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

Кафедра теоретической и прикладной информатики

“УТВЕРЖДАЮ”
ДЕКАН ФПМИ
д.т.н. Тимофеев В. С.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность

Образовательная программа: 02.03.03 Математическое обеспечение и администрирование информационных систем, профиль: Математическое и программное обеспечение информационных технологий

Курс: 4, семестр : 8

Факультет прикладной математики и информатики,

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	49
4	Лекции, час.	20
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	20
7	из них в активной и интерактивной форме, час.	16
8	Аттестация, час.	2
9	Консультации, час.	7
10	Самостоятельная работа, час.	59
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 02.03.03 Математическое обеспечение и администрирование информационных систем

ФГОС введен в действие приказом №222 от 12.03.2015 г. , дата утверждения: 07.04.2015 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 02.03.03 Математическое обеспечение и администрирование информационных систем

Рабочая программа обсуждена на заседании кафедры

ТПИ, протокол заседания кафедры №4 от 20.06.2017

Утверждена на совете факультета прикладной математики и информатики, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Гультяева Т. А.

Заведующий кафедрой:

доцент, д.т.н. Чубич В. М.

Ответственный за образовательную программу:

заведующий кафедрой Чубич В. М.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.1 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*:**
з1. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты
***Компетенция ФГОС*: ОПК.3 готовность анализировать проблемы и направления развития технологий программирования; *в части следующих результатов обучения*:**
з4. Знать основные методологические положения защиты информации
***Компетенция ФГОС*: ПК.7 владение знаниями о содержании, основных этапов и тенденций развития программирования, математического обеспечения и информационных технологий; *в части следующих результатов обучения*:**
з3. Знать основные программно-аппаратные средства защиты компьютеров и программ
***Компетенция НГТУ*: ПК.11.В/П способность формировать суждения о проблемах современной информатики; *в части следующих результатов обучения*:**
з2. Знать основные системы защиты информации в России и в ведущих зарубежных странах

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	
ОПК.3.з4 Знать основные методологические положения защиты информации	
1.Основных понятиях информационной безопасности	Лекции; Лабораторные работы; Самостоятельная работа
2.о теоретических и практических основах симметричной криптографии	Лекции; Самостоятельная работа
ОПК.1.з1 знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	
3.вопросы административного и организационно-правового обеспечения защиты информации,	Лекции; Самостоятельная работа
ПК.11.В/П.з2 Знать основные системы защиты информации в России и в ведущих зарубежных странах	
4.основные системы защиты информации в России и в ведущих зарубежных странах	Лекции; Самостоятельная работа
ОПК.3.з4 Знать основные методологические положения защиты информации	
5.основные методологические положения защиты информации,	Лекции; Лабораторные работы; Самостоятельная работа
ПК.7.з3 Знать основные программно-аппаратные средства защиты компьютеров и программ	
6.основные программно-аппаратные средства защиты компьютеров и программ	Лабораторные работы; Самостоятельная работа
7.общие вопросы обеспечения информационной безопасности при работе в сети,	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.3.з4 Знать основные методологические положения защиты информации	
8.разрабатывать программные приложения для решения поставленных задач в области криптографии	Лабораторные работы; Самостоятельная работа
9.реализовывать симметричные алгоритмы шифрования	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: Основы информационной безопасности				
1. Основные аспекты информационной безопасности	0	4	1	Изучение основных понятияонятий информационной безопасности. Характеристики информации. Основные составляющие информационной безопасности. Задачи информационной безопасности. Угрозы безопасности. Основные определения. Классификация угроз. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности
2. Основы государственной информационно политики и информационной безопасности РФ	0	4	1, 3, 4	Изучение основ законодательного уровня информационной безопасности. Обзор российского законодательства Международные стандарты и спецификации. "Оранжевая книг. Рекомендации Х.800. "Общие критерии. Гармонизированные критерии Европейских стран
Дидактическая единица: Угрозы информационной безопасности				
3. Угрозы информационной безопасности и методы их реализации	0	3	1, 4, 5, 7	Изучение основных угрозы безопасности. Классификация угроз. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности
Дидактическая единица: Обеспечение информационной безопасности				

4. Методы и средства обеспечения информационной безопасности информационных систем	0	3	1, 2, 5, 7	Изучение административного уровеня информационной безопасности. Политика безопасности. Верхний уровень детализации. Средний уровень детализации. Нижний уровень детализации. Программа безопасности. Верхний уровень. Нижний уровень. Процедурный уровень информационной безопасности. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Программно-технический уровень информационной безопасности. Сервисы безопасности. Идентификация и аутентификация. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos. Биометрическая аутентификация. Управление доступом. Основные понятия. Матрица доступа (списки доступа). Ролевое управление доступом. Протоколирование и аудит. Экранирование. Обзор методов криптографии. Методы классической криптографии. Симметричные методы криптографии. Асимметричные методы криптографии. Хэш-функции. Электронная цифровая подпись. Криптографичес
Дидактическая единица: Практические аспекты реализация информационной безопасности				
5. Использование защищенных компьютерных систем	0	3	1, 5, 7	Изучение способов защиты программного обеспечения: регистрационные коды, привязка к носителям информации, аппаратные ключи, протекторы.

6. Защита от разрушающих программных воздействий.	0	3	1, 5, 7	Изучение основ проектирования защищённых приложений. От чего защищают программы. Обзор моделей распространения программного обеспечения. Методы противодействия атакам на приложения. Переполнение буфера. SQL-инъекции. Ошибки канонизации. Межсайтовое кодирование. Минимизация привилегий. Осмысленные имена функций. Проверка входных данных. Сообщения об ошибках. Отказ в обслуживании. Способы защиты программного обеспечения от несанкционированного тиражирования. Регистрационные коды. Привязка к носителям информации. Аппаратные ключи. Протекторы. Избыточная защита приложений. Критерии сравнения средств защиты приложений. Причины ослабления защиты. Нарушения информационной безопасности. Нарушители. Причины появления хакеров. Методика вторжения. Защита паролей . Стратегия выбора пароля. Обнаружение нарушителей. Вредоносные программы. Классификация вредоносных программ. Природа вируса. Антивирусная защита

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 8				
Дидактическая единица: Практические аспекты реализация информационной безопасности				
1. Криптографические хэш-функции. Часть 1.	2	3	6, 7, 8	Изучение существующих алгоритмов вычисления дайджестов сообщений и написания программы, реализующей заданный алгоритм хэширования

2. Криптографические хэш-функции. Часть 2.	3	3	6, 7, 8	Изучение существующих алгоритмов вычисления дайджестов сообщений и написания программы, реализующей заданный алгоритм хэширования
3. Генерация криптографически безопасной псевдослучайной последовательности. Часть 1.	2	3	5, 6, 7, 9	Изучение алгоритма и получение навыка генерации криптографически безопасной псевдослучайной последовательности. Научиться тестировать полученную последовательность на равномерность и случайность.
4. Генерация криптографически безопасной псевдослучайной последовательности. Часть 2.	3	3	5, 6, 7, 9	Изучение алгоритма и получение навыка генерации криптографически безопасной псевдослучайной последовательности. Научиться тестировать полученную последовательность на равномерность и случайность.
5. Криптографические библиотеки	3	4	1, 5, 6, 7, 9	Ознакомление с существующими криптографическими библиотеками. Научиться использовать сторонние криптографические библиотеки при разработке собственных приложений.
6. Ролевое управление доступом. Разработка защищённых приложений.	3	4	5, 6, 7, 9	Ознакомление с концепцией ролевого управления доступом и способами защиты программного обеспечения от существующих угроз. Научиться разрабатывать приложения, которые используют ролевое управление доступом для разграничения полномочий пользователей. Получение навыков защиты разработанной программы от несанкционированного копирования и других угроз, которым может подвергаться программное обеспечение.

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	РГЗ	8	10	2

Проектирование и разработка программного приложения: Гультяева Т. А. Расчетно-графическая работа по курсу "Информационная безопасность" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688072.doc. - Загл. с экрана. Гультяева Т. А. Информационная безопасность [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234868. - Загл. с экрана.				
2	Подготовка к занятиям	1, 2, 3, 4, 5, 6, 7, 9	40	3
Проработка лекционного материала, подготовка к лабораторным работам: Информационная безопасность : методические указания к выполнению лабораторных работ для 4 курса ФПМИ абразовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль - Математическое и программное обеспечение информационных технологий / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 59 с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235034 Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21369_1325681756.pdf. - Загл. с экрана. Гультяева Т. А. Информационная безопасность [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234868. - Загл. с экрана.				
3	Подготовка к аттестации	1, 2, 3, 4, 5, 6, 7	9	2
Консультации с преподавателем, подробная информация приведена в приложениях №1 №2 : Информационная безопасность : методические указания к выполнению лабораторных работ для 4 курса ФПМИ абразовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль - Математическое и программное обеспечение информационных технологий / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 59 с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235034 Гультяева Т. А. Расчетно-графическая работа по курсу "Информационная безопасность" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688072.doc. - Загл. с экрана. Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21369_1325681756.pdf. - Загл. с экрана. Гультяева Т. А. Информационная безопасность [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234868. - 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	Личный типовой сайт:http://ami.nstu.ru/~gultyaeva/
Консультирование	e-mail:t.gultyaeva@corp.nstu.ru
Размещение учебных материалов	Личный типовой сайт:http://ami.nstu.ru/~gultyaeva/

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм	Коды формируемых компетенций
1	Метод проектов	ОПК.3; ПК.7;
Формируемые умения: з3. Знать основные программно-аппаратные средства защиты компьютеров и программ; з4. Знать основные методологические положения защиты информации		
Краткое описание применения: Выполненнение лабораторной работы является проектом для студента.		

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 8		
Лабораторная:	30	60
Контролирующие материалы (список вопросов) приводятся в "Информационная безопасность : методические указания к выполнению лабораторных работ для 4 курса ФПМИ абразовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль - Математическое и программное обеспечение информационных технологий / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 59 с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235034"		
РГЗ:	10	20
Контролирующие материалы (Защита в виде обсуждения) приводятся в "Гультяева Т. А. Расчетно-графическая работа по курсу "Информационная безопасность" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688072.doc. - Загл. с экрана."		
Зачет:	10	20
Контролирующие материалы (список вопросов) приводятся в "Гультяева Т. А. Информационная безопасность [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234868. - Загл. с экрана."		

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Зачет
ОПК.1	з1. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты		+
ОПК.3	з4. Знать основные методологические положения защиты информации	+	+
ПК.7	з3. Знать основные программно-аппаратные средства защиты компьютеров и программ	+	+
	ПК.11.В/П з2. Знать основные системы защиты информации в России и в ведущих зарубежных странах		+

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

7. Литература

Основная литература

1. Нортроп Т. Основы разработки приложений на платформе Microsoft .NET Framework : экзамен-536 MCTS / Тони Нортроп, Шон Уилдермьюс, Билл Райан ; [пер. с англ. А. Е. Соловченко]. - М., 2007. - 842 с. : ил. + 1 CD-ROM.

2. Минин О. В. Информационная безопасность банковской деятельности : учебное пособие / О. В. Минин, И. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 39, [1] с.. - Режим доступа: http://www.ciu.nstu.ru/fulltext/textbooks/2009/minin.pdf

3. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб. : Лань, 2016. — 324 с. — Режим доступа: http://e.lanbook.com/book/75515 — Загл. с экрана.

4. Куприянов А. И. Основы защиты информации : [учебное пособие для вузов по специальностям "Радиоэлектронные системы", "Средства радиоэлектронной борьбы" и "Информационные системы и технологии"] / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М., 2007. - 253, [1] с. : ил.

Дополнительная литература

1. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие для вузов по специальности 510200 "Прикладная математика и информатика" / О. Р. Лапонина ; под ред. В. А. Сухомлина. - М., 2005. - 604, [1] с. : ил., табл.

2. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности : [учебное пособие для вузов по специальностям 090102 (075200) - "Компьютерная безопасность" и др.] / С. В. Запечников. - М., 2007. - 319 с. : ил.

3. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М., 2008. - 330, [1] с. : ил., табл.

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. Курлаев С. А. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие / А. С. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21369_1325681756.pdf. - Загл. с экрана.

2. Гультяева Т. А. Расчетно-графическая работа по курсу "Информационная безопасность" [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://ciu.nstu.ru/fulltext/unofficial/2012/lib_21805_1326688072.doc. - Загл. с экрана.

3. Гультяева Т. А. Информационная безопасность [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234868. - Загл. с экрана.
4. Информационная безопасность : методические указания к выполнению лабораторных работ для 4 курса ФПМИ абразовательной программы 02.03.03 - Математическое обеспечение и администрирование информационных систем, профиль - Математическое и программное обеспечение информационных технологий / Новосиб. гос. техн. ун-т ; [сост.: Т. А. Гультяева, С. А. Курлаев]. - Новосибирск, 2017. - 59 с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235034

8.2 Специализированное программное обеспечение

1 MathType
2 Microsoft Office
3 Visual Studio

9. Материально-техническое обеспечение

Презентационное оборудование

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

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Используется для выполнения студентами лабораторных работ

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

Кафедра теоретической и прикладной информатики

“УТВЕРЖДАЮ”
ДЕКАН ФПМИ
д.т.н., доцент В.С. Тимофеев
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Образовательная программа: 02.03.03 Математическое обеспечение и администрирование информационных систем, профиль: Математическое и программное обеспечение информационных технологий

Новосибирск 2015

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

Обобщенная структура фонда оценочных средств по дисциплине Информационная безопасность 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.1 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	з1. знать правовые основы информационной безопасности и принципы защиты авторского права на программные продукты	Основы государственной информационно политики и информационной безопасности РФ		Зачет: вопросы 7, 8
ОПК.3 готовность анализировать проблемы и направления развития технологий программирования	з4. Знать основные методологические положения защиты информации	Генерация криптографически безопасной псевдослучайной последовательности. Часть 1. Генерация криптографически безопасной псевдослучайной последовательности. Часть 2. Защита от разрушающих программных воздействий. Использование защищенных компьютерных систем Криптографические библиотеки Криптографические хэш-функции. Часть 1. Криптографические хэш-функции. Часть 2. Методы и средства обеспечения информационной безопасности информационных систем Основные аспекты информационной безопасности Основы государственной информационно политики и информационной безопасности РФ Ролевое управление доступом. Разработка защищённых приложений. Угрозы информационной безопасности и методы их реализации	РГЗ	Зачет: вопросы 1-4, 9-50
ПК.11.В/П способность формировать суждения о	з2. Знать основные системы защиты информации в России и в ведущих	Основы государственной информационно политики и информационной безопасности РФ Угрозы		Зачет: вопросы 5,6

проблемах современной информатики	зарубежных странах	информационной безопасности и методы их реализации		
ПК.7/П владение знаниями о содержании, основных этапов и тенденций развития программирования, математического обеспечения и информационных технологий	з3. Знать основные программно-аппаратные средства защиты компьютеров и программ	Генерация криптографически безопасной псевдослучайной последовательности. Часть 1. Генерация криптографически безопасной псевдослучайной последовательности. Часть 2. Защита от разрушающих программных воздействий. Использование защищенных компьютерных систем Криптографические библиотеки Криптографические хэш-функции. Часть 1. Криптографические хэш-функции. Часть 2. Методы и средства обеспечения информационной безопасности информационных систем Ролевое управление доступом. Разработка защищённых приложений. Угрозы информационной безопасности и методы их реализации	РГЗ	Зачет: вопросы 1-4, 9-50

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 8 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ОПК.1, ОПК.3, ПК.11.В/П, ПК.7/П.

Зачет проводится в письменной форме, по билетам .

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

В 8 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

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

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.1, ОПК.3, ПК.11.В/П, ПК.7/П, 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 теоретической и прикладной информатики

Паспорт зачета

по дисциплине «Информационная безопасность», 8 семестр

1. Методика оценки

Зачет проводится в письменной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-25, второй вопрос из диапазона вопросов 26-50 (список вопросов приведен ниже). В ходе зачета преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФПМИ

Билет № __1__
к зачету по дисциплине «Информационная безопасность»

1
1. Законодательный уровень информационной безопасности. Законодательство РФ.

2. Методика вторжения и защита паролей.

Утверждаю: зав. кафедрой ____ _____ д.т.н., профессор, Чубич В.М.
(подпись)
(дата)

2. **Критерии оценки**

- Ответ на билет для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *от 0 до 9 баллов.*
- Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет *от 10 до 13 баллов.*
- Ответ на билет для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику

процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *от 14 до 18 баллов.*

- Ответ на билет для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет *от 19 до 20 баллов.*

3. Шкала оценки

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

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 10 баллов (из 20 возможных).

4. **Вопросы к** зачету **по дисциплине «**Информационная безопасность**»**

1. Понятие информационной безопасности.
2. Характеристики информации.
3. Основные составляющие информационной безопасности.
4. Задачи информационной безопасности.
5. Угрозы безопасности.
6. Уровни информационной безопасности.
7. Законодательный уровень информационной безопасности. Законодательство РФ.
8. Законодательный уровень информационной безопасности. Международные стандарты и спецификации.
9. Административный уровень информационной безопасности. Политика безопасности.
10. Административный уровень информационной безопасности. Программа безопасности.
11. Процедурный уровень информационной безопасности.
12. Программно-технический уровень информационной безопасности.
13. Сервисы безопасности. Идентификация и аутентификация: основные понятия, парольная аутентификация.
14. Сервисы безопасности. Идентификация и аутентификация: одноразовые пароли, сервер аутентификации Kerberos.
15. Сервисы безопасности. Управление доступом.
16. Сервисы безопасности. Протоколирование и аудит.
17. Сервисы безопасности. Экранирование.
18. Обзор методов криптографии. Методы классической криптографии.
19. Симметричные методы криптографии.
20. Асимметричные методы криптографии.
21. Хэш-функции.
22. Электронная цифровая подпись.
23. Криптографические генераторы псевдослучайных чисел.
24. Проблемы, которые могут возникать при применении криптоалгоритмов и протоколов.
25. Стеганографическая защита информации. Основные понятия.
26. Зашита от несанкционированного тиражирования программ в исходных кодах.
27. От чего защищают программы?

28. Обзор моделей распространения программного обеспечения.
29. Атака типа «Переполнение буфера».
30. Атака типа «SQL-инъекция».
31. Атака, эксплуатирующая ошибки канонизации.
32. Атака типа «XSS» (межсайтовое кодирование).
33. Принцип минимизация привилегий.
34. Влияние осмысленных имён функций на защищённость программы.
35. Проверка входных данных как метод противодействия атакам на приложения.
36. Влияние сообщений об ошибках на защищённость программы.
37. Атака типа «Отказ в обслуживании».
38. Способы защиты программного обеспечения: Регистрационные коды.
39. Способы защиты программного обеспечения: Привязка к носителям информации.
40. Способы защиты программного обеспечения: Аппаратные ключи.
41. Способы защиты программного обеспечения: Протекторы.
42. Критерии сравнения средств защиты приложений.
43. Причины ослабления защиты программных продуктов.
44. Нарушители информационной безопасности. Причины появления хакеров.
45. Методика вторжения и защита паролей.
46. Стратегия выбора пароля.
47. Обнаружение нарушителей.
48. Классификация вредоносных программ.
49. Природа и типы вирусов.
50. Антивирусная защита.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра теоретической и прикладной информатики

Паспорт
расчетно-графического задания (работы)

по дисциплине «Информационная безопасность», 8 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны реализовать защищенное от нелегальной установки программное приложение.

При выполнении расчетно-графического задания (работы) студенты должны выбрать модель распространения программы (на выбор): Demoware, Trialware или Nagware. Для регистрации программы реализовать проверку введения регистрационного кода. Реализовать метод проверки регистрационного кода (на выбор): 1) алгоритмический, основанный на принципе "чёрного ящика"; 2) алгоритмический, основанный на математически сложной проблеме; 3) табличный. При необходимости в нужных местах следует применять шифрование. Алгоритм шифрования - на выбор в зависимости от шифруемых данных.

Обязательные структурные части РГЗ.

Обоснование выбора модель распространения программы
Обоснование выбора метода проверки регистрационного кода
Обоснование применения шифрование.
Код программы
Тестирование
Отчет
Демонстрация работы программы

Оцениваемые позиции:

Качество реализации модели распространения - Demoware, Trialware или Nagware.
Как создаётся и проверяется регистрационный код.
Наличие в исполняемом файле осмысленных имён функций.
Когда проверяется корректность введённых регистрационных данных и когда об этом сообщается пользователю.
Используется ли регистрационная информация в "жизненно важных" частях программы.
Шифрование секретных данных.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, диагностические признаки не обоснованы, программные средства не выбраны или не соответствуют современным требованиям, оценка составляет *от 0 до 9* баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, программные средства не соответствуют современным требованиям, оценка составляет *от 10 до 13* баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны ,но не оптимизированы, программные средства выбраны без достаточного обоснования, оценка составляет *от 14 до 18* баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен

в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны и оптимизированы, выбор программных средств обоснован, оценка составляет *от 19 до 20* 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)

1. Калькулятор. Секретная информация: хранящаяся в файле история вычислений, которую в открытом виде можно посмотреть только с помощью калькулятора.
2. Часы с функцией будильника. При срабатывании будильника звучит сигнал и выдаётся окно с сообщением. Сообщение можно задавать при заводе будильника. После срабатывания будильника сообщение добавляется в историю сообщений. Секретные данные: все хранящиеся в истории сообщения.
3. Блокнот, создающий зашифрованный файл. Секретная информация: ключи, используемые для расшифровывания ранее созданных файлов. Ключи можно хранить в некотором файле, ставящем в соответствие каждому созданному файлу ключ.
4. Файловый менеджер. Секретная информация: данные о каталогах, которые были открыты в панелях менеджера при его последнем закрытии.
5. Браузер. Секретная информация: история посещения адресов.
6. Программа учёта домашних финансов (Домашняя бухгалтерия). Секретная информация: все хранящиеся данные о доходах и расходах.
7. Адресно-телефонная книга. Секретная информация: телефоны людей.
8. Органайзер с напоминанием о событиях. Секретная информация: описание события.
9. Домашняя библиотека (каталог книг). Секретная информация: названия книг.
10. Решатель квадратных уравнений. Секретная информация: хранящаяся в файле история решения уравнений, которую в открытом виде можно посмотреть только с помощью решателя.

Примечание: можно использовать другую задачу для написания приложения, если она не проще заданного варианта и согласована с преподавателем.