МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
Государственное образовательное учреждение высшего образования Московской области
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОБЛАСТНОЙ УНИВЕРСИТЕТ
(МГОУ)
Юридический факультет
кафедра гражданского права

УТВЕРЖДЕН
на заседании кафедры гражданского права
Протокол от «15» 06 2021 г. № 11
И.о. Зав. кафедрой __________ (Левушкин А.Н)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Информационная безопасность

Направление подготовки
40.03.01 Юриспруденция

Профиль:

Правозащитная деятельность с интенсивным изучением иностранного языка

Мытищи
2021

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Код и наименование компетенции	**Этапы формирования**
УК-1 – способность осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	1.Работа на учебных занятиях 2.Самостоятельная
СПК-2 – способность квалифицированно применять правовые нормы и принимать правоприменительные акты в конкретных сферах юридической деятельности	1.Работа на учебных занятиях 2.Самостоятельная работа
СПК-3 – способность квалифицированно применять правовые нормы и принимать правоприменительные акты в конкретных сферах юридической деятельности	1.Работа на учебных занятиях 2.Самостоятельная работа

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оцениваемые компетенции	**Уровень сформированности**	**Этап формирования**	**Описание показателей**	**Критерии оценивания**	**Шкала оценивания**
УК-1	Пороговый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** методики поиска, сбора и обработки информации, метод системного анализа ***Уметь:*** применять методики поиска, сбора, обработки информации, системный подход для решения поставленных задач и осуществлять критический анализ и синтез информации, полученной из актуальных	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	41-60 баллов

			российских и зарубежных источников		
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** методики поиска, сбора и обработки информации, метод системного анализа ***Уметь:*** применять методики поиска, сбора, обработки информации, системный подход для решения поставленных задач и осуществлять критический анализ и синтез информации, полученной из актуальных российских и зарубежных источников ***Владеть:*** методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач.	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	61-100 баллов
СПК- 2	Пороговый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** правоприменительную практику в целях решения профессиональных задач ***Уметь*:** понимать значимость и сущность правосудия, различает виды	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	41-60 баллов

			судопроизводства, сущность контрольно-надзорной деятельности, систему соответствующих органов, различает виды контрольно-надзорных полномочий и правоприменительных актов		
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** методику анализа правоприменительной практики в целях решения профессиональных задач ***Уметь:*** понимать значимость и сущность правосудия, различать виды судопроизводства; сущность контрольно-надзорной деятельности, систему соответствующих органов, различать виды контрольно-надзорных полномочий и правоприменительных актов; ***Владеть***: спецификой правоприменения в системе государственной и муниципальной службы	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	61-100 баллов

СПК-3	Пороговый	1. Работа на учебных занятиях 2. Самостоятельная работа	***Знать:*** возможности принятия профессиональных решений в пределах своих полномочий, совершать иные действия, связанные с реализацией правовых норм	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	41-60 баллов
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	***Знать:*** возможности принятия профессиональных решений в пределах своих полномочий, совершать иные действия, связанные с реализацией правовых норм ***Уметь:*** выявлять источники информации, системно их анализировать в целях принятия профессиональных решений ***Владеть:*** способностью обосновывать принимаемые решения в пределах должностных обязанностей	Текущий контроль: опрос, тест Промежуточная аттестация: зачет	61-100 баллов

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к опросу

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности.
4. Место информационной безопасности в системе национальной безопасности.

5. Интересы личности в информационной сфере.
6. Интересы общества в информационной сфере.
7. Интересы государства в информационной сфере.
8. Угрозы информационному обеспечению государственной политики Российской Федерации.
9. Виды угроз информационной безопасности.
10. Внешние источники угроз информационной безопасности.
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны.
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации,
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. Криптографические методы защиты информации

Тесты для проведения текущего контроля и промежуточной аттестации по итогамосвоения дисциплины «Информационная безопасность».

1) **К правовым методам, обеспечивающим информационную безопасность,относятся:**
- разработка аппаратных средств обеспечения правовых данных
- разработка и установка во всех компьютерных правовых сетях журналов учета действий
- разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) **Основными источниками угроз информационной безопасности являются все указанное в списке:**
- хищение жестких дисков, подключение к сети, инсайдерство
- перехват данных, хищение данных, изменение архитектуры системы
- хищение данных, подкуп системных администраторов, нарушение регламентаработы

3) Виды информационной безопасности:
- персональная, корпоративная, государственная
- клиентская, серверная, сетевая
- локальная, глобальная, смешанная

4) **Цели информационной безопасности – своевременное обнаружение, предупреждение:**
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- компьютерные сети, базы данных
- информационные системы, психологическое состояние пользователей
- бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- искажение, уменьшение объема, перекодировка информации
- техническое вмешательство, выведение из строя оборудования сети
- потеря, искажение, утечка информации

7) **К основным принципам обеспечения информационной безопасности относится:**
- экономической эффективности системы безопасности
- многоплатформенной реализации системы
- усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных

9) **К основным функциям системы безопасности можно отнести все перечисленное:**
- установление регламента, аудит системы, выявление рисков
- установка новых офисных приложений, смена хостинг-компании
- внедрение аутентификации, проверки контактных данных пользователей

10) **Принципом информационной безопасности является принцип недопущения:**
- неоправданных ограничений при работе в сети (системе)
- рисков безопасности сети, системы
- презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- невозможности миновать защитные средства сети (системы)
- усиления основного звена сети, системы
- полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
- усиления защищенности самого незащищенного звена сети (системы)
- перехода в безопасное состояние работы сети, системы
- полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

- разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- одноуровневой защиты сети, системы
- совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- компьютерный сбой
- логические закладки («мины»)
- аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
- прочитать приложение, если оно не содержит ничего ценного – удалить
- сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа означает:
- секретность ключа определена секретностью открытого сообщения
- секретность информации определена скоростью передачи данных
- секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- электронно-цифровой преобразователь
- электронно-цифровая подпись
- электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- покупка нелицензионного ПО
- ошибки эксплуатации и неумышленного изменения режима работы системы
- сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- распределенный доступ клиент, отказ оборудования
-моральный износ сети, инсайдерство
- сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- слабый трафик, информационный обман, вирусы в интернет
- вирусы в сети, логические мины (закладки), информационный перехват
- компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
- потерей данных в системе
- изменением формы информации
- изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- целостность
- доступность
- актуальность

23) Угроза информационной системе (компьютерной сети) – это:
- вероятное событие
- детерминированное (всегда определенное) событие
- событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- регламентированной
- правовой
- защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- программные, технические, организационные, технологические
- серверные, клиентские, спутниковые, наземные
- личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютернойсети несет:
- владелец сети
- администратор сети
- пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- руководств, требований обеспечения необходимого уровня безопасности
- инструкций, алгоритмов поведения пользователя в сети
- норм информационного права, соблюдаемых в сети

28) Наиболее важным при реализации защитных мер политики безопасностиявляется:
- аудит, анализ затрат на проведение защитных мер
- аудит, анализ безопасности
- аудит, анализ уязвимостей, риск-ситуаций

Вопросы к зачету.

31. Понятие национальной безопасности.
32. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
33. Определение информационной безопасности.
34. Место информационной безопасности в системе национальной безопасности.

35. Интересы личности в информационной сфере.
36. Интересы общества в информационной сфере.
37. Интересы государства в информационной сфере.
38. Угрозы информационному обеспечению государственной политики РоссийскойФедерации.
39. Виды угроз информационной безопасности.
40. Внешние источники угроз информационной безопасности.
41. Внутренние источники угроз информационной безопасности государства.
42. Информационное оружие, его классификация и возможности.
43. Доктрина информационной войны.
44. Методы и средства ведения информационной войны
45. Понятие информационного противоборства
46. Причины искажения информации,
47. Виды искажения информации
48. Каналы утечки информации
49. Естественные и искусственные каналы утечки информации
50. Правовые, организационно-технические и экономические методы обеспеченияинформационной безопасности.
51. Критерии и классы защищенности средств ВТ
52. Компьютерная система как объект информационной безопасности.
53. Информационные процессы как объект информационной безопасности
54. Влияние человеческого фактора на обеспечение информационной безопасности
55. Программно-аппаратные средства обеспечения информационной безопасности.
56. Классификация программно-аппаратных средств обеспечения информационнойбезопасности
57. Защита от несанкционированного доступа
58. Антивирусная защита
59. Межсетевые экраны
60. Криптографические методы защиты информации

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

В ходе преподавания дисциплины «Информационная безопасность» используютсяследующие *оценочные средства:*

Вид работы	**Кол-во баллов (максимальное значение)**
Опрос	до 40 баллов
Тест	до 40 баллов
зачет	до 20 баллов

Шкала оценивания опроса и собеседования

Уровень оценивания	Критерии оценивания	Баллы
Опрос и собеседование	Свободное владение материалом	40
	Достаточное усвоение материала	39-20
	Поверхностное усвоение материала	19-10
	Неудовлетворительное усвоение материала	9-1

Шкала оценивания тестового задания

Уровень оценивания	Критерии оценивания	Баллы
Тестирование	89-70 правильных ответа	40
	71-40 правильных ответа	39-20
	41-20 правильных ответа	19-10
	менее 12 правильных	9-1

Описание шкалы оценивания зачета

Шкала оценивания зачета

Уровень оценивания	Критерий оценивания	Баллы /конвертируемые баллы	Оценка
Зачет	**Полный и правильный ответ на теоретический вопрос.** Глубокое и прочное усвоение знаний программного материала (умение выделять главное, существенное); исчерпывающее, последовательное, грамотное и логически стройное изложение; правильность формулировки понятий; знание источников и авторов-исследователей по данной проблеме; умение сделать вывод по излагаемому материалу.	81-100 /8-10	Зачтено
	Теоретический вопрос изложен достаточно. Достаточно полное знание программного материала; грамотное изложение материала по существу; отсутствие не существенных неточностей в формулировке понятий; умение сделать вывод. Допускается недостаточно последовательное и логическое изложение материала.	61-80 /5-7	
	Теоретический вопрос изложен неполно. Общие знания основного материала без усвоения некоторых существенных положений; формулировка основных понятий, но – с некоторой неточностью; отсутствие знаний	41-60 /2-4	

	гражданско-правовых источников и авторов-исследователей по данной проблеме.		
	Теоретический вопрос изложен плохо или с грубыми ошибками. Незнание значительной части программного материала; существенные ошибки в процессе изложения; неумение выделить существенное и сделать выводы; незнание или ошибочные определения понятий.	0-40 /0-1	Не зачтено

Перевод баллов в шкалу оценок представлен в таблице.

Количество баллов	**Зачет**
81–100	Зачтено
61–80	
41–60	
0–40	Не зачтено