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

Кафедра вычислительной техники
Кафедра автоматизированных систем управления
Кафедра автоматики

“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 5, семестры : 8 9

Факультет автоматики и вычислительной техники, заочная форма обучения

		Семестр	
№	**Вид деятельности**	**8**	**9**
1	Всего зачетных единиц (кредитов)	0	4
2	Всего часов	0	144
3	Всего занятий в контактной форме, час.	2	28
4	Лекции, час.	2	4
5	Практические занятия, час.	0	0
6	Лабораторные занятия, час.	0	8
7	из них в активной и интерактивной форме, час.	2	0
8	Аттестация, час.	0	2
9	Консультации, час.		14
10	Самостоятельная работа, час.	0	114
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, по выбору студента

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
АВТ, протокол заседания кафедры №10/1 от 20.06.2017

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

Программу разработал:

доцент, к.т.н. Якименко А. А.

Заведующий кафедрой:

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

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	
ПК.3.у4 уметь обосновывать принимаемые проектные решения	
1.уметь обосновывать принимаемые проектные решения	Лекции; Самостоятельная работа
ПК.3.у9 владеть методами оценки трудоемкости программного проекта	
2.владеть методами оценки трудоемкости программного проекта	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.5.з5 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; Самостоятельная работа
ОПК.5.у12 уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	
4.уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	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	
5.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	
6.владеть персональным компьютером как средством управления информацией	Лабораторные работы; 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: Информационная безопасность				
1. Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Современное состояние информационной безопасности.	2	2	1, 2, 3, 4	Треннинг-семинар. Дискуссия.
Семестр: 9				
Дидактическая единица: Проблемы защиты информации				
2. Проблемы защиты информации	0	4	3, 4, 5	

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 9				
Дидактическая единица: Проблемы защиты информации				
1. Проблемы защиты информации. Криптографические методы защиты информации.	0	2	2, 5, 6	Студентами должен быть сделан выбор одного из предложенных методов криптографического шифрования и реализован под консоль.
2. Основные пути обеспечения безопасности информации. Аутентификация. Электронная цифровая подпись.	0	2	4, 6	Генерация открытых и закрытых ключей, подписание сообщений и анализ полученных результатов.
3. Использование биометрического сканера для идентификации пользователей.	0	2	4, 5	Создание ПО для идентификации пользователя по отпечатку пальца.
4. Идентификация личности по образцу голоса	0	2	4, 6	Создание ПО для идентификации по образцу голоса.

Таблица 3.3

Темы для самостоятельного изучения	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 9				
Дидактическая единица: Проблемы защиты информации				
1. Криптографические методы защиты информации	0	32	3, 4, 5	Самостоятельное изучение литературы.
2. Антивирусное программное обеспечение	0	22	3, 4, 5	Самостоятельное изучение литературы
3. Компьютерная стенография	0	0	3, 4, 5	Самостоятельное изучение литературы
3. Основные пути обеспечения безопасности информации в облачных средах	0	10	3, 4, 5	Самостоятельное изучение литературы
4. Основные пути обеспечения безопасности информации	0	20	1, 2, 3, 4, 5	Самостоятельное изучение литературы

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	Дополнительная учебная деятельность	3, 4, 5, 6	0	0
: 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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.			
2	Дополнительная учебная деятельность	3, 4, 5, 6	0	0
: Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана.			
3	Подготовка к аттестации	3, 4, 5, 6	0	0
: 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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.			
Семестр: 9				
1	Контрольные работы	3, 4, 5, 6	14	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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.			
2	Подготовка к занятиям	3, 4, 5, 6	4	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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.				
3	Дополнительная учебная деятельность	3, 4, 5, 6	0	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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.				
4	Подготовка к аттестации	3, 4, 5, 6	12	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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана.				
5	Самостоятельное изучение теоретического материала	1, 2, 3, 4, 5	86	2
Студент изучает темы, приведенные в таблице 3.3 : Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - Загл. с экрана. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983 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://courses.edu.nstu.ru/index.php?show=155&curs=896. - 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; Портал НГТУ; Среда электронного обучения НГТУ

Консультирование	e-mail; Портал НГТУ; Среда электронного обучения НГТУ
Контроль	e-mail; Портал НГТУ; Среда электронного обучения НГТУ
Размещение учебных материалов	Портал НГТУ; Среда электронного обучения НГТУ

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	
Дополнительная учебная деятельность:	
Семестр: 9	
Подготовка к занятиям:	
Самостоятельное изучение теоретического материала:	
Лекция:	
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. 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://courses.edu.nstu.ru/index.php?show=155&curs=896. - Загл. с экрана.

2. Иванов А. В. Техническая защита информации [Электронный ресурс] : электронный учебно-методический комплекс / А. В. Иванов, В. А. Трушин, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208799. - 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. Биометрические системы контроля и управления доступом. Ч. 1 : методические указания по курсу "Информационная безопасность" для магистрантов по направлению "Информатика и вычислительная техника" / Новосиб. гос. техн. ун-т ; [сост. В. В. Вихман]. - Новосибирск, 2012. - 44, [2] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000170983

8.2 Специализированное программное обеспечение

1 Office
2 Windows

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Сопровождение лекционного материала

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 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 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.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	Антивирусное программное обеспечение Компьютерная стенография Криптографические методы защиты информации Основные пути обеспечения безопасности информации Основные пути обеспечения безопасности информации в облачных средах Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Современное состояние информационной безопасности. Проблемы защиты информации	Контрольные работы, все разделы.	Экзамен, вопросы 1-27
ОПК.5	у5. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Использование биометрического сканера для идентификации пользователей. Основные пути обеспечения безопасности информации Основные пути обеспечения безопасности информации в облачных средах Проблемы защиты информации Проблемы защиты информации. Криптографические методы защиты информации.		Экзамен, вопросы 1-27
ОПК.5	у8. владеть персональным компьютером как средством управления информацией	Идентификация личности по образцу голоса Основные пути обеспечения безопасности информации. Аутентификация. Электронная цифровая подпись. Проблемы защиты информации. Криптографические методы защиты информации.		Экзамен, вопросы 1-27
ОПК.5	у12. уметь оценивать состояние и тенденции развития информационных технологий и информатики в современном обществе	Основные пути обеспечения безопасности информации Основные пути обеспечения безопасности информации. Аутентификация. Электронная цифровая подпись. Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Современное состояние информационной безопасности. Проблемы защиты информации		Экзамен, вопросы 1-27

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	Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Современное состояние информационной безопасности.		Экзамен, вопросы 1-27
ПК.3/НИ	у9. владеть методами оценки трудоемкости программного проекта	Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Современное состояние информационной безопасности.		Экзамен, вопросы 1-27

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 9 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 9 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 дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенции 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», 9 семестр

1. Методика оценки

Экзамен проводится в письменной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из нечетного диапазона вопросов, второй вопрос из четного диапазона вопросов (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 № 1
к экзамену по дисциплине «Защита информации»

Вопрос 1. Цель и задачи криптографии.
Вопрос 2. Алгоритм шифрования Эль Гамаля.

Утверждаю: зав. кафедрой ВТ _____, Якименко А.А.
(подпись)

(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *менее 50 баллов.*
- Ответ на экзаменационный билет (тест) 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 *от 50 до 70 баллов.*
- Ответ на экзаменационный билет (тест) 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 *от 71 до 90 баллов.*

- Ответ на экзаменационный билет (тест) 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 от 91 до 100 *баллов.*

3. Шкала оценки

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

4. Вопросы к экзамену по дисциплине «Защита информации»

Вопрос 1. Цель и задачи криптографии.
Вопрос 2. Алгоритм шифрования Эль Гамаля.
Вопрос 3. Система безопасности SQL Server. Группы и пользователи SQL Server.
Вопрос 4. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.
Вопрос 5. Алгоритм защиты БД Access.
Вопрос 6. Что такое хеш-функция и для чего она используется в подписи?
Вопрос 7. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
Вопрос 8. Понятие хранимых процедур и их достоинства. Создание хранимых процедур.
Вопрос 9. Чем отличается режим подписи и шифрования в системе RSA?
Вопрос 10. Шифр многоалфавитной замены и алгоритм его реализации.
Вопрос 11. Задачи и алгоритмы электронной подписи.
Вопрос 12. Уровни безопасности операционных систем.
Вопрос 13. Алгоритм шифрации двойным квадратом. Шифр Enigma.
Вопрос 14. Основные операторы, которые используются в хранимых процедурах. Определение и использование переменных.
Вопрос 15. Права доступа к объектам БД SQL Server. Операторы Grand и Revoke.
Вопрос 16. Алгоритм шифрования DES.
Вопрос 17. Объекты БД Access и права доступа к объектам. Понятие владельца объекта.
Вопрос 18. Для чего используется секретный и для чего - открытый ключ?
Вопрос 19. Алгоритм шифрования ГОСТ 28147-89.
Вопрос 20. Способы защиты информации в БД Access.
Вопрос 21. Опишите особенности реализации RSA в программе pgp.
Вопрос 22. Пользователи и группы в Windows NT. Защищаемые объекты Windows NT.
Вопрос 23. Объясните схему шифрования RSA.
Вопрос 24. Группы и пользователи БД Access . Файл рабочей группы.
Вопрос 25. Алгоритм шифрования RSA.
Вопрос 26. Задачи распределения ключей.
Вопрос 27. Принцип действия систем безопасности в Windows NT.

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», 9 семестр

1. Методика оценки

В рамках данной дисциплины студентам необходимо выполнить контрольную работу.
Для этого необходимо самостоятельно выбрать два алгоритма шифрования (симметричный и ассиметричный) и на языке программирования высшего уровня создать программу с интерфейсным окном (т.е. не консольный вариант!!!).

Обязательные требование:
1. В интерфейсном окне есть строка для ввода текстовой информации для шифрования
2. В интерфейсном окне есть строка для шифрованной информации
3. Наличие минимум двух кнопок "Шифровать", "Дешифровать"
4. Подсчет времени работы алгоритма.
Остальное (дизайн, кнопки по желанию).

Сдать необходимо программу и отчет к ней (ход работы). Важно! Оформление отчета согласно ГОСТ!

Примерное содержание отчета: (возможны дополнительные разделы)
Постановка задачи
Введение
1 Симметричные криптосистемы
1.1 Описание алгоритма шифрования
1.2 Блок-схема алгоритма шифрования
1.3 Текст программы
1.4 Результат работы программы
2 Асимметричные криптосистемы
2.1 Описание алгоритма шифрования
2.2 Блок-схема алгоритма шифрования
2.3 Текст программы
2.4 Результат работы программы
Заключение
Библиографический справочник

2. Критерии оценки

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

Контрольная работа считается **невыполненной,** если не реализовано ни одного алгоритма шифрования. Оценка составляет **менее 50** баллов.

Работа выполнена на **пороговом** уровне, если реализован и подробно описан один из алгоритмов. Оценка составляет **от 50 до 65** баллов.

Работа выполнена на **базовом** уровне, если реализованы и подробно описаны оба алгоритма. Оценка составляет **от 65 до 90** баллов.

Работа считается выполненной **на продвинутом** уровне, если реализованы оба алгоритма, отчет оформлен в соответствии ГОСТ, приведено сравнение производительности алгоритмов, сделан анализ и даны рекомендации к сфере применения. Оценка составляет **от 91 до 100** 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.

4. Пример варианта контрольной работы

Вариант 1.
А.Симметричный алгоритм: Стандарт для обработки информации в государственных учреждениях США DES (Data Encryption Standard).
Б. Ассиметричный алгоритм: алгоритм RSA (Rivest, Shamir, Adleman).