

**ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»**

**ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ**

Кафедра компьютерных технологий

**УТВЕРЖДАЮ:**



Проректор по научно-методической  
и учебной работе

\_\_\_\_\_ Е.И. Скафа

«22» апреля 2020 г.

МП

**Рабочая программа учебной дисциплины**

**«БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В  
ИНФОРМАЦИОННЫХ СИСТЕМАХ»**

Направления подготовки:	09.04.01 Информатика и вычислительная техника
Магистерская программа:	Информатика и вычислительная техника
Образовательная программа:	академическая магистратура
Квалификация:	магистр
Форма обучения:	<u>очная</u> , очно-заочная, <u>заочная</u>

Донецк 2020

УТВЕРЖДАЮ:

Декан физико-технического факультета

С.А. Фоменко

«17» апреля 2020 г.

МП



Программа учебной дисциплины **«Безопасность и защита информации в информационных системах»** составлена на основании Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) направления подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. № 918;

Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки ДНР № 1171 от «10» ноября 2017 г.; учебного плана и основной образовательной программы Информатика и вычислительная техника, направления подготовки 09.04.01 Информатика и вычислительная техника, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчик:

к.т.н, доцент кафедры компьютерных технологий

Бондаренко В.И.

Программа учебной дисциплины утверждена на заседании кафедры компьютерных технологий

Протокол № 12 от «2» апреля 2020 г.

Зав. кафедрой компьютерных технологий

Ермоленко Т.В.

Программа учебной дисциплины одобрена учебно-методической комиссией физико-технического факультета

Протокол № 5 от «15» апреля 2020 г.

Председатель учебно-методической комиссии физико-технического факультета

Котенко В.Н

## 1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Безопасность и защита информации в информационных системах» относится к вариативной части профессионального блока и состоит из двух содержательных модулей.

Основывается на базе дисциплин: «Защита информации», «Методы и средства проектирования информационных систем и технологий», «Современные информационные системы и технологии», «Программирование», «Управление проектированием информационных систем».

## 2. СТРУКТУРА ДИСЦИПЛИНЫ

<i>Характеристика учебной дисциплины</i>		
Направление подготовки	09.04.01 Информатика и вычислительная техника	
Профиль	Информатика и вычислительная техника	
Образовательная программа	Академическая магистратура	
Квалификация	Магистр	
Количество содержательных модулей	2	
Дисциплина базовой / вариативной части образовательной программы	Профессиональный блок. Вариативная часть	
Формы контроля (МК, экзамен, зачет)	Модульный контроль, экзамен	
Показатели	очная форма обучения	заочная форма обучения
Количество зачётных единиц (кредитов)	5	5
Год подготовки	2	2
Семестр	4	4
Количество часов	180	180
- лекционных	20	4
- практических, семинарских		
- лабораторных	40	8
- самостоятельной работы	120	168
в т. ч. индивидуальное задание		
Недельное количество часов, т. ч.	18	
аудиторных	6	

## 3. ОПИСАНИЕ ДИСЦИПЛИНЫ

### Цели и задачи.

**Целью изучения дисциплины «Безопасность и защита информации в информационных системах»** является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

**Основными задачами изучения дисциплины являются** усвоение теоретических основ и приобретение практических навыков:

- изучение концепции защиты информации в информационных системах (ИС);
- изучение теоретических основ защиты информации в ИС;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;

- изучение организационных основ защиты информации в ИС;
- изучение методического обеспечения защиты информации в ИС.

#### **Требования к результатам освоения дисциплины.**

Процесс изучения дисциплины «Безопасность и защита информации в информационных системах» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО РФ направления подготовки 09.04.01 Информатика и вычислительная техника и основной образовательной программы высшего профессионального образования направления подготовки 09.04.01 Информатика и вычислительная техника (магистерская программа: Информатика и вычислительная техника):

##### **а) универсальных (УК):**

- способностью осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1);
- способностью управлять проектом на всех этапах его жизненного цикла (УК-2);
- способностью организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3);
- способностью применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия (УК-4);
- способностью анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия (УК-5);
- способностью определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки (УК-6).

##### **б) общепрофессиональных (ОПК):**

- способностью самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте (ОПК-1);
- способностью разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач (ОПК-2);
- способностью анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями (ОПК-3);
- способностью применять на практике новые научные принципы и методы исследований (ОПК-4);
- способностью разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем (ОПК-5);
- способностью разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования (ОПК-6);
- способностью адаптировать зарубежные комплексы обработки информации и автоматизированного проектирования к нуждам отечественных предприятий (ОПК-7);
- способностью осуществлять эффективное управление разработкой программных средств и проектов (ОПК-8).

##### **в) профессиональных (ПК):**

###### **производственно-технологическая деятельность:**

- способностью управлять развитием баз данных (ПК-1);
- способностью осуществлять управление сервисами информационных технологий (ПК-2);
- способностью осуществлять технологическую поддержку подготовки

технических публикаций (ПК-3);

- способностью осуществлять администрирование систем управления базами данных инфокоммуникационной системы организации (ПК-4);

- способностью осуществлять администрирование системного программного обеспечения инфокоммуникационной системы организации; (ПК-5);

- способностью осуществлять управление развитием инфокоммуникационной системы организации (ПК-6);

- способностью осуществлять администрирование процесса поиска и диагностики ошибок сетевых устройств и программного обеспечения (ПК-7)

- способностью осуществлять научно-методическое и учебно-методическое обеспечение реализации программ профессионального обучения, среднего профессионального образования и дополнительного профессионального образования (ПК-9);

***проектная деятельность:***

- способностью проектировать сложные пользовательские интерфейсы (ПК-10);

***организационно-управленческая деятельность:***

- способностью управлять работами по сопровождению и проектами по созданию (модификации) информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы (ПК-13);

- способностью осуществлять руководство разработкой комплексных проектов на всех стадиях и этапах выполнения работ (ПК-20);

***научно-исследовательская деятельность:***

- способностью осуществлять экспертный анализ эргономических характеристик программных продуктов и/или аппаратных средств (ПК-21).

**В результате изучения учебной дисциплины студент должен:**

***Иметь представление:***

- о критериях оценки защищенности систем;
- о проблемах и направлениях развития аппаратных и программных средств защиты информации;
- о современных криптографических системах.

***Знать:***

- средства и методы предотвращения и обнаружения вторжений;
- технические каналы утечки информации;
- возможности технических средств перехвата информации;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- основные понятия криптографии;
- основные требования к системам криптографической защиты;
- основные алгоритмы криптографической защиты;
- основные алгоритмы электронной цифровой подписи;
- проблемы и направления развития криптографических систем.

***Уметь:***

- оценивать качество готового программного обеспечения с точки зрения безопасности;
- ориентироваться в современной системе источников информации;
- использовать защищенные современные информационные технологии в своей профессиональной деятельности;

- анализировать информационную безопасность многопользовательских систем;
- пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;
- видеть и формулировать проблему защиты информации;
- ставить цели и задачи по обеспечению информационной безопасности.

**Владеть:**

- методами и средствами технической защиты информации;
- методами расчета и инструментального контроля показателей технической защиты информации;
- использования инструментов криптографической защиты информации;
- использования современной терминологии в области информационной безопасности;
- применения методологии защиты в области информационной безопасности.

#### **4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА**

Порядковый номер и тема	Краткое содержание темы
	<b><i>Содержательный модуль 1.</i></b> <b>Основные положения теории информационной безопасности</b>
<b>Тема 1.</b> Международные стандарты информационного обмена. Понятие угрозы.	Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.
<b>Тема 2.</b> Виды возможных нарушений информационной системы. Защита.	Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.
<b>Тема 3.</b> Основные положения теории информационной безопасности. Модели безопасности и их применение.	Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности
<b>Тема 4.</b> Таксономия нарушений информационной безопасности и причины, обуславливающие	Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы. Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.

их существование.	
<b>Тема 5.</b> Использование защищенных компьютерных систем.	Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.
	<b>Содержательный модуль 2.</b> <b>Криптографические методы защиты информации.</b>
<b>Тема 6.</b> Предмет и задачи криптографии.	Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Требования к криптографическим системам защиты информации. Способы реализации криптографических методов. Понятие и виды криптографических атак. Криптографический протокол. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации. Классификация методов шифрования. Требования к современным шифрам.
<b>Тема 7.</b> Методы шифрования с закрытым ключом.	Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Режимы работы блочных алгоритмов. Алгоритм криптографического преобразования данных ГОСТ 28147-89. Использование блочных алгоритмов шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.
<b>Тема 8.</b> Криптографические алгоритмы с открытым ключом.	Основные понятия и классификация средств асимметричной криптографической защиты информации. Основные свойства асимметричных криптосистем. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Алгоритм RSA. Алгоритм Эль-Гамала. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.
<b>Тема 9.</b> Электронная цифровая подпись	История развития. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамала. Стандарты на алгоритмы цифровой подписи. Управление открытыми ключами. Протокол аутентификации Нидхэма-Шредера в случаях симметричной и асимметричной системы шифрования. Модели атак и их возможные результаты.
<b>Тема 10.</b> Совершенно	Основные подходы к измерению информации. Энтропия и неопределенность. Норма языка и избыточность сообщений. Понятие

секретные системы.	совершенно секретной системы. Расстояние единственности.
--------------------	--

Курс дисциплины «Безопасность и защита информации в информационных системах» предусматривает следующие **формы организации учебного процесса**:

1. лекции;
2. лабораторные занятия;
3. самостоятельная работа студента.

Ссылки на электронные материалы по всем формам организации учебного процесса размещены на сайте <http://donnu.ru/phys/kt/bondarenko>.

По источнику передачи и восприятия учебной информации используются словесные (лекция, беседа), наглядные (иллюстрация, демонстрация), практические (исследования, упражнения, лабораторные работы) методы.

По характеру познавательной деятельности студентов используются объяснительно-иллюстративные и репродуктивные методы, проблемное преподавание, частично-поисковый и исследовательский методы.

В зависимости от основной дидактической цели и задач используются методы устного изложения знаний, закрепление учебного материала, самостоятельной работы студентов по осмыслению и усвоению нового материала, работы по применению знаний на практике и выработке умений и навыков, проверки и оценки знаний, умений и навыков.

Используются следующие методы контроля:

1. устный контроль (экспресс-опрос на лекциях);
2. проверка конспектов;
3. защита лабораторных работ;
4. проверка самостоятельных работ;
5. модульная контрольная работа (дидактическое тестирование);
6. экзамен.

### Тематический план

	Содержательный модуль 1											
Названия содержательных модулей и тем	Количество часов											
	Очная форма обучения						Заочная форма обучения					
	всего	В Т.Ч.					всего	В Т.Ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
Тема 1. Международные стандарты информационного обмена. Понятие угрозы.	18	2		4	12		18	0,4		0,8	16,8	



<b>Тема 2.</b> Виды возможных нарушений информационной системы. Защита.	18	2		4	12		18	0,4		0,8	16,8	
<b>Тема 3.</b> Основные положения теории информационной безопасности. Модели безопасности и их применение.	18	2		4	12		18	0,4		0,8	16,8	
<b>Тема 4.</b> Таксономия нарушений информационной безопасности и причины, обуславливающие их существование.	18	2		4	12		18	0,4		0,8	16,8	
<b>Тема 5.</b> Использование защищенных компьютерных систем.	18	2		4	12		18	0,4		0,8	16,8	
<b>Итого по 1-му содержательному модулю</b>	90	10		20	60	0	90	2		4	84	

	Содержательный модуль 2											
Названия содержательных модулей и тем	Количество часов											
	Очная форма обучения						Заочная форма обучения					
	всего	В Т.Ч.					всего	В Т.Ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
<b>Тема 6.</b> Предмет и задачи криптографии.	18	2		4	12		18	0,4		0,8	16,8	

<b>Тема 7.</b> Методы шифрования с закрытым ключом.	18	2		4	12		18	0,4		0,8	16,8	
<b>Тема 8.</b> Криптографические алгоритмы с открытым ключом.	18	2		4	12		18	0,4		0,8	16,8	
<b>Тема 9.</b> Электронная цифровая подпись.	18	2		4	12		18	0,4		0,8	16,8	
<b>Тема 10.</b> Совершенно секретные системы.	18	2		4	12		18	0,4		0,8	16,8	
<b>Итого по 2-му содержательному модулю</b>	90	10		20	60		90	2		4	84	
<b>Всего часов</b>	180	20		40	120		180	4		8	168	

## 5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРОВЕДЕНИЯ ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

### Темы лекционных занятий

<b>№ п/п</b>	<b>Название темы</b>	<b>Количество часов</b>
1.	Международные стандарты информационного обмена. Понятие угрозы.	2
2.	Виды возможных нарушений информационной системы. Защита.	2
3.	Основные положения теории информационной безопасности. Модели безопасности и их применение.	2
4.	Таксономия нарушений информационной безопасности и причины, обуславливающие их существование.	2
5.	Использование защищенных компьютерных систем.	2
6.	Предмет и задачи криптографии.	2
7.	Методы шифрования с закрытым ключом.	2
8.	Криптографические алгоритмы с открытым ключом.	2
9.	Электронная цифровая подпись.	2
10.	Совершенно секретные системы.	2
	<b>ВСЕГО</b>	<b>20</b>

### Темы лабораторных занятий

<b>№ п/п</b>	<b>Название темы</b>	<b>Количество часов</b>
1.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их	6

	существование	
2.	Анализ способов нарушений информационной безопасности	5
3.	Основные технологии построения защищенных систем	5
4.	Программная реализация алгоритма RSA	8
5.	Программная реализация криптографических протоколов	8
6.	Программная реализация ЭЦП	8
	<b>ВСЕГО</b>	<b>40</b>

## 6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

### Организация самостоятельной работы студентов

Самостоятельная работа студентов по курсу «Безопасность и защита информации в информационных системах» предусматривает:

- систематическое ведение конспекта лекций и повседневную проработку лекционного материала;
- изучение дополнительной технической литературы и интернет-источников, рекомендуемых этой программой;
- добросовестную подготовку к лабораторным занятиям;
- самостоятельную разработку алгоритмов и текстов программ лабораторных работ;
- изучение дополнительного инструментария;
- своевременное и качественное оформление отчётов по лабораторным работам.

<b>№ п/п</b>	<b>Название темы</b>	<b>Количество часов</b>
1.	Международные стандарты информационного обмена. Понятие угрозы.	12
2.	Виды возможных нарушений информационной системы. Защита.	12
3.	Основные положения теории информационной безопасности. Модели безопасности и их применение.	12
4.	Таксономия нарушений информационной безопасности и причины, обуславливающие их существование.	12
5.	Использование защищенных компьютерных систем.	12
6.	Предмет и задачи криптографии.	12
7.	Методы шифрования с закрытым ключом.	12
8.	Криптографические алгоритмы с открытым ключом.	12
9.	Электронная цифровая подпись.	12
10.	Совершенно секретные системы.	12
	<b>ВСЕГО</b>	<b>120</b>

## 7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Индивидуальные задания не предусмотрены учебной программой.

## 8. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Что такое информационная безопасность?

2. Какие предпосылки и цели обеспечения информационной безопасности?
3. Что включает в себя информационная борьба?
4. Каковы общие принципы обеспечения защиты информации?
5. Какие имеются виды угроз информационной безопасности предприятия (организации)?
6. Какие источники наиболее распространенных угроз информационной безопасности существуют?
7. Какие виды сетевых атак имеются?
8. Какими способами снизить угрозу sniffing пакетов?
9. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?

## 9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

### ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Физико-технический факультет

<i>Направление подготовки:</i>	<b>09.04.01 Информатика и вычислительная техника</b>
<i>Магистерская программа:</i>	<b>Информатика и вычислительная техника</b>
<i>Программа подготовки:</i>	<b>академическая магистратура</b>
<i>Семестр</i>	<b>1</b>
<i>Учебная дисциплина</i>	<b>Безопасность и защита информации в информационных системах</b>

### МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА 1 ВАРИАНТ №1

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется  
Выберите один ответ.
  - a. Компилятор
  - b. Интернет-черви
  - c. Вирус
2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется  
Выберите один ответ.
  - a. Воздействием (влиянием)
  - b. Потерей
  - c. Силой
3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется  
Выберите один ответ.
  - a. Троянской программой
  - b. Червем

- с. Вирусом
4. Уровень риска, который считается доступным для достижения желаемого результата, называется  
Выберите один ответ.
- a. Устойчивостью
  - b. Терпимостью по отношению к риску
  - c. Независимостью
5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд  
Выберите один ответ.
- a. Две
  - b. Одну
  - c. Сколько зададут
6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:  
Выберите один ответ.
- a. Статическими алгоритмами
  - b. Алгоритмы RMS
  - c. Динамическими алгоритмами
7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются: Выберите один ответ.
- a. Каталоги
  - b. Символьные файлы
  - c. Регулярные файлы
8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются  
Выберите один ответ.
- a. Вирусами
  - b. Руткитами
  - c. Червями
9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:  
Выберите один ответ.
- a. Правилами безопасности
  - b. Требованием безопасности
  - c. Мерами безопасности
10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:  
Выберите один ответ.
- a. Управление риском
  - b. Предупреждением рисков
  - c. Анализом рисков

Заведующий кафедрой  
Преподаватель

Ермоленко Т.В.  
Бондаренко В.И.

### Критерии оценивания модульного контроля

<i>Номер задания</i>	<i>Количество баллов</i>
Задание 1	2
Задание 2	2
Задание 3	2
Задание 4	2
Задание 5	2
Задание 6	2
Задание 7	2
Задание 8	2
Задание 9	2
Задание 10	2
<b>Всего</b>	<b>20</b>

### 10. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

#### ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

Физико-технический факультет

Направление подготовки: **09.04.01 Информатика и вычислительная техника**  
 Магистерская программа: **Информатика и вычислительная техника**  
 Программа подготовки: **академическая магистратура**  
 Семестр: **1**  
 Учебная дисциплина: **Безопасность и защита информации в информационных системах**

#### Экзаменационный билет 1

1. Атаки на систему безопасности и современные методы защиты.
2. Kerberos. Протокол распределения ключей.

Утверждено на заседании кафедры компьютерных технологий,  
протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой  
Экзаменатор

Ермоленко Т.В.  
Бондаренко В.И.

### Критерии оценивания экзамена

<i>Номер задания</i>	<i>Количество баллов</i>
Задание 1	15
Задание 2	25
Всего	40

## 11. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

1. Выберите правильный ответ. Криптография – это:
  - а) наука, изучающая развитие компьютерных технологий;
  - б) наука, занимающаяся изучением методов и средств защиты информации;
  - в) наука, занимающаяся изучением методов и средств распределения информации;
  - г) наука, занимающаяся изучением информации.
  
2. Выберите правильный ответ. Идентификатор – это:
  - а) уникальный признак данной информации, на основе которого можно доказательно установить ее подлинность;
  - б) уникальный признак данной информации, на основе которого можно доказательно установить ее существование;
  - в) уникальный признак нескольких видов информации, на основе которого можно доказательно установить их взаимосвязь;
  - г) уникальный признак информации, на основе которого можно установить ее целостность.
  
3. Выберите правильный ответ. Современная криптография включает в себя:
  - а) симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами;
  - б) симметричные криптосистемы, асимметричные криптосистемы, системы электронной подписи, управление ключами;
  - в) симметричные криптосистемы, криптосистемы с закрытым ключом, системы электронной подписи, управление ключами;
  - г) симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной защиты, блокировку ключами.
  
4. Выберите правильный ответ. Алфавит – это:
  - а) множество символов латинского алфавита;
  - б) конечное множество используемых для кодирования информации знаков;
  - в) бесконечное множество используемых для кодирования информации знаков;
  - г) конечное множество используемых для кодирования информации цифр.
  
5. Выберите правильный ответ. Текст – это:
  - а) неупорядоченный набор из элементов алфавита;
  - б) упорядоченный набор слов;
  - в) упорядоченный набор из элементов алфавита;
  - г) неупорядоченный набор слов.
  
6. Выберите правильный ответ. Шифрование – это:
  - а) процесс получения данных;
  - б) процесс суммирования информации;
  - в) процесс зашифрования и расшифрования;
  - г) процесс преобразования данных.
  
7. Выберите правильный ответ. Криптосистемы подразделяются на:
  - а) симметричные и асимметричные;
  - б) числовые и символьные;

- в) открытые и закрытые;
- г) положительные и отрицательные.

8. Выберите правильный ответ. Один и тот же ключ используется:

- а) симметричных криптосистемах;
- б) асимметричных криптосистемах;
- в) символьных криптосистемах;
- г) числовых криптосистемах.

9. Выберите правильный ответ. Электронной подписью называется:

- а) подпись в конце текста;
- б) набор символов, позволяющий проверить подлинность сообщения;
- в) присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;
- г) присоединяемое к тексту его название, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;

Выберите правильный ответ. Криптостойкость – это:

- а) характеристика шифра, определяющая его стойкость к расшифрованию без знания ключа;
- б) характеристика шифра, определяющая его стойкость к расшифрованию с использованием ключа;
- в) характеристика шифра, определяющая его стойкость к шифрованию без знания ключа;
- г) характеристика шифра, определяющая его стойкость к копированию без знания ключа.

10. Выберите правильный ответ. Моноалфавитные подстановки – это:

- а) вид преобразований, заключающийся в замене символов исходного текста на другие по более или менее сложному правилу;
- б) вид преобразований, заключающийся в добавлении символов по более или менее сложному правилу;
- в) вид преобразований, заключающийся в удалении символов исходного текста по более или менее сложному правилу;
- г) вид преобразований, заключающийся в преобразовании символов исходного текста по более или менее сложному правилу.

## 12. КРИТЕРИИ ОЦЕНИВАНИЯ

***Распределение баллов, которые могут получить студенты  
в процессе изучения дисциплины***

*Четвертый семестр*

Содержательный модуль №1				Содержательный модуль №2				Всего
Лабораторные работы			Мод. контр. работа	Лабораторные работы			Экзамен	
№1	№2	№3	№1	№4	№5	№6	№2	



Макс. балл	5	5	5	20	35	5	10	10	40	65	100
------------	---	---	---	----	----	---	----	----	----	----	-----

Согласно модульному принципу организации учебного процесса, содержание дисциплины включает в себя два зачётных модуля. Каждый зачётный модуль состоит из теоретического материала и практических задач, выполнение которых требует овладения теорией в указанном в модуле объёме.

К первому модульному контролю студент должен защитить 3 лабораторные работы. *За первую, вторую и третью* лабораторные работы студент может получить по 5 балла.

На первом модульном контроле студент имеет возможность получить 20 баллов за ответы на тестовые вопросы. К каждому тестовому вопросу предполагается не менее четырех вариантов ответа.

К экзамену студент должен защитить 3 следующие лабораторные работы. За четвёртую работу студент может получить 5 балла, за пятую и шестую работу - по 10 баллов.

На экзамене студент имеет возможность получить 40 баллов, ответив на 2 вопроса. Ответы на первый вопрос оцениваются в 15 баллов, на второй – в 25.

### ***Шкала соответствия баллов национальной шкале***

<b>Оценка по шкале ECTS</b>	<b>Оценка по 100-балльной шкале</b>	<b>Оценка по государственной шкале (экзамен, дифференцированный зачет)</b>	<b>Оценка по государственной шкале (зачет)</b>
<b>A</b>	90-100	5 (отлично)	зачтено
<b>B</b>	80-89	4 (хорошо)	зачтено
<b>C</b>	75-79	4 (хорошо)	зачтено
<b>D</b>	70-74	3 (удовлетворительно)	зачтено
<b>E</b>	60-69	3 (удовлетворительно)	зачтено
<b>FX</b>	35-59	2 (неудовлетворительно) с возможностью повторной сдачи	не зачтено
<b>F</b>	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

Оценка за овладение курса выставляется по следующим принципам:

– Оценку «отлично» заслуживает студент, который обнаружил глубокие знания при ответах на теоретические вопросы по темам курса, а также выполнил практические задания в полном объёме и набрал более 90 баллов.

– Оценку «хорошо» заслуживает студент, сделавший ошибки в теоретических или практических ответах, которые могут быть интерпретированы как малосущественные для вопросов, которые рассматривались. Студент должен набрать более 75 баллов.

– Оценку «удовлетворительно» заслуживает студент, который выполнил задания неполно и с ошибками, но при этом набрал более 60 баллов.

– Оценку «неудовлетворительно» заслуживает студент, который не выполнил большинства теоретических и практических задач и набрал менее 60 баллов.

## **13. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА**

Лекционные занятия проводятся в аудитории, оснащенной мультимедийной техникой и доской.

Лабораторные занятия проводятся в компьютерном классе, оборудованном компьютерами с лицензионным программным обеспечением, доступом к сети Интернет, столами и доской.

#### 14. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
<i>Основная литература</i>			
1.	Башлы П. Н. Информационная безопасность [Электронный учебник] : учебное пособие / Башлы П. Н.. - Евразийский открытый институт, 2012. - 311 с.		<a href="http://iprbookshop.ru/10677">http://iprbookshop.ru/10677</a>
2.	Ищeyнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации. Учебное пособие - М.: Форум : ИНФРА-М, 2014. – 256 с.		
<i>Дополнительная литература</i>			
3.	Алферов А.П., Зубов А.Ю. и др. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с, ил		

#### 15. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Ссылки на электронные материалы курса. URL: <http://donnu.ru/phys/kt/bondarenko> (дата обращения 10.03.2020 г.)
2. Информационная система "Единое окно доступа к образовательным ресурсам" URL: <http://window.edu.ru/> (дата обращения 10.03.2020 г.)
3. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) URL: <http://www.vlibrary.ru/> (дата обращения 10.03.2020 г.)

#### 16. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Python 3 или более старших версий.
2. Программное средство PGP
3. Visual Studio 2015 или более старших версий

Рабочая программа рассмотрена и переутверждена на заседании кафедры компьютерных технологий с изменениями (без изменений) на 2020 год.

Протокол № 12 от «2» апреля 2020 г.

Заведующий кафедрой

Ермоленко Т.В.

Рабочая программа рассмотрена и переутверждена на заседании кафедры компьютерных технологий с изменениями (без изменений) на 2021 год.

Протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_ 2021 г.

Заведующий кафедрой