

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ**

Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых
объектов КИИ

Код модуля
1156040(1)

Модуль
Гуманитарные аспекты информационной
безопасности

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Каннер Татьяна Михайловна		старший преподаватель	МФТИ
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр "Информационная безопасность"
3	Челноков Владислав Валерьевич	кандидат юридических наук, доцент	Доцент	Учебно-научный центр "Информационная безопасность"

Согласовано:

Управление образовательных программ

Т.Г. Комарова

Авторы:

- Каннер Татьяна Михайловна, старший преподаватель, МФТИ
- Пономарева Ольга Алексеевна, Доцент,
- Челноков Владислав Валерьевич, Доцент,

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ

1.	Объем дисциплины в зачетных единицах	3	
2.	Виды аудиторных занятий	Лекции Практические/семинарские занятия	
3.	Промежуточная аттестация	Зачет	
4.	Текущая аттестация	Контрольная работа	1
		Реферат	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Правовые аспекты информационной безопасности ИСПДн, ГИС и значимых объектов КИИ

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	Планируемые результаты обучения (индикаторы)	Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине
1	2	3
УК-1 -Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	З-1 - Определять принципы критического мышления, методов анализа и оценки информации П-1 - Выявлять и анализировать проблемную ситуацию, выделяя ее структурные составляющие и связи между ними У-1 - Осмысливать явления окружающего мира во взаимосвязи, целостности и развитии, выстраивать логические связи между элементами системы	Зачет Контрольная работа Лекции Практические/семинарские занятия Реферат

<p>ОПК-1 -Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание</p>	<p>З-1 - Понимать основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности З-3 - Понимать методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и оценки надёжности У-2 - Формировать актуальную модель угроз для АИС и учитывать её положения при формировании требований ТЗ на проектируемую систему обеспечения ИБ</p>	<p>Зачет Контрольная работа Лекции Практические/семинарские занятия Реферат</p>
---	--	---

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

<p>1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5</p>		
<p>Текущая аттестация на лекциях</p>	<p>Сроки – семестр, учебная неделя</p>	<p>Максимальная оценка в баллах</p>
<p><i>контрольная работа</i></p>	<p>2,4</p>	<p>100</p>
<p>Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5</p>		
<p>Промежуточная аттестация по лекциям – зачет</p>		
<p>Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5</p>		
<p>2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.5</p>		
<p>Текущая аттестация на практических/семинарских занятиях</p>	<p>Сроки – семестр, учебная неделя</p>	<p>Максимальная оценка в баллах</p>
<p><i>реферат</i></p>	<p>2,12</p>	<p>100</p>
<p>Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1</p>		
<p>Промежуточная аттестация по практическим/семинарским занятиям–нет</p>		
<p>Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено</p>		
<p>3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено</p>		

Текущая аттестация на лабораторных занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет		
Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет		
Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для

	продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Понятие информационного права. Право на информацию.
2. Теоретические и методологические вопросы организационного и правового обеспечения информационной безопасности
3. Правовые режимы обеспечения безопасности информации ограниченного доступа
4. Персональные данные.
5. Актуальные проблемы правового и организационного обеспечения информационной безопасности.
6. Защита прав на результаты интеллектуальной деятельности. Институты права собственности и исключительных прав субъектов в информационной сфере.
7. Юридическая ответственность за правонарушения в информационной сфере

Примерные задания

1. Изучить материал по теме практического занятия
 2. Структурировать материал
 3. Сформулировать вопросы по теме практического задания
- LMS-платформа – не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Правовые аспекты информационной безопасности

Примерные задания

- 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 регламента работы
- 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 относятся:
- + 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, фаерволлы

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

5) 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

LMS-платформа – не предусмотрена

5.2.2. Реферат

Примерный перечень тем

1. Понятие правового режима информации и его разновидности
2. Информационная политика государства
3. Сущность права на информационную безопасность и его гарантии
4. Система законодательства об информационной безопасности
5. Понятие и правовая природа информационного общества
6. Обеспечение информационной безопасности личности
7. Обеспечение информационной безопасности государства
8. Объективная и субъективная стороны информационной безопасности
9. Правоотношения в сфере информационной безопасности (понятие, виды, элементы).

Примерные задания

1. Выбрать тему из перечисленных.
2. Подобрать соответствующие источники информации и литературу.
3. Структурировать изученный материал по теме реферата.
4. Оформить тест реферата по требованиям ГОСТа или предложенному преподавателем шаблону.

5. Подготовить доклад на 5-7 минут по теме реферата.

LMS-платформа – не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Зачет

Список примерных вопросов

1. Понятие информационного права.
2. Содержание права граждан на информацию.
3. Информационная безопасность в системе национальной безопасности Российской Федерации.
4. Правовые режимы тайн в системе организационного и правового обеспечения безопасности информации ограниченного доступа.
5. Правовой режим защиты государственной тайны.
6. Правовой режим коммерческой тайны
7. Ноу-хау как особый объект интеллектуальных прав.
8. Регулирование вопросов персональных данных в Европейском Союзе
9. Регулирование вопросов персональных данных в Российской Федерации
10. Противодействие экстремистской деятельности в информационной сфере.
11. Защита детей от информации, причиняющей вред их здоровью и развитию.
12. Правовое регулирование средств массовых коммуникаций.
13. Общие положения об интеллектуальных правах на результаты интеллектуальной деятельности.

14. Общие положения авторского права.
 15. Общие положения патентного права
 16. Режим служебных результатов интеллектуальной деятельности.
 17. Понятие и виды юридической ответственности в области обеспечения информационной безопасности.
- LMS-платформа – не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направления воспитательной деятельности сопрягаются со всеми результатами обучения компетенций по образовательной программе, их освоение обеспечивается содержанием всех дисциплин модулей.