

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
(факультет / институт / филиал)

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от
«24» апреля 2020 г. № 5

Рабочая программа дисциплины (модуля)

Информационная безопасность

(наименование дисциплины (модуля))

Уровень высшего образования

специалитет

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

38.05.01 – Экономическая безопасность

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Экономико-правовое обеспечение экономической безопасности

(указывается профиль / магистерская программа / специализация)

Квалификация (степень)

экономист

(бакалавр / магистр / специалист)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2020 г.

1. Место дисциплины (модуля) в структуре ОПОП.

Дисциплина относится к вариативной части ОПОП по направлению 38.05.01 «Экономическая безопасность» и обязательна для освоения на 1–м курсе во 2–м семестре. Основное назначение данной дисциплины состоит в эффективном освоении теоретических основ обеспечения информационной безопасности организаций, формирование умения и практических навыков применения методов и средств защиты информации.

В связи с этим, основной целью преподавания дисциплины «Информационная безопасность» является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.

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 проблем создания (концептуального проектирования) систем информационной безопасности;
- Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ.

Тематическим планом преподавания дисциплины предусматриваются следующие виды занятий: лекции, практические занятия, самостоятельная работа. Контроль знаний обучающихся осуществляется в ходе тестирования и сдачи экзамена.

Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, практических занятий и самостоятельной работы, должны всесторонне использоваться студентами на завершающем этапе обучения в специалитете, при обучении в магистратуре, а также в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.

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

Формируемые компетенции (код компетенции, уровень освоения – при наличии в карте компетенции)	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций
ОК-12 Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации (этап освоения базовый)	Знать: основные методы, способы и средства преобразования информации Уметь: работать с компьютером как средством управления информацией Владеть: основными способами обнаружения информационных угроз и использования современных антивирусных программ
ПК-48 Способность проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации (этап освоения начальный)	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.

Формы промежуточной аттестации: экзамен.

3. Структура и содержание дисциплины (модуля).

Объем дисциплины составляет 6 зачетных единиц, всего 216 часов, из которых: 64 часа составляет контактная работа обучающегося с преподавателем (32 часа занятия лекционного типа, 32 часа занятия лабораторного типа (научно-практические занятия, лабораторные работы и т.п.), 72 часа мероприятия текущего контроля успеваемости, 78 часов составляет самостоятельная работа обучающегося в виде рефератов, ознакомления с нормативно-правовой документацией по информационной безопасности.

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					Самостоятельная работа обучающегося, часы
		Контактная работа (работа во взаимодействии с преподавателем), часы				Всего	
		из них					
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Консультации		

	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. Теоретические аспекты ИБ экономических систем	36			4			2								6			12
Тема 2. Понятие информационных угроз и их виды	36			4			4								8			12
Тема 3. Государственное регулирование ИБ	36			8			8		2						16			12
Тема 4. Подходы, принципы, методы и средства обеспечения безопасности	36			8			8		2						16			12
Тема 5. Организация системы защиты информации	36			4			6				2				10			12
Тема 6. Менеджмент и аудит систем ИБ	36			4			4				2				8			18
<i>В случае, когда дисциплина (модуль) полностью формирует какую-то компетенцию и (или) завершает формирование компетенции, одним из разделов дисциплины (модуля) может быть выполнение проекта, формирование портфолио или другой вид комплексной проверки сформированности компетенции в целом</i>																		
Промежуточная аттестация: экзамен																		
Итого	216			32			32								64			78

Тема 1. Теоретические аспекты информационной безопасности экономических систем

Информационное общество. Информационное пространство. Информационная война и информационное противоборство. Информационная преступность. Угрозы безопасности информации. Информационная безопасность (ИБ). Политика безопасности. Объекты и субъекты обеспечения ИБ. Методы и средства обеспечения ИБ. Объекты ИБ на предприятии. Системный подход к защите информации. Структура (подсистемы) системы ИБ. Экономическая информация как товар и объект безопасности.

Информационные ресурсы и информационная безопасность. Правовой режим информационных ресурсов. Информационно-правовые отношения. Документирование информации как обязательное условие включения информации в информационные ресурсы. 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. Понятие информационных угроз и их виды

Информационные угрозы. Угрозы нарушения конфиденциальности информации. Информационная атака. Потенциальные злоумышленники (хакеры, крекеры). Информационные угрозы для государства, для компании (юридического лица), для личности (физического лица). Естественные и человеческие факторы информационных угроз (ИУ). Классификация угроз

безопасности информации. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации. Вредоносные программы. Разглашение и утечка конфиденциальной информации (КИ). Каналы утечки КИ. Исторические аспекты реализации информационных угроз. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации угроз ИБ. Способы воздействия угроз на информационные объекты. Проявления возможного ущерба. Идентификация угроз. Компьютерные преступления и наказания. Исторические примеры и современность. Риски угроз информационным ресурсам.

Тема 3. Государственное регулирование информационной безопасности

Ущерб от компьютерных злоупотреблений. Исторические аспекты борьбы органов уголовной юстиции с компьютерной преступностью (опыт США, стран Западной Европы, России). Меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности. Международные договоры, доктрины в области ИБ. Информационные права граждан. Основные законодательные по ИБ физических и юридических лиц в России (Конституция РФ, федеральные законы, Уголовный кодекс, Налоговый кодекс, Гражданский кодекс и др.). Специальное законодательство в области информатизации информационных технологий и информационной безопасности – федеральные законы, их структура и содержание. Доктрина информационной безопасности России, принятая в 2016 году. Стандарты информационной безопасности. Правовые нормы ИБ в организациях. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.

Повышение образовательной и правовой культуры населения в сфере ИБ.

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

Управление защитой информации. Фрагментарный и комплексный подходы к защите информации. Характеристики методов средств ИБ экономического объекта. Криптография, механизмы цифровой подписи и особенности ее применения. Идентификация и аутентификация. Разграничения доступа. Протоколирование и аудит. Организационно-техническое обеспечение компьютерной безопасности. Организация конфиденциального делопроизводства. Программно-технические методы защиты информации. 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. Методы и средства защиты от вредоносных программ. Профилактика вирусного заражения программ. Защита информации в Интернете.

Тема 5. Организация системы защиты информации

Политика информационной безопасности. Принципы реализации политики безопасности. Этапы построения системы ИБ. Способы устранения (смягчения) воздействия непредвиденных ситуаций. Обеспечение ИБ автоматизированных банковских систем, электронной коммерции и др.

Тема 6. Менеджмент и аудит систем информационной безопасности

Оценка эффективности инвестиций в информационную безопасность.

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.

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 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.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществ-

ляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ. Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для обучающихся с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Обучающимся с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

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 экзамену учитывать общие требования и рекомендации.

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

Вопросы для семинарских занятий

- 1 Информационное право и информационная безопасность.
- 2 Концепция информационной безопасности.
- 3 Анализ законодательных актов об охране информационных ресурсов открытого доступа.
- 4 Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
- 5 Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.
- 6 Информационная безопасность (по материалам зарубежных источников и литературы).
- 7 Правовые основы защиты конфиденциальной информации.
- 8 Экономические основы защиты конфиденциальной информации.
- 9 Организационные основы защиты конфиденциальной информации.
- 10 Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
- 11 Составление инструкции по обработке и хранению конфиденциальных документов.
- 12 Направления и методы защиты документов на бумажных носителях.
- 13 Направления и методы защиты машиночитаемых документов.
- 14 Архивное хранение конфиденциальных документов.
- 15 Направления и методы защиты аудио- и визуальных документов.
- 16 Порядок подбора персонала для работы с конфиденциальной информацией.
- 17 Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
- 18 Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
- 19 Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
- 20 Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
- 21 Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
- 22 Порядок защиты информации в рекламной и выставочной деятельности.

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

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

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

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

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

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

29 Аналитическая работа по выявлению каналов утечки информации фирмы.

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

31 Направления и методы защиты профессиональной тайны.

32 Направления и методы защиты служебной тайны.

33 Направления и методы защиты персональных данных о гражданах.

34 Методы защиты личной и семейной тайны.

35 Построение и функционирование защищенного документооборота.

36 Защита секретов в дореволюционной России.

37 Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Перечень контрольных вопросов

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.

2. Дать определение информационной безопасности.

3. Назвать основные направления и задачи обеспечения информационной безопасности общества.

4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.

5. Охарактеризовать уровни реализации информационной безопасности.

6. Дать определение и классификацию информационных ресурсов.

7. Определить основные виды угроз информационным ресурсам.

8. Охарактеризовать особенности угроз конфиденциальной информации.

9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.

10. Описать причины возникновения каналов несанкционированного доступа к информации.

11. Классифицировать виды каналов несанкционированного доступа к информации.

12. Описать характер действия организационных каналов несанкционированного доступа к информации.

13. Охарактеризовать технические каналы несанкционированного доступа к информации.

14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.

15. Проанализировать особенности угроз автоматизированным информационным системам.

16. Дать классификацию удаленных атак.

17. Проанализировать основные направления правовой защиты информации.

18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.

19. Изложить законный порядок реализации права гражданина на опровержение

ложной информации о нем в средствах массовой информации.

20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.

21. Определить объекты защиты авторских прав.

22. Назвать основные права автора в отношении его произведения.

23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).

25. Дать определение государственной тайны и назвать грифы секретности.

26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.

28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.

32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

33. Назвать основные положения концепции информационной безопасности предприятия.

34. Изложить содержание регламента обеспечения информационной безопасности предприятия.

35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

42. Проанализировать особенности текста конфиденциального документа.

43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.

44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

45. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.

46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.

47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
49. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска 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.

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

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.

ОК-12: Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

Индикаторы компетенции	Критерии оценивания (дескрипторы)						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
Знания Знать: основные методы, способы и средства преобразования информации	отсутствие знаний материала	наличие грубых ошибок в основном материале	знание основного материала с рядом негрубых ошибок	знание основного материала с рядом заметных погрешностей	знание основного материала с незначительными погрешностями	знание основного материала без ошибок и погрешностей	знание основного и дополнительного материала без ошибок и погрешностей
Умения Уметь работать с компьютером как средством управления информацией	Полное отсутствие умений работать с компьютером как средством управления	отсутствие умений работать с компьютером как средством управления	Умение работать с компьютером как средством управления информацией при	Умение работать с компьютером как средством управления информацией при	Умение работать с компьютером как средством управления информацией при	Умение работать с компьютером как средством управления информацией при	Умение работать с компьютером как средством управления информацией и способность принимать

цией	информацией	ния информации	наличии существенных ошибок	наличии незначительных ошибок	ей и делать простейшие выводы	ей и делать аргументированные выводы	решение на основе проведенного анализа
<u>Навыки</u> <i>Владеть</i> основными способами обнаружения информационных угроз и использования современных антивирусных программ	полное отсутствие навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ	отсутствие навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ	наличие минимальных навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ ИБ	Посредственное использование навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ	Достаточное использование навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ	Хорошее использование навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ	Всестороннее использование навыков владения основными способами обнаружения информационных угроз и использования современных антивирусных программ
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 20 %	20 – 50 %	50 – 70 %	70-80 %	80 – 90 %	90 – 99 %	100%

ПК-48: Способность проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации

Индикаторы компетенции	Критерии оценивания (дескрипторы)						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
<u>Знания</u> Знать: теоретические аспекты информационной безопасности (ИБ) экономических систем; типы информационных угроз и их характеристики; организацию системы защиты информации эконо-	отсутствие знаний материала	наличие грубых ошибок в основном материале	знание основного материала с рядом негрубых ошибок	знание основного материала с рядом заметных погрешностей	знание основного материала с незначительными погрешностями	знание основного материала без ошибок и погрешностей	знание основного и дополнительного материала без ошибок и погрешностей

мических систем							
<u>Умения</u> 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
<u>Навыки</u> 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 организации ИБ	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
Шкала оценок по проценту правильно выполненных контрольных заданий	0 – 20 %	20 – 50 %	50 – 70 %	70-80 %	80 – 90 %	90 – 99 %	100%

Описание шкал оценивания результатов обучения по дисциплине

Изучение дисциплины завершается сдачей экзамена. Учитывая большой объем учебного материала, подготовку к итоговому контролю целесообразно начинать заблаговременно,

используя перечень контрольных вопросов по курсу, содержащийся в учебной программе. На основании экзаменационного ответа, студенту определяется отметка, «превосходно», «отлично», «очень хорошо», «хорошо», «удовлетворительно», «неудовлетворительно», «плохо».

Оценка	Уровень подготовки
Превосходно	Высокий уровень подготовки, безупречное владение теоретическим материалом, обучающийся демонстрирует творческий подход к решению нестандартных ситуаций. Обучающийся дал полный и развернутый ответ на все теоретические вопросы билета, подтверждая теоретический материал практическими примерами из практики. Обучающийся активно работал на практических занятиях. 100 %-ное выполнение контрольных экзаменационных заданий
Отлично	Высокий уровень подготовки с незначительными ошибками. Обучающийся дал полный и развернутый ответ на все теоретические вопросы билета, подтверждает теоретический материал практическими примерами из практики. Обучающийся активно работал на практических занятиях. Выполнение контрольных экзаменационных заданий на 90% и выше
Очень хорошо	Хорошая подготовка. Обучающийся дает ответ на все теоретические вопросы билета, но имеются неточности в определениях понятий, процессов и т.п. Обучающийся активно работал на практических занятиях. Выполнение контрольных экзаменационных заданий от 80 до 90%.
Хорошо	В целом хорошая подготовка с заметными ошибками или недочетами. Обучающийся 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. Обучающийся работал на практических занятиях. Выполнение контрольных экзаменационных заданий от 70 до 80%.
Удовлетворительно	Минимально достаточный уровень подготовки. Обучающийся показывает минимальный уровень теоретических знаний, делает существенные ошибки при характеристике нормативно-правовой базы предприятия, но при ответах на наводящие вопросы, может правильно сориентироваться и в общих чертах дать правильный ответ. Обучающийся посещал практические занятия. Выполнение контрольных экзаменационных заданий от 50 до 70%.
Неудовлетворительно	Подготовка недостаточная и требует дополнительного изучения материала. Обучающийся дает ошибочные ответы, как на теоретические вопросы билета, так и на наводящие и дополнительные вопросы экзаменатора. Обучающийся пропустил большую часть практических занятий. Выполнение контрольных экзаменационных заданий до 50%.
Плохо	Подготовка абсолютно недостаточная. Обучающийся не отвечает на поставленные вопросы. Обучающийся отсутствовал на большинстве лекций и практических занятий. Выполнение контрольных экзаменационных заданий менее 20 %.

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

Для оценивания результатов обучения в виде знаний используются следующие процедуры и технологии:

- тестирование;
- устные и письменные ответы на вопросы.

Оценка выполнения тестовых заданий рассчитывается в следующем процентном соотношении :

Шкала оценивания	Показатели
Превосходно	90% -100%
Отлично	80% -90%

Очень хорошо	70%-80%
Хорошо	60%-70%
Удовлетворительно	40%-60%
Неудовлетворительно	10%-40%
Плохо	Менее 10%

Результатом проверки компетенций на разных этапах формирования, полученных обучающимся в ходе освоения данной дисциплины, является оценка, выставаемая по семибалльной балльной шкале в соответствии со следующими критериями:

1. Полнота и правильность ответа
2. Степень осознанности и понимания изученного материала
3. Языковое оформление ответа

Оценка	Уровень подготовки
Превосходно	Материал изложен полно, даны правильные определения основных понятий; Обнаружено понимание материала, обучающийся обосновывает свои суждения, применяет знания на практике, приводит примеры не только из учебника, но и самостоятельно сформулированные; Материал изложен последовательно и грамотно с точки зрения норм литературного языка
Отлично	Материал изложен полно; Обнаружено понимание материала; Материал изложен последовательно и грамотно с точки зрения норм литературного языка
Очень хорошо	Ответ удовлетворяет тем же требованиям, что и для отметки «отлично», но обучающийся допускает 1-2 ошибки, которые способен исправить
Хорошо	Ответ удовлетворяет тем же требованиям, что и для отметки «очень хорошо», но обучающийся допускает 1-2 ошибки, которые способен исправить, и 1-2 недочета в последовательности и языковом оформлении излагаемого материала .
Удовлетворительно	Обучающийся обнаруживает знание и понимание основных положений данной темы, но: 1. материал изложен неполно, допущены неточности в определении понятий или в формулировках правил; 2. не умеет достаточно глубоко и доказательно обосновать свои суждения и приводить примеры; 3. излагает материал непоследовательно и допускает ошибки в языковом оформлении ответа
Неудовлетворительно	Обучающийся обнаруживает незнание большей части ответа соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, непоследовательно и неуверенно излагает материал
Плохо	Обучающийся обнаруживает незнание ответа соответствующего вопроса

Для оценивания результатов обучения в виде умений и владений используются следующие процедуры и технологии:

- семинар

Критерии оценки выполненных практических заданий	
Оценка	Критерии оценивания
Превосходно	изложение материала логично, грамотно, без ошибок; свободное владение профессиональной терминологией.
Отлично	изложение материала логично, без ошибок; умение высказывать и обосновать свои суждения; теория связана с практикой

Очень хорошо	обучающийся грамотно излагает материал; ориентируется в материале, владеет профессиональной терминологией, осознанно применяет, ответ правильный, полный, с незначительными неточностями или недостаточно полный
Хорошо	обучающийся грамотно излагает материал; владеет профессиональной терминологией, осознанно применяет, ответ полный, с неточностями или недостаточно полный
Удовлетворительно	обучающийся излагает материал неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для выполнения задания, не может доказательно обосновать свои суждения; обнаруживается недостаточно глубокое понимание изученного материала.
Неудовлетворительно	в ответе обучающегося проявляется незнание основного материала учебной программы, допускаются грубые ошибки в изложении, не может применять знания для выполнения задания
Плохо	отсутствуют необходимые теоретические знания; допущены ошибки в определении понятий, искажен их смысл

Для проведения итогового контроля сформированности компетенции используются: устный опрос

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

Примеры тестовых заданий

1. Информация это -

1. сведения, поступающие от СМИ
2. только документированные сведения о лицах, предметах, фактах, событиях
3. **сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**
4. только сведения, содержащиеся в электронных базах данных

2. Информация

1. не исчезает при потреблении
2. становится доступной, если она содержится на материальном носителе
3. подвергается только "моральному износу"
4. **характеризуется всеми перечисленными свойствами**

3. Информация, зафиксированная на материальном носителе, с реквизитами,

позволяющими ее идентифицировать, называется

1. достоверной
2. конфиденциальной
3. **документированной**
4. коммерческой тайной

4. Формы защиты интеллектуальной собственности -

1. **авторское, патентное право и коммерческая тайна**
2. интеллектуальное право и смежные права
3. коммерческая и государственная тайна
4. гражданское и административное право

5. По принадлежности информационные ресурсы подразделяются на

1. **государственные, коммерческие и личные**
2. государственные, не государственные и информацию о гражданах
3. информацию юридических и физических лиц
4. официальные, гражданские и коммерческие

6. К негосударственным относятся информационные ресурсы

1. созданные, приобретенные за счет негосударственных учреждений и организаций
2. созданные, приобретенные за счет негосударственных предприятий и физических
3. лиц
4. полученные в результате дарения юридическими или физическими лицами
5. **указанные в п.1-3**

8. По доступности информация классифицируется на

1. открытую информацию и государственную тайну
2. конфиденциальную информацию и информацию свободного доступа
3. **информацию с ограниченным доступом и общедоступную информацию**
4. виды информации, указанные в остальных пунктах

9. К конфиденциальной информации относятся документы, содержащие

1. **государственную тайну**
2. законодательные акты
3. "ноу-хау"
4. сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа

1. информацию о чрезвычайных ситуациях
2. информацию о деятельности органов государственной власти
3. документы открытых архивов и библиотек
4. **все, перечисленное в остальных пунктах**

11. К конфиденциальной информации не относится

1. коммерческая тайна
2. персональные данные о гражданах
3. государственная тайна
4. **"ноу-хау"**

12. Вопросы информационного обмена регулируются (...) правом

1. **гражданским**
2. информационным
3. конституционным
4. уголовным

6.5. Методические материалы, определяющие процедуры оценивания

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утвержденное приказом ректора ННГУ от 13.02.2014 г. №55-ОД,

Положение «О фонде оценочных средств», утвержденное приказом ректора ННГУ от 10.06.2015 №247-ОД.

7. Учебно-методическое обеспечение дисциплины

Основная литература

1. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: <http://znanium.com>

2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов, – 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с. Режим доступа: <http://znanium.com>

Дополнительная литература

1. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. – Режим доступа: <http://znanium.com>

2. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. – Режим доступа: <http://znanium.com>

Интернет-ресурсы и программное обеспечение

1. Операционная система Microsoft Windows
2. Прикладное программное обеспечение Microsoft Office
3. Справочно-правовая система «КонсультантПлюс»

8. Материально-техническое обеспечение дисциплины (модуля)

Для проведения лекционных и семинарских занятий по дисциплине используются специально оборудованные лекционные аудитории, оснащенные компьютером, проектором или ЖК-телевизором, акустической системой и микрофоном (при необходимости), а также доской.

Для выполнения заданий для СРС студентам обеспечен доступ в интернет, а так же доступ к ресурсам электронной библиотеки ННГУ.

Реализация программы предполагает наличие:

- аудиторий для лекционных и практических занятий с необходимым оборудованием;
- 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.

В ходе проведения занятий рекомендуется использовать компьютерные иллюстрации для поддержки различных видов занятий, подготовленные с использованием Microsoft Office или других средств визуализации материала.

Доступ к электронным информационным ресурсам осуществляется в компьютерном классе и библиотеке.

Программа составлена в соответствии с требованиями СУОС ВО с учетом рекомендаций ОПОП ВО по специальности 38.05.01 – «Экономическая безопасность» специализации «Экономико-правовое обеспечение экономической безопасности».

Автор программы:
к.э.н., профессор

В.Н. Ясенов

к.э.н., доцент

А.В. Дорожкин

Рецензенты:

д.э.н., профессор,
зам. генерального директора
федерального казенного учреждения
«Налог-Сервис» ФНС России

Н.Ф.Поляков

Заведующий кафедрой ИТиИМЭ
д.э.н., профессор

Ю.В. Трифонов

Программа одобрена на заседании методической комиссии Института экономики и предпринимательства от 26.03.2020 г., протокол № ____3____.