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

Кафедра вычислительной техники

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность и защита информации

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская программа: Прикладные информационные системы и технологии

Курс: 1, семестр : 1

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**1**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	44
4	Лекции, час.	18
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.	6
10	Самостоятельная работа, час.	64
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	Э

Новосибирск 2017

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

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

Место дисциплины в структуре учебного плана: Блок 1, вариативная

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

Рабочая программа обсуждена на заседании кафедры

ВТ, протокол заседания кафедры №6 от 20.06.2017

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.

Ответственный за образовательную программу:

доцент Якименко А. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОК.7 способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности; *в части следующих результатов обучения*:**
у1. осваивать новые программные средства для профессиональной деятельности
***Компетенция НГТУ*: ПК.20.В способность управлять средой функционирования объектов профессиональной деятельности; *в части следующих результатов обучения*:**
з1. методы и средства обеспечения информационной безопасности компьютерных систем
з2. правовые основы информационной безопасности и принципы защиты авторского права на программные продукты
у1. использовать специализированные программные средства при решении профессиональных задач

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
Информационная безопасность и защита информации	
ОК.7.у1 осваивать новые программные средства для профессиональной деятельности	
1.осваивать новые программные средства для профессиональной деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ПК.20.В.з1 методы и средства обеспечения информационной безопасности компьютерных систем	
2.методы и средства обеспечения информационной безопасности компьютерных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.20.В.з2 правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
3.правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Лекции; Самостоятельная работа
ПК.20.В.у1 использовать специализированные программные средства при решении профессиональных задач	
4.использовать специализированные программные средства при решении профессиональных задач	Лекции; 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: 1				
Дидактическая единица: Проблемы информационной безопасности				
1. Введение Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности.	0	2	2, 3	

2. Современное состояние информационной безопасности. Анализ компьютерных преступлений. Взлом парольной защиты ОС. Методы сбора сведений для вторжения в сеть. Модель нарушителя безопасности информации	4	4	1, 2, 4	Лекция в форме дискуссии.
3. Проблемы защиты информации. Способы НСД к информации через технические средства.Способы НСД к проводным линиям связи.Способы НСД к волоконно-оптическим линиям связи.Способы НСД к беспроводным линиям связи.Технология беспроводной связи Bluetooth. Контроль мобильных средств связи. Способы НСД с использованием побочных электромагнитных излучений и наводок. Способы НСД к компьютерам и сетевым ресурсам. Раскрытие и модификация и подмена трафика. Проблемы защиты сети от перехвата сообщений. Методы защиты от программных закладок.	0	4	2, 3, 4	
4. Антивирусное программное обеспечение. Классификация антивирусных программ. Программы-детекторы. Программы- доктора. Программы - ревизоры. Программы - фильтры. Профилактика вирусного заражения.	4	4	2, 3	Лекция в форме дискуссии.
5. Криптографические методы защиты информации.Основные положения и определения криптографии..Использование шифров и ключей. Шифрование в компьютерной сети. Аппаратное шифрование. Программное шифрование. Стандарт шифрования данных DES и его практическая реализация Отечественный стандарт шифрования данных ГОСТ 28147-89	0	4	2, 3	

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 1				
Дидактическая единица: Проблемы информационной безопасности				
1. Основные пути обеспечения безопасности информации.Политика безопасности информации.Требования к безопасности компьютерных сетей в РФ. Программы обнаружения сетевых атак.Парольная защита ОС.Идентификация по отпечатку пальца.Идентификация по кисти руки Идентификация по лицу Идентификация по глазу человека Идентификация по голосу	0	4	1, 2, 4	Выполнение заданий лабораторной работы
2. Криптографические методы защиты информации: Режим простой замены Режим гаммирования Криптографические ключи Способы генерации ключей Электронная почта Характеристика почтовой программы Реализация цифровой подписи Процедура проверки подписи	4	8	1, 2, 4	Метод проектов
3. Проектирование биометрической СКУД. Выбор аппаратного обеспечения СКУД. Разработка ПО идентификации пользователя	6	6	1, 4	Построение структурной схемы разрабатываемой СКУД. Анализ существующего на рынке ПО для разрабатываемой СКУД. Создать ПО с целью идентификации пользователя.

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 1				
1	РГЗ	1, 2, 3, 4	15	2
: Вихман В. В. Биометрические системы контроля и управления доступом в задачах защиты информации : учебно-методическое пособие / В. В. Вихман, А. А. Якименко ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 52, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232421				
2	Подготовка к занятиям	1, 2, 3, 4	34	2

: Вихман В. В. Биометрические системы контроля и управления доступом в задачах защиты информации : учебно-методическое пособие / В. В. Вихман, А. А. Якименко ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 52, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232421				
3	Дополнительная учебная деятельность	1, 2, 3, 4	5	0
: Вихман В. В. Биометрические системы контроля и управления доступом в задачах защиты информации : учебно-методическое пособие / В. В. Вихман, А. А. Якименко ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 52, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232421				
4	Подготовка к аттестации	1, 2, 3, 4	10	2
: Вихман В. В. Биометрические системы контроля и управления доступом в задачах защиты информации : учебно-методическое пособие / В. В. Вихман, А. А. Якименко ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 52, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232421				

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; Среда электронного обучения НГТУ
Контроль	e-mail; Среда электронного обучения НГТУ
Размещение учебных материалов	e-mail; 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: 1	
Подготовка к занятиям:	
Лабораторная:	40
РГЗ:	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	
		Защита РГЗ	Экзамен
ОК.7	у1. осваивать новые программные средства для профессиональной деятельности	+	+

	ПК.20.В з1. методы и средства обеспечения информационной безопасности компьютерных систем		+
	ПК.20.В з2. правовые основы информационной безопасности и принципы защиты авторского права на программные продукты		+
	ПК.20.В у1. использовать специализированные программные средства при решении профессиональных задач	+	+

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

7. Литература

Основная литература

1. Гультяева Т. А. Основы теории информации и криптографии : конспект лекций / Т. А. Гультяева; Новосиб. гос. техн. ун-т. - Новосибирск, 2010. - 86, [1] с. : ил.. - Режим доступа: http://www.ciu.nstu.ru/fulltext/textbooks/2010/gultyaeva.pdf

2. Башлы П. Н. Информационная безопасность : учебное пособие для образовательных учреждений среднего профессионального образования / П. Н. Башлы. - Ростов н/Д, 2006. - 253, [1] с. : ил., табл.

3. Громов Ю. Ю. Информационная безопасность : учеб / Ю. Ю. Громов. - Москва, 2014

4. 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

5. Якименко А. А. Внедрение биометрической идентификации в системы контроля и управления доступом : учебное пособие / А. А. Якименко, В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 46, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000233370

Дополнительная литература

1. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры : учебное пособие для вузов по специальностям группы "Информационная безопасность" / А. Ю. Зубов. - М., 2005. - 190, [1] с. : ил.

2. Защита программ и данных : учебное пособие для вузов по специальностям "Защищенные телекоммуникационные системы" [и др. / П. Ю. Белкин и др.]. - М., 1999. - 169 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. Вихман В. В. Биометрические системы контроля и управления доступом в задачах защиты информации : учебно-методическое пособие / В. В. Вихман, А. А. Якименко ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 52, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232421

8.2 Специализированное программное обеспечение

1 Microsoft Office

2 Операционная система 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 вычислительной техники

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская программа: Прикладные информационные системы и технологии

Новосибирск 2017

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

Обобщенная структура фонда оценочных средств по **дисциплине** Информационная безопасность и 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)**
ОК.7 способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности	у1. осваивать новые программные средства для профессиональной деятельности	Криптографические методы защиты информации: Режим простой замены Режим гаммирования Криптографические ключи Способы генерации ключей Электронная почта Характеристика почтовой программы Реализация цифровой подписи Процедура проверки подписи Основные пути обеспечения безопасности информации.Политика безопасности информации.Требования к безопасности компьютерных сетей в РФ. Программы обнаружения сетевых атак.Парольная защита ОС.Идентификация по отпечатку пальца.Идентификация по кисти руки Идентификация по лицу Идентификация по глазу человека Идентификация по голосу Проектирование биометрической СКУД. Выбор аппаратного обеспечения СКУД. Разработка ПО идентификации пользователя Современное состояние информационной безопасности. Анализ компьютерных преступлений. Взлом парольной защиты ОС. Методы сбора сведений для вторжения в сеть. Модель нарушителя безопасности информации	РГЗ, все разделы.	Экзамен, вопросы 1-25
ПК.20.В способность управлять средой функционирования объектов профессиональной деятельности	з1. методы и средства обеспечения информационной безопасности компьютерных систем	Антивирусное программное обеспечение. Классификация антивирусных программ. Программы-детекторы. Программы- доктора. Программы - ревизоры. Программы - фильтры. Профилактика вирусного заражения. Введение Предмет и задачи информационной безопасности. Эволюция		Экзамен, вопросы 1-25

		подходов к обеспечению информационной безопасности. Криптографические методы защиты информации: Режим простой замены Режим гаммирования Криптографические ключи Способы генерации ключей Электронная почта Характеристика почтовой программы Реализация цифровой подписи Процедура проверки подписи Криптографические методы защиты информации.Основные положения и определения криптографии..Использование шифров и ключей. Шифрование в компьютерной сети. Аппаратное шифрование. Программное шифрование. Стандарт шифрования данных DES и его практическая реализация Отечественный стандарт шифрования данных ГОСТ 28147-89 Основные пути обеспечения безопасности информации.Политика безопасности информации.Требования к безопасности компьютерных сетей в РФ. Программы обнаружения сетевых атак.Парольная защита ОС.Идентификация по отпечатку пальца.Идентификация по кисти руки Идентификация по лицу Идентификация по глазу человека Идентификация по голосу Проблемы защиты информации. Способы НСД к информации через технические средства.Способы НСД к проводным линиям связи.Способы НСД к волоконно-оптическим линиям связи.Способы НСД к беспроводным линиям связи.Технология беспроводной связи Bluetooth. Контроль мобильных средств связи. Способы НСД с использованием побочных электромагнитных излучений и наводок. Способы НСД к компьютерам и сетевым ресурсам. Раскрытие и модификация и подмена трафика. Проблемы защиты сети от перехвата сообщений. Методы защиты от программных закладок. Современное состояние		

		информационной безопасности. Анализ компьютерных преступлений. Взлом парольной защиты ОС. Методы сбора сведений для вторжения в сеть. Модель нарушителя безопасности информации		
ПК.20.В	з2. правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Антивирусное программное обеспечение. Классификация антивирусных программ. Программы-детекторы. Программы- доктора. Программы - ревизоры. Программы - фильтры. Профилактика вирусного заражения. Введение Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности. Криптографические методы защиты информации.Основные положения и определения криптографии..Использование шифров и ключей. Шифрование в компьютерной сети. Аппаратное шифрование. Программное шифрование. Стандарт шифрования данных DES и его практическая реализация Отечественный стандарт шифрования данных ГОСТ 28147-89 Проблемы защиты информации. Способы НСД к информации через технические средства.Способы НСД к проводным линиям связи.Способы НСД к волоконно-оптическим линиям связи.Способы НСД к беспроводным линиям связи.Технология беспроводной связи Bluetooth. Контроль мобильных средств связи. Способы НСД с использованием побочных электромагнитных излучений и наводок. Способы НСД к компьютерам и сетевым ресурсам. Раскрытие и модификация и подмена трафика. Проблемы защиты сети от перехвата сообщений. Методы защиты от программных закладок.		Экзамен, вопросы 1-25
ПК.20.В	у1. использовать специализированные программные средства при решении профессиональных задач	Криптографические методы защиты информации: Режим простой замены Режим гаммирования Криптографические ключи Способы генерации ключей Электронная почта Характеристика почтовой	РГЗ, все разделы.	Экзамен, вопросы 1-25

		программы Реализация цифровой подписи Процедура проверки подписи Основные пути обеспечения безопасности информации.Политика безопасности информации.Требования к безопасности компьютерных сетей в РФ. Программы обнаружения сетевых атак.Парольная защита ОС.Идентификация по отпечатку пальца.Идентификация по кисти руки Идентификация по лицу Идентификация по глазу человека Идентификация по голосу Проблемы защиты информации. Способы НСД к информации через технические средства.Способы НСД к проводным линиям связи.Способы НСД к волоконно-оптическим линиям связи.Способы НСД к беспроводным линиям связи.Технология беспроводной связи Bluetooth. Контроль мобильных средств связи. Способы НСД с использованием побочных электромагнитных излучений и наводок. Способы НСД к компьютерам и сетевым ресурсам. Раскрытие и модификация и подмена трафика. Проблемы защиты сети от перехвата сообщений. Методы защиты от программных закладок. Проектирование биометрической СКУД. Выбор аппаратного обеспечения СКУД. Разработка ПО идентификации пользователя Современное состояние информационной безопасности. Анализ компьютерных преступлений. Взлом парольной защиты ОС. Методы сбора сведений для вторжения в сеть. Модель нарушителя безопасности информации		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 1 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОК.7, ПК.20.В.

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

В 1 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

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

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

Общая характеристика уровней освоения компетенций.

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

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

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

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

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

Паспорт экзамена

по дисциплине «Информационная безопасность и защита информации», 1 семестр

1. Методика оценки

Экзамен проводится в письменной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона четных номеров вопросов, второй вопрос из диапазона нечетных номеров 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 «Информационная безопасность и защита информации»

1. Понятие «информация» с точки зрения безопасности.
2. Категории информации. Особенности.

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 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 65 баллов.*

- Ответ на экзаменационный билет 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 66 до 87 баллов.*
- Ответ на экзаменационный билет билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет от 88 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 «**Информационная безопасность и защита информации**»**

1. Понятие «информация» с точки зрения безопасности.
2. Категории информации. Особенности.
3. Понятие информационной безопасности.
4. Виды информации по категориям доступа.
5. Виды конфиденциальной информации.
6. Обобщенная модель технического канала утечки конфиденциальной информации.
7. Понятие угрозы. Виды угроз.
8. Понятие атаки.
9. Признаки классификации угроз безопасности.
10. Компьютерное преступление.
11. Категории нарушителей. Особенности.
12. Модель нарушителя безопасности информации.
13. Понятие НСД.
14. Способы ЕСД с использованием побочных электромагнитных излучений и наводок.
15. Способы НСД к проводным линиям связи.
16. Способы НСД к волоконно-оптическим линиям связи.
17. Способы НСД к беспроводным линиям связи.
18. Особенности перехвата информации передаваемой по радиоканалу.
19. Технология Bluetooth.
20. Контроль мобильных средств связи. Проблема безопасности при пользовании сотовым телефоном.
21. WAP-приложения.
22. Особенности определения текущего положения владельца мобильного телефона.
23. Биометрическая система идентификации. Показатели биометрических систем.
24. Способы НСД к компьютерам и сетевым ресурсам.
25. Основные группы формирования паролей для доступа к сети.

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

Паспорт
расчетно-графического задания (работы)

по дисциплине «Информационная безопасность и защита информации», 1 семестр

1. Методика оценки

Цель РГЗ - приобретение опыта изучения и применения основ криптографической защиты информации, алгоритмов электронной цифровой подписи в системах защиты информации, оценки качества функционирования защищенных информационных систем.

Тематика РГЗ. Тема индивидуального задания выбирается магистрантов как из предложенного преподавателем списка прикладных задач из их сферы профессиональной деятельности, так и в порядке личной инициативы. Содержание индивидуального РГЗ определяется по результатам собеседования преподавателя и магистранта в начале учебного семестра.

Содержание работы:

1. Знакомство с литературой по выбранной теме;
2. Постановка прикладной задачи в определенной предметной области;
3. Определение целей и задач в данной теме;
4. Разработка структуры защищенной информационной системы;
5. Разработка интерфейса защищенной информационной системы
6. Выбор и реализация алгоритмов криптографической защиты информации;
7. Выбор и реализация алгоритмов электронной цифровой подписи в системах защиты информации;
8. Написание отчета о проделанной работе.

Требования к оформлению отчета

Отчет предоставляется на листах формата А4, объемом до 20 страниц. Содержание отчета: введение; задание; краткое описание выбранных алгоритмов; структурная схема защищенной системы; реализация защищенной системы; заключение.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р). Оценка составляет менее 50 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально, присутствует большой объем заимствованного текста, работа оформлена не по ГОСТ. Оценка составляет от 50 до 65 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 от 66 до 90 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 от 91 до 100 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)

В качестве задания на РГЗ(Р) студенту предлагается выбрать предприятие, под задачи которого разрабатывается защищенная информационная система.