

Приложение 2

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

**Юридический факультет**

(факультет / институт / филиал)

УТВЕРЖДЕНО  
решением президиума Ученого совета ННГУ  
протокол от «14» декабря 2021 г. № 4.

**Рабочая программа дисциплины  
Информационная безопасность**

*(наименование дисциплины (модуля))*

Уровень высшего образования

Специалитет

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

**40.05.01 «Правовое обеспечение национальной безопасности»**

*(указывается код и наименование направления подготовки / специальности)*

Направленность образовательной программы

**Международно-правовая специализация**

*(указывается профиль / магистерская программа / специализация)*

Форма обучения

очная, заочная

*(очная / очно-заочная / заочная)*

Нижегород  
2022 год

## 1. Место дисциплины в структуре ОП

Дисциплина Б1.В.03 «Информационная безопасность» относится к части, формируемой участниками образовательных отношений ОП, специальности 40.05.01 «Правовое обеспечение национальной безопасности».

## 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**	
<i>УК-1.</i> Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	<i>УК-1.3</i> Осуществляет поиск информации для решения поставленной задачи по различным типам запросов, критически оценивая надежность источников информации	<i>Знать</i> методы поиска информации для решения поставленной задачи по различным типам запросов. <i>Уметь</i> использовать методы поиска информации для решения поставленной задачи по различным типам запросов. <i>Владеть</i> навыками поиска информации для решения поставленной задачи по различным типам запросов.	<i>Тестирование, собеседование, решение задач-кейсов</i>
<i>ПК-7</i> Способен осуществлять действия по силовому пресечению правонарушений, использовать для решения профессиональных задач специальную технику, оружие, специальные средства, применяемые в деятельности правоохранительных органов	<i>ПК-7.1.</i> Владеет способами и методами применения силовых способов пресечения правонарушений.	<i>Знать</i> способы и методы применения силовых способов пресечения правонарушений <i>Уметь</i> использовать различные способы и методы применения силовых способов пресечения правонарушений <i>Владеть</i> способами и методами применения силовых способов пресечения правонарушений	<i>Тестирование, собеседование, решение задач-кейсов</i>

	ПК-7.2. Применяет при решении профессиональных задач специальную технику, оружие, специальные средства	<p><i>Знать</i> виды и структуру специальной техники, орудия, специальных средств при решении профессиональных задач.</p> <p><i>Уметь</i> применять при решении профессиональных задач специальную технику, оружие, специальные средства.</p> <p><i>Владеть</i> навыками применения при решении профессиональных задач специальную технику, оружие, специальные средства.</p>	Тестирование, собеседование, решение задач-кейсов
--	--	---	---

### 3. Структура и содержание дисциплины

#### 3.1 Трудоемкость дисциплины

	очная форма обучения	Заочная форма
<b>Общая трудоемкость</b>	<b>4 з.е.</b>	<b>4 з.е.</b>
<b>Часов по учебному плану</b>	<b>144</b>	<b>144</b>
<b>в том числе</b>		
<b>аудиторные занятия (контактная работа):</b>		
- занятия лекционного типа	<b>14</b>	<b>4</b>
- занятия семинарского типа (практические занятия / лабораторные работы)	<b>28 (28/0)</b>	<b>8</b>
<b>самостоятельная работа</b>	<b>64</b>	<b>121</b>
<b>КСР</b>	<b>2</b>	<b>2</b>
<b>Промежуточная аттестация – экзамен/зачет</b>	<b>Экзамен (36)</b>	<b>Экзамен (9)</b>

#### 3.2. Содержание дисциплины

	Всего	в том числе	
		Контактная работа (работа во взаимодействии с преподавателем), часы из них	Самостоятельная работа обучающегося

Наименование и краткое содержание разделов и тем дисциплины	(часы)		Занятия лекционного типа		Занятия семинарского типа		Занятия лабораторного типа		Всего			
	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная	Очная	Заочная
Тема №1 Понятие и предмет информационной безопасности	12	12	1	1	2				3	1	9	11
Тема №2 Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности	12	12	1	1	2	2			3	3	9	9
Тема №3 Правовое обеспечение информационной безопасности личности	14	14	1		3	2			4	2	10	12
Тема №4 Правовое обеспечение защиты личности и общества от воздействия вредной информации	13	13	1		3				4		9	13
Тема №5 Правовое обеспечение информационной безопасности государства. Государственная и служебная тайна в системе обеспечения информационной безопасности государства	14	14	2	2	3	2			5	4	9	10
Тема №6 Коммерческая, банковская и профессиональная тайна в системе обеспечения	14	14	2		3	2			5	2	9	12

информационной безопасности												
Тема №7 Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности	15	15	2		4				6		9	15
Тема №8 Правовое регулирование вопросов лицензирования и сертификации в области защиты информации	15	15	2		4				6		9	15
Тема №9 Юридическая ответственность за нарушение правовых норм в области информационной безопасности	15	15	2		4				6		9	15
КСР	2	2										
Экзамен	36	9										
<b>Итого</b>	<b>144</b>	<b>144</b>	<b>14</b>	<b>4</b>	<b>28</b>	<b>8</b>			<b>42</b>	<b>12</b>	<b>82</b>	<b>121</b>

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

Практическая подготовка предусматривает: решение прикладных(ситуационных) задач-кейсов, выполнение тестовых заданий, подготовка письменных работ (рефератов).

На проведение практических занятий (семинарских занятий /лабораторных работ) в форме практической подготовки отводится 28 часов.

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа.

#### **4. Учебно-методическое обеспечение самостоятельной работы обучающихся**

СРС направлена на решение следующих задач в процессе формирования у студентов требуемых компетенций:

- развитие и совершенствование навыков поиска и обработки (анализа, обобщения, систематизации) правовой и иной информации, в т.ч. навыков работы с нормативными правовыми актами, актами правоприменительной практики;
- развитие навыков работы с юридическими документами (подготовка, оформление, анализ);
- развитие навыков толкования информационно-правовых норм, правовой квалификации юридически значимых обстоятельств социальной ситуации;
- развитие и совершенствование у студентов способностей формирования собственной правовой позиции, ее аргументации и защиты.

Самостоятельная работа студента предполагает изучение нормативных актов и литературы, выполнение заданий по курсу и тестов, подготовку к аудиторным семинарским

и практическим занятиям, выполнение курсовой работы, подготовка к промежуточной аттестации по дисциплине.

#### **Рекомендации по подготовке к семинарским занятиям.**

Для подготовки к семинарскому занятию следует изучить рекомендуемую литературу по теме, а также нормативные акты. Приветствуется изучение студентами иных источников (монографий, статей из периодических изданий, материалов судебной практики), помимо рекомендованных. Такие источники можно отыскать в СПС «КонсультантПлюс» или «Гарант», используя ресурсы библиотек, а также в сети Интернет. Тем самым студент продемонстрирует владение навыками поиска информации и работы с информацией – навыками, которые являются чрезвычайно необходимыми для юриста.

#### **Рекомендации по выполнению заданий.**

Рекомендации по решению задач. Большинство заданий представлены в виде задач (казусов), т.е. модельных ситуаций в сфере информационно-правовых отношений.

Решение задачи студентом включает: изучение условий задачи (описанной ситуации) и ответы на поставленные задачей вопросы.

При выполнении данного задания (решения задачи) студенту обязательно необходимо использовать нормативно-правовые акты и ссылаться на их нормы (статьи) при ответе.

Перед ответом на поставленные в задаче вопросы, студенту необходимо внимательно ознакомиться с условиями задачи, выявив юридически значимые обстоятельства, и найти в нормативно правовом акте нормы, регулирующие данный вид правовых отношений.

Ответы на поставленные в задаче вопросы должны быть мотивированными и развернутыми. Например: "да, в соответствии с п. X. ст. X. Федерального закона «Об информации информационных технологиях и защите информации» гражданка РФ X имеет право предоставления ей запрашиваемой информации, поскольку последняя отнесена к видам информации доступ, к которой не может быть ограничен" и т.п..

Ответы: "да", "нет" без их аргументации ссылками на нормы права не допускаются.

Рекомендации по выполнению других заданий. Задания (в особенности, дополнительные задания), могут предусматривать необходимость ответить на поставленные теоретические вопросы, а также разработать (составить) юридический документ. Ответы на вопросы должны быть конкретными, выводы обязательно должны быть аргументированы ссылками на нормы права.

Приветствуются и ссылки на материалы правоприменительной практики, мнения ученых и специалистов, опубликованные в различных изданиях (статьях, комментариях, монографиях, пособиях).

Ответ студента оценивается не только по его правильности (истинности), но и по его полноте и аргументации. При составлении юридического документа (договора, доверенности и т.п.), следует придерживаться полному соответствию его содержания требованиям правовых норм, а также четкости в формулировках (избегать двусмысленности и противоречий положений документа).

#### **Вопросы для самостоятельной проработки по темам:**

##### Тема №1 Понятие и предмет информационной безопасности.

1. Понятие и предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
2. Объекты информационной безопасности: личность, общество, государство, - особенности каждого из объектов.
3. Информация и информационные системы как объекты правового регулирования в сфере обеспечения информационной безопасности.
4. Право и законодательство в сфере обеспечения информационной безопасности.

Тема №2 Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере и угрозы информационной безопасности.

1. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства.
2. Концепция национальной безопасности и Доктрина информационной безопасности России.
3. Национальные интересы России в информационной сфере: для личности, общества и государства.
4. Характеристика основных угроз в информационной сфере для личности, общества и государства.

#### Тема № 3 Правовое обеспечение информационной безопасности личности.

1. Основные угрозы информационной безопасности личности.
2. Право на информацию и на доступ к информации как важнейшие информационные права личности.
3. Право на неприкосновенность частной жизни, личную и семейную тайну и его содержание.
4. Персональные данные, как особый правовой институт охраны прав и интересов личности в информационной сфере.

#### Тема №4 Правовое обеспечение защиты личности и общества от воздействия вредной информации.

1. Понятие и структура вредной информации.
2. Законодательство в области защиты прав личности и общества от воздействия вредной информации.
3. Правовая охрана прав и законных интересов личности от воздействия вредной информации.

#### Тема № 5 Правовое обеспечение информационной безопасности государства. Государственная и служебная тайна в системе обеспечения информационной безопасности государства.

1. Основные угрозы информационной безопасности государства.
2. Понятие государственной тайны.
3. Критерии отнесения информации к государственной тайне.
4. Доступ и допуск к государственной тайне, категории допуска. Порядок засекречивания и рассекречивания информации, отнесенной к государственной тайне.
5. Служебная тайна. Понятие служебной тайны и критерии охраноспособности прав на нее.

#### Тема № 6 Коммерческая, банковская и профессиональная тайна в системе обеспечения информационной безопасности.

1. Понятие коммерческой тайны и критерии охраноспособности прав на нее.
2. Понятие банковской тайны и критерии охраноспособности прав на нее.
3. Понятие профессиональной тайны и критерии охраноспособности прав на нее.

#### Тема № 7 Правовое обеспечение информационной безопасности в сфере интеллектуальной собственности.

1. Особенности режима интеллектуальных прав.
2. Защита интеллектуальных прав. Споры, связанные с защитой интеллектуальных прав.
3. Понятие авторских и смежных прав. Способы защиты авторских и смежных прав.
4. Право на программы для ЭВМ и базы данных. Характерные особенности правовой охраны программ для ЭВМ и баз данных.
5. Понятие патентного права. Способы защиты патентных прав.
6. Особенности правовой охраны прав на фирменное наименование, товарные знаки и знаки обслуживания, наименования мест происхождения товара, коммерческие обозначения.
7. Международно-правовая охрана объектов интеллектуальных прав

Тема № 8 Правовое регулирование вопросов лицензирования и сертификации в области защиты информации.

1. Основные виды деятельности по защите информации, подлежащие лицензированию.
2. Система государственного лицензирования деятельности в области защиты информации.
3. Общий порядок лицензирования в области защиты информации.
4. Система сертификации средств защиты информации.
5. Аттестация объектов информатизации (информационных систем) по требованиям информационной безопасности.

Тема №9 Юридическая ответственность за нарушение правовых норм в области информационной безопасности

1. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности.
2. Уголовно-правовая ответственность за нарушение правовых норм в области информационной безопасности.
3. Административная ответственность за нарушение правовых норм в сфере информационной безопасности.
4. Особенности юридической ответственности за нарушение правовых норм в области информационной безопасности в гражданско-правовых и трудовых отношениях.

Для обеспечения самостоятельной работы обучающихся используется электронный курс Информационная безопасность (<https://e-learning.unn.ru/course/view.php?id=5603>), созданный в системе электронного обучения ННГУ - <https://e-learning.unn.ru/>.

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

включающий:

**5.1. Описание шкал оценивания результатов обучения по дисциплине**

**УК-1.3.** «Осуществляет поиск информации для решения поставленной задачи по различным типам запросов, критически оценивая надежность источников информации»

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<b>Знания</b> - способы работы с различными источниками информации, и информационным и ресурсами и технологиями; - использование в профессиональной деятельности компьютерную технику, прикладные программные средства, современные средства телекоммуникации, автоматизированные	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.

информационно-справочные, информационно-поисковые системы, базы данных, автоматизированные рабочие места							
<p><b>Умения</b> Уметь: - работать с различными источниками информации, информационными ресурсами и технологиями - использовать в профессиональной деятельности компьютерную технику, прикладные программные средства, современные средства телекоммуникации, автоматизированные информационно-справочные, информационно-поисковые системы, базы данных, автоматизированные рабочие места</p>	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач 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
<p><b>Навыки</b> Владеть: - опытом работы с различными источниками информации, информационными ресурсами и технологиями - опытом использования в профессиональной деятельности компьютерной техники, прикладных программных средств, современных средств телекоммуникации, автоматизированных информационно-справочных, информационно-поисковых систем, баз данных, автоматизированных рабочих мест</p>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач 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

**ПК-7.1. «Владеет способами и методами применения силовых способов пресечения правонарушений»**

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<b>Знания</b> Знать: способы и методы применения силовых способов пресечения правонарушений в области информационной безопасности и защиты информации	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<b>Умения</b> Уметь: использовать различные способы и методы применения силовых способов пресечения правонарушений в области информационной безопасности и защиты информации	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения, Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<b>Навыки</b> Владеть: способами и методами применения силовых способов пресечения правонарушений в области информационной безопасности и защиты информации	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач

**ПК-7.2. Применяет при решении профессиональных задач специальную технику, оружие, специальные средства**

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<b>Знания</b>	Отсутствие	Уровень	Минимально	Уровень	Уровень	Уровень	Уровень

Знать: виды и структуру специальной техники, орудия, специальных средств при решении профессиональных задач в области информационной безопасности и защиты информации	знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	знаний ниже минимальных требований. Имели место грубые ошибки.	допустимый уровень знаний. Допущено много негрубых ошибок.	знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	знаний в объеме, соответствующем программе подготовки, без ошибок.	знаний в объеме, превышающем программу подготовки.
<u>Умения</u> Уметь: применять при решении профессиональных задач специальную технику, оружие, специальные средства в области информационной безопасности и защиты информации	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
Навыки Владеть: навыками применения при решении профессиональных задач специальную технику, оружие, специальные средства в области информационной безопасности и защиты информации	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
	<b>превосходно</b>	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
<b>зачтено</b>	<b>отлично</b>	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»
	<b>очень хорошо</b>	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»
	<b>хорошо</b>	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»
	<b>удовлетворительно</b>	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»
<b>не зачтено</b>	<b>неудовлетворительно</b>	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	<b>плохо</b>	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

<i>вопросы</i>		<i>Код формируемых компетенции</i>
1.	Понятие и предмет информационной безопасности.	<b>УК-1.3</b>
2.	Соотношение понятий безопасность и информационная безопасность.	
3.	Уровни обеспечения безопасности: личностный, гражданское общество, государственный.	
4.	Общая структура правового института информационной безопасности. Объекты информационной безопасности: личность, общество, государство, - особенности каждого из объектов.	
5.	Основные теории понимания национальных интересов России в информационной сфере.	
6.	Классификация национальных интересов по срокам их реализации, соотношение интереса и информации.	
7.	Разработка и принятие Концепции национальной безопасности и Доктрины информационной безопасности России.	
8.	Понятие источника угрозы национальной безопасности, информационной безопасности и их разновидности.	
9.	Информационные войны, понятие, основы теории информационных войн.	
10.	Информационный терроризм.	
11.	Информационное оружие.	
12.	Принципы обеспечения информационной безопасности.	
13.	Основные задачи, функции и стандарты обеспечения информационной безопасности.	
14.	Конституционное закрепление и охрана информационных прав граждан.	
15.	Право на неприкосновенность частной жизни, личной и семейной тайны.	
16.	Персональные данные. Понятие, правовое регулирование.	
17.	Понятие и виды вредной информации.	

18.	Правовые средства противодействия деятельности общественных организаций, распространяющих вредную информацию, религиозных сект, политических партий, фондов.
19.	Коммерческая тайна. Понятие и правовое регулирование.
20.	Банковская тайна. Понятие и правовое регулирование.
21.	Профессиональная тайна. Понятие и правовое регулирование.
22.	Служебная тайна. Понятие и правовое регулирование.
23.	Проблемы правового обеспечения информационной безопасности государства, противодействия информационным войнам и терроризму.
24.	Понятие государственной тайны.
25.	Доступ и допуск к государственной тайне, категории допуска.
26.	Порядок засекречивания и рассекречивания информации, отнесенной к государственной тайне. Предварительное засекречивание.
27.	Ответственность за нарушение порядка обращения с информацией, составляющей государственную тайну.
28.	Основные виды деятельности по защите информации, подлежащие лицензированию.
29.	Система государственного лицензирования деятельности в области защиты информации.
30.	Органы государственной власти, полномочные в сфере лицензирования деятельности по защите информации и их правовой статус.
31.	Общий порядок лицензирования в области защиты информации.
32.	Система сертификации средств защиты информации.
33.	Государственные стандарты в области защиты информации.
34.	Общий порядок проведения сертификации средств защиты информации.
35.	Аттестация объектов информатизации (информационных систем) по требованиям информационной безопасности.

## 5.2.2. Типовые тестовые задания для оценки сформированности компетенции УК-1.3

### Пример тестовых заданий:

1. Хищение информации – это
  - а. Несанкционированное копирование информации
  - б. Утрата информации
  - в. Блокирование информации
  - г. Искажение информации
  - д. Продажа информации
2. Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации - это:
  - а. Конфиденциальная информация
  - б. Факс
  - в. Личный дневник
  - г. Законы РФ

### **3. Обеспечение информационной безопасности есть обеспечение...**

- а. Независимости информации*
- б. Изменения информации*
- в. Копирования информации*
- г. Сохранности информации*
- д. Преобразования информации*

#### **Примеры тем для устного собеседования:**

1. Понятие и предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.
2. Право и законодательство в сфере обеспечения информационной безопасности.
3. Направления государственной политики РФ в сфере информатизации и информационной безопасности личности, общества, государства.
4. Национальные интересы России в информационной сфере: для личности, общества и государства.
5. Право на информацию и на доступ к информации как важнейшие информационные права личности.
6. Право на неприкосновенность частной жизни, личную и семейную тайну и его содержание.
7. Персональные данные, как особый правовой институт охраны прав и интересов личности в информационной сфере.
8. Понятие и структура вредной информации.
9. Законодательство в области защиты прав личности и общества от воздействия вредной информации.
10. Правовая охрана прав и законных интересов личности от воздействия вредной информации.

#### **Пример ситуационной задачи:**

К руководству акционерного общества «Синтез» обратилась общественная организация «Здоровье» с просьбой представить данные о производственном травматизме на предприятии за последние три года. Руководство акционерного общества отказалось удовлетворить просьбу общественной организации, мотивируя свое отказное решение тем, что указанные данные являются секретом производства. Общественная организация повторно обратилась с аналогичной просьбой, указав в письме на имя акционерного общества на ст. 5 Федерального закона «О коммерческой тайне», согласно которой режим коммерческой тайны не может быть установлен в отношении сведений, касающихся показателей производственного травматизма. На повторное обращение общественной организации поступил повторный отказ с указанием на то, что сведения, которые не могут составлять коммерческую тайну, могут находиться в режиме секретов производства. Общественная организация была вынуждена 3 обратиться в экспертно-правовой центр юридического факультета за получением соответствующих разъяснений.

Дайте разъяснения по существу сложившейся ситуации

### **5.2.3. Типовые задания/задачи для оценки сформированности компетенции ПК-7**

#### **Примеры тестовых заданий:**

#### **1. Степени секретности информации, составляющей гостайну:**

- а. особо секретно;*
- б. конфиденциально;*
- в. строго конфиденциально;*
- г. совершенно конфиденциально;*
- д. секретно;*

*е. особой важности.*

**2. Не подлежат отнесению к государственной тайне сведения:**

*а. о состоянии обороноспособности объектов жизнеобеспечения населения;*

*б. о фактах нарушения прав и свобод человека и гражданина;*

*в. о размерах золотого запаса и государственных валютных резервах Российской Федерации;*

*г. о состоянии и средствах защиты государственной тайны;*

*д. о состоянии здоровья высших должностных лиц Российской Федерации;*

**3. К видам информации с ограниченным доступом не относятся:**

*а. коммерческая тайна;*

*б. государственная тайна;*

*в. сведения для служебного пользования;*

*г. персональные данные;*

*д. запрещенные к распространению сведения;*

*е. нотариальная тайна.*

**Примеры тем для устного собеседования:**

1. Понятие государственной тайны.

2. Критерии отнесения информации к государственной тайне.

3. Доступ и допуск к государственной тайне, категории допуска. Порядок засекречивания и рассекречивания информации, отнесенной к государственной тайне.

4. Служебная тайна. Понятие служебной тайны и критерии охраноспособности прав на нее.

5. Понятие коммерческой тайны и критерии охраноспособности прав на нее.

6. Понятие банковской тайны и критерии охраноспособности прав на нее.

7. Понятие профессиональной тайны и критерии охраноспособности прав на нее.

8. Особенности режима интеллектуальных прав.

9. Защита интеллектуальных прав. Споры, связанные с защитой интеллектуальных прав.

10. Понятие авторских и смежных прав. Способы защиты авторских и смежных прав.

11. Право на программы для ЭВМ и базы данных. Характерные особенности правовой охраны программ для ЭВМ и баз данных.

12. Понятие патентного права. Способы защиты патентных прав.

13. Система сертификации средств защиты информации.

14. Аттестация объектов информатизации (информационных систем) по требованиям информационной безопасности.

15. Понятие и виды юридической ответственности за нарушение правовых норм в области информационной безопасности.

16. Уголовно-правовая ответственность за нарушение правовых норм в области информационной безопасности.

**Примеры ситуативных задач-кейсов.**

**Задание 1.**

Работник В. по случайности в обеденный перерыв, решив отобедать в кафе неподалеку, вынес с территории предприятия в портфеле папку с документами с грифом «Секретно». После обеда по рассеянности сотрудник В. оставил папку с документами на стуле, которая была найдена официантом К., сообщившего о находке в отделение полиции.

Предположите, какова будет ответственность работника В.? Предположите ситуацию, когда В. тоже может быть привлечен к ответственности?

**Задание 2.**

Работника предприятия привлекли к ответственности за разглашение коммерческой тайны. В свое оправдание работник заявил о том, что сведения ему были предоставлены в рамках исполнения служебных обязанностей и он ранее не был ознакомлен с перечнем сведений

составляющих коммерческую тайну на этом предприятии. В трудовом договоре указание на обязанность работника по сохранению конфиденциальности сведений, составляющих коммерческую тайну были указаны.

Укажите было ли привлечение к ответственности работника законным? Свой ответ аргументируйте?

## **6. Учебно-методическое и информационное обеспечение дисциплины**

а) основная литература:

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/469235> (дата обращения: 29.06.2021).
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/471159> (дата обращения: 29.06.2021).

б) дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : [www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1](http://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1)
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : [www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7](http://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7)
3. Хомяков Эдуард Геннадьевич Информационная безопасность как составляющая прав граждан Российской Федерации // Вестник Удмуртского университета. Серия «Экономика и право». 2011. №3. URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-sostavlyayuschaya-prav-grazhdan-rossiyskoy-federatsii>

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

1. Портал «Гуманитарное образование» <http://www.humanities.edu.ru/>
2. Федеральный портал «Российское образование» <http://www.edu.ru/>
3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» <http://school-collection.edu.ru/>
4. Открытая электронная библиотека <http://www.elibrary.ru/>
5. Справочная правовая система «Консультант Плюс».
6. Справочная правовая система «Гарант».
7. ЭБС «Лань».
8. ЭБС «Консультант студента».
9. ЭБС «Юрайт»
10. ЭБС «Znanium.com»
11. <http://www.pravo.gov.ru> – Официальный интернет-портал правовой информации.
12. <http://echr.ru/> - сайт о деятельности Европейского суда по правам человека.

## **7. Материально-техническое обеспечение дисциплины**

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: компьютером, проектором или ЖК-телевизором, акустической системой и микрофоном (при необходимости), а также доской.

Помещения для самостоятельной работы обучающихся оснащены компьютерной

техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ВО ННГУ с учетом рекомендаций и ОП ВО по специальности 40.05.01 «Правовое обеспечение национальной безопасности».

Авторы: к.ю.н., М.В. Бундин

Заведующий кафедрой: д.ю.н., профессор Мартынов А.В.

Программа одобрена на заседании Учебно-методической комиссии юридического факультета ННГУ им. Н.И. Лобачевского от «13» декабря 2021 года, протокол № 4.