

Федеральное государственное образовательное бюджетное  
учреждение высшего образования  
**«Финансовый университет при Правительстве Российской Федерации»**

**Уфимский филиал Финуниверситета**

## **ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

по дисциплине  
**«ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ»**

Разработчик: кафедра «Философия, история и право»

Направление подготовки: 40.03.01 Юриспруденция

Образовательная программа: «Юриспруденция»

Профиль подготовки: «Экономическое право»

Форма образования: заочная

**Уфа 2021**

РАССМОТРЕН  
На заседании кафедры  
«Философия, история и право»

Разработан на основе  
**40.03.01 Юриспруденция: ОС ВО**  
**ФУ**  
Приказ ФУ от 03.06.2021 № 1313/о

Протокол № 10  
от «7» июня 2021 г.  
Зав. кафедрой



Галлямов Р.Р.

## 1. Цель, задачи и результаты изучения дисциплины

### Цели дисциплины –

1.Формирование у студентов профессиональных навыков, связанных с правовым обеспечением информационной безопасностью высокопроизводительных вычислительных комплексов при решении прикладных задач.

2.Создание представления об основах правового управления информационной безопасностью высокопроизводительных вычислительных комплексов при решении прикладных задач, принципах и методах правового противодействия несанкционированному информационному воздействию.

### Задачи дисциплины:

1.Изучить основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;

2.Сформировать навыки организации правового противодействия утечке информации, правовых способов и средств защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы и методы противодействия несанкционированному информационному воздействию на высокопроизводительные вычислительные комплексы при решении прикладных задач в сфере финансовых технологий.

3.Сформировать умения и навыки проведения анализа и оценки правовых угроз информационной безопасности при решении прикладных задач.

4. Обучить юридическим методам формирования требований по защите информации; управления информационной безопасностью.

### Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с компетенциями / индикаторами достижения компетенции
ПКП-1	Способность использовать фундаментальные знания в области частного права и публичного	1. Анализирует юридические факты и возникающие в связи с ними правоотношения, толкует и правильно применяет правовые нормы.	<b>знать:</b> нормы российского законодательства о информационной безопасности <b>уметь:</b> грамотно применять законодательство об информационной безопасности в правовой деятельности

	права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	2. Принимает решения и совершает юридические действия в точном соответствии с законом.	<b>знать:</b> структуру, основные цели, задачи, организационные формы и методы информационной безопасности в России <b>уметь:</b> ориентироваться в основных понятиях кибербезопасности в Российской Федерации
		3. Демонстрирует навыки анализа правоприменительной практики, обеспечивает реализацию норм процессуального права.	<b>знать:</b> способы работы с документами, относящимися к информационной безопасности <b>уметь:</b> грамотно и правильно составлять и оформлять документы о кибербезопасности
ПКП-2	Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении и предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	1. Выявляет и предлагает способы устранения проблем, связанных с кризисными ситуациями в экономике.	<b>знать:</b> основы законодательства о информационной безопасности с точки зрения государственного регулирования экономики <b>уметь:</b> применять на практике законодательство Российской Федерации, в том числе Конституцию Российской Федерации, федеральные конституционные законы и федеральные законы, а также общепризнанные принципы, нормы международного права относительно кибербезопасности
		2. Анализирует проблемные ситуации на рынке товаров, работ, услуг, выявляет правонарушения при осуществлении предпринимательской деятельности	<b>знать:</b> способы соблюдения законодательства Российской Федерации субъектами права в сфере кибербезопасности <b>уметь:</b> применять нормативные правовые акты, реализовывать нормы материального и процессуального права в сфере информационной безопасности
		3. Находит пути решения ситуаций, связанных с преодолением правонарушений при осуществлении предпринимательской деятельности	<b>знать:</b> основы законодательства в области защиты интересов предпринимателей в сфере информационной безопасности <b>уметь:</b> представлять интересы предпринимателей в судах в сфере кибербезопасности

## **2. Оценочные средства для оценки форсированности компетенций (контроль остаточных знаний)**

### **Тестовые задания по курсу «Правовое обеспечение кибербезопасности» (ПКП-1, ПКП-2)**

1. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право? **ПКП-1**
  - 1) конфиденциальность
  - 2) доступность
  - 3) целостность
  - 4) аутентичность
2. Как называется состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право? **ПКП-1**
  - 1) конфиденциальность
  - 2) доступность
  - 3) целостность
  - 4) аутентичность
3. Как называется состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно? **ПКП-1**
  - 1) конфиденциальность
  - 2) доступность
  - 3) целостность
  - 4) аутентичность
4. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации? **ПКП-2**
  - 1) атака
  - 2) угроза
  - 3) уязвимость
  - 4) слабое место системы
5. Как называется попытка реализации угрозы? **ПКП-2**
  - 1) атака
  - 2) нападение
  - 3) уязвимость
  - 4) слабое место системы
6. Следствием наличия уязвимостей в информационной системе является: **ПКП-2**
  - 1) угроза

- 2) атака
- 3) нападение
- 4) необходимость замены компонентов системы

7. Какой уровень защиты информации состоит из мер, реализуемых людьми?  
**ПКП-2**

- 1) законодательный
- 2) процедурный
- 3) программно-технический
- 4) административный

8. Какой уровень защиты информации представляет собой комплекс мер, применяемых руководством организации? **ПКП-2**

- 1) законодательный
- 2) процедурный
- 3) программно-технический
- 4) административный

9. На каком уровне защиты информации находятся непосредственно средства защиты? **ПКП-1**

- 1) законодательный
- 2) процедурный
- 3) программно-технический
- 4) административный

10. Совокупность содержащейся в базах данных информации, и информационных технологий и технических средств, обеспечивающих ее обработку, называется: **ПКП-1**

- 1) система защиты информации
- 2) автоматизированная система
- 3) информационная система
- 4) система обработки персональных данных

11 (**ПКП-1**). Цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации изложены в ...

12 (**ПКП-2**). Органы, государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований ФЗ “О персональных данных” называют ...

13 (**ПКП-2**). Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на ...

14 (**ПКП-1**). Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать

доступ к информации, определяемой по каким-либо признакам называется...

15 (ПКП-2). ... должен своевременно обнаруживать факты несанкционированного доступа к персональным данным.

Номер теста	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ответ	1	3	2	2	1	1	2	4	3	3	Стратегия национальной безопасности РФ	регуляторами	оператора персональных данных	обладателем информации	Оператор персональных данных

### 3. Методические материалы, определяющие процедуры оценивания знаний и умений, характеризующих степень сформированности компетенций

#### Критерии оценки знаний при проведении устного/письменного опроса

Оценка **«отлично»** – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов дисциплины.

Оценка **«хорошо»** – выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, но допускает в ответе некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка **«удовлетворительно»** – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка **«неудовлетворительно»** – выставляется обучающемуся, который не знает большей части основного содержания вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий.

#### Критерии оценки знаний при решении задач

Оценка **«отлично»** – выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания вопросов дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка **«хорошо»** – выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе некоторые неточности, которые может устранить с помощью дополнительных вопросов преподавателя.

Оценка **«удовлетворительно»** – выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными понятиями, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации.

Оценка **«неудовлетворительно»** – выставляется обучающемуся, который не знает большей части основного содержания вопросов тем дисциплины, допускает грубые ошибки в формулировках основных понятий, не умеет использовать полученные знания при решении типовых практических задач.

### **Критерии оценки знаний при проведении тестирования**

Оценка **«отлично»** выставляется при условии правильного ответа студента не менее чем на 85 % тестовых заданий;

Оценка **«хорошо»** выставляется при условии правильного ответа студента не менее чем на 70 % тестовых заданий;

Оценка **«удовлетворительно»** выставляется при условии правильного ответа студента не менее чем на 51 %;

Оценка **«неудовлетворительно»** выставляется при условии правильного ответа студента менее чем на 50 % тестовых заданий.