

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Сыров Игорь Анатольевич  
Должность: Директор  
Дата подписания: 30.10.2023 12:25:55  
Уникальный программный ключ:  
b683afe664d7e9f64175886cf9626a196149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Юридический  
Кафедра Теории и истории государства и права

**Оценочные материалы по дисциплине (модулю)**

дисциплина Информационная безопасность в правоохранительной сфере

**Блок Б1, обязательная часть, Б1.О.08**

цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

40.04.01  
код

Юриспруденция  
наименование направления

Программа

Юрист в правоохранительной деятельности

Форма обучения

Очная

Для поступивших на обучение в  
2022 г.

Разработчик (составитель)  
к.и.н., доцент  
Алешин П. Н.  
ученая степень, должность, ФИО

<b>1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю) .....</b>	<b>3</b>
<b>2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю).....</b>	<b>7</b>
<b>3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания .....</b>	<b>10</b>

**1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)**

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
			1	2	3	4	
			неуд.	удовл.	хорошо	отлично	
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Знает этику делового общения, что такое коррупционное и иное противоправное поведение в сфере своей профессиональной деятельности, в том числе в части антикоррупционных стандартов поведения	Обучающийся должен знать методы аналитической работы в подготовке правового обеспечения информационной безопасности правоохранительной сфере; основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации	Не знает методы аналитической работы в подготовке правового обеспечения информационной безопасности правоохранительной сфере; основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации	Плохо знает методы аналитической работы в подготовке правового обеспечения информационной безопасности правоохранительной сфере; основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации	Достаточно знает методы аналитической работы в подготовке правового обеспечения информационной безопасности правоохранительной сфере; основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации	В полном объеме знает методы аналитической работы в подготовке правового обеспечения информационной безопасности правоохранительной сфере; основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации	Контрольные вопросы

	ОПК-7.2. Осуществляет комплексную проверку правовых актов на предмет коррупционных положений, умеет проявлять непримиримость к коррупционному и иному противоправному поведению	Обучающийся должен уметь применять нормы информационного права в правоохранительной сфере; составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации, определять виды и формы информации, подверженной угрозам, формировать комплекс мер по информационно	Не умеет применять нормы информационного права в правоохранительной сфере; составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации, определять виды и формы информации, подверженной угрозам, формировать комплекс мер по информационно	Не достаточно, с определенными трудностями, умеет применять нормы информационного права в правоохранительной сфере; составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации, определять виды и формы информации, подверженной угрозам, формировать	В целом умеет применять нормы информационного права в правоохранительной сфере; составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации, определять виды и формы информации, подверженной угрозам, формировать комплекс мер по информационно	В полной мере умеет применять нормы информационного права в правоохранительной сфере; составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации, определять виды и формы информации, подверженной угрозам, формировать комплекс мер по информационно	Тестирование

		й безопасности с учетом его правовой обоснованности	учетом его правовой обоснованности	комплекс мер по информационно й безопасности с учетом его правовой обоснованности	учетом его правовой обоснованности	учетом его правовой обоснованности	
ОПК-7.3. Выявляет коррупционное и иное противоправное поведение, в том числе в сфере своей профессиональной деятельности, способен предъявлять требования к соблюдению служебного поведения	Обучающийся должен владеть навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками анализа информационны х угроз в правоохранительной сфере навыками организации	Не владеет навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками анализа информационны х угроз в правоохранительной сфере навыками организации	Не в полной мере, с трудностями владеет навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками анализа информационны х угроз в правоохранительной сфере навыками организации	Достаточно приобрел навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками анализа информационны х угроз в правоохранительной сфере навыками организации	В полной мере овладел навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками анализа информационны х угроз в правоохранительной сфере навыками организации	Контроль ные задания	

--	--	--	--	--	--	--	--

## **2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)**

### **Перечень вопросов к устному опросу**

*Перечень вопросов для оценки уровня сформированности компетенции **ОПК-7** на этапе «Знания»*

1. Какие существуют основания классификации информации в правовой сфере?
2. Как можно классифицировать информацию по уровню доступа?
3. Охарактеризуйте содержание понятия «информационные системы».
4. Определите понятие «автоматизированная справочная система».
5. Какова роль информационно-поисковых систем в правовой сфере?

### **Тестовые задания**

*Перечень тестовых заданий для оценки уровня сформированности компетенции **ОПК-7** на этапе «Умения»*

1. Опасными тенденциями информатизации являются:
  - а) глобальный характер информационных технологий;
  - б) усложнение отбора качественной и достоверной информации;
  - в) возрастающая возможность проникновения в частную жизнь посредством информационных технологий;
2. Информационная технология базируется на следующих основных принципах:
  - а) интерактивный (диалоговый) режим работы с компьютером
  - б) интегрированность с другими программными продуктами
  - в) гибкость процесса изменения данных и постановок задач
  - г) все варианты верны
3. Хранение информации – это:
  - а) это состояние документа, программы или технических средств, характеризующее степень удержания их эксплуатационных свойств.
  - б) это создание рабочих, резервных и страховых электронных архивов.
  - в) это процесс точного восстановления электронной информации, ранее сжатой и хранящейся в файле-архиве.
  - г) это способ длительного удержания информации и (или) данных на каком-либо носителе.
4. Протокол передачи данных в сети — это:
  - 1) юридически оформленный документ для обеспечения сохранности данных;
  - 2) правила передачи данных и поиска адресата в сети, язык общения в сети;
  - 3) алгоритм взаимодействия, оформленный документально;
  - 4) название способа управления передачей данных.
5. Протокол IP определяет
  - 1) как отображается информация на экране компьютера;
  - 2) как происходит передача информации;
  - 3) куда происходит передача информации;
  - 4) как упаковывается информация.
6. Основными задачами информатизации являются:

- 1) формирование массива информационных ресурсов;
  - 2) оснащение правоохранительных органов современной вычислительной и другой техникой обработки и передачи информации;
  - 3) внедрение информационных технологий;
  - 4) все варианты верны
7. Под информационно-телекоммуникационными технологиями в правоохранительной деятельности понимают
- 1) операции по сбору информации с помощью компьютеров
  - 2) хранение информации с помощью компьютеров
  - 3) обработку и передачу правоохранительной информации с помощью компьютеров.
  - 4) все варианты верны
8. Примерами информационных процессов могут служить:
- 1) процессы строительства зданий и сооружений,
  - 2) процессы химической и механической очистки воды,
  - 3) процессы поиска нужной литературы с помощью библиотечного каталога,
  - 4) процессы производства электроэнергии,
  - 5) процессы извлечения полезных ископаемых из недр Земли.
9. Примером процесса хранения информации может служить процесс:
- 1) распространения в обществе сведений с помощью средств массовой информации,
  - 2) направленный на сохранение структуры данных и их значений,
  - 3) ограничения доступа к информации людям, не имеющим на это право,
  - 4) несанкционированного использования информации,
  - 5) создания банков данных и базы знаний.
10. Информационные системы, сети и сети связи, используемые при международном информационном обмене это:
- а) средства международного информационного обмена;
  - б) методы международного информационного обмена;
  - в) обеспечение международного информационного обмена.

### **Контрольные задания**

*Перечень контрольных заданий для оценки уровня сформированности компетенции **ОПК-7** на этапе «Навыки»*

1. Найдите Приказ Генпрокуратуры РФ № 39 «О применении бланков процессуальных документов». Сохраните документ в папку, созданную под своим именем.
2. В адресной строке программы ввести [www.yandex.ru](http://www.yandex.ru). На главной странице информационно-поисковой системы Яндекс найти поле для ввода ключевых слов. Ввести в этом поле ключевые слова «Государственная автоматизированная система «Правосудие». Необходимо найти Web-страницы, посвященные автоматизированной системе «Правосудие». Просмотреть результаты поиска. Выбрать первую гиперссылку. Внимательно рассмотреть загруженную страницу. Поочередно выбрать всю первую группу ссылок на найденные страницы. Сколько из этих страниц можно считать полезными? В пункте меню Поиск на панели инструментов набрать ключевые слова «Государственная автоматизированная система «Правосудие». Сравнить результаты поиска.



### Вопросы к зачету

1. Понятие и виды информации. Документированная и недokumentированная информация.
2. Предмет информационно-правового регулирования.
3. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации.
4. Система и компетенция органов, обеспечивающих охрану государственной тайны.
5. Компетенция органов государственной власти по обеспечению правового режима конфиденциальной информации.
6. Режимы защиты информации.
7. Государственная тайна как предмет, изъятый из гражданского оборота.
8. Понятие и структура персональных данных
9. Право на защиту персонифицированной информации.
10. Понятие и виды информационно-правовых систем
11. Понятие и виды информационной безопасности.
12. Понятие информационной безопасности личности, общества, государства.
13. Обеспечение защиты информационных ресурсов от несанкционированного доступа.
14. Общая характеристика и виды ответственности за правонарушения в информационной сфере.
15. Угрозы безопасности в информационной сфере.
16. Правовое обеспечение безопасности в информационной сфере.
17. Защита прав граждан в информационной сфере.
18. Обеспечение законности в информационной сфере.
19. Контроль и надзор в информационной сфере.
20. Виды правонарушений в информационной сфере.
21. Гражданско-правовая, административно-правовая и уголовно-правовая, дисциплинарная ответственность за правонарушения в информационной сфере.
22. Проблемы правовой ответственности в информационной сфере.
23. Понятие и виды информационно-правовых систем.
24. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства
25. Противодействие экстремистской деятельности в информационной сфере
26. Информационная инфраструктура судопроизводства
27. Административная и уголовная ответственность за правонарушения экстремистской направленности
28. Порядок признания информационных материалов экстремистскими. Федеральный список экстремистских материалов
29. Понятие экстремистской деятельности в информационной сфере
30. Реализация принципа единства судебной систем в информационно-телекоммуникационной сфере и формирование единого информационного пространства в области судопроизводства.
31. Процессуальная специфика защиты электронных документов в сфере судопроизводства
32. Проблемы исключения фальсификаций доказательств, представляемых в электронном виде.

33. Системы информационного обеспечения функциональной деятельности прокуратуры.
34. Основные потребители информации, информационных ресурсов, информационных продуктов, информационных систем правоохранительной органов.
35. Функция информационного обеспечения обвинения и юридической защиты в уголовном процессе
36. Роль информационных технологий в обеспечении правопорядка
37. Анализ и характеристика наиболее перспективных направлений развития в области информационной безопасности.

### 3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Виды учебной деятельности магистрантов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Раздел 1 Понятие, организация и основы обеспечения информационной безопасности</b>			0	<b>50</b>
<b>Текущий контроль</b>			0	<b>25</b>
1. Контрольные вопросы	1	5	0	5
2. Тестирование	5	3	0	15
3. Контрольные задания	1	5	0	5
<b>Рубежный контроль</b>				<b>25</b>
Тестирование		1	0	25
<b>Раздел 2 Правовое обеспечение информационной безопасности</b>			0	<b>50</b>
<b>Текущий контроль</b>			0	<b>25</b>
1. Контрольные вопросы	1	5	0	5
2. Тестирование	5	3	0	15
3. Контрольные задания	1	5	0	5
<b>Рубежный контроль</b>				<b>25</b>
Тестирование		1	0	25
<b>Поощрительные баллы</b>				<b>10</b>
1. Публикация статей			0	5

2.Участие в конференциях			0	5
<b>Промежуточный контроль</b>				
<b>Зачет</b>				
<b>Итого баллов</b>			0	<b>110</b>

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл =  $k \times$  Максимальный балл,

где  $k = 0,2$  при уровне освоения «неудовлетворительно»,  $k = 0,4$  при уровне освоения «удовлетворительно»,  $k = 0,8$  при уровне освоения «хорошо» и  $k = 1$  при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:

На зачете выставляется оценка:

- зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.