компетенция ФГОС*: ПК.26 способность администрировать подсистему информационной безопасности автоматизированной системы; *в части следующих результатов обучения*:**
з1. знать источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению
***Компетенция ФГОС*: ПК.27 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы; *в части следующих результатов обучения*:**
у1. уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем
***Компетенция ФГОС*: ПК.8 способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем; *в части следующих результатов обучения*:**
з1. уметь разрабатывать положения, инструкции и другие организационно-распорядительные документы по обеспечению информационной безопасности

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Безопасность информационных систем персональных данных	
ПК.8.з1 уметь разрабатывать положения, инструкции и другие организационно-распорядительные документы по обеспечению информационной безопасности	
1.методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности систем;	Лекции; Самостоятельная работа
ПК.13.з2 знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	
2.научно-техническую информацию, нормативные и методические материалы	Лекции; Лабораторные работы; Самостоятельная работа

ПК.23.у3 уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	
3.составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах;	Лекции; Лабораторные работы; Самостоятельная работа
ПК.22.у2 уметь участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;	
4.анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем	Лекции; Лабораторные работы
ПК.22.з1 знать правила формирования политики информационной безопасности организации	
5.автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Лекции; Лабораторные работы
ПК.27.у1 уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем	
6.методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систе	Лекции; Лабораторные работы
ПК.24.у1 уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем	
7.выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем; уб. навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем	Лекции; Лабораторные работы
ПК.26.з1 знать источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению	
8.технические регламенты для различных видов деятельности по обеспечению информационной безопасности	Лекции; Лабораторные работы

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Система государственного регулирования отношений, связанных с обработкой персональных данных				
1. Аспекты и современное понимание проблемы ОБ ИСПДн	0	4	2	Формирование требований к системе
3. Правовые основы информационной безопасности в РФ.	0	2	1, 3	Формирование требований к системе
Дидактическая единица: Обеспечение безопасности (ОБ) ПДн в ИСПДн				
4. Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в информационной сфере	0	4	2, 4	Формирование требований к системе
5. Административный регламент исполнения государственной функции по осуществлению государственного контроля ОБ ИСПДн	0	2	3, 4, 5	Формирование требований к системе

Дидактическая единица: Содержание мер защиты информации в ИСПДн				
7. Основные угрозы безопасности при работе в компьютерной и сетевой среде	0	8	5, 6, 8	Содержание и порядок выполнения работ по ЗИ
8. Обеспечение безопасности персональных данных пользователями на рабочих местах в информационных системах персональных данных	0	10	3, 7	Разработка предварительных проектных решений по системе и ее частям
Дидактическая единица: Особенности обработки персональных данных				
9. Обработка биометрических персональных данных	0	4	4, 5	разрабатывать технические регламенты
10. Требования и методы электронного цензурирования	0	2	4, 5, 7	Выделять свойства и признаки информации

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Система государственного регулирования отношений, связанных с обработкой персональных данных				
2. Системные компоненты безопасности MS Windows	1	4	3, 5, 8	Формирование требований к системе
Дидактическая единица: Обеспечение безопасности (ОБ) ПДн в ИСПДн				
1. Управление доступом к съёмным машинным носителям информации	1	4	3	Разработка предварительных проектных решений по системе и ее частям
7. Средства контроля работы пользователей в терминальных сессиях	0	4	3, 4	Применять методы анализа защищенности
Дидактическая единица: Содержание мер защиты информации в ИСПДн				
8. Контроль сетевой активности пользователей средствами анализа сетевого трафика	1	4	2, 3, 8	способность создавать и исследовать модели
Дидактическая единица: Особенности обработки персональных данных				
6. Система биометрической аутентификации пользователей	1	4	3, 4, 7	Содержание и порядок выполнения работ по ЗИ
9. Использование MS SQL Server Analysis Services для построения хранилищ данных	2	8	2, 4, 8	проводить анализ, предлагать и обосновывать выбор решений
10. Тестирование на проникновение	2	8	4, 5, 6, 8	проводить контрольные проверки работоспособности

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	РГЗ	2	40	8
, подробная информация приведена в приложении №1 : Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.				

2	Подготовка к занятиям	1	26	0
: Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.				
3	Дополнительная учебная деятельность	2	0	8
: Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.				
4	Подготовка к аттестации	3	20	4
Работа с литературой, подробная информация приведена в приложении №2 : Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.				

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	e-mail; Социальные сети
Консультирование	Социальные сети
Контроль	e-mail
Размещение учебных материалов	Социальные сети

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм
1	Лекция в форме дискуссии:Дополнит материалы
Краткое описание применения:	
Подробная информация об использовании технологии приводится в приложении №1	

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять 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: 8	
Лабораторная:	30
РГЗ:	30
Контролирующие материалы - список вопросов	

Зачет:	20
Контролирующие материалы - список вопросов	
Экзамен:	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	Зачет
ПК.13	з2. знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации		+
ПК.22	з1. знать правила формирования политики информационной безопасности организации		+
	у2. уметь участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;		+
ПК.23	у3. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем		+
ПК.24	у1. уметь выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем	+	
ПК.26	з1. знать источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению		+
ПК.27	у1. уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем	+	
ПК.8	з1. уметь разрабатывать положения, инструкции и другие организационно-распорядительные документы по обеспечению информационной безопасности		+

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

7. Литература

Основная литература

1. Электронная библиотека МГППУ [Электронный ресурс] : для лиц с ограниченными возможностями здоровья. - Москва, 2014-. - Режим доступа: http://psychlib.ru/index.php. - Загл. с экрана.

2. ЭБС Издательство «Лань» [Электронный ресурс] : электронно-библиотечная система. - [Россия], 1993. - Режим доступа: http://e.lanbook.com. - Загл. с экрана.

Дополнительная литература

1. ЭКБСОН [Электронный ресурс] : информационная система. - Россия, 2014. - Режим доступа: http://www.vlibrary.ru/. - Загл. с экрана.

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. Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.

8.2 Специализированное программное обеспечение

1 Операционные системы семества LINUX

2 Vmware

9. Материально-техническое обеспечение

Презентационное оборудование

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

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Лабораторные работы

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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность информационных систем персональных данных

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине Безопасность информационных систем персональных данных 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)**
ПК.13/ПК способность участвовать в проектировании средств защиты информации автоматизированной системы	з2. знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	Аспекты и современное понимание проблемы ОБ ИСПДн Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в информационной сфере		Зачет, вопросы...
ПК.22/ОУ способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	з1. знать правила формирования политики информационной безопасности организации	Административный регламент исполнения государственной функции по осуществлению государственного контроля ОБ ИСПДн Основные угрозы безопасности при работе в компьютерной и сетевой среде		Зачет, вопросы...
ПК.22/ОУ	у2. уметь участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;	Административный регламент исполнения государственной функции по осуществлению государственного контроля ОБ ИСПДн Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в информационной сфере		Зачет, вопросы...
ПК.23/ОУ способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	у3. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	Административный регламент исполнения государственной функции по осуществлению государственного контроля ОБ ИСПДн Обеспечение безопасности персональных данных пользователями на рабочих местах в информационных системах персональных данных		Зачет, вопросы...
ПК.24/Э способность обеспечить эффективное применение	у1. уметь выявлять уязвимости информационно-технологических ресурсов	Обеспечение безопасности персональных данных пользователями на рабочих местах в информационных системах персональных	РГЗ, разделы...	

информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	информационных систем, проводить мониторинг угроз безопасности информационных систем	данных		
ПК.26/Э способность администрировать подсистему информационной безопасности автоматизированной системы	з1. знать источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению	Основные угрозы безопасности при работе в компьютерной и сетевой среде Системные компоненты безопасности MS Windows		Зачет, вопросы...
ПК.27/Э способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	у1. уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем	Основные угрозы безопасности при работе в компьютерной и сетевой среде	РГЗ, разделы...	
ПК.8/ПК способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	з1. уметь разрабатывать положения, инструкции и другие организационно-распорядительные документы по обеспечению информационной безопасности	Правовые основы информационной безопасности в РФ.		Зачет, вопросы...

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 8 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПК.13/ПК, ПК.22/ОУ, ПК.23/ОУ, ПК.24/Э, ПК.26/Э, ПК.27/Э, ПК.8/ПК.

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

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

В 8 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 ПК.13/ПК, ПК.22/ОУ, ПК.23/ОУ, ПК.24/Э, ПК.26/Э, ПК.27/Э, ПК.8/ПК, 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.

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

Паспорт зачета

по дисциплине «Безопасность информационных систем персональных данных», 8 семестр

1. Методика оценки

Зачет проводится в устной (письменной) форме, по билетам (тестам). Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-28, второй вопрос из диапазона вопросов 29-56 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Безопасность информационных систем персональных данных»

1. Вопрос 1
2. Вопрос 2.

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

2. Критерии оценки

- Ответ на билет для зачета 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 *19 баллов.*
- Ответ на билет для зачета 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 билет для зачета 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 *25 баллов.*

- Ответ на билет для зачета 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

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 20 баллов (из 40 возможных).

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

4. **Вопросы к** зачету **по дисциплине «**Безопасность информационных систем персональных данных**»**

1) Законодательство Российской Федерации в области персональных данных.
2) Принципы обработки персональных данных.
3) Условия обработки персональных данных.
4) Конфиденциальность персональных данных.
5) Общедоступные источники персональных данных.
6) Согласие субъекта персональных данных на обработку его персональных данных.
7) Специальные категории персональных данных.
8) Биометрические персональные данные.
9) Трансграничная передача персональных данных.
10) Права субъекта персональных данных.
11) Обязанности оператора.
12) Меры по обеспечению безопасности персональных данных при их обработке, определенные федеральным законом.
13) Уведомление об обработке персональных данных.
14) Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований настоящего федерального закона.
15) Подходы к регулированию персональных данных в Европе, США и в иных зарубежных странах.
16) «Право быть забытым» в международном, зарубежном и российском законодательстве.
17) Существующие модели регулирования правового института персональных данных в

международно-правовых и национальных зарубежных правовых источниках.

18) Условия сбора, хранения, использования и передачи персональных данных крупнейшими компаниями, оказывающими услуги в области использования информационных технологий, в том числе в интернете.

19) Зарубежный опыт в области создания систем доверительного управления информацией, определения и защиты персональных данных при проведении электронной идентификации и оказании аналогичных услуг доверенными лицами (доверенные сервисы).

20) Концепция регулирования и защиты персональных данных с учетом развития информационных технологий

21) Элементы структуры обеспечения приватности.

22) Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами. Постановление Правительства РФ от 21 марта 2012 г. № 211.

23) Требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных. . Постановление Правительства РФ от 1 ноября 2012 г. N 1119

24) Содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

25) Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

26) Регламент исполнения государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

27) Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

28) Классификация информационной системы по требованиям защиты информации.

29) Определение угроз безопасности информации в информационной системе. Порядок определения актуальных угроз безопасности персональных данных в ИСПДн.

30) Общие требования к структуре и описания уязвимости и правилам описания уязвимости информационной системы.

31) Классификация уязвимостей информационных систем.

32) Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Классификация СК и задачи, решаемые при проведении анализа СК.

33) Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Рекомендации по организации защиты информации.

34) Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации.

35) Содержание мер защиты информации . Идентификация и аутентификация субъектов доступа и объектов доступа

36) Содержание мер защиты информации . Управление доступом субъектов доступа к объектам доступа

37) Содержание мер защиты информации . Ограничение программной среды

38) Содержание мер защиты информации . Защита машинных носителей информации

39) Содержание мер защиты информации . Регистрация событий безопасности

40) Содержание мер защиты информации . Антивирусная защита.

41) Содержание мер защиты информации . Обнаружение (предотвращение) вторжений.

42) Содержание мер защиты информации . Контроль (анализ) защищенности информации.

43) Содержание мер защиты информации . Обеспечение целостность информационной системы и информации.

44) Содержание мер защиты информации . Обеспечение доступности информации.

45) Содержание мер защиты информации . Защита среды виртуализации.

46) Содержание мер защиты информации . Защита технических средств.

47) Содержание мер защиты информации . Защита информационной системы, ее средств и систем связи и передачи данных.

48) Требований безопасности информации к операционным системам.

49) Методические документы, содержащие профили защиты межсетевых экранов.

50) Требования к средствам доверенной загрузки.

51) Требования к системам обнаружения вторжений.

52) Требования к средствам контроля съемных машинных носителей информации.

53) Требования к средствам антивирусной защиты

54) Защита информации при использовании технологий виртуализации. Угрозы безопасности.

55) Защита информации при использовании технологий виртуализации. Особенности защиты.

56) Требования и методы электронного цензурирования.

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

Паспорт
расчетно-графического задания (работы)

по дисциплине «Безопасность информационных систем персональных данных», 8 семестр

1. Методика оценки

При выполнении расчетно-графического задания (работы) студенты должны провести анализ объекта диагностирования, выбрать и обосновать диагностические признаки и параметры, разработать алгоритмы диагностирования, выбрать аппаратные средства.

Обязательные структурные части РГЗ.

Построение VPN с использованием OpenVPN Access Server. Для освоения навыков создания VPN требуется создать виртуальную подсеть включающую два компьютера с ОС Debian и Windows 7.

Оцениваемые позиции:

Подключиться к папке предоставленной в общий доступ в Windows 7 по VPN туннелю.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, диагностические признаки не обоснованы, аппаратные средства не выбраны или не соответствуют современным требованиям, оценка составляет 19 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, аппаратные 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 обоснованы, алгоритмы разработаны ,но не оптимизированы, аппаратные средства выбраны без достаточного обоснования, оценка составляет 25 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны и оптимизированы, выбор аппаратных 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)**

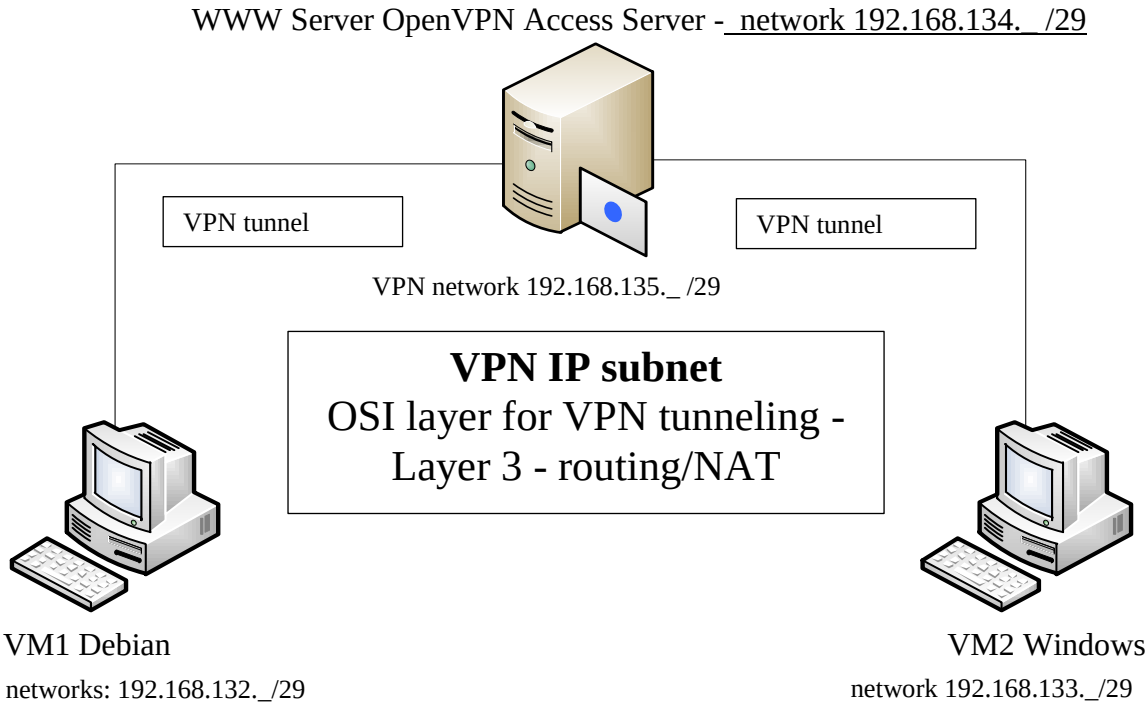

Рис. 2. Конфигурация подсети **Virtual VPN OpenVPN Access Server**

IP Адрес сервера OpenVPN определяется по формуле:

$IP = 192.168.134.n/29;$

$n = N_g - 3 + N_{st} * 5$

где: N_g - две последних цифры номера группы; N_{st} - номер студента по списку группы.

Маска сети - 255.255.255.248

Пример:

1)Группа -шифр - 220, студент - 1. $n=20-3+1*8=25$. IP адрес сервера 192.168.134.25.

2) Группа -шифр - 221, студент - 1. $n=21-3+1*8=26$. IP адрес сервера 192.168.134.26.

3) Группа -шифр - 223, студент - 1. $n=23-3+1*8=28$. IP адрес сервера 192.168.134.28.

IP Адрес VPN tunnel (зоны динамических адресов) определяется по формуле:

$IP = 192.168.135.n/29;$

$n = N_{network\_OVPN}$;

где: $N_{network\_OVPN}$ - n адреса подсети сервера OpenVPN

По результатам вычисления IP адресов интерфейсов заполнить таблицы:

	Адрес подсети	IP адрес интерфейса	Широковещательный адрес
WWW Server OpenVPN			
VPN tunnel			

IP Адрес сервера VM1 определяется по формуле:

$IP = 192.168.132.n/29;$

$n = N_{OVPN} + 1;$

где: N_{OVPN} - n адреса сервера OpenVPN.
Маска сети - 255.255.255.248
IP Адрес сервера VM2 определяется по формуле:

$$IP = 192.168.133.n/29;$$

$$n = N_{OVPN} + 2;$$

где: N_{OVPN} - n адреса сервера OpenVPN.
Маска сети - 255.255.255.248

	Адрес подсети	IP адрес интерфейса	Маска подсети	Шлюз
VM1				
VM2				