

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ

УТВЕРЖДАЮ:

Проректор по научной и учебной работе

«_____» _____ 2020 г.

«_____»



Рабочая программа учебной дисциплины
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Укрупненная группа направлений подготовки и специальностей	38.00.00 Экономика и управление
Специальность	38.05.01 Экономическая безопасность
Специализация	Экономико-правовое обеспечение экономической безопасности
Образовательная программа	Специалитет
Квалификация	Экономист
Форма обучения	Очная, заочная

Донецк 2020

УТВЕРЖДАЮ:

Декан факультета математики и
информационных технологий
И.А. Моисеенко
« » 2020
МП

Рабочая программа учебной дисциплины «Информационная безопасность» составлена на основании Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по специальности 38.05.01 Экономическая безопасность (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от 16 января 2017 г. № 20.

Программа составлена с учетом ГОС ВПО по специальности 38.05.01 Экономическая безопасность, утвержденного приказом Министерства образования и науки ДНР от 04 мая 2020 г. № 59-НП; Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики, утвержденного приказом Министерства образования и науки ДНР № 1171 от 10.11.2017 г. (с изменениями, внесенными от 03.05.2019 г. №567); учебного плана по специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности», разработанного в ГОУ ВПО «Донецкий национальный университет»

Разработчики:

доцент, кандидат экономических наук,

зав. кафедрой 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 № 13 от «15» июня 2020 г.

Заведующий кафедрой

Н. Ш. Пономаренко

Программа учебной дисциплины одобрена учебно-методической комиссией факультета математики и информационных технологий

Протокол № 10 от «17» июня 2020 г.

Председатель учебно-методической
комиссии факультета

Л.И. Селякова

Программа учебной дисциплины одобрена учебно-методической комиссией экономического факультета.

Протокол № 10 от «16» июня 2020 г.

Председатель учебно-методической
комиссии экономического факультета

Е.Н. Стрелина

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И МЕСТО ДИСЦИПЛИНЫ В УЧЕБНОМ ПРОЦЕССЕ

Учебная дисциплина «Информационная безопасность» является дисциплиной базовой части образовательной программы. Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими (история, информационные технологии и системы в экономике, современные технологии, основы безопасности предпринимательской деятельности, экономическая безопасность, документационное обеспечение управленческой деятельности, кадровая безопасность, управление рисками, уголовное право) и сопутствующими (судебная экономическая экспертиза, стратегия обеспечения экономической безопасности организации, моделирование экономической безопасности, экономическая безопасность во ВЭД) дисциплинами. Данная дисциплина является основой для подготовки дипломной работы.

2. СТРУКТУРА ДИСЦИПЛИНЫ

Характеристика учебной дисциплины	Форма обучения	
	Очная	Заочная
Специальность	38.05.01 Экономическая безопасность	
Специализация	Экономико-правовое обеспечение экономической безопасности	
Образовательная программа	Специалитет	
Квалификация	Экономист	
Количество содержательных модулей и тем	1 (9)	
Дисциплина базовой / вариативной части образовательной программы	Вариативная часть	
Формы контроля	1 модульный контроль, зачет в 9-м семестре	
Количество зачетных единиц	2	2
Количество часов	72	72
Год подготовки	5	5
Семестр	9	×
Количество часов	72	72
- лекционных	-	-
- практических, семинарских	36	8
- лабораторных	-	-
- самостоятельной работы	36	64
в т.ч. индивидуальное задание		
Недельное количество часов, т.ч.		
аудиторных	2	×
самостоятельной работы студента	2	×

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:

Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и

затрагивают предметные сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

Требования к результатам освоения дисциплины: Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по специальности 38.05.01 Экономическая безопасность (уровень специалитета), утвержденного приказом Министерства образования и науки Российской Федерации от 16 января 2017 г. № 20:

а) общекультурных (ОК) (соотнесенных с видами деятельности и их коды);

способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (ОК-12).

б) общепрофессиональных (ОПК):

способностью применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов (ОПК-3).

в) профессиональных (ПК):

расчетно-экономическая и проектно-экономическая деятельность:

способностью осуществлять планово-отчетную работу организации, разработку проектных решений, разделов текущих и перспективных планов экономического развития организации, бизнес-планов, смет, учетно-отчетной документации, нормативов затрат и соответствующих предложений по реализации разработанных проектов, планов, программ (ПК-5);

правоохранительная деятельность:

способностью соблюдать и защищать права и свободы человека и гражданина (ПК-8);

способностью осуществлять мероприятия, направленные на профилактику, предупреждение преступлений и иных правонарушений, на основе использования закономерностей экономической преступности и методов ее предупреждения; выявлять и устранять причины и условия, способствующие совершению преступлений, в том числе коррупционных проявлений (ПК-10);

способностью реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков и угроз экономической безопасности, предупреждения, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере экономики (ПК-11);

способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-20);

контрольно-ревизионная деятельность:

способностью анализировать результаты контроля, исследовать и обобщать причины и последствия выявленных отклонений, нарушений и недостатков и готовить предложения, направленные на их устранение (ПК-27);

информационно-аналитическая деятельность:

способностью строить стандартные теоретические и эконометрические модели, необходимые для решения профессиональных задач, анализировать и интерпретировать полученные результаты (ПК-30);

способностью проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности (ПК-32);

способностью проводить комплексный анализ угроз экономической безопасности при планировании и осуществлении инновационных проектов (ПК-34);

организационно-управленческая деятельность:

способностью принимать участие в разработке стратегии обеспечения экономической безопасности организаций, подготовке программ по ее реализации (ПК-41);

научно-исследовательская деятельность:

способностью исследовать условия функционирования экономических систем и объектов, формулировать проблемы, обосновывать актуальность и практическую значимость разрабатываемых мероприятий по обеспечению экономической безопасности, методов и средств анализа экономической безопасности организаций, оценивать их эффективность (ПК-46);

способностью проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации (ПК-48);

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

и 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.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И ФОРМЫ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА

Курс дисциплины предусматривает следующие формы организации учебного процесса: практические занятия, самостоятельная работа студента.

В учебном процессе широко применяются активные и интерактивные формы проведения занятий (разбор конкретных ситуаций, 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 выполнения практических заданий.

Самостоятельная работа студентов предусматривает выполнение индивидуальных заданий, подготовку к практическим занятиям, изучение учебной и методической литературы, составление конспектов, защита презентаций и докладов.

Тематический план дисциплины «Информационная безопасность»

Порядковый номер и тема	Краткое содержание темы
Тема 1. Информационная безопасность как составляющая общественной безопасности	1. Понятие безопасности. Национальная безопасность. Безопасность в экономической сфере. Цели экономической безопасности, ее содержание и структура. 2. Международные договоры, доктрины в области информационной безопасности. 3. Соперничество в информационной сфере, информационные войны. 4. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. 5. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности.
Тема 2. Виды и особенности угроз информационной безопасности	1. Риски угроз информационным ресурсам. 2. Угрозы безопасности информационных ресурсов ограниченного доступа.

	<p>3. Правомерные методы получения предпринимательской информации, их состав.</p> <p>4. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкуренции.</p> <p>5. Промышленный и экономический шпионаж, его сущность, история и сфера распространения. Легальные способы получения ценной и конфиденциальной информации, их состав. Нелегальные (противоправные, незаконные) способы получения ценной и конфиденциальной информации, их состав. Понятия злоумышленника, постороннего и случайного лица.</p> <p>6. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации.</p> <p>7. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений.</p>
Тема 3. Правовая защита информационных ресурсов	<p>1. Понятие тайны, секрета, конфиденциальности. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной предпринимательской информации.</p> <p>2. 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.</p> <p>3. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной.</p> <p>4. Конфиденциальность информации в вычислительных системах и сетях.</p>
Тема 4. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия	<p>1. Понятие аналитической работы, ее цели и задачи. Аналитическая работа по выявлению каналов несанкционированного доступа к информации.</p> <p>2. Понятие, цели и задачи системы защиты конфиденциальной информации.</p> <p>3. Компьютерные технологии и формирование основ системы защиты информации.</p> <p>4. Структура комплексной системы защиты информации (КСЗИ).</p> <p>5. Система защиты информации в малом бизнесе. Сертификация Систем и средств защиты информационных систем и информационных ресурсов.</p>
Тема 5. Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	<p>1. Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности.</p> <p>2. Задачи службы безопасности, основные функции. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации, аналитического подразделения, подразделения охраны и пропускного режима.</p> <p>3. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в не крупных фирмах и малом бизнесе.</p> <p>4. Профессиональные и психологические требования к сотрудникам службы безопасности.</p> <p>5. Анализ и оценка надежности и эффективности применяемой системы защиты.</p>
Тема 6. Защищенный	<p>1. Виды угроз традиционным и электронным документопотокам, задачи</p>

документооборот	<p>защиты документопотоков.</p> <p>2. Понятие, принципы, цели и задачи защищенного документооборота как совокупности документопотоков.</p> <p>3. Критерии безопасности документооборота. Основные требования к защищенному документообороту.</p> <p>4. Взаимосвязь персональной избирательности в доставке информации и разрешительной системы доступа.</p> <p>5. Особенности защищенного безбумажного (электронного) документооборота.</p> <p>6. Принципиальная взаимосвязь документопотока и применяемой технологической системы обработки и хранения документов.</p>
Тема 7. Технологические системы защиты и обработки конфиденциальных документов	<p>1. Виды угроз документированной информации, исходящие от технологической системы.</p> <p>2. Задачи защиты информации, решаемые технологической системой. Место и назначение технологической системы обработки и хранения конфиденциальных документов в системе защиты информации и защищенном документообороте.</p> <p>3. Принципиальные особенности автоматизированной технологической системы обработки конфиденциальных документов.</p> <p>4. Системы на единичном компьютере. Возможности создания различных типов АСОД для конфиденциальных документов безбумажного (электронного) документооборота на базе локальных сетей.</p>
Тема 8. Инженерно-техническая защита	<p>1. Физические средства защиты. Угрозы безопасности собственности фирмы и персоналу.</p> <p>2. Виды охраняемых объектов, категории защищаемых помещений.</p> <p>3. Построение системы охраны объекта, многорубежная охрана.</p> <p>4. Классификация и характеристика классификационных групп технических средств охраны. Охранные системы. Охранное телевидение. Ограждение и физическая изоляция. Запирающие устройства.</p> <p>5. Классификация экстремальных (чрезвычайных) ситуаций. Аппаратные средства защиты.</p>
Тема 9. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	<p>1. Программно-технические методы обеспечения информационной безопасности.</p> <p>2. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа.</p> <p>3. Межсетевые экраны как средство защиты от несанкционированного доступа.</p> <p>4. Критерии оценки защищенности систем информационной безопасности.</p> <p>5. 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.</p> <p>6. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования.</p>

Структура дисциплины «Информационная безопасность» по видам учебной деятельности

Названия содержательных модулей и тем	Количество часов											
	Очная форма обучения (нормативный срок)						Заочная форма обучения (нормативный срок)					
	всего	в т.ч.					всего	в т.ч.				
		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа		лекции	практические	лабораторные	самостоятельная работа	индивидуальная работа
Тема 1. Информационная безопасность как составляющая общественной безопасности	8		4		4		8		0,5		7,5	
Тема 2. Виды и особенности угроз информационной безопасности	8		4		4		8		0,5		7,5	
Тема 3. Правовая защита информационных ресурсов	8		4		4		8		1		7	
Тема 4. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия	8		4		4		8		1		7	
Тема 5. Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	8		4		4		8		1		7	
Тема 6. Защищенный документооборот	8		4		4		8		1		7	
Тема 7. Технологические системы защиты и обработки конфиденциальных документов.	8		4		4		8		1		7	
Тема 8.Инженерно-техническая защита	8		4		4		8		1		7	
Тема 9. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	8		4		4		8		1		7	
Всего:	72		36		36		72		8		64	

5. ТЕМАТИКА ЛЕКЦИОННЫХ, ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Темы лекционных занятий – не предусмотрено учебным планом

Темы практических занятий

Название темы	Количество часов	
	Очная форма	Заочная форма
Тема 1. Информационная безопасность как составляющая общественной безопасности	4	0,5
Тема 2. Виды и особенности информационной безопасности.	4	0,5
Тема 3. Правовая защита информационных ресурсов	4	1
Тема 4. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия.	4	1
Тема 5. Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	4	1
Тема 6. Защищенный документооборот	4	1
Тема 7. Технологические системы защиты и обработки конфиденциальных документов.	4	1
Тема 8. Инженерно-техническая защита.	4	1
Тема 9. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи.	4	1
ВСЕГО	36	8

6. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ И ИНДИВИДУАЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Согласно «Порядка организации учебного процесса в образовательных организациях высшего профессионального образования Донецкой Народной Республики», самостоятельная работа студента является основным средством овладения учебным материалом во внеучебное время. Ее содержание определяется рабочей программой, методическими материалами, заданиями и рекомендациями преподавателя.

Основные задачи самостоятельной работы:

- овладение навыками самостоятельного обучения, формирования потребностей в самообразовании;
- освоение содержания дисциплины в рамках тем, предназначенных для самостоятельного изучения студента;
- осознание, углубление содержания и основных положений курса во время усвоения законспектированного на лекциях материала, его проработки на протяжении подготовки к практическим занятиям;
- использование материалов, полученных во время выполнения самостоятельных заданий, написания рефератов, для эффективной подготовки к модульным контрольным заданиям и экзамену.

Самостоятельная работа студентов по дисциплине «Информационная безопасность» содержит следующие виды учебной деятельности:

- первичное ознакомление с материалами лекций, составление конспекта;
- изучение и усвоение лекционного материала;
- самостоятельная проработка литературных источников и обобщение изученных материалов;

подготовка к практическим занятиям и деловым играм;
 подготовка устных ответов на вопросы для самопроверки;
 подготовка к тестовым заданиям по усвоенному материалу;
 индивидуальная работа по заданию преподавателя;
 подготовка к выполнению письменных модульных контрольных работ;
 подготовка к экзамену.

Контрольными формами самостоятельной работы по дисциплине могут быть следующие: проверка конспекта; проверка ответов на контрольные или тестовые вопросы; проверка рефератов; проверка практических заданий; проверка выполненных индивидуальных заданий.

Организация самостоятельной работы студентов

<i>Название темы</i>	<i>Количество часов</i>	
	<i>Очная форма</i>	<i>Заочная форма</i>
Тема 1. Информационная безопасность как составляющая общественной безопасности	4	7,5
Тема 2. Виды и особенности информационной безопасности.	4	7,5
Тема 3. Правовая защита информационных ресурсов	4	7
Тема 4. Основные направления и этапы работ по созданию комплексной системы безопасности предприятия.	4	7
Тема 5. Основные направления деятельности службы безопасности предприятия по защите информационных ресурсов	4	7
Тема 6. Защищенный документооборот	4	7
Тема 7. Технологические системы защиты и обработки конфиденциальных документов.	4	7
Тема 8. Инженерно-техническая защита.	4	7
Тема 9. Программные средства защиты информации в компьютерах, локальных сетях и средствах связи.	4	7
ВСЕГО	36	64

7. КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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.

8. ОБРАЗЕЦ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

**ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ
по дисциплине «Информационная безопасность»**

Специальность: 38.05.01 «Экономическая безопасность»,

Специализация: «Экономико-правовое обеспечение экономической безопасности»

Программа подготовки: специалитет

Семестр: 9 (очная форма обучения); курс: 5 (заочная форма обучения)

МОДУЛЬНАЯ КОНТРОЛЬНАЯ РАБОТА

Вариант № 1

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 _____

Н. Ш. Пономаренко

Преподаватель _____

А.И.Балдынюк

9. КРИТЕРИИ ОЦЕНИВАНИЯ ЗАДАНИЯ МОДУЛЬНОГО КОНТРОЛЯ

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

10. КОНТРОЛЬНЫЕ ВОПРОСЫ К ЗАЧЕТУ

Контрольные вопросы к зачету

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.

12. ОБРАЗЕЦ ТЕСТОВОГО ЗАДАНИЯ

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, сбоя 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 ОБЩЕЙ УСПЕВАЕМОСТИ

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	3,5
2.	Ответы на контрольные вопросы	0,5
	Тема 2.	
1.	Практическое задание	4
2.	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.	Практическое задание	4
2.	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
2.	Ответы на контрольные вопросы и тесты	0,5
	Тема 8	
1.	Практическое задание	4
1.	Ответы на контрольные вопросы и тесты	0,5
	Тема 9	
1.	Практическое задание	4
2.	Ответы на контрольные вопросы и тесты	0,5
	Модульный контроль	10
	Индивидуальное задание	20
	Зачет	30
	Всего за семестр:	100

Порядок оценивания учебных достижений обучающихся

Оценка по шкале ECTS	Оценка по 100-балльной шкале	Оценка по государственной шкале (экзамен, дифференцированный 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 аттестации	не зачтено
F	0-34	2 (неудовлетворительно) с возможностью повторной сдачи при условии обязательного набора дополнительных баллов	не зачтено

14. РЕСУРСЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Материалы по дисциплине «Информационная безопасность» для студентов специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности» доступны по ссылке: <https://cloud.mail.ru/public/37me/BHdkLxZ2F> на облаке сервиса mail.ru Балдынюк А.И. Папка «ЭФ_Информационная безопасность»

15. РЕКОМЕНДОВАННАЯ ЛИТЕРАТУРА

Основная 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"	10	-

	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.		
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: концептуальные 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 информ., информ. процессов и технологий (МАН ИИПТ). - 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 лицензия № 46472919);
3. Microsoft Visual Studio (лицензия программы DreamSpark для высших учебных заведений);
4. Лицензии GPL для свободного программного обеспечения: Антивирус Касперского, Libre Office, Adobe Acrobat Reader, xPDF, Paint.NET.