

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 Ученого совета ННГУ
протокол от «31» мая 2023 г. № 6

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Уровень высшего образования

Бакалавриат

Направление подготовки / специальность

40.03.01 Юриспруденция

Направленность образовательной программы

Гражданское и предпринимательское право

Квалификация (степень)

Бакалавр

Форма обучения

заочная

Нижний Новгород

2023 год

1. Место дисциплины в структуре ООП

Дисциплина Б1.В.ДВ.04.02 Информационная безопасность относится к части ООП, формируемая участниками образовательных отношений, по направлению подготовки 40.03.01 «Юриспруденция».

№ вари-анта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
1	Блок 1. Дисциплины (модули) Часть, формируемая участниками образовательных отношений	Дисциплина Б1.В.ДВ.04.02 Информационная безопасность относится к части ООП направления подготовки 40.03.01 «Юриспруденция», формируемой участниками образовательных отношений.

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

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции* (код, содержание индикатора)	Результаты обучения по дисциплине**	
УК-11. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-11.1. Представляет сущность проявлений экстремизма, терроризма, коррупционного поведения и их взаимосвязь с социальными, экономическими, политическими и иными условиями	<i>Знать:</i> значение основных правовых категорий, сущность коррупционного поведения, формы его проявления в различных сферах общественной жизни <i>Уметь:</i> идентифицировать и оценивать коррупционное поведение <i>Владеть:</i> навыками взаимодействия в обществе на основе нетерпимого отношения к коррупции	Тесты, разноуровневые задачи и задания
	УК-11.2. Применяет правовые нормы о противодействии проявлениям экстремизма, терроризма, коррупционного поведения	<i>Знать:</i> действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности <i>Уметь:</i> анализировать правовые нормы о противодействии коррупционному поведению <i>Владеть:</i> навыками использования нормативных основ антикоррупционной деятельности	Тесты, разноуровневые задачи и задания

	УК-11.3. Выполняет профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета	<p><i>Знать:</i> традиционные и современные методы, позволяющие выполнять служебный долг, профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета</p> <p><i>Уметь:</i> выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета</p> <p><i>Владеть:</i> навыками выполнения профессиональных задач в соответствии с нормами морали, профессиональной этики и служебного этикета</p>	Тесты, разноуровневые задачи и задания
ПК-7 Способен выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения	ПК-7.1 Знает организацию и деятельность правоохранительных органов в Российской Федерации	<p><i>Знать:</i> организацию, функции, систему, основные задачи и полномочия правоохранительных органов в Российской Федерации.</p> <p><i>Уметь:</i> применять нормативно-правовые акты в деятельности конкретных правоохранительных и правоприменительных органов.</p> <p><i>Владеть:</i> навыками анализа нормативных правовых актов, регулирующих организационные, территориальные основы деятельности правоохранительных органов в Российской Федерации.</p>	Тесты, разноуровневые задачи и задания
	ПК-7.2 Организует и планирует расследования преступлений и правонарушений	<p><i>Знать:</i> формы и методы организации раскрытия расследования преступлений и правонарушений отдельных видов и групп</p> <p><i>Уметь:</i> применять специальные средства и методы, способствующие расследованию преступлений и правонарушений.</p> <p><i>Владеть:</i> навыками анализа различных правовых явлений и правовых отношений, являющихся объектами профессиональной деятельности при организации и планировании расследования преступлений и правонарушений.</p>	Тесты, разноуровневые задачи и задания

	ПК-7.3 Осуществляет производство следственных и иных процессуальных действий	<p><i>Знать:</i> технико-криминалистические средства, методы и тактику производства следственных действий.</p> <p><i>Уметь:</i> использовать тактические приемы при производстве следственных действий и тактических операций.</p> <p><i>Владеть:</i> методикой квалификации и разграничения различных видов правонарушений.</p>	Тесты, разноуровневые задачи и задания
	ПК-7.4 Осуществляет сбор и представляет доказательства	<p><i>Знать:</i> виды и структуры специальной техники, специальных средств, способствующих осуществлению сбора и представления доказательств.</p> <p><i>Уметь:</i> правильно ставить вопросы, подлежащие разрешению, при назначении судебных экспертиз и предварительных исследований в целях осуществления сбора и представления доказательств</p> <p><i>Владеть:</i> навыками применения технико-криминалистических средств и методов обнаружения, фиксации и изъятия следов и вещественных доказательств</p>	Тесты, разноуровневые задачи и задания
	ПК-7.5 Знает уголовно-процессуальное законодательство Российской Федерации и практику его применения	<p><i>Знать:</i> нормы действующего уголовно-процессуального законодательства, регулирующие вопросы квалификации преступлений, методологические основы квалификации преступлений, ее социальное и правовое значение.</p> <p><i>Уметь:</i> применять нормы уголовно-процессуального законодательства в деятельности правоохранительных органов.</p> <p><i>Владеть:</i> навыками анализа и обобщения практики применения уголовно-процессуальных норм.</p>	Тесты, разноуровневые задачи и задания

3. Структура и содержание дисциплины (модуля).

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	___ ЗЕТ	___ ЗЕТ	3 ЗЕТ

Тема 6. Тема 6. Менеджмент и аудит систем ИБ					1			1										2		16
Промежуточная аттестация: зачет 4ч.																				
Итого			108		4			6									1		11	93

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, крэкеры). 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. 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. 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 акты 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. Судебная практика.

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 и 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 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.

Организационно-техническое обеспечение информационной безопасности. Организация конфиденциального делопроизводства. 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 предпринимательской деятельности автоматизированных банковских систем и электронной коммерции.

Тема 6. Менеджмент и аудит систем ИБ

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. Профессионализм и технические знания сотрудников. Средства контроля. Контроль факторов, влияющих на риски и указывающих на эффективность информационной безопасности. Новые методы и средства контроля.

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 выполнение практических заданий.

На проведение практических занятий (семинарских занятий) в форме практической подготовки отводится 2 часа.

Практическая подготовка направлена на формирование и развитие:

- практических навыков в соответствии с профилем ОП;
- планирование и принятие решений в области выбранной профессиональной деятельности и оценка их эффективности;

- обоснование и принятие в пределах должностных обязанностей решений, а также совершение действий, связанных с реализацией правовых норм;
- составление юридических документов;
- компетенции:

ПК-7 Способен выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения.

Текущий контроль успеваемости проходит в рамках занятий семинарского и практического типа, групповых или индивидуальных консультаций. Промежуточная аттестация проходит на зачете.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

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 юридического 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.

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 и юриспруденции;
- 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.

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

Для обеспечения самостоятельной работы обучающихся используется электронный курс «Информационная безопасность», <https://e-learning.unn.ru/course/view.php?id=758>, созданный в системе электронного обучения ННГУ - <https://e-learning.unn.ru/>

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

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту	Уровень знаний ниже минимальных требований. Имели место грубые	Минимально допустимый уровень знаний. Допущено много негрубых	Уровень знаний в объеме, соответствующем программе подготовки. Допущено не-	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько	Уровень знаний в объеме, соответствующем программе подготовки, без	Уровень знаний в объеме, превышающем программу подготовки.

	знаний вследствие отказа обучающегося от ответа	ошибки.	ошибки.	сколько негрубых ошибок	несущественных ошибок	ошибок.	
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

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

		сформирована на уровне «хорошо»
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

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

5.2.1 Контрольные вопросы

Вопрос	Код формируемой компетенции
<ol style="list-style-type: none"> 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 	УК-11; ПК-7

<p>произведения (промышленного образца, полезной модели).</p> <p>25. Дать определение государственной тайны и назвать грифы секретности.</p> <p>26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.</p> <p>27. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.</p> <p>28. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.</p> <p>29. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.</p> <p>30. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.</p> <p>31. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.</p> <p>32. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.</p> <p>33. Назвать основные положения концепции информационной безопасности предприятия.</p> <p>34. Изложить содержание регламента обеспечения информационной безопасности предприятия.</p> <p>35. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.</p> <p>36. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.</p> <p>37. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.</p> <p>38. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.</p> <p>39. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.</p> <p>40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.</p> <p>41. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.</p> <p>42. Проанализировать особенности текста конфиденциального документа.</p> <p>43. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.</p> <p>44. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.</p> <p>45. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.</p> <p>46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.</p> <p>47. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.</p> <p>48. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.</p> <p>49. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.</p> <p>50. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.</p> <p>51. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией.</p> <p>52. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.</p> <p>53. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень</p>	
---	--

<p>опасности каждого канала.</p> <p>54. Назвать основные элементы физической защиты территории и помещений предприятия.</p> <p>55. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.</p> <p>56. Дать классификацию компьютерных вирусов.</p> <p>57. Описать основные антивирусные программы.</p> <p>58. Охарактеризовать основные способы криптографического преобразования данных.</p>	
--	--

5.2.2. Типовые тестовые задания для оценки сформированности компетенции УК-11; ПК-7

Примеры тестовых заданий

На каждый вопрос предложено три варианта ответа. Выберите один правильный и отметьте его ✓.

1. Третьим этапом построения системы защиты является:
 - планирование;
 - реализация;
 - анализ.
2. «Люком» называется..?
 - использование после окончания работы части данных, оставшиеся в памяти;
 - передача сообщений в сети от имени другого пользователя;
 - неописанная в документации на программный продукт возможность работы с ним.
3. Правовое обеспечение информационной безопасности - это..?
 - нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
 - документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
 - широкое использование технических средств защиты информации.
4. К активным угрозам относятся:
 - попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
 - разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы;
 - копирование информации.
5. Какого подхода к обеспечению безопасности информации не существует?
 - комплексный;
 - фрагментарный;
 - теоретический.
6. Типовыми путями несанкционированного доступа к информации, являются:
 - дистанционное фотографирование;
 - выход из строя ПЭВМ;
 - ураганы.
7. Первым этапом построения системы защиты является:
 - анализ;
 - планирование;
 - сопровождение.
8. «Троянский конь»- это ...?
 - способ, состоящий в тайном введении в чужую программу вредоносных команд;
 - встраивание в программу набора команд, срабатываемых при определенных условиях;
 - проникновение в компьютерную систему злоумышленников, выдающих себя за законного пользователя.

9. В политике безопасности основным принципом является усиление самого слабого звена?
- нет;
 - да;
 - отчасти.
10. Криптографические средства - это..?
- регламентация правил использования, обработки и передачи информации ограниченного доступа;
 - средства защиты с помощью преобразования информации (шифрование);
 - средства, в которых программные и аппаратные части полностью взаимосвязаны.
11. Шифрование с симметричным ключом предполагает, что..?
- используются два разных ключа;
 - оба ключа одинаковы;
 - невозможно отказаться от авторства.
12. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети предусмотрено в ..?
- ст. 272 УК РФ;
 - ст. 273 УК РФ;
 - ст. 274 УК РФ.

5.2.3. Типовые задачи (практические задачи) для оценки сформированности компетенции УК-11; ПК-7

Введение в информационную безопасность

1. Определить место роль информационной безопасности при использовании личного компьютера и мобильных устройств. Охарактеризовать последствия взлома ваших личных аккаунтов в соц. сетях, электронной почты.
2. Вы работаете бухгалтером-экономистом. Под Вашим логином и паролем со счета предприятия ушли большие суммы денег неизвестным контрагентам. Последствия, Ваша ответственность.
3. Вы работаете клиентским менеджером. С Вашего компьютера похищена клиентская база. Конкуренты предложили Вашим клиентам более привлекательные условия и цены. Последствия. Ваша ответственность.
4. Приведите примеры нарушения информационной безопасности из собственной практики. Охарактеризуйте последствия. Какие действия предпринимало руководство Вашей организации? Как в дальнейшем складывалась карьера виновных сотрудников?

Угрозы информационной безопасности

1.Защита информации от сбоев оборудования и случайной потери

1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»
2. Определите методы защиты
 - 1 периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);
 - 2 автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.

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

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

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

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

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

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

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

2. Защита информации от кражи

Ответьте на вопрос: «Что означает защита информации от кражи»

Определите методы защиты информации.

Необходимые пояснения. По данным аналитиков, источник 80% угроз информационной безопасности компании - это ее собственный персонал. Сотрудники работают с документами составляющими коммерческую тайну, следовательно они получают возможность нанести существенный урон предприятию передавая конфиденциальную информацию конкурентам, выкладывая в публичный доступ или предоставляя любым заинтересованным лицам. Причин для подобных действий может быть сколько угодно - конфликт с работодателем, внешние угрозы, шантаж, желание заработать и т.д. Возможностей тоже хватает - документы можно скопировать на usb-диск, послать по электронной почте или просто выложить в интернет.

Запретить доступ к документам содержащим коммерческую тайну абсолютно всем сотрудникам нельзя - ведь кто-то же должен их создавать и обрабатывать. Но контролировать персонал имеющий доступ к секретной информации необходимо.

Системы Защиты Информации построенные на базе файрволов и антивирусов не могут защитить от хищений (краж) конфиденциальной информации предприятия, сотрудниками, имеющими в силу своих служебных обязанностей беспрепятственный доступ к секретным данным. Они просто для этого не предназначены.

В настоящее время можно выделить следующие способы защиты от кражи конфиденциальной информации сотрудниками:

1. Отключить дисководы, usb-порты, сеть - эффективность максимальная, затраты минимальны, но применить практически невозможно - через usb-порты часто подключают мышь с клавиатурой, сеть является основой ИТ-инфраструктуры предприятия и доступ в интернет в большинстве случаев нужен для работы. К тому же возможно, что сотруднику часто надо по работе переносить большие объемы информации (не вся же информация с которой он работает секретная), так что возможность подключать usb-диски желательно тоже оставить.

2. Передаваемую в сеть информацию фильтровать анализаторами трафика и блокировать передачу секретной. К сожалению эти методы годятся только для фильтрации входящей информации - т.е. для блокировки вирусов и развлекательного например контента. Максимум чего можно достичь - это защита от непреднамеренных действий персонала, влекущих случайную утечку секретной информации. От преднамеренного хищения конфиденциальных данных подобное ПО не спасет, т.к. защиту можно обмануть например. К тому же остаются не подконтрольными съемные носители (в основном usb-диски , т.к. пишущими оптическими приводами рабочие места оснащаются не очень часто).

3. Разграничение доступа к портам ввода/вывода. Большинство подобных программ представляет собой просто графический интерфейс, являющийся надстройкой над стандартными защитными механизмами ОС Windows, который позволяет устанавливать права доступа к различным портам (например usb) для любого пользователя. Это решение также не лишено серьезных недостатков:

- во-первых - контроль не распространяется на информацию передаваемую по сети;

- во-вторых - права статичны, т.е. невозможно разрешить пользователю копировать на usb-диск несекретную информацию и запретить копировать секретную.

4. Система Защиты Информации SecrecyKeeper Corporate - разрабатывалась с учетом недостатков первых трех способов. Основное назначение Системы Защиты Информации SecrecyKeeper Corporate - предотвращение несанкционированного распространения (краж и утечек) конфиденциальной информации.

SecrecyKeeper Corporate дает службе безопасности предприятия следующие возможности:

- реализовать полномочный контроль доступа к сменным носителям информации, таким как дискеты, usb- флеш-диски и т.п.;

- ограничить доступ к конфиденциальной информации сотрудников ИТ-подразделений;

- разделять информацию хранящуюся как на рабочих станциях сотрудников, так и на серверах по степени секретности;

- присвоить каждому сотруднику предприятия персональный уровень доступа к конфиденциальной информации;

- ограничить несанкционированное распространение конфиденциальной информации на основе степени секретности данных и уровней доступа сотрудников;

- динамически регулировать права доступа сотрудников к устройствам переноса информации (дискеты, usb-диски, интернет) в зависимости от уровня доступа сотрудника и уровней секретности документов с которыми ведется работа;

- предоставлять данные по работе с конфиденциальной информацией.

На любой файл можно установить метку конфиденциальности - гриф (общедоступная, служебная, секретная);

Гриф может быть установлен на информацию доступ к которой предоставляется по сети (удаленно), такую как например базы данных, корпоративные интернет-порталы и т.п.

Для сотрудников вводятся следующие уровни доступа (каждый из которых также может принимать значения - общедоступная, служебная, секретная):

- уровень доступа к информации - определяет к информации с каким максимальным грифом может получить доступ сотрудник;

- уровень доступа к сети - определяет информацию с каким максимальным грифом, сотрудник может передать в сеть;

- уровень доступа к сменным носителям - определяет информацию с каким максимальным грифом, сотрудник может скопировать на сменный носитель.

Разобрать практические ситуации

1. Как по отношению к информации Вашей организации ведут себя конкурирующие фирмы?

Пытаются ли они заполучить важную информацию? Каким образом это происходит?

2. Сайт фирмы. Что допустимо на нем размещать? Уместно ли размещать образцы договоров?

Выскажите Ваше мнение. Как сейчас в условиях кризиса размещать прайсы? С минимальной ценой от какой то суммы? Поясните Вашу позицию.

3. Некая фирма решила торговать тем же ассортиментом что и ваша фирма. Запрашивает прайс у поставщика, программисты полностью копируют ваш интернет-магазин, меняют только главную страницу сайта. Как это предупредить заранее? Опишите Ваши действия.

4. У Вас небольшая фирма. Вид деятельности придумайте сами. Как угрозы информационной безопасности вашей деятельности вы предполагаете? Как вы будете защищать информацию?

5. ИТ-специалист вашей фирмы. Как вы будете работать с ним? По договору? Возьмете его в штат? Какие обязанности вы для него предусмотрите с учетом требований информационной безопасности? Бюджет ограничен. На что вы планируете потратить деньги в первую очередь при сотрудничестве с ИТ-специалистом?

6. На какой платформе вы бы поручили разработать сайт компании? Обоснуйте решение.

6. 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. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФЦИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1094244>

3. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - <http://www.studentlibrary.ru/book/ISBN9785940747680.html>

4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1013711>

Б) Дополнительная литература

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1137902>

2. Кузнецов, П.У. Основы информационного права. [Электронный ресурс] — Электрон. дан. — М. : Проспект, 2015. — 312 с. — Режим доступа: <http://e.lanbook.com/book/54645>.

3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60х90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5 <http://znanium.com/bookread2.php?book=423927>

Рекомендуемые Интернет-ресурсы

1. www.cyberpol.ru Компьютерная преступность и способы борьбы.

2. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.
3. www.itsec.ru Интернет-журнал «Информационная безопасность».
4. www.inside-zi.ru Информационно-методический журнал «Защита информации. Ин-сайд»
5. www.kaspersky.ru Лаборатория Касперского.

7. Материально-техническое обеспечение дисциплины (модуля)

Материально-технические условия для реализации данной учебной дисциплины соответствуют действующим санитарным и противопожарным нормам.

Реализация данной учебной дисциплины осуществляется с использованием учебных аудиторий для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения занятий используется справочно-правовая система «Консультант Плюс».

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (электронным библиотекам) («Консультант студента», «Лань», «Znanium», «Юрайт») и к электронной информационно-образовательной среде организации (portal.unn.ru). Данные электронно-библиотечные системы (электронные библиотеки) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории организации (в библиотеке ИЭП ННГУ), так и вне ее.

При необходимости 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.

Программа «Информационная безопасность» составлена в соответствии с требованиями ОС ВО ННГУ с учетом рекомендаций ООП ВО по направлению 40.03.01 «Юриспруденция», профиль «Гражданское и предпринимательское право».

Автор программы: _____ к.э.н., профессор Ясенов В.Н.

_____ к.э.н., доцент Дорожкин А.В.

Рецензенты: _____ д.э.н., зав. кафедрой ИТиИМЭ Трифонов Ю.В.

_____ д.э.н., глава МСУ Городецкого муниципального района Нижегородской области Поляков Н.Ф.

Заведующий кафедрой ИСвФКС _____ к.э.н., профессор Ясенов В.Н.

Программа одобрена на заседании методической комиссии от 14.11.2022г., протокол № 6.