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

Институт экономики и предпринимательства

УТВЕРЖДЕНО
решением президиума Ученого совета ННГУ
протокол от
«20» апреля 2021 г. № 1

Рабочая программа дисциплины

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования
бакалавриат

Направление подготовки
38.03.01 Экономика

Направленность образовательной программы
Экономика, международный бизнес и предпринимательство

Квалификация
бакалавр

Форма обучения

очная, заочная, очно-заочная

Нижний Новгород

2021 год

1. Место дисциплины (модуля) в структуре ООП

Дисциплина Б1.Б.15 «Информационная безопасность» относится к обязательной части.

Место дисциплины в учебном плане образовательной программы	
Блок 1. Дисциплины (модули) Обязательная часть	Дисциплина Б1.Б.15 «Информационная безопасность» относится к обязательной части ООП направления подготовки 38.03.01 «Экономика»

Минимальный уровень освоения содержания дисциплины предполагает:

- Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности;

- Уяснение вопросов обеспечения информационной безопасности организации и проблемам создания (концептуального проектирования) систем информационной безопасности;

-Знакомство с особенностями создания информационной безопасности автоматизированных банковских систем (АБС), защиты учетной информации организации и пр.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников).

Формируемые компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ОПК-1 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** теоретические аспекты информационной безопасности (ИБ) экономических систем типы информационных угроз и их характеристики организацию системы защиты информации экономических систем **Уметь:** формулировать цели и задачи защиты информации экономических объектов принимать обоснованные решения по выбору политики безопасности и оценке эффективности инвестиций в ИБ работать в среде специализированных программных комплексов и систем, применяемых в ИБ **Владеть:** методами развития комплексов и технологий ИБ подходами к организации ИБ экономических систем
ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии	*знать* виды программного обеспечения; виды экономических информационных систем по уровням управления *уметь* работать с реляционными базами данных; проводить расчеты в табличных процессорах с использованием финансовых функций и специальных средств владеть навыками, позволяющими им решать практические задачи, используя экономические информационные системы

3. Структура и содержание дисциплины (модуля).
Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	**4_ ЗЕТ**	**4_ ЗЕТ**	**4_ ЗЕТ**
Часов по учебному плану	**144**	**144**	**144**
в том числе			
аудиторные занятия (контактная работа) **- занятия лекционного типа** **- занятия семинарского типа (практические занятия)**	 **32** **32**	 **16** **16**	 **4** **8**
самостоятельная работа	**42**	**74**	**121**
КСР	**2**	**2**	**2**
Промежуточная аттестация – экзамен	**36**	**36**	**9**

Структура и содержание дисциплины (модуля)

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**			**Консультации**			**Всего**					
	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заочная	Очная	Очно-заочная	Заччная	Очная	Очно-Заочная	Заочная				Очная	Очно-заочная	заочная	очная	Очно-заочная	заочная
Тема 1. Введение в информационную безопасность	14	16	33	4	3	1	4	1	1			1				8	4	3	6	12	30
Тема 2. Угрозы информационной безопасности	16	18	31	4	3	1	4	1			2					8	6	1	8	12	30
Тема 3. Программно-технические методы защиты информации	24	19	23	8	3	1	8	2	1		2	1				16	7	3	8	12	20
Тема 4. Менеджмент и аудит информационной безопасности на уровне предприятия	24	26	24	8	3	1	8	2	1		2	1				16	7	3	8	19	21

Тема 5. Управление рисками информационной безопасности	28	27	22	8	4	-	8	2	1		2	1				16	8	2	12	19	20
Текущий контроль	2	2	2													2	2	2			
Промежуточная аттестация экзамен																					
Контроль	36	36	9																		
Итого	144	144	144	32	16	4	32	8	4		8	4				66	34	14	42	74	121

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 предусматривает решение прикладных заданий по темам дисциплины, позволяющих выработать практические навыки у обучающихся в соответствии с видом будущей профессиональной деятельности и закрепленными за дисциплиной компетенциями. Выполняемые практические здания позволяют развить навыки работы с фактическим материалом, умение ориентироваться в реальной ситуации, делать выводы и обосновывать свои предложения.

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

Практическая подготовка направлена на формирование и развитие:

- практических организационно-управленческих навыков в соответствии с профилем ОПОП;
- компетенции – **ПК-10** способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

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

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 конкуренции. 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. Ответственность 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 ин-

формации. 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.

4. Образовательные технологии

Реализация компетентностного подхода при изучении дисциплины «Информационная безопасность» предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр по актуальным статистическим проблемам, 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, государственных и муниципальных органов.

Все занятия, проводимые по дисциплине, в том числе и самостоятельная работа студентов, предусматривают сочетание передовых методических приемов с новыми образовательными информационными технологиями.

На занятиях используются современные формы и методы обучения (тренинги, исследовательские методы, проблемное и проектное обучение), направленные на развитие творческих способностей и самостоятельности студентов, привитие им интереса к исследовательской работе, формирование убеждения о необходимости при решении любых прикладных задач использования инновационных информационных технологий.

Лекционные занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет.

Практические занятия проводятся в компьютерных классах с применением специализированных информационных систем, комплексов и технологий бизнес-индустрии.

Тематика практических заданий ориентирована на рассмотрение аналитических типовых и исследовательских задач финансово-экономического характера.

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.

5. Учебно-методическое обеспечение самостоятельной работы обучающихся

5.1. Рекомендации преподавателю

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.

5.2. Рекомендации студентам

Для лучшего усвоения положений дисциплины студенты должны:

- постоянно и систематически, с использованием рекомендованной литературы и электронных источников информации, закреплять знания, полученные на лекциях;
- находить решения проблемных вопросов, поставленных преподавателем в ходе лекций и практических заданий;
- регулярно и своевременно изучать материал, выданный преподавателем на самостоятельную проработку;
- с использованием средств информационных систем, комплексов и технологий, электронных учебников и практикумов, справочных правовых и тренинго-тестирующих систем, информационных ресурсов сети Интернет выполнить на компьютере тематические практические задания, предназначенные для самостоятельной работы;
- находить, используя разные источники информации, ответы на теоретические и практические контрольные вопросы по темам дисциплины;
- использовать информацию, найденную на сайтах фирм–разработчиков информационных систем и технологий, применяемых в экономике;
- при подготовке к зачету учитывать общие требования и рекомендации.

При освоении данного курса бакалаврам может быть предложено выполнение инициативной научно-исследовательской работы.

Методические указания по выполнению научно-исследовательской работы

Целью выполнения работы является:

– закрепление знаний, полученных студентами в процессе теоретического обучения;

проведение исследования проблемы;активное использование пакетов прикладных программ; анализ библиографических материалов.

– отработка приемов и способов аналитических расчетов на практическом материале.

Выбор темы производится студентом и утверждается преподавателем. Рекомендуемый объем работы 35-40 страниц машинописного текста.

В каждой работе, кроме основных разделов, независимо от темы, предусматривается «Введение», «Заключение», «Список используемой литературы», «Приложения».

Список литературы должен быть составлен в соответствии с библиографическими требованиями.

Выполнять научно-исследовательскую работу необходимо с использованием текстового редактора MS Word, электронных таблиц Excel, а также можно использовать пакеты прикладных программ (ППП).

К оформлению научно-исследовательской работы предъявляются общие типовые требования.

Рекомендуемые направления научно-исследовательских работ

1 Информационное право и информационная безопасность.

2 Концепция информационной безопасности.

3 Основы экономической безопасности предпринимательской деятельности.

4 Анализ законодательных актов об охране информационных ресурсов открытого доступа.

5 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

6 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

7 Информационная безопасность **(**по материалам зарубежных источников и литературы).

8 Правовые основы защиты конфиденциальной информации.

9 Экономические основы защиты конфиденциальной информации.

10 Организационные основы защиты конфиденциальной информации.

11 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

12 Составление инструкции по обработке и хранению конфиденциальных документов.

13 Направления и методы защиты документов на бумажных носителях.

14 Направления и методы защиты машиночитаемых документов.

15 Архивное хранение конфиденциальных документов.

16 Направления и методы защиты аудио- и визуальных документов.

17 Порядок подбора персонала для работы с конфиденциальной информацией.

18 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

19 Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

20 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

21 Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

22 Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

23 Порядок защиты информации в рекламной и выставочной деятельности.

24 Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

25 Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26 Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27 Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28 Назначение, виды, структура и технология функционирования системы защиты информации.

29 Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30 Аналитическая работа по выявлению каналов утечки информации фирмы.

31 Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32 Направления и методы защиты профессиональной тайны.

33 Направления и методы защиты служебной тайны.

34 Направления и методы защиты персональных данных о гражданах.

35 Методы защиты личной и семейной тайны.

36 Построение и функционирование защищенного документооборота.

37 Защита секретов в дореволюционной России.

38 Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

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/.

6. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю).

6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования.

ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Индикаторы компетенции	Критерии оценивания (дескрипторы)						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
Знания Знать: теоретические аспекты информационной безопасности (ИБ)	отсутствие знаний материала	наличие грубых ошибок в основном материале	знание основного материала с рядом негрубых ошибок	знание основного материалом с рядом заметных погрешностей	знание основного материала с незначительными погрешностями	знание основного материала без ошибок и погрешностей	знание основного и дополнительным материала без ошибок и погрешностей

экономических систем; типы информационных угроз и их характеристики; организацию системы защиты информации экономических систем							
Умения *Уметь* формулировать цели и задачи защиты информации экономических объектов; принимать обоснованные решения по выбору политики безопасности и оценке эффективности инвестиций в ИБ; работать в среде специализированных программных комплексов и систем, применяемых в ИБ	Полное отсутствие умений формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ	отсутствие умений формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ	Умение формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ при наличии существенных ошибок	Умение умений формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ при наличии незначительных ошибок	Умение умений формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ и делать простейшие выводы	Умение умений формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ и делать аргументированные выводы	Умение умений формулировать цели, принимать решения и работать в среде специализированных программных комплексов и систем, применяемых в ИБ и способность принимать решение на основе проведенного анализа
Навыки *Владеть* методами развития комплексов и технологий ИБ; подходами к организации ИБ экономических систем	полное отсутствие навыков владения методами развития комплексов и технологий ИБ и подходами к организации ИБ	отсутствие навыков владения методами развития комплексов и технологий ИБ и подходами к организации ИБ	наличие минимальных навыков владения методами развития комплексов и технологий ИБ и подходами к организации ИБ	Посредственное использование навыков владения методами развития комплексов и технологий ИБ и подходами к организации ИБ	Достаточное использование навыков владения методами развития комплексов и технологий ИБ и подходами к организа-	Хорошее использование навыков владения методами развития комплексов и технологий ИБ и подходами к организации ИБ	Всестороннее использование навыков владения методами развития комплексов и технологий ИБ и подходами к организации ИБ

					ции ИБ		
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 20 %	20 – 50 %	50 – 70 %	70-80 %	80 – 90 %	90 – 99 %	100%

ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии.

Индикаторы компетенции	Критерии оценивания (дескрипторы)						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
Знания Знать виды программного обеспечения	отсутствие знаний видов программного обеспечения	наличие грубых ошибок в основном материале	знание основного материала с рядом негрубых ошибок	знание основного материалом с рядом заметных погрешностей	знание основного материала с незначительными погрешностями	знание основного материала без ошибок и погрешностей	знание основного и дополнительным материала без ошибок и погрешностей
Знания Знать виды экономических информационных систем по уровням управления	отсутствие знаний видов экономических информационных систем по уровням управления	наличие грубых ошибок в основном материале	знание основного материала с рядом негрубых ошибок	знание основного материалом с рядом заметных погрешностей	знание основного материала с незначительными погрешностями	знание основного материала без ошибок и погрешностей	знание основного и дополнительным материала без ошибок и погрешностей
Умения *Уметь* работать с реляционными базами данных	Полное отсутствие умений работать с реляционными базами данных	отсутствие умений работать с реляционными базами данных	Умение работать с реляционными базами данных при наличии существенных ошибок	Умение работать с реляционными базами данных при наличии незначительных ошибок	Умение работать с реляционными базами данных и делать простейшие выводы	Умение работать с реляционными базами данных и делать аргументированные выводы	Умение работать с реляционными базами данных и способность принимать решение на основе проведенного анализа
Умения *Уметь* проводить расчеты в табличных процессорах с использованием	Полное отсутствие умений проводить расчеты в табличных процессорах с использо-	отсутствие умений проводить расчеты в табличных процессорах с	Умение проводить расчеты в табличных процессорах с использованием финансо-	Умение проводить расчеты в табличных процессорах с использованием финансо-	Умение проводить расчеты в табличных процессорах с исполь-	Умение проводить расчеты в табличных процессорах с исполь-	Умение работать с проводить расчеты в табличных процессорах с использованием финансовых функций и

финансовых функций и специальных средств	ванием финансовых функций и специальных средств	использованием финансовых функций и специальных средств	вых функций и специальных средств при наличии существенных ошибок	вых функций и специальных средств при наличии незначительных ошибок	зованием финансовых функций и специальных средств и делать простейшие выводы	зованием финансовых функций и специальных средств и делать аргументированные выводы	специальных средств и способность принимать решение на основе проведенного анализа
Навыки *Владеть* навыками, позволяющими им решать практические задачи, используя экономические информационные системы	полное отсутствие навыков владения навыками, позволяющими им решать практические задачи, используя экономические информационные системы ИБ	отсутствие навыков, позволяющих им решать практические задачи, используя экономические информационные системы	наличие минимальных навыков, позволяющих им решать практические задачи, используя экономические информационные системы	Посредственное использование навыков, позволяющих им решать практические задачи, используя экономические информационные системы	Достаточное использование навыков, позволяющих им решать практические задачи, используя экономические информационные системы	Хорошее использование навыков, позволяющих им решать практические задачи, используя экономические информационные системы	Всестороннее использование навыков, позволяющих им решать практические задачи, используя экономические информационные системы
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 20 %	20 – 50 %	50 – 70 %	70-80 %	80 – 90 %	90 – 99 %	100%

6.2. Описание шкал оценивания результатов обучения по дисциплине

Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде экзамена, на котором определяется:

- уровень усвоения студентами основного учебного материала по дисциплине;
- уровень понимания студентами изученного материала
- способности студентов использовать полученные знания для решения конкретных задач.

Экзамен проводится в устной форме. Устная часть экзамена заключается в ответе студентом на теоретические вопроса курса (с предварительной подготовкой) и последующем собеседовании в рамках тематики курса. Собеседование проводится в форме вопросов, на которые студент должен дать краткий ответ.

6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.

Оценка	Уровень подготовки
Превосходно	Высокий уровень подготовки, безупречное владение теоретическим материалом, студент демонстрирует творческий поход к решению нестандартных ситуаций. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждая теоретический материал практическими примерами из практики. Студент активно работал на практических занятиях.
Отлично	Высокий уровень подготовки с незначительными ошибками. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждает теоретический материал практическими примерами из практики. Студент активно работал на практических занятиях.
Очень хорошо	Хорошая подготовка. Студент дает ответ на все теоретические вопросы билета, но имеются неточности в определениях понятий, процессов и т.п. Студент активно работал на практических занятиях.
Хорошо	В целом хорошая подготовка с заметными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы билета, но имеются неточности в определениях понятий, процессов и т.п. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы экзаменатора. Студент работал на практических занятиях.
Удовлетворительно	Минимально достаточный уровень подготовки. Студент показывает минимальный уровень теоретических знаний, делает существенные ошибки при характеристике нормативно-правовой базы валютного регулирования, но при ответах на наводящие вопросы, может правильно сориентироваться и в общих чертах дать правильный ответ. Студент посещал практические занятия.
Неудовлетворительно	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на наводящие и дополнительные вопросы экзаменатора. Студент пропустил большую часть практических занятий.

6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.

Вопросы к экзамену по дисциплине «Информационная безопасность»

Вопрос	Код компетенции
Основные тенденции развития информатизации в экономике.	ОПК – 1
Основные понятия информационной безопасности в экономике.	ОПК – 1
Информационная безопасность в цифровой экономике.	ОПК – 1
Экономическая информация как товар и объект безопасности.	ОПК – 1
Система защиты информации и её структура.	ОПК – 1
Информационные угрозы, их виды и причины возникновения.	ОПК – 1
Информационные угрозы для государства.	ОПК – 1
Информационные угрозы для компании.	ОПК – 1
Информационные угрозы для личности (физического лица).	ОПК – 1
Действия и события, нарушающие информационную безопасность.	ОПК – 1

Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.	ОПК – 1
Способы воздействия информационных угроз на объекты.	ОПК – 1
Внешние и внутренние субъекты информационных угроз.	ОПК – 1
Компьютерные преступления и их классификация.	ОПК – 1
Исторические аспекты компьютерных преступлений и современность.	ОПК – 1
Субъекты и причины совершения компьютерных преступлений.	ОПК – 1
Вредоносные программы, их виды.	ОПК – 1
История компьютерных вирусов и современность.	ОПК – 1
Государственное регулирование информационной безопасности.	ОПК – 1
Деятельность международных организаций в сфере информационной безопасности.	ОПК – 1
Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.	ОПК – 1
Доктрина информационной безопасности России.	ОПК – 1
Уголовно-правовой контроль над компьютерной преступностью в России.	ОПК – 1
Федеральные законы по ИБ в РФ.	ОПК – 1
Политика безопасности и ее принципы.	ОПК – 1
Фрагментарный и системный подход к защите информации.	ОПК – 1
Методы и средства защиты информации.	ОПК-1
Организационное обеспечение ИБ.	ОПК – 5
Организация конфиденциального делопроизводства.	ПК – 10
Комплекс организационно-технических мероприятий по обеспечению защиты информации.	ПК – 10
Инженерно-техническое обеспечение компьютерной безопасности.	ПК – 10
Организационно-правовой статус службы безопасности.	ПК – 10
Защита информации в Интернете.	ПК – 10
Электронная почта и ее защита.	ПК – 10
Защита от компьютерных вирусов.	ПК – 10
«Больные» мобильники и их «лечение».	ПК – 10
Популярные антивирусные программы и их классификация.	ПК – 10
Организация системы защиты информации экономических объектов.	ПК – 10
Криптографические методы защиты информации.	ПК – 10
Этапы построения системы защиты информации.	ПК – 10
Оценка эффективности инвестиций в информационную безопасность.	ПК – 10
План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.	ПК – 10
Управление информационной безопасности на государственном уровне.	ПК – 10
Аудит ИБ автоматизированных банковских систем.	ПК – 10
Электронная коммерция и ее защита.	ПК – 10
Менеджмент и аудит информационной безопасности на уровне предприятия.	ПК-10
Информационная безопасность предпринимательской деятельности.	ПК-10
Обеспечение информационной безопасности должностных лиц.	ПК-10

6.5. Методические материалы, определяющие процедуры оценивания.

1. Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся при реализации образовательных программ высшего образования в ННГУ, утв. решением ученого совета ННГУ протокол от 27.12.2017 № 10 (приказ ректора ННГУ от 29.12.2017 № 630-ОД).

2. Положение о фонде оценочных средств, утвержденное приказом ректора ННГУ от 10.06.2015 г. № 247-ОД.

7. Учебно-методическое обеспечение дисциплины

а) 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. 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. - ISBN 978-5-369-01178-2

3. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов -е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60x90 1/16. - (Профессиональное образование) (nepenneT)ISBN 978-5-91134-627-0, 200 экз. http://znaniurn.com/bookread2.php?book=516806

4. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189349

б) дополнительная литература:

1. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложкаДБВИ 978-5-00091-007-8, 300 экз. http://znanium.com/bookread2.php?book=491597

2. Информационная безопасность и защита информации: Учебное посо- бие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. -Рабочая программа и ФОС составлены в соответствии с требованиями ОС ННГУ по направлению подготовки 38.03.01 «Экономика», профиль «Экономика, международный бизнес и предпринимательство».

в) программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины)

A. www.gks.ru / Федеральная служба государственной статистики.
B. Операционная система Microsoft Windows
C. Прикладное программное обеспечение Microsoft Office
D. Справочно-правовая система «КонсультантПлюс»

8. Материально-техническое обеспечение дисциплины (модуля)

Аудитории, оборудованные посадочными местами, персональным компьютером, ЖК монитор и/или проекционном экраном, проектором, доской.

На компьютере должно быть установлено минимальное ПО: MSWindows, MicrosoftOffice, KasperskyEndpointSecurity, Консультант Плюс

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки 38.03.01 «Экономика», профиль «**Экономика, международный бизнес и предпринимательство**».

Авторы программы:
к.э.н., профессор В.Н.Ясенев

к.э.н., ст. преподаватель А.В.Дорожкин

Рецензенты:

д.э.н., профессор, зам.
генерального директора федерального казенного учреждения Н. Ф. Поляков

Заведующий кафедрой информационных технологий и инструментальных методов в экономике д.э.н Ю.В.Трифонов

Программа одобрена на заседании методической комиссии Института экономики и предпринимательства от «_15__» марта___ 2021 года, протокол № __3___.