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

Кафедра вычислительной техники
Кафедра автоматизированных систем управления

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Защита информации

Образовательная программа: 09.03.01 Информатика и вычислительная техника, профиль: Программное обеспечение компьютерных систем и сетей

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**7**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	64
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	8
10	Самостоятельная работа, час.	80
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	контр.
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 09.03.01 Информатика и вычислительная техника

ФГОС введен в действие приказом №5 от 12.01.2016 г. , дата утверждения: 09.02.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 09.03.01 Информатика и вычислительная техника

Рабочая программа обсуждена на заседании кафедры

ВТ, протокол заседания кафедры №6 от 20.06.2017
АСУ, протокол заседания кафедры №7 от 20.06.2017

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

Программу разработал:

доцент, к.т.н. Зыбарев В. М.

Заведующий кафедрой:

доцент, к.т.н. Якименко А. А.
профессор, д.т.н. Гриф М. Г.

Ответственный за образовательную программу:

доцент Романов Е. Л.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.5 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; *в части следующих результатов обучения*:**
з5. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты
у12. уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе
у5. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств
у8. владеть персональным компьютером как средством управления информацией
***Компетенция ФГОС*: ПК.3 способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности; *в части следующих результатов обучения*:**
у4. уметь обосновывать принимаемые проектные решения
у9. владеть методами оценки трудоемкости программного проекта

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Защита информации	
ОПК.5.з5 знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
1.знает социальные основы партнерских и конфликтных отношений в социально-трудовой сфере и методы управления конфликтом в организации	Лекции; Лабораторные работы; Самостоятельная работа
2.знает отраслевую направленность правовых норм, в том числе с учетом особенностей профессиональной деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.у12 уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	
3.умеет осуществлять реализацию нормативно-правовых актов в сфере профессиональной деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.з5 знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
4.знать сущность и значение информации в развитии современного общества, опасности и угроз, возникающие в этом процессе	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.у12 уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	
5.уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.з5 знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
6.знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.у5 уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	
7.уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.у8 владеть персональным компьютером как средством управления информацией	

8.владеть персональным компьютером как средством управления информацией	Лекции; Лабораторные работы; Самостоятельная работа
ПК.3.у4 уметь обосновывать принимаемые проектные решения	
9. уметь обосновывать принимаемые проектные решения	Лабораторные работы
ПК.3.у9 владеть методами оценки трудоемкости программного проекта	
10.владеть методами оценки трудоемкости программного проекта	Лабораторные работы

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Введение				
1. Содержание и характеристика курса	0	2	1, 4, 5	Посещение лекции
Дидактическая единица: Основы информационной безопасности				
2. Основные принципы, подходы и меры по обеспечению информационной безопасности и защиты информации	0	4	4, 5, 6	Посещение лекций
Дидактическая единица: Криптографические методы и средства защиты информации				
3. Основы криптологии	0	6	3, 4, 5, 6, 7	Посещение лекций
Дидактическая единица: Защита от несанкционированного доступа к информации в компьютерных системах, комплексах и сетях				
4. Методы, системы и средства защиты информации от НСД	0	6	5, 6, 7, 8	Посещение лекций
Дидактическая единица: Защита программного обеспечения вычислительных систем				
5. Организация многоуровневой и комплексной защиты информации ОС	0	4	5, 6, 7, 8	Посещение лекций
Дидактическая единица: Основы защиты компьютерных сетей				
6. Системы и технологии защиты сетей	0	6	5, 6, 7, 8	Посещение лекций
Дидактическая единица: Нормативно- правовые основы защиты информации				
7. Нормативно-правовые обеспечение информационной безопасности и защиты персональных данных	0	2	1, 2, 3, 6	Посещение лекций
Дидактическая единица: Защита информации на предприятиях				
8. Инженерно-технические и организационно-административные мероприятия защиты информации	0	4	1, 2, 3, 6, 7	Посещение лекций
Дидактическая единица: Заключение				
9. Современное состояние и перспективы совершенствования методов и средств защиты компьютерной информации	0	2	4, 5, 6	

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Криптографические методы и средства защиты информации				
1. Применение и анализ эффективности симметричных и асимметричных криптоалгоритмов защиты информации.	4	4	10, 2, 3, 4, 5, 6, 7, 8, 9	Изучает основы криптографических алгоримов и анализирует криптографическую стойкость шифров
Дидактическая единица: Защита от несанкционированного доступа к информации в компьютерных системах, комплексах и сетях				
2. Защита баз данных в среде СУБД	4	4	1, 10, 3, 4, 6, 7, 8, 9	Применение и анализ эффективности защиты баз данных средствами СУБД
Дидактическая единица: Защита программного обеспечения вычислительных систем				
3. Защита информации пользователя и приложений в среде ОС	4	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Обеспечение информационной безопасности данных пользователя и интернет приложений
Дидактическая единица: Основы защиты компьютерных сетей				
4. Применение и анализ сетевых средств защиты компьютерной безопасности	6	6	1, 10, 3, 4, 5, 6, 7, 8, 9	Применение брандмуэра и анализ сетевой защищенности компьютерных систем методом сканирования

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	Контрольные работы	2, 3, 4, 5, 6, 7, 8	20	2
: Вихман В. В. Методы и средства защиты компьютерной информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000156312. - Загл. с экрана. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				
2	Подготовка к занятиям	1, 2, 3, 4, 5, 6, 7, 8	40	4
: Вихман В. В. Методы и средства защиты компьютерной информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000156312. - Загл. с экрана. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768				
3	Подготовка к аттестации	1, 2, 3, 4, 5, 6, 7	20	2

: Вихман В. В. Методы и средства защиты компьютерной информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000156312. - Загл. с экрана. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

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
Консультирование	e-mail
Размещение учебных материалов	Личный типовой сайт

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм
1	Тренинг:Проверка приобретенных навыков
Краткое описание применения: Контроль на примерах действий студентов	

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: 7	
Лабораторная:	40
Контрольные работы:	20
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	
		Контр. раб.	Экзамен
ОПК.5	з5. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	+	+

	у12. уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	+	+
	у5. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	+	+
	у8. владеть персональным компьютером как средством управления информацией	+	+
ПК.3	у4. уметь обосновывать принимаемые проектные решения	+	+
	у9. владеть методами оценки трудоемкости программного проекта	+	+

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

7. Литература

Основная литература

1. Грибунин В. Г. Комплексная система защиты информации на предприятии : [учебное пособие для вузов по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информации" направления подготовки "Информационная безопасность"] / В. Г. Грибунин, В. В. Чудовский. - М., 2009. - 411, [1] с. : ил., табл.

2. Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 57, [1] с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

3. Мельников В. П. Информационная безопасность и защита информации : [учебное пособие для вузов по специальности "Информационные системы и технологии"] / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М., 2011. - 330, [1] с. : ил., табл., схемы

4. Рябко Б. Я. Основы современной криптографии и стеганографии : [монография] / Б. Я. Рябко, А. Н. Фионов. - М., 2010. - 232 с.

Дополнительная литература

1. Смирнов С. Н. Безопасность систем баз данных : [учебное пособие для вузов по специальности в области информационной безопасности] / С. Н. Смирнов. - М., 2007. - 350, [1] с. : ил.

2. Романов О. А. Организационное обеспечение информационной безопасности : [учебник для вузов по специальностям "Организация и технология защиты информации" и "Комплексная защита объектов информации" направления подготовки "Информационная безопасность"] / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М., 2008. - 188, [1] с.

3. Рябко Б. Я. Криптографические методы защиты информации : учебное пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - М., 2005. - 229 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. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

2. Вихман В. В. Методы и средства защиты компьютерной информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000156312. - Загл. с экрана.

8.2 Специализированное программное обеспечение

1 Kaspersky Anti-Spam

2 Kaspersky Endpoint Security 8

3 Outpost Firewall Pro

4 Microsoft Office

5 Microsoft Windows

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Проведение учебных занятий и консультаций

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Проведение лабораторных работ

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

Кафедра автоматизированных систем управления
Кафедра вычислительной техники

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

Образовательная программа: 09.03.01 Информатика и вычислительная техника, профиль: Программное обеспечение компьютерных систем и сетей

Новосибирск 2017

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

Обобщенная структура фонда оценочных средств по **дисциплине** Защита информации

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.5 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	з5. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Защита баз данных в среде СУБД Защита информации пользователя и приложений в среде ОС Инженерно-технические и организационно-административные мероприятия защиты информации Методы, системы и средства защиты информации от НСД Нормативно-правовые обеспечение информационной безопасности и защиты персональных данных Основные принципы, подходы и меры по обеспечению информационной безопасности и защиты информации Основы криптологии Применение и анализ эффективности симметричных и асимметричных криптоалгоритмов защиты информации. Применение и анализ сетевых средств защиты компьютерной безопасности Современное состояние и перспективы совершенствования методов и средств защиты компьютерной информации Содержание и характеристика курса	Контрольные работы, разделы:. 1, 2,3,4, 5,6,7	Экзамен, вопросы: 1 - 56
ОПК.5	у5. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Защита баз данных в среде СУБД Защита информации пользователя и приложений в среде ОС Методы, системы и средства защиты информации от НСД Организация многоуровневой и комплексной защиты информации ОС Применение и анализ эффективности симметричных и асимметричных криптоалгоритмов защиты информации. Применение и анализ сетевых средств защиты компьютерной безопасности Системы и технологии защиты сетей	Контрольные работы, разделы: 3,4, 5,6	Экзамен, вопросы: 10 - 43

ОПК.5	у8. владеть персональным компьютером как средством управления информацией	Защита баз данных в среде СУБД Защита информации пользователя и приложений в среде ОС Методы, системы и средства защиты информации от НСД Организация многоуровневой и комплексной защиты информации ОС Применение и анализ эффективности симметричных и асимметричных криптоалгоритмов защиты информации. Применение и анализ сетевых средств защиты компьютерной безопасности Системы и технологии защиты сетей	Контрольные работы, разделы: 3,4, 5,6	Экзамен, вопросы: 10 - 43
ОПК.5	у12. уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	Защита информации пользователя и приложений в среде ОС Инженерно-технические и организационно-административные мероприятия защиты информации Методы, системы и средства защиты информации от НСД Нормативно-правовые обеспечение информационной безопасности и защиты персональных данных Организация многоуровневой и комплексной защиты информации ОС Основные принципы, подходы и меры по обеспечению информационной безопасности и защиты информации Основы криптологии Применение и анализ сетевых средств защиты компьютерной безопасности Системы и технологии защиты сетей Современное состояние и перспективы совершенствования методов и средств защиты компьютерной информации Содержание и характеристика курса	Контрольные работы, разделы:. 1, 2,3,4, 5,6,7	Экзамен, вопросы: 1 - 56
ПК.3/НИ готовность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	у4. уметь обосновывать принимаемые проектные решения	Защита баз данных в среде СУБД Защита информации пользователя и приложений в среде ОС Применение и анализ эффективности симметричных и асимметричных криптоалгоритмов защиты информации. Применение и анализ сетевых средств защиты компьютерной безопасности	Контрольные работы, разделы: 3,4, 5,6	Экзамен, вопросы: 10 - 43

ПК.3/НИ	у9. владеть методами оценки трудоемкости программного проекта	Защита баз данных в среде СУБД Защита информации пользователя и приложений в среде ОС Применение и анализ эффективности симметричных и асимметричных криптоалгоритмов защиты информации. Применение и анализ сетевых средств защиты компьютерной безопасности	Контрольные работы, разделы: 3,4, 5,6	Экзамен, вопросы: 10 - 43

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 7 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК.5, ПК.3/НИ.

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

В 7 семестре обязательным этапом текущей аттестации является контрольная работа. Требования к выполнению контрольной работы, состав и правила оценки сформулированы в паспорте контрольной работы.

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

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.5, ПК.3/НИ, 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 автоматизированных систем управления
Кафедра вычислительной техники

Паспорт экзамена

по дисциплине «Защита информации», 7 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. 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 экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Защита информации»

---

1. Уровни обеспечения информационной безопасности в автоматизированных системах.
2. Построение парольных систем защиты от несанкционированного доступа к информации.

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, в ответах допускает принципиальные ошибки, оценка составляет до10 *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, в ответах допускает непринципиальные ошибки, например, вычислительные, оценка составляет *11-20 баллов.*
- Ответ на экзаменационный 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, в ответах не допускает ошибок, оценка составляет *21 -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, в ответах не допускает ошибок, оценка составляет 31-40 *баллов.*

3. Шкала оценки

К экзамену допускаются студенты, набравшие не менее 40 баллов по результатам текущего рейтинга. Максимальное значение текущего рейтинга складывается: лабораторные работы до 40 баллов, КР - до 20 баллов

Итоговая оценка определяется: менее 50 баллов - неудовлетворительно; 50-72 (удовлетворительно), 73-87 (хорошо), 88-100 (отлично).

Таблица соответствия баллов, традиционной оценки и буквенной оценки ECTS :

Оценка ECTS	Диапазон баллов рейтинга	Оценка
A+	99-100	Отлично 88-100
A	93-98	
A-	90-92	
B+	88-89	
B	83-87	Хорошо 73-87
B-	80-82	
C+	78-79	
C	73-77	
C-	70-72	Удовлетворительно 50-72
D+	68-69	
D	62-67	
D-	60-62	
E	50-59	
FX	25-49	Неудовлетворительно
F	0-24	Без права пересдачи!

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 «Защита информации»

3. Понятие информационной безопасности и защиты информации.
4. Классификация угроз информационной безопасности автоматизированных систем. Примеры реализации различных видов угроз.
5. Уровни обеспечения информационной безопасности в автоматизированных системах.
6. Основные принципы обеспечения информационной безопасности
7. Понятие политики безопасности. Основные типы политики безопасности.

8. Сформулируйте достаточное условие гарантированного выполнения политики безопасности в компьютерной системе.
9. Математические модели безопасности. Сравнение моделей.
10. Какие факторы вызывают необходимость защиты информации в компьютерных системах обработки информации.
11. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.
12. Почему компьютерные сети более уязвимы с точки зрения защиты информации, чем изолированные системы?
13. Какими свойствами должна обладать защищенная система обработки информации?
14. Чем определяется надежность средств защиты компьютерных систем от не санкционированного доступа?
15. Назовите функции и концепцию диспетчера доступа.
16. Классы каналов несанкционированного получения информации.
17. Криптографические методы защиты. Требования к средствам криптографической защиты информации.
18. Методы защиты памяти автоматизированных систем.
19. Электронная цифровая подпись.
20. Сформулируйте концепцию изолированной программной среды.
21. Какие методы и средства применяются для защиты программ от изучения.
22. Каким образом осуществляется защита от разрушающих программных воздействий.
23. Каким образом осуществляется защита программ от изменения.
24. Каким образом осуществляется защита от разрушающих программных воздействий.
25. Каким образом осуществляется защита авторского права на программы.
26. Каким образом осуществляется контроль целостности программ.
27. Перечислите набор функций защищенной операционной системы.
28. Классы задач функций защиты,
29. Функции защиты информации. Стратегии защиты информации.
30. Перечислите основные способы и средства защиты информации.
31. Архитектура и требования к системам защиты информации.
32. Построение систем защиты от угрозы нарушения целостности информации.
33. Построение систем защиты от угрозы отказа доступа к информации.
34. Основные механизмы безопасности: средства и методы аутентификации в ОС, модели разграничения доступа, организация и использование средств аудита.

35. Администрирование ОС: основные задачи и принципы сопровождения системного ПО, управления безопасностью ОС.
36. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа.
37. Основные принципы обеспечения безопасности в INTERNET.
38. Основные проблемы информационной безопасности электронной почты.
39. Системы антивирусной защиты.
40. Назначение, основные компоненты и функции межсетевых экранов.
41. Средства обеспечения безопасности БД: средства идентификации и аутентификации объектов БД, языковые средства разграничения доступа, организация аудита в системах БД. Задачи и средства администратора безопасности БД.
42. Методы и средства обеспечения конфиденциальности и целостности баз данных.
43. Методология построения защищенных автоматизированных систем.
44. Назовите программно-аппаратные средства защиты информации в сетях передачи данных.
45. Построение парольных систем защиты от несанкционированного доступа к информации.
46. Система защиты информации в Российской Федерации.
47. Структура и состав системы нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
48. Правовой режим защиты государственной и коммерческой тайны.
49. Роль стандартов информационной безопасности. Перечислите известные Вам стандарты информационной безопасности и их разделы.
50. Назовите требования к процессу сертификации продукта информационных технологий.
51. Руководящие и нормативные документы ФСТЭК
52. Показатели защищенности средств вычислительно техники и автоматизированных систем от несанкционированного доступа согласно документам ФСТЭК
53. Критерии оценки безопасности компьютерных систем министерства обороны США (TCSEC). Классы защищенности компьютерных систем по TCSEC.
54. Европейские критерии безопасности информационных технологий.
55. Симметричные и асимметричные критоалгоритмы
56. Криптостойкость шифров и паролей
57. Состав и характеристики основных функций криптографических преобразований.
58. Криптографические алгоритмы, системы и протоколы

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автоматизированных систем управления
Кафедра вычислительной техники

Паспорт контрольной работы

по дисциплине «Защита информации», 7 семестр

1. Методика оценки

Контрольная работа выполняется письменно и проводится по темам:

1. Качественные и количественные характеристики стойкости пароля.
2. Методов и средства оценки уровня защищённости компьютерных систем.
3. Многоуровневая защита информации пользователя ПК (на примере выбранного типа файла) в среде MS Office.
4. Применение криптографических средств защиты сообщений электронной почты.
5. Организация системы защиты персональных данных в информационной системе.
6. Применение электронных подписей для обеспечения информационной безопасности программных приложений и файлов.
7. Защита базы данных в среде конкретной СУБД (по выбору студента).
8. Комплексным обеспечением информационной безопасности ОС (по выбору студента).
9. Обеспечение информационной безопасности Интернет-браузеров (по выбору студента).
10. Аудит сетевой защищённости информационно-вычислительной.
11. Проверка уровня сетевой защищённости информационно-вычислительной системы методом сканирования системы.
12. Политика информационной безопасности обеспечения коммерческой тайны на предприятии.
13. Организационно-управленческие мероприятий для обеспечения заданного (нормативного) уровня информационной безопасности КС
14. Лицензирование и сертификации в сфере защиты компьютерной информации.

2. Критерии оценки

Максимальное количество баллов 20 баллов.

Каждое задание контрольной работы оценивается в соответствии с приведенными ниже критериями.

- Контрольная работа считается **невыполненной,** если тема не раскрыта, содержит грубые ошибки и мало убедительное обоснование, без примеров. Оценка составляет **до 5** баллов.
- Работа выполнена на **пороговом** уровне, если части КР выполнены формально, в целом тема раскрыта не в полном объёме и с мало убедительным обоснованием, оценка составляет 5-10 баллов.
- Работа выполнена на **базовом** уровне, если части КР выполнены не формально, в целом тема раскрыта в полном объёме без ошибок и с убедительным обоснованием и комментариями, изложение четкое, содержимое актуально, оценка составляет 11-15 баллов

- Работа считается выполненной **на продвинутом** уровне, если КР выполнено творчески и оригинально, в тема раскрыта в полном объёме без ошибок и с убедительным обоснованием и иллюстрациями на современном материале, оценка составляет 16-20 баллов.

3. Шкала оценки

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

Максимальное значение текущего рейтинга складывается: лабораторные работы до 40 баллов, КР - до 20 баллов.

Итоговая экзаменационная оценка определяется: менее 50 баллов - неудовлетворительно; 50-72 (удовлетворительно), 73-87 (хорошо), 88-100 (отлично).

4. Пример варианта контрольной работы

Обеспечение информационной безопасности Интернет-браузеров (по выбору студента).

1. Основные защитные функции обозревателей
2. Обеспечение конфиденциальности и повышение безопасности личных данных пользователя.
3. Применение протоколов информационной безопасности.
4. Обнаружение и блокирование подозрительных и известных поддельных веб-узлов.
5. Защита от мошенничества.
6. Безопасное блокирование содержимого.
7. Управление и контроль безопасности браузера.