

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



**УТВЕРЖДАЮ:**

Проректор по научно-  
исследовательской работе

Бирюков А.Б.

(подпись)

июня 2020 года

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**Б1.В3 Информационная безопасность**

Направление подготовки: 09.04.04 Программная инженерия  
(код и наименование направления / специальности)

Магистерская программа: Методы и средства разработки программного обеспечения  
(наименование профиля / магистерской программы / специализации)

Программа: магистратура  
(бакалавриат, магистратура, специалитет)

Форма обучения: очная, заочная  
(очная, заочная, очно-заочная)

Форма обучения	очная	заочная
Семестр(ы)	1	1
Общая трудоёмкость в з.е./часах	4/144	4/144
Контактная работа (час.), в том числе:	58	17
Лекции (час.)	34	4
Лабораторные работы (час.)	17	4
Самостоятельная работа (час.), в том числе	57	100
Курсовой проект/работа (1семестр)	36	36
Подготовка к экзамену	36	36
Форма промежуточной аттестации	Экз.-1сем	Экз.-1сем

Донецк, 2020г.

Рабочая программа дисциплины **«Информационная безопасность»** составлена в соответствии с учебным планом магистров по направлению подготовки 09.04.04 Программная инженерия (магистерская программа Методы и средства разработки программного обеспечения) для 2020 года приёма.

Составитель:

доцент кафедры компьютерного моделирования и дизайна

к.т.н., доцент  Губенко Н.Е.

Рабочая программа рассмотрена и принята на заседании кафедры компьютерного моделирования и дизайна.

Протокол от « 11 » февраля 2020 года № 6

Заведующий кафедрой  Карабчевский В.В.

Рабочая программа **согласована с выпускающей кафедрой** программной инженерии.

Заведующий кафедрой  Федяев О.И.

Рабочая программа **одобрена учебно-методической комиссией** ГОУВПО «ДОННТУ» по направлению подготовки 09.04.04 Программная инженерия.

Протокол от « 20 » мая 2020 года № 10

Председатель  Федяев О.И.

Рабочая программа **продлена** для 20\_\_ года приёма на заседании кафедры компьютерного моделирования и дизайна.

Протокол от «\_\_\_\_» \_\_\_\_\_ 20\_\_ года № \_\_\_\_\_  
Заведующий кафедрой \_\_\_\_\_  
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20\_\_ года приёма на заседании кафедры компьютерного моделирования и дизайна.

Протокол от «\_\_\_\_» \_\_\_\_\_ 20\_\_ года № \_\_\_\_\_  
Заведующий кафедрой \_\_\_\_\_  
(подпись) (Ф.И.О.)

Рабочая программа **продлена** для 20\_\_ года приёма на заседании кафедры компьютерного моделирования и дизайна.

Протокол от «\_\_\_\_» \_\_\_\_\_ 20\_\_ года № \_\_\_\_\_  
Заведующий кафедрой \_\_\_\_\_  
(подпись) (Ф.И.О.)

## 1 ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина рассматривает вопросы организации и применения современных моделей, методов и средств информационной безопасности и технологий защиты информационных систем.

**Целью дисциплины является:** подготовка магистра к исследованию, разработке и использованию инструментов, методов и моделей информационной безопасности для защиты и противодействия информационным и техническим атакам в рамках правового поля и законодательства страны.

В результате освоения дисциплины студент должен знать:

- методы системного и критического анализа;
- методики разработки стратегии действий для выявления и решения проблемных ситуаций в сфере защиты информации;
- правила и закономерности личной и деловой устной и письменной коммуникации;
- современные коммуникативные технологии на русском и английском языках;
- существующие профессиональные сообщества для профессионального взаимодействия;
- методы постановки новых задач анализа и синтеза новых проектных решений в сфере информационной безопасности;
- методы проектирования средств защиты информационных систем;

уметь:

- применять методы системного подхода и критического анализа проблемных ситуаций в области защиты информации;
- разрабатывать стратегию действий, принимать конкретные решения в сфере информационной безопасности;

- применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия;
- использовать методы проектирования средств защиты информационных систем;

владеть:

- методологией системного и критического анализа проблемных ситуаций в сфере информационной безопасности;
- методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий;
- методиками постановки цели, определения способов ее достижения, разработки стратегий действий по защите информации;
- применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия;
- навыками постановки новых задач анализа и синтеза новых проектных решений в области технологий информационной защиты;
- навыками программной реализации средств защиты информационных систем.

Процесс изучения дисциплины направлен на формирование у студентов следующих компетенций:

УК-1 - способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-4 - способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального общения;

ПК-5 - способен выполнить постановку новых задач анализа и синтеза новых проектных решений;

ПСК-1- способен применять и разрабатывать средства защиты информационных систем.

## **2 МЕСТО В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ**

Дисциплина **Информационная безопасность** относится к части, формируемой участниками образовательных отношений, Блока 1 дисциплин (модулей) учебного плана.

Базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин. Пререквизитами данной дисциплины являются дисциплины бакалавриата: «Дискретная математика», «Базы данных», «Операционные системы», «Архитектура компьютеров», «Протоколы компьютерных сетей», «Основы программирования и алгоритмические языки», «Безопасность программ и данных».

Знания и умения, приобретенные при освоении данной дисциплины, будут реализованы магистром при выполнении курсового проекта по дисциплине «Информационная безопасность», прохождении учебной и/или производственной практики, прохождении государственной итоговой аттестации, а также в реальной профессиональной деятельности при:

- формировании политики безопасности предприятия;
- организации сетевого администрирования с учетом принятой политики безопасности;
- установке и использовании специализированного программного обеспечения для защиты отдельных компьютеров и сети предприятия;
- при пользовании стандартными приложениями для защиты конфиденциальной информации и электронной цифровой подписи;
- анализе сценариев атак на информационные системы;
- проведении аудита безопасности;
- определении уровня безопасности систем в соответствии с принятыми стандартами.

### 3 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

#### 3.1 Распределение учебных часов по темам дисциплины и видам занятий

Наименование тем (содержательных модулей)	Количество часов (очная, заочная)				
	Всего	В том числе			
		Лекции	Практ. (Се- мин.)	Лабор.	СРС
<b>Тема 1.</b> Введение в дисциплину. Современная ситуация в области информационной безопасности.	9/7	4/0.5		2/0.5	3/6
<b>Тема 2.</b> Нормативные документы для решения задач информационной безопасности	5/9,5	2/0.5			3/9
<b>Тема 3.</b> Базовые криптографические протоколы.	13/11	6/1		4/1	3/9
<b>Тема 4.</b> Инфраструктура криптосистем	13/10,5	6/0.5		4/1	3/9
Тема 5. Сетевая безопасность. Управление безопасностью в компьютерной системе.	10/10	4/0.5		3/0.5	3/9
<b>Тема 6.</b> Угрозы и уязвимости. Анализ рисков безопасности и их оценка. Аудит информационной безопасности.	9/9,5	6/0.5			3/9
<b>Тема 7.</b> Комплексная система безопасности	13/10,5	6/0.5		4/1	3/9
Курсовой проект	36/36				36/36
Подготовка к экзамену	36/36				
<b>Всего часов за семестр</b>	<b>144</b>	<b>34/4</b>		<b>17/4</b>	<b>57/96</b>

#### 3.2 Лекции

**Тема 1.** Введение в дисциплину. Современная ситуация в области информационной безопасности.

Определение информационной безопасности. Понятие информационной безопасности. Краткая история развития информационной безопасности. Основные компоненты информационной безопасности. Категории атак. Абстрактные модели защиты информации.

Литература к теме 1: [1,2,3,4]

**Тема 2.** . Нормативные документы для решения задач информационной безопасности.

Общие критерии информационной безопасности их концепция. Документы Гостехкомиссии России. Критерии безопасности компьютерных систем Министерства обороны США. Европейские критерии безопасности.

Литература к теме 2: [1,2]

**Тема 3.** Базовые криптографические протоколы.

Закономерности организации сложных криптосистем. Основы теории криптопротоколов. Вероятностные доказательства. Протоколы аутентификации. Специальные схемы цифровой подписи. Схемы разделения секрета.

Литература к теме 3: [1,2,3,4]

**Тема 4.** Инфраструктура криптосистем

Управление ключами. Жизненный цикл криптоключей. Модели управления. Структура ключевой системы симметричных криптосхем. Методы распространения и сертификации открытых ключей. Протоколы распределения ключей. Конференц-связь.

Литература к теме 4: [1,2,3]

**Тема 5.** Сетевая безопасность. Управление безопасностью в компьютерной системе.

Атакуемые сетевые компоненты . Среда передачи информации. Узлы коммутации сетей. Серверы. Рабочие станции. Создание механизмов безопасности в распределенной компьютерной системе.

Литература к теме 5: [2,3]

**Тема 6.** Угрозы и уязвимости. Анализ рисков безопасности и их оценка. Аудит информационной безопасности.

Литература к теме 6: [1,2,5]

**Тема 7.** Комплексная система безопасности

Классификация информационных объектов. Классификация по требуемой степени безотказности. Классификация по уровню конфиденциальности. Требования по работе с конфиденциальной информацией. Политика ролей. Создание политики информационной безопасности. Выводы по дисциплине.

Литература к теме 7: [1,2,5]



### 3.3 Лабораторные работы

№ п/п	Тема занятия	Объем, час. Очн./заоч.	Литера- тура
1	Лабораторная работа №1. Базовые методы нейтрализации систем защиты от несанкционированного копирования .	2/0	[8]
3	Лабораторная работа № 2. Криптографические модели и методы защиты. Симметричные алгоритмы шифрования	4/2	[8]
4	Лабораторная работа № 3. Криптографические модели и методы защиты. Асимметричные алгоритмы шифрования	4/2	[8]
5	Лабораторная работа № 4. Модели электронной цифровой подписи	3/0	[8]
8	Лабораторная работа № 5. Стеганографические протоколы подтверждения авторских прав	4/0	[8]
	Итого за семестр	17/4	

### 3.5 Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час. Очн./заоч.
1	Изучение лекционного материала	10/30
2	Подготовка к лабораторным работам	11/30
3	Выполнение курсового проекта	36/36
Итого:		57/96

### 3.6 Курсовой проект

Тематика курсового проекта связана с самостоятельной разработкой политики безопасности для информационной системы предприятия, структура, функции и локальная вычислительная сеть (ЛВС) которого согласовывается с преподавателем – руководителем курсового проекта.

В проекте должна быть обоснована важность защиты информации и соблюдения политики информационной безопасности. Проанализированы стандарты безопасности, приведена схема ЛВС предприятия, дана оценка АО и ПО, достаточного для функционирования ИС и определен существующий класс безопасности. Проанализированы процедуры информационной безопасности и разработан аварийный план.

Проект выполняется в соответствии с методическими рекомендациями, приведенными в методических указаниях [7].

Объем учебной нагрузки согласно учебному плану составляет 36 часов.

Рекомендуемый объем пояснительной записки с приложениями – не более 50 страниц формата А4 (210×297 мм).

Оформление курсового проекта должно соответствовать общим требованиям к текстовым документам, принятым на кафедре.

Рекомендуемый план пояснительной записки.

## ВВЕДЕНИЕ

*Обоснование важности защиты информации и разработки и соблюдении политики безопасности.*

1. Анализ концепций и стандартов информационной безопасности. *Общая характеристика ИС предприятия (назначение и цели). Этапы и направления разработки политики безопасности.*

2. Стандарты информационной безопасности

2.1. Структурная схема ЛВС.

2.2. Информационные ресурсы (классификация объектов).

2.3. Пользователи ИС (классификация субъектов).

2.4. Определение класса.

2.5. Характеристика АО и ПО достаточного для функционирования ИС (требования по составу и характеристикам оборудования для сервера и клиента).

3. Управление рисками.

3.1. Характеристика и классификация угроз и уязвимостей и определение рисков.

3.2 Экономические аспекты управления информационными рисками (например, простой предприятия или потеря управляемости фирмой и т.п.).

4. Процедуры информационной безопасности.

4.1 Законодательные меры (применимые к ИС).

4.2 Административные меры (принятые на предприятии «xxx»).

4.3 Процедурные меры.

4.3.1 Управление персоналом.

4.3.2 Разделение полномочий.

4.3.3 Физическая защита.

4.3.4 Поддержка работоспособности системы.

4.4 Программно-технические меры.

5. Разработка способов защиты и аварийного плана (конкретизировать и согласовать с преподавателем виды атак и угроз, для которых будет разработана модель защиты-нападения).

## ЗАКЛЮЧЕНИЕ

## ПРИЛОЖЕНИЯ

Приложение А – Техническое задание к курсовому проекту

Приложение Б – Листинги программ

Приложение В – Экранные формы работы в системе ГРИФ

## 4 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 4.1 Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Обобщенная оценка на экзамене выставляется с учетом основных составляющих компетенций: полноты знаний, умений и навыков.

Составляющая компетенции – полнота знаний

- нулевой уровень: неверные, не аргументированные, с множеством грубых ошибок ответы на вопросы / ответы на два вопроса из трех полностью отсутствуют. Уровень знаний ниже минимальных требований;
- минимальный уровень: даны не полные, не точные и аргументированные ответы на вопросы. Уровень знаний ниже минимальных требований. Допущено много грубых ошибок;
- пороговый уровень: даны недостаточно полные, точные и аргументированные ответы на вопросы. Плохо знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено много негрубых ошибок;
- средний уровень: Даны достаточно полные, точные и аргументированные ответы на вопросы. В целом знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;
- продвинутый уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько негрубых ошибок;
- высокий уровень: даны полные, точные и аргументированные ответы на вопросы. Знает термины, определения и понятия; основные закономерности, соотношения, принципы. Допущено несколько неточностей.

Составляющая компетенции – умения

- нулевой уровень: полное отсутствие понимания сути методики решения задачи, допущено множество грубейших ошибок / задания не выполнены вообще;
- минимальный уровень: слабое понимание сути методики решения задачи, допущены грубые ошибки. Решения не обоснованы. Не умеет использовать нормативно-техническую литературу. Не ориентируется в специальной научной литературе, нормативно-правовых актах;
- пороговый уровень: достаточное понимание сути методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую литературу. Слабо ориентируется в специальной научной литературе, нормативно-правовых актах;

- средний уровень: в целом понимает суть методики решения задачи, допущены ошибки. Решения не всегда обоснованы. Умеет использовать нормативно-техническую и специальную научную литературу, нормативно-правовые акты;
- продвинутый уровень: в целом понимает суть методики решения задачи, допущены неточности. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу, нормативно-правовые акты;
- высокий уровень: понимает суть методики решения задачи. Способен обосновать решения. Умеет использовать нормативно-техническую и специальную научную литературу, передовой зарубежный опыт, нормативно-правовые акты.

#### Составляющая компетенции – владение навыками

- нулевой уровень: не продемонстрировал навыки выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;
- минимальный уровень: не продемонстрировал навыки выполнения профессиональных задач. Испытывает существенные трудности при выполнении отдельных заданий;
- пороговый уровень: владеет опытом готовности к профессиональной деятельности и профессиональному самосовершенствованию на пороговом уровне. Трудовые действия выполняет медленно и некачественно;
- средний уровень: владеет средним опытом готовности к профессиональной деятельности и профессиональному самосовершенствованию. Трудовые действия выполняет на среднем уровне по скорости и качеству;
- продвинутый уровень: владеет опытом и достаточно выраженной личностной готовности к профессиональной деятельности и профессиональному самосовершенствованию. Быстро и качественно выполняет трудовые действия;
- высокий уровень: владеет опытом и выраженностью личностной готовности к профессиональной деятельности и профессиональному самосовершенствованию. Быстро и качественно выполняет трудовые действия.

#### Обобщенная оценка сформированности компетенций

- нулевой уровень: компетенции не сформированы;
- минимальный уровень: значительное количество компетенций не сформировано;
- пороговый уровень: все компетенции сформированы, но большинство на пороговом уровне;
- средний уровень: все компетенции сформированы на среднем уровне;
- продвинутый уровень: все компетенции сформированы на среднем или высоком уровне;
- высокий уровень: все компетенции сформированы на высоком уровне.

Обобщенная оценка выставляется в соответствии с рекомендациями, которые содержатся в «Положении об организации учебного процесса в Донецком национальном техническом университете, утвержденном приказом ДонНТУ № 1006-14 от 01.12.2016г.

## 4.2 Вопросы к экзамену и пример экзаменационного билета

### Вопросы к экзамену

1. Определение и понятия информационной безопасности.
2. История развития информационной безопасности.
3. Основные компоненты информационной безопасности.
4. Категории атак.
5. Абстрактные модели защиты информации.
6. Нормативные документы для решения задач информационной безопасности.
7. Общие критерии информационной безопасности и их концепция.
8. Базовые криптографические протоколы.
9. Закономерности организации сложных криптосистем.
10. Вероятностные доказательства.
11. Протоколы аутентификации.
12. Специальные схемы цифровой подписи.
13. Схемы разделения секрета.
14. Управление ключами. Жизненный цикл криптоключей.
15. Структура ключевой системы симметричных криптосхем.
16. Методы распространения и сертификации открытых ключей.
17. Протоколы распределения ключей.
18. Конференц-связь.
19. Сетевая безопасность. Управление безопасностью в компьютерной системе.
- Атакуемые сетевые компоненты .
20. Среда передачи информации. Узлы коммутации сетей. Серверы. Рабочие станции.
21. Создание механизмов безопасности в распределенной компьютерной системе.
22. Угрозы и уязвимости.
23. Анализ рисков безопасности и их оценка.
24. Аудит информационной безопасности.
25. Комплексная система безопасности.
26. Классификация информационных объектов.
27. Требования по работе с конфиденциальной информацией.
28. Политика ролей.
30. Создание политики информационной безопасности.

### Пример экзаменационного билета

**ГОУВПО «Донецкий национальный технический университет»**  
**Уровень высшего профессионального образования:** Магистратура  
**Направление подготовки:** 09.04.04 "Программная инженерия"  
**Магистерская программа:** Методы и средства разработки программного обеспечения:  
**Семестр:** 1  
**Учебная дисциплина:** "Информационная безопасность"

### **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1**

- 1 Основные компоненты информационной безопасности.
- 2 Методы распространения и сертификации открытых ключей.
- 3 Разработать алгоритм, реализующий электронную цифровую подпись для аутентификации документа на основе симметричных принципов шифрования.

Утверждено на заседании кафедры компьютерного моделирования и дизайна

Протокол № \_\_\_\_\_ от „\_\_\_” \_\_\_\_\_ года

**Зав. кафедрой КМД** \_\_\_\_\_ **Карабчевский В.В.**  
**Экзаменатор** \_\_\_\_\_ **Губенко Н.Е.**

#### **4.4 Критерии оценивания экзаменационной работы и выставления экзаменационной оценки по дисциплине "Информационная безопасность"**

В каждом билете содержится 3 вопроса: два теоретических вопроса (задания №1,2) и два практических задания №3. Максимальное количество баллов за 1,2,3 вопросы - по 35 баллов за каждый вопрос, за 3 вопрос максимальное количество баллов- 30.

Максимальное количество баллов за экзаменационную работу составляет 100 баллов.

При оценивании вопросов №1,2 максимальное количество баллов за каждый вопрос ставится в случае полного системного раскрытия вопросов без каких-либо неточностей. Баллы снимаются, если в ответе упущены какие-либо второстепенные моменты (до 2 баллов), допущены несущественные неточности (до 4 баллов), допущены существенные неточности при правильном ответе в целом (до 6 баллов), при недостаточном представлении материалов баллы снимаются как процент недостающего материала с учетом его значимости.

При оценивании вопроса №3 максимальное кол-во баллов ставится в случае представления полного решения с правильным ходом и точным ответом. Баллы снимаются, если в решении есть несущественные неточности, не повлиявшие на результат (до 5 баллов), если в ответе упущены какие-либо второстепенные моменты (до 10 баллов), допущены отдельные неточности в ходе решения, не искажившие ход решения в целом (до 15 баллов), при недостаточном представлении

материалов баллы снимаются как процент недостающего материала с учетом его значимости.

Итоговая оценка за экзамен рассчитывается как сумма баллов по каждому из вопросов экзаменационного билета.

При определении уровня знаний студентов преподаватель руководствуется вышеописанными критериями оценки знаний, являющимися составляющей учебно-методического комплекса дисциплины.

Для определения уровня знаний студентов преподаватель должен руководствоваться шкалой оценивания и следующими критериями.

Сумма баллов за все виды учебной дель- ности	Оценка ECTS	Оценка по националь- ной шкале
		для экзамена, курсового проекта (работы), прак- тики
90 – 100	A	отлично
80-89	B	хорошо
75-79	C	
70-74	D	удовлетворительно
60-69	E	
35-59	FX	неудовлетворительно с возможностью повтор- ной сдачи
0-34	F	неудовлетворительно с обязательным повтор- ным изучением дисци- плины

100-90% от максимального количества баллов студент получает, когда обобщенная оценка сформированности компетенций – «высокий уровень»;

89-80% от максимального количества баллов студент получает, когда обобщенная оценка сформированности компетенций – «продвинутый уровень»;

79-75% от максимального количества баллов студент получает, когда обобщенная оценка сформированности компетенций – «средний уровень»;

74-60% от максимального количества баллов студент получает, когда обобщенная оценка сформированности компетенций – «пороговый уровень»;

59-35% от максимального количества баллов студент получает, когда обобщенная оценка сформированности компетенций – «минимальный уровень»;

34-0% от максимального количества баллов студент получает, когда обобщенная оценка сформированности компетенций – «нулевой уровень».

Итоговая оценка за экзамен рассчитывается исходя из баллов по каждому из вопросов экзаменационного билета.

#### 4.5 Пример текущего опроса на лабораторных занятиях

##### Контрольные вопросы

1. В чем суть понятия ЭЦП?
2. Каким образом может реализовываться ЭЦП в симметричных системах шифрования?
3. Каким образом использовать ЭЦП для подтверждения авторских прав?
4. Как и зачем применяется хеширование в схемах и протоколах простановки ЭЦП?
5. Какие функции хеширования сегодня наиболее эффективны и почему?

#### 4.6 Согласно учебному плану, по дисциплине "Информационная безопасность" предусмотрен курсовой проект.

Примерная тематика курсовых работ, их содержание и оформление описаны в пункте 3.6

**Текущий контроль** знаний студентов производится по результатам выполнения лабораторных работ, курсового проекта, во время контрольных опросов в ходе проведения практических занятий.

**Промежуточная аттестация** по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена в соответствии с «Положением об организации учебного процесса в Донецком национальном техническом университете», утвержденном приказом ДонНТУ от 02.05.2018г. № 337-14.

При определении уровня знаний студентов преподаватель руководствуется критериями оценки знаний, являющимися составляющей учебно-методического комплекса дисциплины.



## 5 РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

### I Основная литература

1. Методы и средства комплексной защиты информации в технических системах: учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 224 с. — ISBN 978-5-9515-0429-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/101925.html> (дата обращения: 28.08.2020). — Режим доступа: для авторизир. Пользователей
2. Щеглов, А. Ю. Математические модели и методы формального проектирования систем защиты информационных систем: учебное пособие / А. Ю. Щеглов, К. А. Щеглов. — Санкт-Петербург: Университет ИТМО, 2015. — 93 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/67260.html> (дата обращения: 28.08.2020). — Режим доступа: для авторизир. Пользователей
3. Лапони́на, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О. Р. Лапони́на ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/97571.html> (дата обращения: 28.08.2020). — Режим доступа: для авторизир. Пользователей
4. Стеганографические системы. Критерии и методическое обеспечение: учебно-методическое пособие / В. Г. Грибунин, В. Е. Костюков, А. П. Мартынов [и др.] ; под редакцией В. Г. Грибунин. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2016. — 324 с. — ISBN 978-5-9515-0317-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/60864.html> (дата обращения: 28.08.2020). — Режим доступа: для авторизир. Пользователей

### II Дополнительная литература

5. Нестеров, С.А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров; Санкт-Петербург. политехн. ун-т Петра Великого. — М.: Юрайт, 2017. — 321 с. — 10 экз.
6. Тюльпинова, Н. В. Защита интеллектуальной собственности и компьютерной информации: учебное пособие для магистров / Н. В. Тюльпинова. — Саратов: Вузовское образование, 2020. — 341 с. — ISBN 978-5-4487-0611-0. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. URL: <http://www.iprbookshop.ru/88755.html> (дата обращения: 28.08.2020). — Режим доступа: для авторизир. Пользователей

## 6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Учебно-методические издания, разработанные в ДонНТУ

7. Методические указания к выполнению курсового проекта по дисциплине профессионального цикла вариативной части дисциплины «Информационная безопасность» [Электронный ресурс] : для студентов уровня профессионального образования «Магистр» направления подготовки 09.04.04 «Программная инженерия» магистерская программа: «Методы и средства разработки программного обеспечения» / ГОУВПО «ДонНТУ», кафедра компьютерного моделирования и дизайна : сост. : Губенко Н.Е., Чернышова А.В.- Электрон. дан. (1 файл). - Донецк: ДонНТУ, 2020. - Систем.требования: Acrobat Reader.32 ст - Электронно-библиотечная система ЭБС ДОННТУ: URL:  
<http://library.donntu.org/erkaf.php?kaf=%EA%E0%F4%E5%E4%F0%E0+%EA%E5%EC%EF%FC%FE%F2%E5%F0%ED%EE%E3%EE+%EC%EE%E4%E5%EB%E8%F0%EE%E2%E0%ED%E8%FF+%E8+%E4%E8%E7%E0%E9%ED%E0> (дата обращения: 28.08.2020) Режим доступа: для авторизир. Пользователей
8. Методические указания для проведения лабораторных работ по дисциплине профессионального цикла вариативной части дисциплин «Информационная безопасность» [Электронный ресурс] : для студентов уровня профессионального образования «Магистр» направления подготовки 09.04.04 «Программная инженерия» / ГОУВПО «ДонНТУ», кафедра компьютерного моделирования и дизайна : сост. : Губенко Н.Е., Чернышова А.В.- Электрон. дан. (1 файл). - Донецк: ДонНТУ, 2020. - Систем.требования: Acrobat Reader. - Электронно-библиотечная система ЭБС ДОННТУ: URL:  
<http://library.donntu.org/erkaf.php?kaf=%EA%E0%F4%E5%E4%F0%E0+%EA%E5%EC%EF%FC%FE%F2%E5%F0%ED%EE%E3%EE+%EC%EE%E4%E5%EB%E8%F0%EE%E2%E0%ED%E8%FF+%E8+%E4%E8%E7%E0%E9%ED%E0> (дата обращения: 28.08.2020) Режим доступа: для авторизир. Пользователей

### Периодические издания:

1. Информатика и её применения: научный журнал (2012-2013).
2. Математическое моделирование: журнал. – М.: Наука (2004-2014).
3. Научные труды Донецкого национального технического университета. Серия «Информатика, кибернетика и вычислительная техника» (2008-2017).

### Internet-ресурсы

1. Вопросы кибербезопасности (2010-2017) . <http://cyberrus.com/issues> - Дата обращения-15.04.2020
2. Информационная безопасность. ИТ-портал компании "ИнфосистемыДжет" - <http://www.jetinfo.ru/article/ib> - Дата обращения-10.05.2020

3. Экономические оценки информационной безопасности.

<http://citforum.ru/security/articles/sec/1.shtml> - Дата обращения - 12.06.2020

### Электронно-информационные ресурсы

1. ЭБС ДОННТУ – <http://donntu.org/library>.
2. Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: <http://www.iprbookshop.ru/>

## 7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 1. Лекционные занятия:

Учебная аудитория № 4.42 учебный корпус 4 (мультимедийное оборудование: 1 ПК 2x2400GHz, 2Гб RAM, 120GB HDD, ОС Windows 7 Professional x86 (академическая подписка), LibreOffice 4.3.2.2, Google Slides (бесплатная версия)), бесплатные программы JeticoBCArchive и Ratool; 8 ПК Intel Celeron 2.0 GHz, 1Гб RAM, 60GB HDD, ОС Windows XP, LibreOffice 4.3.2.2, Google Slides (бесплатная версия)), бесплатные программы JeticoBCArchive и Ratool; мультимедийный проектор EPSON EB-X9; экран проекционный ELIT SCRE; специализированная мебель: доска аудиторная, парты). Комплект презентационных материалов.

### 2. Лабораторные работы:

Учебная аудитория № 4.42 учебный корпус 4 (мультимедийное оборудование: 1 ПК 2x2400GHz, 2Гб RAM, 120GB HDD, ОС Windows 7 Professional x86 (академическая подписка), LibreOffice 4.3.2.2, Google Slides (бесплатная версия)), бесплатные программы JeticoBCArchive и Ratool; 8 ПК Intel Celeron 2.0 GHz, 1Гб RAM, 60GB HDD, ОС Windows XP, LibreOffice 4.3.2.2, Google Slides (бесплатная версия)), бесплатные программы JeticoBCArchive и Ratool; мультимедийный проектор EPSON EB-X9; экран проекционный ELIT SCRE; специализированная мебель: доска аудиторная, парты). Комплект презентационных материалов.

### 3. Самостоятельная работа:

Помещения для самостоятельной работы с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации: читальные залы, учебные корпуса 2,3 (Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду (ЭИОС ДОННТУ) и электронно-библиотечную систему (ЭБС IPRbooks), а также возможностью индивидуального неограниченного доступа обучающихся в ЭБС и ЭИОС посредством Wi-Fi с персональных мобиль-

ных устройств. ОС- Microsoft Windows 7, OpenOffice 2.0.3 – общественная лицензия MPL 2.0/ Grub loader for ALT Linux - лицензия GNU LGPL v3/ Mozilla Firefox - лицензия MPL2.0, Moodle (Modular Object-Oriented Dynamic Learning Environment) - лицензия GNU GPLect-OrientedDynamicLearning Environment, лицензия GNUGPL.