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: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 4, семестр : 8

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	63
4	Лекции, час.	18
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	25
10	Самостоятельная работа, час.	45
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	З

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 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): 10.03.01 Информационная безопасность

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*: ОПК.4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации; *в части следующих результатов обучения*:**
з2. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты
у3. уметь использовать специализированные программные средства при решении профессиональных задач
у8. уметь пользоваться наиболее распространенными офисными и математическими пакетами прикладных программ
***Компетенция ФГОС*: ПК.10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; *в части следующих результатов обучения*:**
з2. знать требования стандартов в области информационной безопасности
з3. знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области
у2. уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
***Компетенция ФГОС*: ПК.13 способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации; *в части следующих результатов обучения*:**
у3. уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем
***Компетенция ФГОС*: ПК.3 способность администрировать подсистемы информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
***Компетенция ФГОС*: ПК.4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
з4. знать принципы формирования политики информационной безопасности на объекте защиты
у4. уметь разрабатывать частные политики информационной безопасности информационных систем

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.4.з4 знать принципы формирования политики информационной безопасности на объекте защиты	
1.знает отраслевую направленность правовых норм, в том числе с учетом особенностей профессиональной деятельности	Лекции; Самостоятельная работа
ПК.3.у1 уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
2.может осуществлять реализацию нормативно-правовых актов в сфере профессиональной деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.4.з2 знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
3.знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Лекции; Лабораторные работы; Самостоятельная работа

ОПК.4.у3 уметь использовать специализированные программные средства при решении профессиональных задач	
4.уметь использовать специализированные программные средства при решении профессиональных задач	Лекции; Лабораторные работы; Самостоятельная работа
ПК.4.у4 уметь разрабатывать частные политики информационной безопасности информационных систем	
5.уметь проводить библиографическую и информационно-поисковую работы, использовать ее результаты при решении профессиональных задач и оформлении научных трудов	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.4.у8 уметь пользоваться наиболее распространенными офисными и математическими пакетами прикладных программ	
6.уметь пользоваться наиболее распространенными офисными и математическими пакетами прикладных программ	Лекции; Лабораторные работы
ПК.13.у3 уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем	
7.уметь использовать языки и системы программирования для решения профессиональных задач	Лекции; Лабораторные работы
ПК.10.з2 знать требования стандартов в области информационной безопасности	
8.технические регламенты для различных видов деятельности по обеспечению информационной безопасности	Лекции; Самостоятельная работа
ПК.10.з3 знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области	
9.технологический процесс защиты информации ограниченного доступа	Лекции; Самостоятельная работа
ПК.10.у2 уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	
10.выполненять комплекс мер по обеспечению информационной безопасности, управлять процессом их реализации	Лекции; Самостоятельная работа

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. Правовые основы информационной безопасности в РФ.	0	2	2, 4	организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами
2. Аспекты и современное понимание проблемы ОБ ИСПДн.	0	4	1, 4	технологический процесс защиты информации ограниченного доступа
Дидактическая единица: Обеспечение безопасности (ОБ) ПДн в ИСПДн				
3. Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в информационной сфере	0	4	3, 5, 6	анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

4. Административный регламент исполнения государственной функции по осуществлению государственного контроля ОБ ИСПДн	0	2	1, 2	технологический процесс защиты информации ограниченного доступа
5. Методика определения актуальных угроз безопасности персональных данных	0	2	3, 4	определение актуальных угроз
6. Основы обеспечения приватности	0	2	6, 8	нормативная база
Дидактическая единица: Особенности обработки персональных данных				
7. Обработка биометрических персональных данных	0	2	10, 7, 9	нормативная база

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				
1. Системные компоненты безопасности MS Windows	2	4	2, 4	работы по установке, настройке и обслуживанию программных, программно-аппаратных и ТСЗИ
3. Управление доступом к съёмным машинным носителям информации	2	4	2, 3, 4	работы по установке, настройке и обслуживанию программных, программно-аппаратных ТСЗИ
Дидактическая единица: Обеспечение безопасности (ОБ) ПДн в ИСПДн				
4. Средства контроля работы пользователей в терминальных сессиях	2	4	6, 7	работы по установке, настройке и обслуживанию программных, программно-аппаратных ТСЗИ
5. Контроль сетевой активности пользователей средствами анализа сетевого трафика	0	2	4, 5, 6	работы по установке, настройке и обслуживанию программных, программно-аппаратных ТСЗИ
Дидактическая единица: Особенности обработки персональных данных				
7. Система биометрической аутентификации пользователей	2	4	2, 4	работы по установке, настройке и обслуживанию программных, программно-аппаратных

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	РГЗ	2, 3, 4	16	4
реализация мер защиты, подробная информация приведена в приложении №3 : 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, 3	10	9
работа с нормативной базой, 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.				
3	Дополнительная учебная деятельность	3, 4, 5	11	8
нормативно -правовые документы , 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.				
4	Подготовка к аттестации	10, 8, 9	8	4
применение требований нормативно правовой базы, 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	Портал НГТУ; Среда электронного обучения НГТУ
Консультирование	e-mail; Среда электронного обучения НГТУ
Контроль	e-mail; Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ; ЭБС

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	Мин. балл	Максимальный балл
Семестр: 8		
Лабораторная:	20	40
Контролирующие материалы - список вопросов		
РГЗ:	20	40
Контролирующие материалы - список вопросов		
Зачет:	10	20
Контролирующие материалы - список вопросов		

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
ОПК.4	з2. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	+	+
	у3. уметь использовать специализированные программные средства при решении профессиональных задач		+
	у8. уметь пользоваться наиболее распространенными офисными и математическими пакетами прикладных программ		+
ПК.10	з2. знать требования стандартов в области информационной безопасности		+
	з3. знать основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области		+
	у2. уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности		+
ПК.13	у3. уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем	+	+
ПК.3	у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты		+
ПК.4	з4. знать принципы формирования политики информационной безопасности на объекте защиты		+
	у4. уметь разрабатывать частные политики информационной безопасности информационных систем	+	+

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

7. Литература

Основная литература

1. Галицкий А. В. Защита информации в сети - анализ технологий и синтез решений / Галицкий, А. В. Рябко С. Д., Шаньгин В. Ф. - М., 2004. - 613 с. : ил.

2. Девянин П. Н. Модели безопасности компьютерных систем : учебное пособие для вузов по специальностям 075200 "Компьютерная безопасность" и 075500 "Комплексное обеспечение информационной безопасности автоматизированных систем" / П. Н. Девянин. - М., 2005. - 142, [1] с.

3. Садердинов А. А. Информационная безопасность предприятия : учебное пособие / А. А. Садердинов, В. А. Тайнёв, А. А. Федулов ; Междунар. акад. наук информации, информ. процессов и технологий (МАН ИПТ). - Москва, 2004. - 335 с. : ил., табл.

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. Информационная безопасность открытых систем. [В 2 т.]. Т. 1 : учебник для вузов по специльности 075500 (090105) - "Комплексное обеспечение информационной безопасности автоматизированных систем" / С. В. Запечников [и др.]. - М., 2006. - 535 с. : ил., табл.

3. Волков А. М. Комплексная безопасность предприятий : учебное пособие / А. М. Волков, В. Н. Легкий, Ю. А. Попков ; Новосиб. гос. техн. ун-т. - Новосибирск, 2007. - 70, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000074126

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 Windows
2 Office

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)	выполнение лабораторных работ

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: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

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)**
ОПК.4 способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	з1. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Методика определения актуальных угроз безопасности персональных данных Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в информационной сфере Управление доступом к съёмным машинным носителям информации	РГЗ, разделы...	Зачет, вопросы...
ОПК.4	у2. уметь использовать специализированные программные средства при решении профессиональных задач	Аспекты и современное понимание проблемы ОБ ИСПДн. Контроль сетевой активности пользователей средствами анализа сетевого трафика Правовые основы информационной безопасности в РФ. Система биометрической аутентификации пользователей Системные компоненты безопасности MS Windows Управление доступом к съёмным машинным носителям информации		Зачет, вопросы...
ОПК.4	у7. уметь пользоваться наиболее распространенными офисными и математическими пакетами прикладных программ	Контроль сетевой активности пользователей средствами анализа сетевого трафика Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в информационной сфере Средства контроля работы пользователей в терминальных сессиях		Зачет, вопросы...
ПК.10/ЭИ способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	з2. знать требования стандартов в области информационной безопасности	Основы обеспечения приватности		Зачет, вопросы...
ПК.10/ЭИ	з3. знать основные нормативные правовые акты в области	Обработка биометрических персональных данных		Зачет, вопросы...

	информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области			
ПК.10/ЭИ	у2. уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности	Обработка биометрических персональных данных		Зачет, вопросы...
ПК.13/ОУ способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	у3. уметь разрабатывать модели угроз и нарушителей информационной безопасности информационных систем	Обработка биометрических персональных данных Средства контроля работы пользователей в терминальных сессиях	РГЗ, разделы...	Зачет, вопросы...
ПК.3/Э способность администрировать подсистемы информационной безопасности объекта защиты	у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Правовые основы информационной безопасности в РФ. Система биометрической аутентификации пользователей Системные компоненты безопасности MS Windows Управление доступом к съёмным машинным носителям информации		Зачет, вопросы...
ПК.4/Э способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	з3. знать принципы формирования политики информационной безопасности на объекте защиты	Аспекты и современное понимание проблемы ОБ ИСПДн.		Зачет, вопросы...
ПК.4/Э	у2. уметь разрабатывать частные политики информационной безопасности информационных	Контроль сетевой активности пользователей средствами анализа сетевого трафика Проблема защиты ИСПДН в контексте обеспечения кибербезопасностии в	РГЗ, разделы...	Зачет, вопросы...

	систем	информационной сфере		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 8 семестре - в форме зачета, который направлен на оценку сформированности компетенций ОПК.4, ПК.10/ЭИ, ПК.13/ОУ, ПК.3/Э, ПК.4/Э.

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 ОПК.4, ПК.10/ЭИ, ПК.13/ОУ, ПК.3/Э, ПК.4/Э, 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 . Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-17, второй вопрос из диапазона вопросов 18-34 (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.

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)**

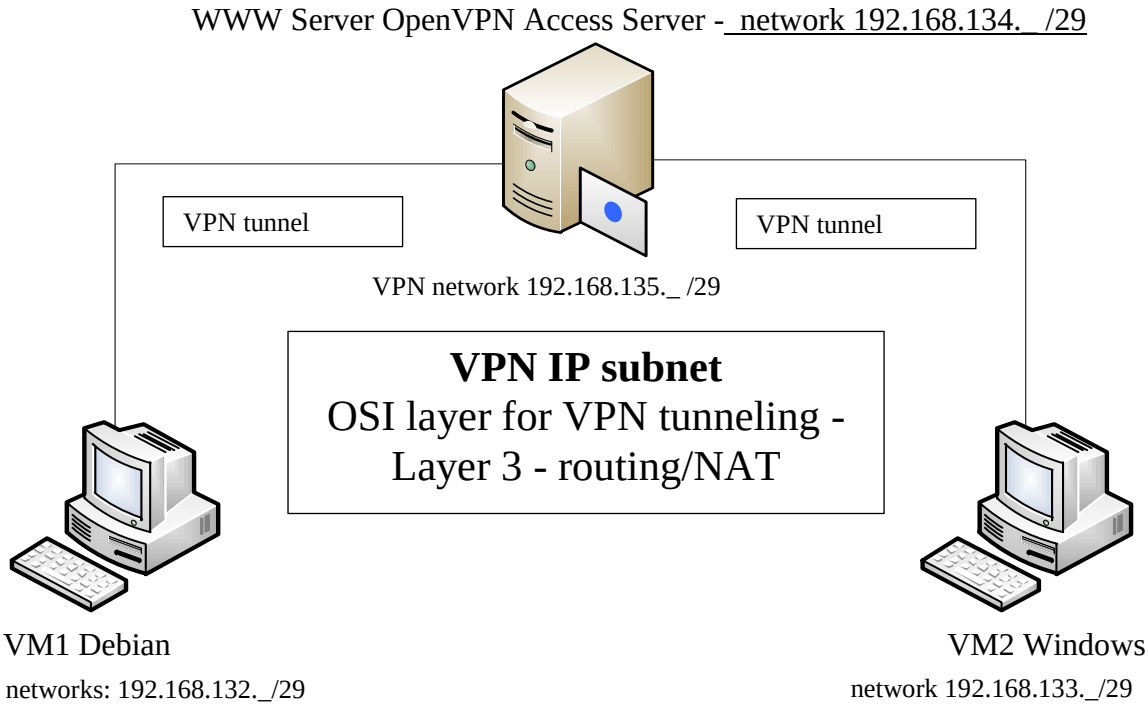

Рис. 2. Конфигурация подсети **Virtual VPN OpenVPN Access Server**

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				