МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

Дзержинский филиал ННГУ

УТВЕРЖДЕНО
Решением президиума ученого совета ННГУ
протокол от «14» декабря 2021 г. № 4

Рабочая программа дисциплины

Информационная безопасность
(наименование дисциплины)

Уровень высшего образования
Бакалавриат
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
38.03.01 ЭКОНОМИКА
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
ФИНАНСЫ И КРЕДИТ
(указывается профиль / магистерская программа / специализация)

Форма обучения
Очная, очно-заочная
(очная / очно-заочная / заочная)

Год набора: 2022

Дзержинск
2021 год

1. Место и цели дисциплины (модуля) в структуре ОПОП

Дисциплина Б1.О.15. «Информационная безопасность» относится к обязательной части образовательной программы направления подготовки 38.03.01 Экономика.

Дисциплина предназначена для освоения.

- студентами очной формы обучения - в 6 семестре.
- студентами очно-заочной формы - в 6 семестре.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**
	Индикатор достижения компетенции	**Результаты обучения по дисциплине**	
ПК-3. Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений	ПК 3.1. Формирует, анализирует и интерпретирует финансово-экономическую информацию	Знать: нормативные, организационные средства защиты информации при формировании отчетности, планов, проектов хозяйствующих субъектов Уметь: использовать современные средства и технологии защиты данных. Владеть: средствами сбора, обработки и анализа данных с применением систем информационной безопасности.	Задачи, тест, дискуссия
	ПК 3.2. Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений	Знать: современные средства и возможности систем информационной безопасности при обработке отчетности в целях принятия управленческих решений Уметь: использовать средства информационных технологий при решении профессиональных задач. Владеть: навыками работы с современными системами информационной безопасности при принятии управленческих решений	Задачи, тест, дискуссия
ОПК-6 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1 Понимает принципы работы современных информационных технологий	Знать: основные методы, способы и средства преобразования информации Уметь: работать с компьютером как средством управления информацией Владеть: основными способами обнаружения информационных угроз и использования с антивирусных программ	Задачи, тест, дискуссия
	ОПК 6.2. Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности	Знать: функции и задачи менеджмента и аудита систем информационной безопасности Уметь: выявлять информационные угрозы, выбирать методы и средства управления и аудита систем информационной безопасности Владеть: принципами менеджмента и аудита систем информационной безопасности	Задачи, тест, дискуссия

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения
Общая трудоемкость	**__4_ ЗЕТ**	**__4_ ЗЕТ**
Часов по учебному плану	**144**	**144**
в том числе		
аудиторные занятия (контактная работа): **- занятия лекционного типа** **- занятия семинарского типа (практические занятия)** **- КСРИФ**	**50** **24** **24** **2**	**26** **12** **12** **2**
самостоятельная работа	**58**	**82**
Промежуточная аттестация – Экзамен - 36		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины (модуля), форма промежуточной аттестации по дисциплине (модулю)	**Всего (часы)**			В том числе													
				Контактная работа (работа во взаимодействии с преподавателем), часы из них												**Самостоятельная работа обучающегося, часы**		
				Занятия лекционного типа			**Занятия семинарского типа**			**Занятия лабораторного типа**			**Всего**					
	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная
Тема 1. Введение в информационную безопасность	16	16		4	2		4	2					8	4		8	12	
Тема 2. Угрозы информационной безопасности	18	18		4	2		4	2					8	4		10	14	
Тема 3. Программно-технические методы защиты информации	18	18		4	2		4	2					8	4		10	14	
Тема 4. Менеджмент и аудит информационной безопасности на уровне предприятия	18	18		4	2		4	2					8	4		10	14	
Тема 5. Управление рисками информационной безопасности	18	18		4	2		4	2					8	4		10	14	
Тема 6. Управление информационной безопасностью на государственном уровне	18	18		4	2		4	2					8	4		10	14	
КСРИФ	2	2											2	2				
Промежуточная аттестация - экзамен	36	36																
ИТОГО	144	144		24	12		24	12					50	26		58	82	

Содержание разделов дисциплины

Тема 1. Введение в информационную безопасность

Понятие безопасности. Национальная безопасность. Доктрина безопасности Российской Федерации. Безопасность в экономической сфере России. Цели экономической безопасности, ее содержание и структура. Концепция информационной безопасности России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан. Соперничество в информационной сфере, информационные войны. Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Безопасность функционирования предпринимательской структуры. Основные задачи и уровни реализации информационной безопасности.

Информационное общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Цели, задачи, направления исследования и практической реализации информационной безопасности. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере. Место, цели и задачи информационной безопасности в бизнесе. Информационная безопасность и компьютеризация информационной среды. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения. Соотношение понятий информационной безопасности и безопасности информации. Взаимосвязь понятий информационной безопасности и защиты информации. Научные взгляды, теории и дискуссии. Концепция защиты информации. Понятие и цели защиты информации, формирование и эволюция понятия. Обеспечивающий технологический аспект защиты информации.

Понятие информационных ресурсов. Информационные ресурсы и информационные системы. Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. Правовое двуединство документированных информационных ресурсов. Понятие ценной (собственной) предпринимательской информации. Ценность и полезность информации. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации. Понятие уязвимости информации. Типовые классификационные группы ценной предпринимательской информации. Информационные ресурсы государственные и негосударственные. Классификация информационных продуктов и услуг. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования.

Тема 2. Угрозы информационной безопасности

Риски угроз информационным ресурсам. Угрозы безопасности информационных ресурсов ограниченного доступа. Правомерные методы получения предпринимательской информации, их состав. Предпосылки и причины утраты информационных ресурсов ограниченного доступа. Понятие разведки в бизнесе как одной из форм маркетингового исследования. Понятие и методы аналитической работы. Виды недобросовестной конкурен-

ции. 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.

Понятие и классификация источников конфиденциальной информации. Характеристика каждого источника. Классификация каналов объективного распространения конфиденциальной информации. Характеристика каждого канала. Уязвимость информации. Интерес к информации как предпосылка возникновения угрозы. Понятие угрозы (опасности) информации, виды угроз. Риск угрозы и механизм реализации угрозы. Понятие несанкционированного канала утраты конфиденциальной информации. Случайные и преднамеренные условия возникновения этого канала. Поиск или формирование такого канала злоумышленником. Последствия образования канала несанкционированного доступа к информации: утрата носителя и конфиденциальности информации, разрушение информации, ее кража, модификация, подмена, фальсификация и др. Понятия разглашения и утечки информации, их отличие. Классификация организационных каналов разглашения (оглашения, утраты) конфиденциальной информации. Характеристика каждого канала. Классификация технических каналов утечки конфиденциальной информации. Характеристика каждого канала. Комплексность использования организационных и технических каналов. Особенности структуры каналов распространения информации в компьютерах, локальных сетях, оргтехнике и средствах связи.

Назначение и классификация технических средств промышленного шпионажа. Классификация угроз информационной безопасности автоматизированных систем. Классификация удаленных атак. Виды компьютерных правонарушений.

Тема 3. Программно-технические методы защиты информации

Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасности. Международные критерии. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. 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.

Тема 4. Менеджмент и аудит информационной безопасности на уровне предприятия

Понятие, цели и задачи системы защиты конфиденциальной информации. Принципы построения системы, ее технологичность, иерархичность и факторы эффективности. Принцип разграничения доступа. Принцип регламентации состава защищаемой информации. Принцип персональной ответственности. Принцип коллегиальности контроля. Принципы надежности и превентивности. Принцип эволюции структуры системы в условиях реальных угроз информации. Обязательная совокупность простейших (несистемных) методов и средств защиты конфиденциальной предпринимательской информации. Преимущества и недостатки. Компьютерные технологии и формирование основ системы защиты информации. Место системы в обеспечении безопасности информации в компьютерах, вычислительных системах и сетях. Комплексность системы защиты. Структура комплексной системы защиты информации (КСЗИ). Содержание элемента правовой защиты информации. Содержание элемента организационной защиты информации. Содержание элемента инженерно-технической защиты информации и технических средств охраны.

Содержание элемента программно-аппаратной защиты информации. Содержание элемента криптографической защиты информации. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом предпринимательской структуры и видами угроз. Система защиты информации в малом бизнесе. Стоимость системы и критерии выбора системы. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

Разработка и ведение перечня сведений, составляющих предпринимательскую тайну. Цели и задачи перечня сведений, составляющих предпринимательскую тайну. Состав сведений, которые не могут быть тайной. Место перечня в системе защиты информации. Классификация ценной информации в предпринимательских структурах различного типа. Принципы определения состава ценных сведений, подлежащих защите в конкретной фирме. Перечни инвентарные и матричные. Структура перечней различных типов. Перечни списочные и проблемно-ориентированные. Организационные формы составления и ведения перечней. Содержание процедуры разработки перечня. Существующие методики сбора, анализа и обобщения сведений. Место маркетингового исследования в процедуре разработки перечня. Разграничение уровня конфиденциальности сведений, определение срока конфиденциальности, регламентация места документирования, использования и хранения, состава сотрудников, которым эти сведения необходимы для работы.

Назначение нормативно-методических материалов по регламентации системы защиты информации. Регламентация права предпринимательской структуры на защиту своей тайны. Регламентация структуры и содержания комплексной системы защиты информации фирмы. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала фирмы с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны фирмы. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и иных наглядных пособий.

Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая структура службы безопасности. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Задачи и функции аналитического подразделения. Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе. Профессиональные и психологические требования к сотрудникам службы безопасности. Плановая и контрольная работа в службе безопасности. Назначение и взаимосвязь плановой и контрольной работы службы безопасности. Их место в построении и функционировании комплексной системы защиты информации фирмы. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций.

Тема 5. Управление рисками информационной безопасности

Основные принципы управления рисками информационной безопасности:

Шестнадцать методов, используемые для реализации пяти принципов управления рисками. Оценка риска и определение потребности. Признание информационных ресурсов в качестве существенных (неотъемлемых) активов организации. Разработка практических процедур оценки рисков, связывающих безопасность и требования бизнеса. Ответ-

ственность менеджеров бизнес-подразделений и менеджеров, участвующих в программе обеспечения безопасности. Непрерывное управление рисками. Централизованное управление. Определение бюджета и персонала. Профессионализм и технические знания сотрудников. Средства контроля. Контроль факторов, влияющих на риски и указывающих на эффективность информационной безопасности. Новые методы и средства контроля.

Тема 6. Управление информационной безопасностью на государственном уровне

Защита информации институтом интеллектуальной собственности. Информационный характер интеллектуальной и материальной собственности. Охрана результатов творческой деятельности. Объекты интеллектуальной собственности. Промышленная собственность. Промышленные образцы. Информация о происхождения товара. Собственность на результаты творческого труда. Российский и зарубежный опыт охраны интеллектуальной собственности. Международные правовые акты. Реализация интеллектуальной собственности на документированную информацию. Характеристика норм патентного права. Характеристика норм авторского права и смежных прав. Торговый знак, знак обслуживания, торговая марка, фирменное наименование, эмблема предприятия. Страхование ценной информации. Законодательные акты,охраняющие вещную собственность на документированную информацию. Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации. Организация деятельности средств массовой информации. Отношения средств массовой информации с гражданами и организациями. Ответственность за нарушение законодательства о средствах массовой информации.

Понятие тайны, секрета, конфиденциальности. Направления и методы защиты тайны в дореволюционной России и зарубежных странах. Институт тайн в законодательстве Российской Федерации. Защита информации институтом государственной тайны. Субъекты и объекты информационных правоотношений в области государственной тайны. Отнесение сведений к государственной тайне и их засекречивание. Распоряжение сведениями, составляющими государственную тайну. Рассекречивание сведений и их носителей. Защита государственной тайны. Предпринимательская (коммерческая) тайна как форма защиты ценной деловой и производственной предпринимательской информации. 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. Понятие конфиденциальности как определение сферы несекретной информации ограниченного доступа. Сущность термина, особенности и условия применения, дискуссионность. Правовые и технологические аспекты присвоения информации категории конфиденциальной. Конфиденциальная информация и ее виды. Персональные данные. Ограничения на отнесение информации к категории конфиденциальной. Понятие конфиденциального документа, его особенности. Общая классификация конфиденциальных документов. Сроки (период) конфиденциальности. Деление документов на документы кратковременного и долговременного периода конфиденциальности. Конфиденциальность информации в вычислительных системах и сетях.

Практические занятия (семинарские занятия) организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, госу-

дарственных и муниципальных органов.

На проведение практических занятий (семинарских занятий) в форме практической подготовки отводится __4__ часа.

Практическая подготовка направлена на формирование и развитие:

- практических навыков в соответствии с профилем ОП: *аналитической деятельности и компетенции ПК-3*: Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений.

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа, групповых или индивидуальных консультаций.

4. Учебно- методическое обеспечение самостоятельной работы обучающихся

В ходе изучения дисциплины уделяется внимание как теоретическому усвоению понятий информационной безопасности, так и приобретению, развитию и закреплению практических навыков и умений по использованию специализированных информационных средств и технологий при организации ИБ экономических систем.

На лекциях раскрываются основные вопросы рассматриваемой темы, делаются акценты на наиболее важные, сложные и проблемные положения изучаемого материала, которые должны быть приняты студентами во внимание.

На практических занятиях, ориентированных на предметную область будущей профессиональной деятельности студентов, выборочно контролируется степень усвоения студентами основных теоретических положений. Рассматривается технология применения аппаратно-программных средств для организации ИБ. При решении практических заданий используются не только инструментальные средства информационных технологий бизнес-индустрии, но и методы и понятия дисциплин финансово-экономического блока.

После изучения каждой темы предусматривается выполнение студентами самостоятельной работы с проверкой как степени усвоения ими теоретических, знаний, так и объема и качества приобретенных практических навыков и умений.

В ходе самостоятельной работы, при подготовке к плановым занятиям, экзамену студенты анализируют поставленные преподавателем задачи и проблемы и с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет, находят пути их разрешения.

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

- изучение теоретического материала дисциплины на лекции с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием Internet-ресурсов, информационных баз, методических разработок, специальной и научной литературы;
- закрепление теоретического материала при проведении практических занятий с использованием учебного и научного оборудования, выполнения проблемно- ориентированных, поисковых, творческих заданий.

Самостоятельная работа является наиболее деятельным и творческим процессом, который выполняет ряд дидактических функций: способствует формированию диалектического мышления, вырабатывает высокую культуру умственного труда, совершенствует способы организации познавательной деятельности, воспитывает ответственность, целеустремленность, систематичность и последовательность в работе студентов, развивает у них бережное отношение к своему времени, способность доводить до конца начатое дело.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

Для обеспечения самостоятельной работы обучающихся используется электронные курсы «Информационная безопасность» (*https://e-learning.unn.ru/enrol/index.php?id=4715 и https://e-learning.unn.ru/enrol/index.php?id=4760*), созданные в системе электронного обучения ННГУ - https://e-learning.unn.ru/.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций	**Шкала оценивания сформированности компетенций**						
	плохо	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
Умения	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения,решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка		**Уровень подготовки**
	превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
зачтено	**отлично**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	удовлетво-	Все компетенции (части компетенций), на формирование которых направлена дисциплина,

	рительно	сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения

5.2.1 Контрольные вопросы

Перечень контрольных вопросов к экзамену

Вопрос	Код компетенции
1. Определить место информационной безопасности в обеспечении системы общественной безопасности.	ОПК-6
2. Дать определение информационной безопасности.	ОПК-6
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.	ОПК-6
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.	ОПК-6
5. Охарактеризовать уровни реализации информационной безопасности.	ОПК-6
6. Дать определение и классификацию информационных ресурсов.	ОПК-6
7. Определить основные виды угроз информационным ресурсам.	ПК-3
8. Охарактеризовать особенности угроз конфиденциальной информации.	ПК-3
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.	ПК-3
10. Описать причины возникновения каналов несанкционированного доступа к информации.	ОПК-6
11. Классифицировать виды каналов несанкционированного доступа к информации.	ОПК-6
12. Описать характер действия организационных каналов несанкционированного доступа к информации.	ОПК-6
13. Охарактеризовать технические каналы несанкционированного доступа к информации.	ОПК-6
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.	ОПК-6
15. Проанализировать особенности угроз автоматизированным информационным системам.	ПК-3
16. Дать классификацию удаленных атак.	ПК-3
17. Проанализировать основные направления правовой защиты информации.	ОПК-6
18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.	ОПК-6
19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.	ОПК-6
20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.	ОПК-6
21. Определить объекты защиты авторских прав.	
22. Назвать основные права автора в отношении его произведения.	
23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.	ОПК-6 ОПК-6
24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).	ОПК-6

25. Дать определение государственной тайны и назвать грифы секретности.	ОПК-6
26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.	ОПК-6
27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.	ОПК-6
28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.	ОПК-6
29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.	ОПК-6
30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.	ОПК-6
31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.	ОПК-6
32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.	ОПК-6
33. Назвать основные положения концепции информационной безопасности предприятия.	ОПК-1
34. Изложить содержание регламента обеспечения информационной безопасности предприятия.	ОПК-1
35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.	ОПК-1
36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.	ОПК-1
37. Проанализировать содержание понятия разрешительнойсистемы доступа персонала к конфиденциальным сведениям фирмы.	ОПК-1
38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.	ОПК-1
39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.	ОПК-1
40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.	ОПК-1
41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.	ОПК-1
42. Проанализировать особенности текста конфиденциального документа.	ОПК-1
43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.	ОПК-1
44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.	ОПК-1
45. Сформулировать возможности, трудности и направления использованияэлектронной почты для передачи конфиденциальных документов.	ОПК-1
46. Составить фрагмент номенклатуры дел, содержащих конфиденциальныедокументы.	ОПК-1
47. Проанализировать задачи защиты информации, которые должны бытьрешены при формировании и оформлении дел с конфиденциальными документами.	ОПК-1
48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.	ОПК-6
49. Проанализировать пути поиска документов и дел, не обнаруженных припроверке их наличия, дать рекомендации, повышающие эффектив-	

ностьпоиска и предотвращающие утрату документов и дел. 50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией. 51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. 52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции. 53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала. 54. Назвать основные элементы физической защиты территории и помещений предприятия. 55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов. 56. Дать классификацию компьютерных вирусов. 57. Описать основные антивирусные программы. 58. Охарактеризовать основные способы криптографического преобразования данных.	ОПК-6 ОПК-6 ОПК-6 ОПК-6 ОПК-6 ОПК-6 ПК-3 ПК-3 ПК-3 ПК-3 ПК-3

5.2.1 Примеры тестовых заданий

Тесты для оценки компетенций (ПК-3)

Тест 1

1. Информационная война – это…

А. злословие в адрес другого человека;

Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

В. акт применения информационного оружия.

2. Информационная безопасность – это…

А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:

А. природоохранные мероприятия;

Б. надежность работы компьютера;

В. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:

А. информационные ресурсы;

Б. средства вычислительной и организационной техники;

В. Конституция России.

5. Обеспечение безопасности информации – это…

А. одноразовое мероприятие;

Б. комплексное использование всего арсенала имеющихся средств защиты;

В. разработка каждой службой плановых мер по защите информации.

6. Лингвистическое обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;

В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

7. Эргономическое обеспечение информационной безопасности – это?

А. антивирусные программы;

Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;

В. комплекс математических методов, связанных с оценкой опасности технических средств.

8.Информационное обеспечение информационной безопасности – это?

А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

Б. антивирусные программы;

В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

9. Организационное обеспечение информационной безопасности – это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;

Б. совокупность средств;

В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:

А. раскрытие конфиденциальной информации;

Б. нарушение принципов экономической безопасности;

В. отказ от обслуживания.

11. Информационное оружие – это?

А. комплекс технических средств, методов и технологий, направленных против управленческих систем;

Б. нормативно-правовая база по информационной безопасности;

В. комплекс индивидуального и общественного сознания.

12. Правовое обеспечение информационной безопасности – это..?

А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;

Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;

В. широкое использование технических средств защиты информации.

5.2.3 Пример разноуровневых задач и заданий для оценки компетенций (ОПК-6):

1.Защита информации от сбоев оборудования и случайной потери

1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»

2. Определите методы защиты

1периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);

2автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.

3периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ. Например: Disk Doctor, ScanDisk . Подобные программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.

4периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.

Определите методы защиты от случайной потери или искажения информации, хранящейся в компьютере:

1автоматический запрос на подтверждение команды, приводящей к изменению содержимого какого-либо файла. Если вы хотите удалить файл или разместить новый файл под именем уже существующего, на экране дисплея появится диалоговое окно с требованием подтверждения команды либо её отмены;

2установка специальных атрибутов документов. Например, многие программы-редакторы позволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;

3возможность отменить последние действия. Если вы редактируете документ, то можете пользоваться функцией отмены последнего действия или группы действий, имеющейся во всех современных редакторах. Если вы ошибочно удалили нужный файл, то специальные программы позволяют его восстановить, правда, только в том случае, когда вы ничего не успели записать поверх удаленного файла;

4разграничение доступа пользователей к ресурсам файловой системы, строгому разделению системного и пользовательского режимов работы вычислительной системы.

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326

2. Глинская Е.В.Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. – Режим доступа: (Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=507334

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2017. - 239 с. – (Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=612572)

Дополнительная литература

1. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.(Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=405000)

2. Вдовенко Л.А.Информационная система предприятия: Учебное пособие/Вдовенко Л. А., 2-е изд., перераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с.(Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=501089)

3. Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с. – (Доступно в ЭБС «Знаниум», режим доступа: http://znanium.com/catalog.php?bookinfo=471787)

4. Ерохин В.В Безопасность информационных систем [Электронный ресурс] / Ерохин В.В. - М. : ФЛИНТА, 2015. – 182 с.(Доступно в ЭБС «Консультант студента», режим доступа: (http://www.studentlibrary.ru/book/ISBN9785976519046.html)

5. Шаньгин В.Ф.Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. 702 с. (Доступно в ЭБС «Консультант студента», режим доступа: http://www.studentlibrary.ru/book/ISBN9785940747680.html)

Интернет-ресурсы

1. Фонд образовательных электронных ресурсов ННГУ [Электронный ресурс]. - Режим доступа: http://www.unn.ru/books/resources — Загл. с экрана. [Дата обращения: 26.03.2020]
2. Электронная библиотека учебников[Электронный ресурс]. - Режим доступа: http://studentam.net— Загл. с экрана.[Дата обращения: 26.03.2020]
3. Российская государственная библиотека [Электронный ресурс]. - Режим доступа: http://www.rsl.ru— Загл. с экрана.[Дата обращения: 26.03.2020]
4. Научная электронная библиотека[Электронный ресурс]. - Режим доступа: http://elibrary.ru/— Загл. с экрана.[Дата обращения: 26.03.2020]

8. Материально-техническое обеспечение дисциплины (модуля)

Реализация программы предполагает наличие:

- учебных аудиторий для проведения занятий лекционных типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.
- компьютерного класса, имеющего компьютеры, объединенные сетью с выходом в Интернет;
- лицензионного (операционная система Microsoft Windows, пакет прикладных программ Microsoft Office) и свободно распространяемого программного обеспечения.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки 38.03.01 «Экономика», профиль «Финансы и кредит».

Автор(ы):

к.пед.н., доцент Поляков.Е.А.

Программа одобрена Методической комиссией Дзержинского филиала ННГУ, протокол № 7 от 03.12.2021 года