

**ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Кафедра информационных систем управления

УТВЕРЖДАЮ:

Проректор по научно-методической
и учебной работе

Е.И. Скафа
«22» апреля 2020 г.
МП



**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И
ЗАЩИТА ИНФОРМАЦИИ»**

Направление подготовки:	46.03.02 Документоведение и архивоведение
Образовательная программа:	бакалавриат
Квалификация:	академический бакалавр
Форма обучения:	очная, в том числе с ускоренным сроком обучения; заочная, в том числе с ускоренным сроком обучения

Донецк 2020

УТВЕРЖДАЮ:


Декан факультета математики и
информационных технологий
И.А. Моисеенко



Программа учебной дисциплины «Информационная безопасность и защита информации» составлена на основании Государственного образовательного стандарта высшего профессионального образования (ГОС ВПО) Донецкой Народной Республики (ДНР) по направлению подготовки 46.03.02 Документоведение и архивоведение, утвержденного приказом Министерства образования и науки ДНР от 20 апреля 2016 г. № 411 (в редакции Приказа Министерства образования и науки Донецкой Народной Республики от 22 мая 2018 г. № 485); 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 высшего профессионального образования направления подготовки 46.03.02 Документоведение и архивоведение, разработанных в ГОУ ВПО «Донецкий национальный университет».

Разработчики:

доцент, кандидат экономических наук, доцент
кафедры информационных систем управления

 Н. Ш. Пономаренко

старший преподаватель
кафедры информационных систем управления

 А.И. Балдынюк

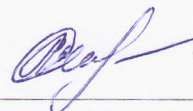
Программа учебной дисциплины утверждена на заседании кафедры
информационных систем управления

Протокол №11 от «14» апреля 2020 г.
Заведующий кафедрой

 Н. Ш. Пономаренко

Программа учебной дисциплины одобрена учебно-методической комиссией
факультета математики и информационных технологий
Протокол № 8 от «15» апреля 2020 г.

Председатель учебно-методической
комиссии факультета

 Л.И. Селякова

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Информационная безопасность и защита информации» относится к базовой части профессионального блока дисциплин по направлению подготовки 46.03.02 Документоведение и архивоведение. Изучение данной дисциплины основывается на базе дисциплин: информатика, информационные технологии, информационное право, информационные системы в предпринимательстве.

Дисциплина является базовой для последующего изучения дисциплин профессионального цикла: правовые основы управления документацией и архивами за рубежом, информационная деятельность в государственных органах и учреждениях.

Нормативные ссылки – не предусмотрено

2. СТРУКТУРА ДИСЦИПЛИНЫ

<i>Характеристика учебной дисциплины</i>				
Направление подготовки	46.03.02 Документоведение и архивоведение			
Образовательная программа	бакалавриат			
Квалификация	академический бакалавриат			
Количество содержательных модулей (тем)	1 (12)			
Дисциплина базовой / вариативной части образовательной программы	Базовая часть профессионального блока			
Формы контроля	1 модульный контроль и 1 экзамен			
Показатели	очная форма обучения		заочная форма обучения	
	нормат. срок	ускор. срок	нормат. срок	ускор. срок
Количество зачетных единиц (кредитов)	3	3	3	3
Год подготовки	4	2	4	2
Семестр	7	3	-	-
Количество часов	108	108	108	108
- лекционных	18	18	2	2
- практических, семинарских	36	36	8	8
- лабораторных				
- самостоятельной работы	54	54	98	98
в т.ч. индивидуальное задание				
Недельное количество часов,	6	6		
в т.ч. аудиторных	3	3		

АР- академразница

3.ОПИСАНИЕ ДИСЦИПЛИНЫ

Цели и задачи

Цель – овладение теоретическими, практическими и методическими вопросами

обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения.

Задачи дисциплины:

формирование у студентов знаний об (о):

- основных понятиях, используемых в сфере информационной безопасности и защиты информации;
- основных нормативно-правовых основ информационной безопасности и защиты информации;
- направлениях, возможностях и преимуществах информационной безопасности и защиты информации;
- существующих направлениях использования современных средств информационной безопасности и защиты информации;
- основных характеристиках различных программно-технических средств информационной безопасности и защиты информации;
- современном состоянии информационного рынка специализированного программного обеспечения в области информационной безопасности и защиты информации;
- основных этапах внедрения средств защиты информации;
- структуре, составе и свойствах информационных процессов, систем и технологий, используемых при защите информации.

Требования к результатам освоения дисциплины: процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с требованиями ГОС ВПО по направлению подготовки 46.03.02 Документоведение и архивоведение и основной образовательной программы высшего образования направления подготовки 46.03.02 Документоведение и архивоведение:

а) общекультурных (ОК)

способность к самоорганизации и самообразованию (ОК-7);

способностью к использованию основных методов, способов и средств получения, хранения, переработки информации (ОК-10);

б) общепрофессиональных (ОПК):

владение базовыми знаниями в области информационных технологий (программные продукты, используемые в управлении документами, системы электронного документооборота, технологии сканирования документов) (ОПК-2);

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-6).

в) профессиональных (ПК):

научно-исследовательская деятельность:

способность анализировать ценность документов с целью их хранения (ПК-8);

технологическая деятельность:

владение методами защиты информации (ПК-17); **организационно-**

управленческая деятельность:

способностью и готовностью создавать и вести единые (корпоративные) системы документационного обеспечения управления и архивного хранения документов в

организации на базе новейших технологий (ПК-13);

владением нормами и навыками работы с документами, содержащими государственные и иные виды тайн (ПК-18).

В результате изучения учебной дисциплины студент должен

знать:

правовые, организационные и технические основы систем и средств защиты информации; методы и средства противодействия несанкционированному доступу к информации; классификацию систем и средств обеспечения информационной безопасности; базовые принципы законы, на которых основано функционирование различных систем и средств защиты информации;

уметь:

выявлять возможные способы нарушения информационной безопасности при работе с автоматизированными системами обработки и хранения; применять нормативные и правовые базы обеспечения деятельности в области информационной безопасности и защиты информации; осуществлять организационные и технические мероприятия по обеспечению информационной безопасности;

владеть:

навыками профессиональной работы с научной литературой и источниками по информационной безопасности и защите информации; навыками получения в интернет-среде научно-корректной информации по информационной безопасности и защите информации.

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Курс дисциплины «Информационная безопасность и защита информации» предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельную работу студента.

Материал излагается с использованием объяснительно-иллюстративных, эвристических и исследовательских методов преподавания. При проведении лекции-визуализации для обсуждения материала широко используются мультимедийные презентации, анимации. Также проводятся проблемные, информационные лекции.

В учебном процессе широко применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, выполнение заданий по составлению и оформлению документов, дискуссия, полемика), внеаудиторная самостоятельная работа, балльно-рейтинговая система оценки успеваемости, личностно-ориентированное обучение, проблемное обучение, блочно-модульное обучение.

Предусмотрено использование в учебном процессе Интернет-ресурсов по данному курсу для решения практических заданий и проведения практических занятий.

Самостоятельная работа студентов предусматривает выполнение индивидуальных заданий, подготовку к практическим занятиям, изучение учебно-методической литературы и ресурсами сети Интернет, составление конспектов, защита презентаций и докладов, участие в проведении экспертных опросов.

Порядковый номер и тема	Краткое содержание темы
Тема 1. Информационная безопасность как составляющая общественной безопасности	Понятие безопасности. Национальная безопасность. Безопасность в экономической сфере. Цели экономической безопасности, ее содержание и структура. Международные договоры, доктрины в области информационной безопасности. Соперничество в информационной сфере, информационные войны. Законодательство в области интеллектуальной

	собственности, информационных ресурсов, информационных продуктов и информационных услуг. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности.
Тема 2. Основы информационной безопасности и защиты информации	Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Место, цели и задачи информационной безопасности в бизнесе. Правовые механизмы защиты в нормах законов, регулирующие отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения. Соотношение понятий информационной безопасности и безопасности информации.
Тема 3. Виды и особенности угроз информационной безопасности	Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений
Тема 4. Правовое регулирование открытых информационных ресурсов	Защита информации институтом интеллектуальной собственности. Реализация интеллектуально собственности на документированную информацию. Отношения средств массовой информации с гражданами и организациями. Ответственность за нарушение законодательства о средствах массовой информации.
Тема 5. Правовая защита информационных ресурсов	Понятие тайны, секрета, конфиденциальности. Субъекты и объекты информационных правоотношений в области государственной тайны. Производственная тайна. Служебная тайна. Профессиональная тайна. Банковская тайна. Тайны личная и семейная. Понятия-"фирменные секреты", технологические секреты (ноу-хау)", "научные секреты (ноу-ноу)". Документированная информация (документы) секретная и несекретная. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Конфиденциальность информации в вычислительных системах и сетях.
Тема 6. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия	Понятие аналитической работы, ее цели и задачи. Аналитическая работа по выявлению каналов несанкционированного доступа к информации. Понятие, цели и задачи системы защиты конфиденциальной информации. Компьютерные технологии и формирование основ системы защиты информации. Структура комплексной системы защиты информации (КСЗИ).
Тема 7. Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Задачи службы безопасности, основные функции. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации, аналитического подразделения, подразделения охраны и пропускного режима. Взаимодействие службы безопасности и

	службы персонала. Профессиональные и психологические требования к сотрудникам службы безопасности. Анализ и оценка надежности и эффективности применяемой системы защиты.
Тема 8. Защита информации при проведении совещаний и переговоров	Угрозы безопасности информации и задачи ее защиты в процессе проведения совещаний и переговоров, приеме посетителей. Виды совещаний и переговоров. Правила подготовки и проведения совещаний и переговоров. Документирование информации, оформление стенограмм, протоколов и итоговых документов. Порядок использования аудио- и видеозаписи. Инженерно-технические требования к помещениям, их охране.
Тема 9. Защищенный документооборот	Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков. Понятие, принципы, цели и задачи защищенного документооборота как совокупности документопотоков. Критерии безопасности документооборота. Основные требования к защищенному документообороту. Взаимосвязь персональной избирательности в доставке информации и разрешительной системы доступа. Особенности защищенного безбумажного (электронного) документооборота. Принципиальная взаимосвязь документопотока и применяемой технологической системы обработки и хранения документов.
Тема 10. Технологические системы защиты и обработки конфиденциальных документов	Виды угроз документированной информации, исходящие от технологической системы. Задачи защиты информации решаемые технологической системой. Место и назначение технологической системы обработки и хранения конфиденциальных документов в системе защиты информации и защищенном документообороте.
Тема 11. Инженерно-техническая защита	1 Физические средства защиты. Угрозы безопасности собственности фирмы и персоналу. Виды охраняемых объектов, категории защищаемых помещений. Построение системы охраны объекта. Классификация и характеристика классификационных групп технических средств охраны. Охранные системы. Охранное телевидение. Ограждение и физическая изоляция. Запирающие устройства. Классификация экстремальных (чрезвычайных) ситуаций. Аппаратные средства защиты.
Тема 12. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Критерии оценки защищенности систем информационной безопасности. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Методика применения антивирусных программ. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования.

Тематический план

Названия содержательных модулей и тем	Количество часов																							
	Очная форма												Заочная форма											
	Нормативный срок обучения						Ускоренный срок обучения						Нормативный срок обучения						Ускоренный срок обучения					
	всего	в т.ч.					всего	в т.ч.					всего	в т.ч.					всего	в т.ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	Самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Тема 1. Информационная безопасность как составляющая общественной безопасности	9	1,5	3		4,5		9	1,5	3		4,5		8,8	0,1	0,6		8,1		8,8	0,1	0,6		8,1	
Тема 2. Основы информационной безопасности и защиты информации	9	1,5	3		4,5		9	1,5	3		4,5		8,8	0,1	0,6		8,1		8,8	0,1	0,6		8,1	
Тема 3. Виды и особенности угроз информационной безопасности	9	1,5	3		4,5		9	1,5	3		4,5		8,8	0,1	0,6		8,1		8,8	0,1	0,6		8,1	
Тема 4. Правовое регулирование открытых информационных ресурсов	9	1,5	3		4,5		9	1,5	3		4,5		8,8	0,1	0,6		8,1		8,8	0,1	0,6		8,1	
Тема 5. Правовая защита информационных ресурсов	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Тема 6. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Тема 7. Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	

Тема 8. Защита информации при проведении совещаний и переговоров	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Тема 9. Защищенный документооборот	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Тема 10. Технологические системы защиты и обработки конфиденциальных документов	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Тема 11. Инженерно-техническая защита	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Тема 12. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	9	1,5	3		4,5		9	1,5	3		4,5		9	0,2	0,7		8,2		9	0,2	0,7		8,2	
Всего:	108	18	36		54		108	18	36		54		108	2	8		98		108	2	8		98	

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

Темы лекционных занятий

<i>№ п/п</i>	<i>Название темы</i>	Количество часов			
		Очная форма с нормативным сроком обучения	Очная форма с ускоренным сроком обучения	Заочная форма нормативным сроком обучения	Заочная форма с ускоренным сроком обучения
1	Информационная безопасность как составляющая общественной безопасности	1,5	1,5	0,1	0,1
2	Основы информационной безопасности и защиты информации	1,5	1,5	0,1	0,1
3	Виды и особенности информационной безопасности	1,5	1,5	0,1	0,1
4	Правовое регулирование открытых информационных ресурсов	1,5	1,5	0,1	0,1
5	Правовая защита информационных ресурсов.	1,5	1,5	0,2	0,2
6	Основные направления и этапы работ по созданию комплексной системы безопасности Предприятия	1,5	1,5	0,2	0,2
7	Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	1,5	1,5	0,2	0,2
8	Защита информации при проведении совещаний и переговоров.	1,5	1,5	0,2	0,2
9	Защищенный документооборот	1,5	1,5	0,2	0,2
10	Технологические системы защиты и обработки конфиденциальных документов	1,5	1,5	0,2	0,2
11	Инженерно-техническая защита	1,5	1,5	0,2	0,2
12	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	1,5	1,5	0,2	0,2
	ВСЕГО	18	18	2	2

Темы практических занятий

№ n/n	Название темы	Количество часов			
		Очная форма с нормативным сроком обучения	Очная форма с ускоренным сроком обучения	Заочная форма нормативны м сроком обучения	Заочная форма с ускоренным сроком обучения
1	Информационная безопасность как составляющая общественной безопасности	3	3	0,6	0,6
2	Основы информационной безопасности и защиты информации	3	3	0,6	0,6
3	Виды и особенности информационной безопасности	3	3	0,6	0,6
4	Правовое регулирование открытых информационных ресурсов	3	3	0,6	0,6
5	Правовая защита информационных ресурсов.	3	3	0,7	0,7
6	Основные направления и этапы работ по созданию комплексной системы безопасности Предприятия	3	3	0,7	0,7
7	Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	3	3	0,7	0,7
8	Защита информации при проведении совещаний и переговоров.	3	3	0,7	0,7
9	Защищенный документооборот	3	3	0,7	0,7
10	Технологические системы защиты и обработки конфиденциальных документов	3	3	0,7	0,7
11	Инженерно-техническая защита	3	3	0,7	0,7
12	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	3	3	0,7	0,7
	ВСЕГО	36	36	8	8

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа имеет особенное значение для креативного (творческого) усвоения основных понятий и категорий архивоведения. Самостоятельная работа студента является важной формой учебного процесса, которая позволяет приобрести, а также закрепить новые знания, навыки и умения, сформировать личные убеждения, использовать полученные знания и умения в практической деятельности. Она осуществляется на протяжении всего процесса обучения и имеет следующие формы:

- 1) подготовка к лекции;
- 2) подготовка к практическому занятию;
- 3) индивидуальная работа по заданию преподавателя в виде подготовки доклада с мультимедийной презентацией (индивидуального творческого проекта или реферата).
- 4) подготовка к экзамену.

Организация самостоятельной работы студентов

№ п/п	Название темы	Количество часов			
		Очная форма с нормативным сроком обучения	Очная форма с ускоренным сроком обучения	Заочная форма нормативны м сроком обучения	Заочная форма с ускоренным сроком обучения
1	Информационная безопасность как составляющая общественной безопасности	4,5	4,5	8,1	8,1
2	Основы информационной безопасности и защиты информации	4,5	4,5	8,1	8,1
3	Виды и особенности информационной безопасности	4,5	4,5	8,1	8,1
4	Правовое регулирование открытых информационных ресурсов	4,5	4,5	8,1	8,1
5	Правовая защита информационных ресурсов.	4,5	4,5	8,2	8,2
6	Основные направления и этапы работ по созданию комплексной системы безопасности Предприятия	4,5	4,5	8,2	8,2
7	Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	4,5	4,5	8,2	8,2
8	Защита информации при проведении совещаний и переговоров.	4,5	4,5	8,2	8,2
9	Защищенный документооборот	4,5	4,5	8,2	8,2
10	Технологические системы защиты и обработки конфиденциальных документов	4,5	4,5	8,2	8,2
11	Инженерно-техническая защита	4,5	4,5	8,2	8,2
12	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	4,5	4,5	8,2	8,2
	ВСЕГО	54	54	98	98

7. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Одним из видов индивидуальной работы студентов является подготовка доклада с мультимедийной презентацией. Цель данной работы – осмысление и углубление знаний по данной дисциплине, развитие навыков самостоятельной работы по сбору, систематизации материала, проведению исследования и анализа. Являясь одним из видов научно-исследовательской работы студентов, подготовка доклада с мультимедийной презентацией способствует формированию у студентов аналитического, творческого мышления.

Темы индивидуальных заданий

1. Угрозы сохранности данных в компьютере случайного характера.
2. Устройства электропитания компьютера, применяемые для защиты компьютера от неблагоприятных воздействий питающей электросети.
3. Дефекты магнитных дисков.
4. Простые приемы, используемые для защиты компьютера от умышленных действий.
5. Классификация вирусов.
6. Классификация антивирусных программ.
7. Компьютерная преступность. Виды преступной деятельности.
8. Преступления, связанные с нарушением частной тайны.
9. Информационные процессы.
10. Информационные технологии и их основные свойства.
11. Понятия сигнала, сообщения и данных.
12. Методы защиты информации от преднамеренного доступа.
13. Методы обеспечения безопасности каналов передачи данных.
14. Методы обеспечения достоверности передачи информации (методов защиты от ошибок).
15. Механизмы обеспечения безопасности радиолиний.
16. Криптографическая защита информации (основные понятия).
17. Методы шифрования данных.
18. Стандарт шифрования данных DES.
19. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
20. Особенности процессов аутентификации в корпоративной среде.
21. Квантовая криптография.
22. Утечки информации: как избежать. Безопасность смартфонов.
23. Безопасность применения пластиковых карт - законодательство и практика.
24. Защита CD- и DVD-дисков от копирования.
25. Современные угрозы и защита электронной почты.
26. Программные средства анализа локальных сетей на предмет уязвимостей.
27. Безопасность применения платежных систем - законодательство и практика.
28. Аудит программного кода по требованиям безопасности.
29. Антишпионское ПО (antispysware).
30. Обеспечение безопасности Web-сервисов.
31. Защита от внутренних угроз.
32. Технологии RFID.

Критерии оценивания индивидуальной работы студента:

1. Цель работы: насколько четко сформулирована.
2. Структура: логичность и последовательность изложения материала.
3. Аргументация: обоснованность, убедительность, наличие позитивной оценки и возможной критики, серьезность научных источников.

4. Научный поиск: использование соответствующей литературы, объем проведенных научных исследований.
5. Язык работы: понятность, грамотность.
6. Творческий момент: творческое отношение к отбору, обработке материалов, наличие оригинальных выводов.

8. ВОПРОСЫ К МОДУЛЬНОМУ КОНТРОЛЮ

1. Раскрыть понятия: информации, компьютерной информации (формы существования компьютерной информации).
2. Информационная безопасность. Основные компоненты концептуальной модели информационной безопасности.
3. Информация как собственность. Собственник, владелец и пользователь информационных ресурсов.
4. Угроза информации в нарушении ее целостности.
5. Угроза информации в нарушении ее конфиденциальности.
6. Угроза информации в нарушении ее доступности.
7. Неправомерные способы овладения информацией. Разглашение. Утечка. Несанкционированный доступ.
8. Основные способы, средства и направления защиты компьютерной информации.
9. Коллизии между информационными угрозами. Угроза раскрытия системы информационной защиты.
10. Требования к системе защиты информации.
11. Модель информационного нарушителя. Цели информационных нарушителей. Иерархия информационных нарушителей.
12. Хакеры. Классификации хакеров.
13. Определение и классификация правовой защиты информации.
14. Интересы личности, общества и государства в информационной сфере.
15. Информация как собственность. Собственник, владелец и пользователь информационных ресурсов.
16. Структура информационных ресурсов по характеру доступа.
17. Привести примеры правонарушений в сфере защиты информации. Составы преступлений, предусмотренные за нарушение режима защиты информации.
18. Электронная цифровая подпись. Закон об электронной цифровой подписи.
19. Факты, свидетельствующие о существовании у человечества «магнитно-информационной зависимости».
20. Проблема целостности и проблема конфиденциальности информации на магнитных носителях.
21. Используемые методы защиты от непосредственного доступа к магнитным носителям.
22. Интеллектуальные возможности контроллера жесткого магнитного диска. Программное обеспечение для доступа и управления этими возможностями.
23. Технология самонаблюдения, анализа и сообщения жесткого магнитного диска (SMART).
24. Физические принципы удаления и восстановления информации на магнитных носителях. Способы уничтожения информации на жестких магнитных дисках.
25. Обычные способы удаления файлов в файловых системах FAT, NTFS. Возможности программ «шредеров». Программные и аппаратные средства уничтожения информации на HDD.
26. Гарантированное уничтожение с разрушением магнитного носителя.

9. ОБРАЗЕЦ МОДУЛЬНОГО КОНТРОЛЯ

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ» ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ	
Направление подготовки:	46.03.02 Документоведение и архивоведение
Образовательная программа	бакалавриат
Семестр	7
Учебная дисциплина	Информационная безопасность и защита информации
МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА Вариант № 1	
<ol style="list-style-type: none"> 1. Информационная безопасность. Основные компоненты концептуальной модели информационной безопасности. 2. Обычные способы удаления файлов в файловых системах FAT, NTFS. Возможности программ «шредеров». Программные и аппаратные средства уничтожения информации на HDD. 	
Утверждено на заседании кафедры информационных систем управления, протокол № ____ от “__” _____ 20__ г.	
Зав. кафедрой _____ Преподаватель _____	Н. Ш. Пономаренко А.И. Балдынюк

Критерии оценивания модульного контроля

Номер задания	Количество баллов
Задание 1	5
Задание 2	5
Всего	10 баллов

10. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Контрольные вопросы к экзамену

1. Основные понятия информационной безопасности и защиты информации.
2. Определить место информационной безопасности в обеспечении системы общественной безопасности.
3. Система защиты информации.
4. Методы, способы и техника защиты информации.
5. Структура информационной сферы.
6. Основные составляющие национальных интересов (интересы личности, общества и государства) в информационной сфере.
7. Уровни формирования режима информационной безопасности
8. Политика безопасности.
9. Информационная безопасность и безопасность информации.
10. Основные субъекты государственной системы защиты информации.
11. Каналы утечки информации.
12. Принципы государственной политики обеспечения информационной безопасности.

13. Особенности построения единой системы информационной безопасности в государстве.
14. Государственная система организационно-правового обеспечения информационной безопасности.
15. Понятие и классификация угроз безопасности информации
16. Информационная сфера и информационная безопасность государственных органов. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности.
17. Контроль эффективности защиты информации.
18. Структура угроз безопасности.
19. Соотношение понятий информационной безопасности и безопасности информации.
20. Задачи информационной безопасности общества.
21. Классификация технических каналов утечки информации.
22. Характеристика и классификация способов подслушивания.
23. Способы несанкционированного доступа к информации в компьютерных системах по типу используемых слабостей системы информационно-компьютерной безопасности.
24. Инженерно-технические мероприятия по защите информации.
25. Криптографические средства защиты информации.
26. Похищение документов, содержащих защищаемые сведения.
27. Незаконное получение конфиденциальной информации путем перехвата информации, циркулирующей в технических средствах и помещениях.
28. Незаконное получение конфиденциальной информации.
29. Незаконное завладение конфиденциальной информацией содержащейся в средствах вычислительной техники и автоматизированных системах.
30. Правовые меры, регламентирующие вопросы защиты информации.
31. Признаки умышленных действий, направленных на похищение документов.
32. Классификация автоматизированных систем и требования по защите информации.
33. Особенности построения единой системы информационной безопасности в государстве.
34. Незаконное получение конфиденциальной информации путем внедрения агентов.
35. Классификация угроз безопасности информации в компьютерных системах.
36. Разграничение доступа к информации в компьютерных системах.
37. Понятие и классификация видов и методов несанкционированного доступа.
38. Вредоносные программы: определение и классификация. Защита информации от разрушающих программных воздействий.
39. Государственные стандарты шифрования.
40. Криптографические методы и средства защиты информационных процессов в компьютерных системах.
41. Разновидности вредоносных программ.
42. Направления разработки правового обеспечения защиты информации.
43. Общие принципы шифрования информации.
44. Основные составляющие национальных интересов в ДНР (интересы личности, общества и государства) в информационной сфере.
45. Контроль эффективности защиты информации.
46. Похищение документов, содержащих защищаемые сведения.
47. Основные категории органов защиты информации.
48. Агентурная разведка как наиболее эффективный способ получения защищаемой информации.

49. Задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.

50. Факты, свидетельствующие о существовании у человечества «магнитно-информационной зависимости».

51. Модель информационного нарушителя. Цели информационных нарушителей.

52. Неправомерные способы овладения информацией. Разглашение. Утечка. Несанкционированный доступ.

53. Критерии выделения конфиденциальных документов из общего потока поступающих документов.

54. Последовательность, условия и формы допуска должностных лиц к государственной тайне.

55. Каналы утечки информации.

56. Задачи информационной безопасности общества.

11.ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ» ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	
<i>Направление подготовки:</i> 46.03.02 Документоведение и архивоведение <i>Образовательная программа</i> бакалавриат <i>Семестр</i> 7 <i>Учебная дисциплина</i> Информационная безопасность и защита информации	
БИЛЕТ №1	
1. Основные понятия информационной безопасности и защиты информации. 2. Система защиты информации. 3. Методы, способы и техника защиты информации	
Утверждено _____ на _____ заседании _____ кафедры _____, протокол № ____ от «____» _____ 20__ г.	
Заведующий кафедрой Экзаменатор	_____ _____
Н.Ш. Пономаренко А.И. Балдынюк	

12.ОБРАЗЕЦ ТЕСТОВЫХ ЗАДАНИЙ

1.Защита информации от несанкционированного воздействия - это деятельность по предотвращению:

а. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

б. воздействия с нарушением установленных прав и/или правил на изменение

информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

с. воздействия на защищаемую информацию ошибок пользователя информацией, сбой технических и программных средств информационных систем, а также природных явлений;

д. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

е. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

13. КРИТЕРИИ ОЦЕНИВАНИЯ

В течение семестра обучающийся может заработать баллы за следующие виды деятельности: модульную контрольную работу, практические задания по дисциплине, индивидуальные творческие задания (рефераты, презентации, доклады), индивидуальную творческую работу (подготовка и выступление с докладом на студенческой научной конференции).

Оценка знаний студентов проводится по 100-балльной шкале согласно следующим критериям:

№ п/п	Виды контрольных мероприятий	Количество баллов
	Тема 1	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы	0,5
	Тема 2.	
1.	Ответы на контрольные вопросы и тесты	0,5
	Тема 3	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 4	
1.	Ответы на контрольные вопросы и тесты	0,5
	Тема 5	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 6	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 7	
1.	Практическое задание	4
3.	Ответы на контрольные вопросы и тесты	0,5
	Тема 8	
1.	Ответы на контрольные вопросы и тесты	0,5
	Тема 9	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 10	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 11	
1.	Практическое задание	4

2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 12	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Модульный контроль	10
	Индивидуальное задание	11,5
	Экзамен	40
	Всего за семестр:	100

Шкала соответствия баллов государственной шкале

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

14. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Лекционные и практические занятия проводятся в учебной аудитории для проведения занятий лекционного типа, практических занятий, текущего контроля и промежуточной аттестации, оснащенной комплектом учебной мебели, комплектом рабочего места преподавателя, меловой (маркерной) доской, 1 мультимедийным проектором, ноутбуком (1 шт.).

15. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

№ п/п	Наименование	Кол-во экземпляров в библиотеке ДонНУ	Наличие электронной версии в ЭБС
Основная литература			
1.	Мельников, В. П. Информационная безопасность : учеб. пособие для студентов среднего проф. образования / В. П. Мельников и др. ; под ред. С. А. Клейменова. - 2-е изд. - Москва : Академия, 2007. - 331,[1] с.	1	-
2.	Информационная безопасность: (письменная справка) / [сост. Н. А. Фесенко] ; ДонНУ. Науч. б-ка. Справ.-библиогр. отд. - Донецк : ДонНУ, 2016. - 16 с.	1	-

Дополнительная литература			
3.	Бабак, В. П. Інформаційна безпека та сучасні мережеві технології : Англо-укр.-рос. слов. термінів / В. П. Бабак, О. Г. Корченко ; Нац. авіац. ун-т. - К. : НАУ, 2003. - 667 с.	2	-
4.	Информационная безопасность открытых систем [Текст] : учебник для студентов вузов, обучающихся по специальности 075500 (090105) - "Комплексное обеспечение информационной безопасности автоматизированных систем" : [в 2 т.]. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. - М. : Горячая Линия-Телеком, 2006. - 535 с.	10	-
5.	Ленков, С. В. Методы и средства защиты информации [Текст] : в 2 т. Т. 2 : Информационная безопасность / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. - Киев : Арий, 2008. - 342 с.	1	-
6.	Малюк, А. А. Информационная безопасность: концептуальны и методологические основы защиты информации : [Учеб. пособие для студентов вузов специальности 075400 "Комплексная защита объектов информации"] / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с.	2	-
7.	Садердинов, Али А. Информационная безопасность предприятия : Учеб. пособие / Садердинов А.А., Трайнев В.А., Федулов А.А. ; Междунар. акад. наук информации., информ. процессов и технологий (МАН ИПТ). - 2-е изд. - М. : Дашков и К, 2004. - 335 с.,	2	-
8.	Защита от хакеров Web-приложений / Д. Форристал, К. Брумс, Д. Симонис и др. ; Пер. с англ. В. Зорина. - М. : АйТи : ДМК Пресс, 2004. - 492 с.,	1	-

16. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Информационная безопасность [Электронный ресурс] : (письменная справка) / [сост. Н. А. Фесенко] ; Донецкий нац. ун-т, Науч. б-ка, Справ.-библиогр. отд. - Донецк : ДонНУ, 2016. - электронные данные (1 файл)., 1 экз.

17. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонНУ №46484614),
2. Microsoft Office (корпоративная лицензия ДонНУ №46472919),
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений).

18. ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

<i>Дисциплина или другой вид учебной работы</i>	<i>ФИО преподавателя и вид электронного взаимодействия преподаватель-студент по дисциплине</i>
Информационная безопасность и защита информации	Балдынюк А.И.: Облако (https://cloud.mail.ru/public/2DFj/DaYj1D2ee) e-mail (h.baldyniuk@donnu.ru)

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 2020-2021 год.

В рабочую программу дисциплины внесены следующие изменения и дополнения:

Протокол заседания кафедры № ____ от ____ . Зав.кафедрой _____

Рабочая программа рассмотрена и переутверждена на заседании кафедры с изменениями (без изменений) на 2021-2022 год.

В рабочую программу дисциплины внесены следующие изменения и дополнения:

Протокол заседания кафедры № ____ от ____ . Зав.кафедрой _____