

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

Кафедра автоматизированных систем управления
Кафедра вычислительной техники

“УТВЕРЖДАЮ”
ДЕКАН АВТФ

к.т.н. Рева И. Л.

“ ____ ” _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность

Образовательная программа: 09.04.03 Прикладная информатика, магистерская программа:
Информационные технологии в моделировании и организации бизнес-процессов

Курс: 2, семестр : 3

Факультет автоматики и вычислительной техники,

		Семестр
№	Вид деятельности	3
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	30
4	Лекции, час.	10
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	10
7	из них в активной и интерактивной форме, час.	20
8	Аттестация, час.	2
9	Консультации, час.	8
10	Самостоятельная работа, час.	78
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	3

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 09.04.03 Прикладная информатика

ФГОС введен в действие приказом №1404 от 30.10.2014 г. , дата утверждения: 28.11.2014 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 09.04.03 Прикладная информатика

Рабочая программа обсуждена на заседании кафедры

АСУ, протокол заседания кафедры №7 от 20.06.2017

ВТ, протокол заседания кафедры №6 от 20.06.2017

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

Программу разработал:

старший преподаватель, Денисов В. В.

Заведующий кафедрой:

профессор, д.т.н. Гриф М. Г.

доцент, к.т.н. Якименко А. А.

Ответственный за образовательную программу:

профессор Мезенцев Ю. А.

1. Внешние требования

Таблица 1.1

Компетенция ФГОС: ОПК.6 способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры; в части следующих результатов обучения:	
31. знать правовые основы информационной безопасности и принципы защиты	
у1. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	
Компетенция ФГОС: ПК.5 способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций; в части следующих результатов обучения:	
32. знать основные принципы разработки систем защиты в информационных системах	
33. знать структуру проектных затрат и методы практической оценки рисков, оценивать размер ущерба от возможного нарушения информационной безопасности	

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	
ПК.5.32 знать основные принципы разработки систем защиты в информационных системах	
1. знать основные принципы разработки систем защиты в информационных системах	Лекции; Лабораторные работы; Самостоятельная работа
ПК.5.33 знать структуру проектных затрат и методы практической оценки рисков, оценивать размер ущерба от возможного нарушения информационной безопасности	
2. знать структуру проектных затрат и методы практической оценки рисков, оценивать размер ущерба от возможного нарушения информационной безопасности	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.6.31 знать правовые основы информационной безопасности и принципы защиты	
3. знать правовые основы информационной безопасности и принципы защиты	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.6.у1 уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	
4. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	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: 3				
Дидактическая единица: Методы защиты информации				
1. Технология защиты информации. Термины и определения.	2	2	1	Конспектирование
Дидактическая единица: Организационно-правовое обеспечение				

2. Организационно-правовое обеспечение защиты информации.	2	2	2	Конспектирование
Дидактическая единица: Методы защиты информации				
3. Методы защиты информации. Средства защиты и их классификация.	4	4	4	Конспектирование
Дидактическая единица: Технология защиты: что, от чего, как защищаем ?				
4. Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности	0	2	2, 3, 4	Конспектирование

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 3				
Дидактическая единица: Информационные элементы и технические объекты				
1. Инвентаризация информационных систем.	2	2	1	Выполнение индивидуальных заданий по инвентаризации потоков данных
2. Классификация данных по доступности, целостности, конфиденциальности	1	2	2	Выполнение индивидуального задания
Дидактическая единица: Организационно-правовое обеспечение				
3. Защита персональных данных, ФЗ-152	1	2	3	Выполнение индивидуальных заданий
Дидактическая единица: Технология защиты: что, от чего, как защищаем ?				
4. Выявление вредоносных воздействий на информационную систему	4	2	2	Индивидуальное задание по исследованию каналов утечки
Дидактическая единица: Методы защиты информации				
5. Инвентаризация средств защиты, классификация защитных функций	4	2	1, 2, 3, 4	Инвентаризация средств защиты, классификация защитных функций

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 3				
1	РГЗ	1, 2, 3, 4	10	4
Анализ состояния защиты данных в информационной системе, подробная информация приведена в приложении №3 : Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050				
2	Подготовка к занятиям	1, 2, 3, 4	24	1
Выполнение индивидуальных заданий, подробная информация приведена в приложениях №1 №2 : Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050				
3	Дополнительная учебная деятельность	1, 2, 3, 4	34	1

Выявление угроз и уязвимостей, подробная информация приведена в приложениях №1 №2 : Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050

4	Подготовка к аттестации	1, 2, 3, 4	10	2
---	-------------------------	------------	----	---

Подготовка к зачету, подробная информация приведена в приложении №2 : Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050

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
Консультирование	e-mail; Портал НГТУ
Контроль	e-mail; Портал НГТУ; 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 выставять 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: 3		
<i>Лекция:</i>	0	10
Контролирующие материалы (Конспект лекций) приводятся в "Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000173944 . - Загл. с экрана."		
<i>Лабораторная:</i>	16	34
Контролирующие материалы (список вопросов) приводятся в "Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176937 . - Загл. с экрана."		
<i>РГЗ:</i>	18	36
Контролирующие материалы (список вопросов) приводятся в "Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050 "		
<i>Зачет:</i>	10	20
Контролирующие материалы (тесты) приводятся в "Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050 "		

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 ЛР	Защита РГЗ	Зачет
ОПК.6	з1. знать правовые основы информационной безопасности и принципы защиты	+	+	+
	у1. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	+	+	+
ПК.5	з2. знать основные принципы разработки систем защиты в информационных системах	+	+	+
	з3. знать структуру проектных затрат и методы практической оценки рисков, оценивать размер ущерба от возможного нарушения информационной безопасности	+	+	+

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

7. Литература

Основная литература

1. Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000173944. - Загл. с экрана.
2. Денисов В. В. Информационные технологии в управлении качеством и защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176927. - Загл. с экрана.
3. Хворостов В. А. Безопасность веб-приложений [Электронный ресурс] : конспект лекций / В. А. Хворостов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2013]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000180050. - Загл. с экрана.
4. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 с.— Режим доступа: <http://www.iprbookshop.ru/52160.html>.— ЭБС «IPRbooks»
5. Денисов В. В. Защита информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Денисов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2012]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000176937. - Загл. с экрана.

Дополнительная литература

1. Захарова Е. Я. Информационные аспекты экономики : учебное пособие [для 2 курса ФБ (направление 521600-Экономика)] / Е. Я. Захарова ; Новосиб. гос. техн. ун-т. - Новосибирск, 2003. - 99, [1] с. : ил. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000023698
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://elibrary.nstu.ru/source?bib_id=vtls000121782

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 "Znaniium.com" : <http://znaniium.com/>
5. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Саратов : Профобразование, 2017.— 702 с. — Режим доступа : <http://www.iprbookshop.ru/63594.html>. — Загл. с экрана.
6. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Анализ состояния защиты данных в информационных системах : учебно-методическое пособие / Новосиб. гос. техн. ун-т ; [сост. В. В. Денисов]. - Новосибирск, 2012. - 51, [1] с. : табл. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000171050

8.2 Специализированное программное обеспечение

- 1 Microsoft Windows
- 2 Microsoft Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Чтение лекций

Компьютерный класс

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

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

Кафедра вычислительной техники
Кафедра экономической информатики

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Образовательная программа: 09.04.03 Прикладная информатика, магистерская программа:
Информационные технологии в моделировании и организации бизнес-процессов

1. Обобщенная структура фонда оценочных средств учебной дисциплины

Обобщенная структура фонда оценочных средств по дисциплине Информационная безопасность приведена в Таблице.

Таблица – Структура фонда оценочных средств (раздел 1)

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.6 способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	з1. знать правовые основы информационной безопасности и принципы защиты	Защита персональных данных, ФЗ-152 Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций	РГЗ: Раздел <u>Введение</u> : Описание предприятия: основной бизнес-процесс, обеспечивающие бизнес-процессы и другие бизнес - процессы. Описание производственного процесса. <u>Раздел 1</u> : Выявление информационных потоков, средств их поддержки. Классификация результатов инвентаризации данных: Выявление информационных потоков, средств их поддержки в обязательном порядке требующих защиты.	Зачет, вопросы: Характеристика каналов утечки информации на объекте. Основные принципы создания систем ИБ и цели их реализации. Общая технология проведения инвентаризации информационной системы для анализа состояния информационной информации. Классификация категорий объектов информационной системы по результатам инвентаризации: уровни доступности, целостности, конфиденциальности.
ОПК.6	у1. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций Методы защиты информации. Средства защиты и их классификация.	РГЗ: Раздел 2: <u>От чего защищать ?</u> Получение навыков выявления элементов информационного взаимодействия по результатам ДЦК – классификации; Получение навыков инвентаризации вредоносных воздействий и оценки степени их влияния; Отображение результатов оценки степени вредоносного воздействия в виде 2-х мерной матрицы. <u>Лабораторная работа</u> : Перечень вредоносных воздействий, наблюдаемых, предполагаемых и потенциально возможных	<u>Зачет, вопросы:</u> Технология обнаружения и идентификации вирусов на компьютере. Типовая технология установления полномочий пользователя. Классификация и характеристика локальных атак. Классификация и характеристика удаленных атак. Методика оценки рисков при создании системы ИБ.

ПК.5/НИ способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	32. знать основные принципы разработки систем защиты в информационных системах	Инвентаризация информационных систем. Инвентаризация средств защиты, классификация защитных функций Технология защиты информации. Термины и определения.	РГЗ: Раздел 2: Как защищать ? Провести инвентаризацию имеющихся средств защиты. Заполнить таблицу оценки эффективности. <u>Лабораторная работа</u> : Перечень средств защиты, наблюдаемых, предполагаемых и потенциально возможных. Классификация средств защиты.	Зачет, <u>вопросы</u> : Характеристика, область применения и технология применения организационных средств защиты. Характеристика, область применения и технология применения законодательных средств защиты.
ПК.5/НИ	33. знать структуру проектных затрат и методы практической оценки рисков, оценивать размер ущерба от возможного нарушения информационной безопасности	Выявление вредоносных воздействий на информационную систему Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций Классификация данных по доступности, целостности, конфиденциальности Организационно-правовое обеспечение защиты информации.	РГЗ: Раздел 2: От чего защищать ? Выявление наиболее атакуемых информационных элементов, наиболее активных ВВ Отображение результатов оценки степени вредоносного воздействия в виде 2-х мерной матрицы. <u>Лабораторная работа</u> : Перечень вредоносных воздействий, анализ активности угроз, выявление уязвимостей	Зачет, <u>вопросы</u> : Классификация вредоносных программ. Технология обнаружения и идентификации вирусов на компьютере. Типовая технология установления полномочий пользователя. Классификация и характеристика локальных атак. Классификация и характеристика удаленных атак. Методика оценки рисков при создании системы ИБ.
ОПК.6 способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	31. знать правовые основы информационной безопасности и принципы защиты	Защита персональных данных, ФЗ-152 Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций	РГЗ: Раздел 3: Как защищать ? Заполнить таблицу оценки эффективности работы средств защиты. Выявить незадействованные, слабо функционирующие и имеющие не использованный потенциал средства защиты. <u>Лабораторная работа</u> : Перечень средств защиты, наблюдаемых, предполагаемых и потенциально возможных. Классификация средств защиты	Зачет, <u>вопросы</u> : Технология шифрации и дешифрации (криптоанализа) в методе моноалфавитной и многоалфавитной подстановок. Стеганография. Электронная цифровая подпись, технология и проблемы применения. Технология защиты информации при передаче по каналам связи.
ОПК.6	у1. уметь применять основные методы, способы и средства получения, хранения и переработки информации с помощью компьютеров и компьютерных средств	Инвентаризация информационных систем. Классификация по доступности, целостности, конфиденциальности Инвентаризация средств защиты, классификация защитных функций Методы защиты информации. Средства защиты и их классификация.	РГЗ: Раздел 4: <u>Повышение уровня защиты</u> . По заполненной таблице оценки эффективности работы средств защиты выявить не использованный потенциал средств защиты. <u>Лабораторная работа</u> : Выявление наименее защищенных	Зачет, <u>вопросы</u> : Технология шифрации и дешифрации (криптоанализа) в методе моноалфавитной и многоалфавитной подстановок. Стеганография. Электронная цифровая подпись, технология и проблемы применения. Технология защиты информации при передаче по каналам связи.

			элементов, модификация используемых средств защиты	
ПК.5/НИ способность исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	32. знать основные принципы разработки систем защиты в информационных системах	Инвентаризация информационных систем. Инвентаризация средств защиты, классификация защитных функций. Технология защиты информации. Термины и определения.	РГЗ: Раздел 4: <u>Повышение уровня защиты.</u> По заполненной таблице оценки эффективности работы средств защиты выявить не использованный потенциал средств защиты. Рекомендации по их модификации <u>Лабораторная работа</u> : Выявление наименее защищенных элементов, модификация перечня средств защиты за счет новых регламентационных	<u>Зачет, вопросы:</u> Характеристика, область применения и технология применения аппаратных средств защиты. Характеристика, область применения и технология применения технических средств защиты. Характеристика, область и технология применения методов регламентации. Характеристика, область и технология применения программных средств защиты. Типовая технология установления подлинности пользователя. Технологии установления подлинности пользователя методом паролей. Классификация методов и технология установления подлинности пользователя с использованием биометрических параметров человека. Технология антивирусной защиты

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 3 семестре - в форме зачета, который направлен на оценку сформированности компетенций ОПК.6, ПК.5/НИ.

Экзамен проводится по тестам. Тестовое задание во время зачета формируется по следующему правилу: проверочные вопросы открытого и закрытого типа предлагаются в случайном порядке (список вопросов приведен ниже). Для закрытых вопросов перечень вариантов ответов предлагается тоже в случайном порядке. В заключении зачета преподаватель вправе задавать студенту дополнительные вопросы из общего перечня

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

В 3 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.6, ПК.5/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.

Паспорт зачета

по дисциплине «Информационная безопасность», 3 семестр

1. Методика оценки

Зачет проводится в тестах. Тестовое задание во время зачета формируется по следующему правилу: проверочные вопросы открытого и закрытого типа предлагаются в случайном порядке (список вопросов приведен ниже). Для закрытых вопросов перечень вариантов ответов предлагается тоже в случайном порядке. В заключении зачета преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Пример теста для зачета

1. Принцип проектирования системы информационной безопасности, при котором в коллектив разработчиков включаются предполагаемые пользователи
Правильный ответ: *Не секретность проектирования*
2. В качестве мер защиты в Интернет можно рекомендовать...(отметить пункты)
Правильный ответ (несколько вариантов):
Не открывать подозрительные вложения
Сообщать свой пароль только друзьям
Дублировать важные сведения
Не отвечать на письма незнакомых адресатов
Не пересылать непрошенные письма, даже , если они интересны
3. Метод защиты от несанкционированного доступа, при котором каждому пользователю присваивается шифр, вводится пароль, определяется перечень доступных для работы (полный доступ или просмотр) модулей, ведется протокол доступа
Правильный ответ: *Авторизация доступа*
4. Группа методов закрытия (скрытия) информации, основанных на размещении данных внутри других, тривиальных данных: в звуке (AUDIO-файлы), в изображении (VIDEO-файлы) называется...
Правильный ответ: *Стеганография*
5. Промежуток времени от момента, когда появляется возможность использовать уязвимость, и до того, когда она устраняется
Правильный ответ: *Окно опасности*

2. Критерии оценки

- Ответ на тест считается **неудовлетворительным**, если студент при ответе на вопросы не выбрал правильный ответ для более, чем 49% вопросов
оценка составляет 0 баллов.
- Ответ на тест засчитывается на **пороговом** уровне, если студент суммарно набрал не менее 50 % баллов. Оценка составляет 10-15 баллов.

- Ответ на тест засчитывается на **базовом** уровне, если студент суммарно набрал не менее 90 % баллов, оценка составляет 16-19 *баллов*.
- Ответ на тест билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы суммарно набрал 100 % баллов, ответил на дополнительные вопросы оценка составляет 20 *баллов*.

3. Шкала оценки

Итоговая оценка ECTS складывается из баллов за продуктивное посещение лекций (10 баллов), лабораторные работы (34 баллов), баллов за выполнение РГЗ (36 баллов), баллов за тест (20) .

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

Таблица – Оценка ECTS

Сумма набранных баллов	Оценка по шкале ECTS	Итог
100-97	A+	Зачтено
96-93	A	
92-89	A-	
88-84	B+	
83-80	B	
79-76	B-	
75-72	C+	
71-70	C	
69-65	C-	
64-58	D+	
57-50	D	Не зачтено
49-40	D-	
39-35	E	
34-30	FX	
29-0	F	

4. Вопросы к зачету по дисциплине «Информационная безопасность»

- 1) Характеристика каналов утечки информации на объекте.
- 2) Основные принципы создания систем ИБ и цели их реализации.
- 3) Общая технология проведения инвентаризации информационной системы для анализа состояния информационной информации.
- 4) Классификация категорий объектов информационной системы по результатам инвентаризации: уровни доступности, целостности, конфиденциальности.
- 5) Поддержка информационной безопасности для различных классов объектов. Основные виды работ, выполняемые роли.
- 6) Классификация методов защиты.
- 7) Характеристика, область применения и технология применения организационных средств защиты.
- 8) Характеристика, область применения и технология применения законодательных средств защиты.
- 9) Характеристика, область применения и технология применения аппаратных средств защиты.
- 10) Характеристика, область применения и технология применения технических средств защиты.
- 11) Характеристика, область и технология применения методов регламентации.
- 12) Характеристика, область и технология применения программных средств защиты.
- 13) Типовая технология установления подлинности пользователя.
- 14) Технология установления подлинности пользователя методом паролей.

- 15) Классификация методов и технология установления подлинности пользователя с использованием биометрических параметров человека.
- 16) Технология антивирусной защиты.
- 17) Классификация вредоносных программ.
- 18) Технология обнаружения и идентификации вирусов на компьютере.
- 19) Типовая технология установления полномочий пользователя.
- 20) Классификация и характеристика локальных атак.
- 21) Классификация и характеристика удаленных атак.
- 22) Методика оценки рисков при создании системы ИБ.
- 23) Технология шифрации и дешифрации (криптоанализа) в методе моноалфавитной и многоалфавитной подстановок. Стеганография.
- 24) Электронная цифровая подпись, технология и проблемы применения.
- 25) Технология защиты информации при передаче по каналам связи.

Паспорт расчетно-графического задания (работы)

по дисциплине «Информационная безопасность», 3 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны выявить информационные потоки, средств их поддержки. Классифицировать результаты инвентаризации данных по потенциальному ущербу от нарушения защиты. Провести инвентаризацию вредоносных воздействий на систему, инвентаризацию средств защиты: выявить средства защиты всех типов. Оценить степень нейтрализации вредоносных воздействий на систему. На основании результатов обследования, содержащихся в материалах инвентаризации данных, результатов классификации по уровню ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ, КОНФИДЕНЦИАЛЬНОСТИ. Материалы инвентаризаций и анализа заносятся в таблицы и матрицы, разработанные в Excel. Следует обработать данные матриц.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ защищенности реально существующего объекта (рабочего места, подразделения, предприятия в целом), выявив информационные ресурсы, средства защиты и их эффективность работы. Найти уязвимости в информационной системе, предложить способы их устранения.

Обязательные структурные части РГЗ: ВВЕДЕНИЕ, 1 Объект автоматизации. 2 Оценка материального ущерба по ДЦК. 3 Перечень вредоносных воздействий. 4 Средства защиты. 5 Характеристика уровня защищенности системы. 6 Улучшение степени защищенности. ЗАКЛЮЧЕНИЕ. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Оцениваемые позиции:

- 1) Информационные ресурсы и средства их поддержки, полученные в результате инвентаризации.
- 2) Классификация результатов инвентаризации по ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ, КОНФИДЕНЦИАЛЬНОСТИ.
- 3) Перечень вредоносных воздействий (ВВ) на информационную систему (ИС).
- 4) Перечень имеющихся (предполагаемых) средств информационной защиты с анализом эффективности их работы (перекрываемые ВВ).
- 5) Оценка степени защищенности ИС, возможные направления её повышения.
- 6) Рекомендации по расширению перечня средств защиты.

2. Критерии оценки

- Работа считается **не выполненной**, если выполнены не все части РГЗ(Р), отсутствует хотя бы одна из оцениваемых позиций, оценка составляет 0 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, аппаратные средства не соответствуют современным требованиям. Обязательные структурные части присутствуют все, но анализ не завершен. Оценка составляет 18-20 баллов.
- Работа считается выполненной **на базовом** уровне, если части РГЗ(Р) выполнены: анализ объекта выполнен с декомпозицией, диагностические признаки обоснованы, аппаратные средства не соответствуют современным требованиям. Обязательные структурные части присутствуют все, анализ не завершен, Предложен путь усиления

защищенности. Оценка составляет 21-28 баллов.

- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, рассмотренный объект реальный, предложены эффективные меры по усилению защиты. Оценка составляет 29-36 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. Оценка РГР (36 баллов) входит в слагаемые оценки «зачет». Складывается из 2-х частей: оценка содержимого пояснительной записки по РГР (8-16 баллов), оценка защиты РГР - качество доклада, ответы на вопросы, качество презентации, оформление доклада, (8-20 баллов)

4. Примерный перечень тем РГЗ(Р)

- 1) Анализ защищенности данных в Интернет-магазине одежды, обуви и аксессуаров
- 2) Анализ защищенности данных в Оптовой компании медицинских товаров ЗАО «Vita»
- 3) Анализ защищенности данных в Шоколадная фабрика «АНЭД»
- 4) Анализ защищенности данных в ООО "Стальной аргумент"
- 5) Анализ состояния защиты «домашнего» компьютера
- 6) Выявление угроз, уязвимостей и вредоносных воздействий учебного процесса в терминальном классе (ТК-605, ТК-602, ТК-509)
- 7) Анализ эффективности работы средств защиты в учебных аудиториях НГТУ на примере терминального класса (лекционной аудитории, 6-609 и т.п.)
- 8) Анализ эффективности регламентных методов защиты, используемых на рабочем месте (произв.)
- 9) Разработка рекомендаций по повышению эффективности технических и организационных средств защиты в подразделении предприятия
- 10) Разработка рекомендаций по повышению эффективности регламентных средств защиты в подразделении предприятия