Федеральное государственное бюджетное образовательное учреждение
высшего образования

РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА и ГОСУДАРСТВЕННОЙ СЛУЖБЫ
при ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ

«Факультет таможенного администрирования и безопасности»

Утвержден
решением учебно-методической
комиссии по специальности
Правовое обеспечение
национальной безопасности

Протокол № 1

от «31» августа 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Б1.В.03.05 Правовое обеспечение информационной безопасности

УРвТД

40.05.01 «Правовое обеспечение национальной безопасности»

Государственно-правовая специализация

Квалификация: юрист

Формы обучения: очная/заочная

Год набора - 2021

Автор–составитель:
старший преподаватель кафедры таможенного администрирования М. Е. Рахконен

Заведующий кафедрой
экономической безопасности, к.э.н., доцент Т. Н. Тарасова

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Код индикатора достижения	Наименование индикатора достижения
ПКр ОС-1	Способность обеспечивать безопасность личности, общества, государства правовыми средствами	ПКр ОС-1.2	Принимает правовые меры по нейтрализации угроз безопасности личности, общества, государства

2. Оценочные средства по дисциплине

2.1 Текущий контроль

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению
Вопросы для устного опроса:

1. Понятие ИБ и информационного общества.
2. Цели, задачи и принципы обеспечения ИБ.
3. Угроза национальной безопасности и их виды.
4. Информационные войны и информационное оружие.
5. Информационный терроризм.
6. Информационное общество в РФ и его характеристики.
7. Информационная сфера и ее области.
8. Национальные интересы России в информационной сфере.
9. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тест:

1. Виды информационной безопасности

а. Персональная, корпоративная, государственная
б. Клиентская, серверная, сетевая
в. Локальная, глобальная, смешанная

2. К основными рискам в сфере информационной безопасности относятся

а. Искажение, уменьшение объема, перекодировка информации
б. Техническое вмешательство, выведение из строя оборудования сети
в. Потеря, искажение, утечка информации

3. Основными субъектами информационной безопасности являются

а. Руководители, менеджеры, администраторы компаний
б. Органы права, государства, бизнеса
в. Сетевые базы данных

4. Данные независимо от формы их представления

а. Информация
б. Информационные технологии
в. Информационная система

5. Действия, направленные на получение/передачу информации

а. Распространение информации
б. Предоставление информации
в. Доступ к информации

6. Основными рисками информационной безопасности являются

а. Искажение, уменьшение объема, перекодировка информации
б. Техническое вмешательство, выведение из строя оборудования сети
в. Потеря, искажение, утечка информации

7. Защита информации - это

а. Компьютерная программа для выполнения определенной задачи
б. Комплекс мероприятий, направленных на обеспечение информационной безопасности
в. Кодирование информации

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

.

***Вопросы для устного опроса**:*

1. Понятие правового обеспечения и правовой защиты
2. Международно-правовые нормы и стандарты в сфере информационной безопасности
3. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения информационной безопасности
4. Предмет и метод правового регулирования в сфере информационной безопасности страны
5. Основные правовые документы, регулирующие информационную безопасность РФ
6. Правовое регулирование деятельности средств массовой информации
7. Особенности стандартизации нормативной базы в сфере ИБ в современном мире
8. Основные тенденции развития законодательства РФ в сфере информационной безопасности

Тема 3. Информация как объект правового регулирования и защиты.

***Вопросы для устного опроса**:*

1. Информация, ее виды и признаки
2. Информация как объект юридической защиты
3. Информационные ресурсы
4. Виды и источники информации, подлежащие защите.
5. Правовой режим защиты государственной тайны.
6. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты.
7. Конфиденциальная информация и возможные каналы ее утечки
8. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития

Тесты

1. **К субъектам информационной системы не относится** …

а. Владелец;
б. Пользователь;
в. Собственник
г. Все перечисленные

2. Несанкционированный доступ – это …

а. Доступ или воздействие с нарушением правил доступа;
б. Изменение пароля с правами администратора;
в. Изменение пароля доступа в систему пользователем.

3. Что не относится к непреднамеренным воздействиям?

а. Сбой технических средств;
б. **Сбой программных средств**;
в. Внедрение вируса в автоматическом режиме.

4. Что не является характеристикой информации?

а. Статичность;
б. Время отклика;
в. Стоимость создания.

.

5. Время жизни информации – это …

а. **Время, пока информация хранится в информационной системе**;
б. Время, пока информация актуальна;
в. Время, пока стоимость создания информации выше стоимость потери.

6. Как называется информация, к которой ограничен доступ?

а. Конфиденциальная
б. Противозаконная
в. Открытая

7. Основной документ, на основе которого проводится политика информационной безопасности?

а. Программа информационной безопасности
б. Регламент информационной безопасности
в. Протекторат

8. **Принципы GDPR**

а. Ограничение хранения
б. Управление данными.
в. Передача данных третьим лицам

9. Возможно ли использование данных после изменения цели

а. Да
б. Нет
в. В случае особых ситуаций возможно

10. Альянс по безопасности сети Интернет создан в

а. 2001 году

б. 2014 году

в. 2016 году

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Вопросы для устного опроса:

1. Понятие государственного управления в сфере обеспечения ИБ.
2. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности.
3. ***Межведомственные и государственные комиссии по аспектам обеспечения информационной безопасности***
4. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации.
5. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами.
6. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус

Тест:

1. **Основные предметные направления Защиты Информации*?***

а. Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности

б. Охрана золотого фонда страны

в. Определение ценности информации

2. Что можно отнести к правовым мерам ИБ?

а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

б. Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра

в. Охрану вычислительного центра, установку сигнализации и многое другое

3. **Что можно отнести к техническим мерам ИБ*?***

а. Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

б. Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое

в. В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

4. Какие методы реализуют контроль соблюдения установленного порядка к защищаемой информации?

а. Правовые;
б. Административные;
в. Технические;
г. Все перечисленные

5. К правовым методам обеспечения информационной безопасности не относят

а. Определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;
б. Определение ответственности физических и юридических лиц за несанкционированный доступ к информации;
в. Определение ответственности физических и юридических лиц

6. **Какой документ представляет собой совокупность взглядов на цели, задачи и принципы и основные направления обеспечения информационной безопасности Российской Федерации**:

а. Конституция Российской Федерации;
б. Доктрина информационной безопасности Российской Федерации;
в. Федеральный закон "Об информации, информатизации и защите информации".

7. К какому уровню правового обеспечения информационной безопасности относятся Постановления Правительства Российской Федерации

а. 2
б. 3
в. 4

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика

Вопросы для устного опроса:

1. Понятие и виды преступности в информационной сфере.
2. Основные этапы и тенденции развития компьютерной преступности в России
3. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации
4. Служба Специальной связи и информации Федеральной службы охраны РФ
5. Неформальная модель нарушителя
6. Классификация нарушителей

Тест:

1. **Какая система идентификации по биометрическим показателям является наиболее распространённой**?

а. По отпечаткам пальцев;
б. По сетчатке глаза;
в. По клавиатурному почерку.

2. **Что понимается под информационной безопасностью**:

а. Защита душевного здоровья телезрителей
б. Защита от нанесения неприемлемого ущерба субъектам информационных отношений
в. Обеспечение информационной независимости России

3. **Большинство людей не совершают противоправных действий потому, что это**:
а. осуждается и/или наказывается обществом
б. технически невозможно
в. сулит одни убытки

4. Криптография – это...?
а. **Наука о шифровании (преобразовании) информации**;
б. Наука о вирусах;
в. Наука об информационных войнах.

5. Лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом и использующее для этого различные возможности и средства называется
а. Нарушитель
б. Злоумышленник
в. Непрофессионал

6. По отношению к системе всех нарушителей делят на следующие группы
а. Внутренние
б. Внешние
в. Посторонние лица

7. Специфика баз данных, с точки зрения их уязвимости, связана в основном с наличием
а. Взаимодействия между самой базой данных и элементом системы,
б. Взаимодействия между самой базой данных и обслуживающим персоналом
в. Между двух (и более) заинтересованных субъектов

8. Компьютерный терроризм и экстремизм переходит в
а. Информационные войны
б. Коррупционные схемы
в. Фактор уязвимости

1. Компьютерная клевета относится к
а. Преступлениям против личности
б. Нарушению персональных данных
в. Преступлениям против общественного порядка

10. Различные неправомерные действия с компьютерной информацией, влекущие за собой угрозу жизни людей, общественной безопасности называется
а. Кибертерроризм.
б. Киберэкстремизм
в. Компьютерный шпионаж

Тема 6 Правовая защита личности в информационной сфере.

Вопросы для устного опроса

1. Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.

2. Конституционные гарантии правовой охраны прав личности в информационной сфере.
3. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни
4. Врачебная тайна как институт защиты интересов личности.
5. Защита права на личную информацию с ограниченным доступом.
6. Персональная тайна и ее виды.
7. Обработка и правовая охрана персональных данных.
8. Правовая база обеспечения защиты личности от воздействия «вредной» информации.
9. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации

Тест

1. **Информация, составляющая профессиональную тайну, может предоставлена третьим лицам в соответствии**:

а. **С федеральными законами и (или) по решению суда;** □
б. С федеральными законами; □
в. По решению суда.

2. **Что такое конфиденциальность информации**:

а. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
б. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без законодательно оформленного соглашения
в. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без росписи в журнале посетителей о полученной информации

3. Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются

а. **Запрещение разработки, распространения и применения "информационного оружия**”
б. Обеспечение безопасности международного информационного обмена
в. Обмен новыми технологиями в области информационного обеспечения

4. Что такое персональные данные?

а. Конфиденциальная информация;
б. **Информация для служебного пользования**;
в. Информация ограниченного распространения.

5. Что такое врачебная тайна

а. Любая информация, связанная с состоянием здоровья человека, которая становится известна медработнику, в том числе и сведения о самом факте обращения за медицинской помощью
б. Секреты, связанные со здоровьем пациента, обратившегося в медицинское учреждение

в. Информация, связанная с врачом

6. В каких случаях допускается разглашение врачебной тайны
а. С письменного согласия гражданина или его законного представителя
б. При угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
в. Все перечисленное

7. К угрозам информационной безопасности личности можно отнести:
а. Угрозы, которые связаны с развитием девиантного поведения личности;
б. Угрозы, связанные с вестернизацией сознания граждан; угрозы, связанные с дестабилизацией социальной преемственности поколений
в. Обострение международной конкуренции за обладание информационными технологиями и ресурсами

8. Передача ложной информации относится к
а. Манипуляционному воздействию
б. К инструменту принуждения
в. К ослаблению критического мышления

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.
Вопросы для устного опроса
1. Понятие государственной тайны и правового режима ее обеспечения.
2. Принципы и механизм отнесения сведений к государственной тайне (ГТ).
3. Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус.
4. Организационно-правовые меры защиты ГТ.
5. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией.
6. Система контроля за режимом обеспечения ГТ.

Тест

1. **Требованиями каких законов регулируется защита информации составляющей государственную тайну**:
а. Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;
б. Указом президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне»;
в. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «об информации, информационных технологиях и о защите информации»

2. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Секретно»:
а. первая
б. вторая;
в. **третья**.

3. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Сов. Секретно»:
а. первая;
б. **вторая**;

в. третья.

4. Сколько существует классов защищенности АС от несанкционированного доступа:

а. три
б. пять
в. семь
г. девять.

5. Что такое государственная тайна?

а. Конфиденциальная информация;
б. Информация для служебного пользования;
в. Информация ограниченного распространения.

6. Что такое источники права на доступ к информации?

а. **Правовая база РФ по безопасности информации**;
б. Форма допуска сотрудника;
в. Решение руководителя организации.

7. В каких случаях пользователю может быть отказано в предоставлении информации из государственных информационных ресурсов:

а. Пользователь – лицо без гражданства;
б. При непредставлении обоснования необходимости получения информации;
в. При наличии в запрашиваемой информации сведений ограниченного доступа

8. Допуск должностных лиц и граждан к государственной тайне предусматривает

а. Письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
б. Процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
в. Все перечисленное

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Вопросы для устного опроса

1. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий.
2. Компьютерные преступления и особенности их идентификации и предупреждения.
3. Правовые основы применения «электронной цифровой подписи» (ЭЦП).
4. Криптографическая защита информации (КЗИ).
5. Контроль за разработкой, производством и применением криптографических средств.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Вопросы для устного опроса

1. Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных права
2. Объекты и субъекты ПИС
3. Патентное право и патентные правоотношения

4. Государственная регистрация товарного знака
5. Программы для ЭВМ и механизм их правовой защиты

Тесты:

1. Что охраняется с помощью товарных знаков?
а. Произведения искусства
б. Логотипы, названия и бренды
в. Внешний вид, форма и восприятие продукта

2. **Какие объекты не охраняются законодательством Российской Федерации об интеллектуальной собственности?**
а. Топологии интегральных микросхем;
б. Защита от недобросовестной конкуренции;
в. Полезные модели;
г. Программы для ЭВМ.

3. **Какие из объектов авторского права могут быть по желанию автора зарегистрированы в Патентном ведомстве?**
а. **Программы для ЭВМ и базы данных**;
б. Аудиовизуальные произведения;
в. Фотографии.

4. Система институтов интеллектуальной собственности в настоящее время является подотраслью:
а. Конституционного права
б. Административного права
в. Гражданского права

5. Правоотношения в сфере интеллектуальной собственности основаны на принципах:
а. Соподчинения одних субъектов другим
б. Равенства, автономии воли и имущественной самостоятельности участников
в. Юридической зависимости друг от друга субъектов права на результаты интеллектуальной деятельности

6. **Виды результатов интеллектуальной деятельности ИТ-компании, регистрируемые в Роспатенте**:
а. Программа для ЭВМ или База данных
б. Алгоритмическая концепция или любой другой элемент ноу-хау;
в. Принципиальные схемы авторского информационного преобразования;
г. Все перечисленное

7. Обладатель исключительного права на созданную им базу данных:
а. Может зарегистрировать ее по своему желанию в Реестре баз данных;
б. Обязан зарегистрировать эту базу в федеральном исполнительном органе по интеллектуальной собственности;
в. Не может осуществить регистрацию базы, поскольку эта процедура законом не предусмотрена.

8. **К объектам патентных прав относятся**:
а. Промышленные образцы

б. Компьютерные программы научные теории и математические методы
в. Логотипы

Тема 10. Правовая защита коммерческой тайны (КТ).

Вопросы для устного опроса

1. Понятие КТ и ее правовой статус.
2. Объекты защиты КТ.
3. Промышленный шпионаж и его объекты.
4. Критерии определения секретности при определении режима КТ
5. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений
6. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений

Тесты:

1. Что предполагает гражданско-правовой способ защиты КТ

а. Увольнение за разглашение КТ
б. Лишение специального права
в. Арест

2. Какой уполномоченный орган рассматривает споры о нарушении прав на КТ

а. Арбитражный суд
б. Третейский суд
в. Суд

3. Что такое коммерческая тайна?

а. документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ
б. **информация, которую компания не разглашает, чтобы увеличить доходы, избежать неоправданных расходов, сохранить или улучшить своё положение на рынке либо получить любую другую коммерческую выгоду**
в. сведения о численности работников, о нарушении антимонопольного законодательства, о реализации продукции, причинившей вред здоровью населения

4. К внутренним нарушителям в информационной среде относится

а. Конкуренты
б. Хакеры
в. Любые лица, находящиеся внутри контролируемой территории

5. К коммерческой тайне могут относиться:

а. Учредительные документы, документы о платежеспособности, документы об уплате налогов;
б. **Сведения о деловых переговорах, содержание "ноу-хау", планы инвестиционной деятельности, рыночная стратегия**;
в. Сведения о численности работников, о нарушении антимонопольного законодательства, о реализации продукции, причинившей вред здоровью населения

6. **Коммерческой тайне не могут быть отнесены**:

а. Сведения о загрязнении окружающей среды

б. Сведения о наличии свободных мест
в. Сведения о численности работников

7. **Промышленный шпионаж это:**

а. Получение обманным путем конфиденциальной информации, используемой в различных противоправных целях
б. Информация маркетингового, финансового и технологического характера, составляющую коммерческую тайну
в. Разглашения конфиденциальной информации

8. **Конкурентная разведка это**

а. Незаконное (тайное или силовое) изъятие информации, которую руководство конкурирующих компаний хотело бы скрыть от посторонних
б. Получение легальными: аналитическими и/или исследовательскими методами из открытых источников информации о рынке, конкурентах, технологиях и разработках, которая необходима руководству компании для принятия правильных стратегических решений
в. Установка подслушивающей или сканирующей аппаратуры

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.
Вопросы для устного опроса

1. Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ
2. Виды деятельности, подлежащие лицензированию в сфере ИБ.
3. Система государственного лицензирования в сфере ИБ и ее функции.
4. Субъекты лицензирования в сфере ИБ и их правовой статус.
5. Цели создания системы ССЗИ
6. Объекты сертификационной деятельности и режимы сертификации
7. Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тест

1. Лицензированию подлежат
а. Образовательная деятельность
б. Продажа сигарет
в. Фармацевтическая деятельность
г. Все перечисленное

2. Лицензирующими органами являются
а. Независимые экспертные организации
б. Органы исполнительной власти
в. Налоговые инспекции

3. К планированию СОИБ относится
а. Область и границы действия СОИБ
б. Идентификация рисков
в. Цели и меры управления для обработки рисков

г. Все перечисленное

4. Этапы стадии создания систем защиты информации
а. Требования и критерии систем защиты информации
б. **Разработка систем защиты информации**
в. Покупка систем защиты информации

5. К основным принципам и целям построения систем защиты информации можно отнести
а. Принцип полноты защищаемой информации
б. Принцип создания штата разработчиков
в. Принцип своевременной оплаты сотрудников

6. Совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения *работ* или оказания услуг в области защиты информации это
а. ССЗИ
б. ГОСТы
в. Национальные стандарты

7. На какой стадии создания системы защиты информации АС создается частное техническое задание на СЗИ?
а. Стадия классификации АС
б. Предпроектная стадия
в. Стадия проектирования

8. На какой стадии создания системы защиты информации АС происходит аттестация объекта информатизации по требованиям безопасности информации?
а. Предпроектная стадия
б. Стадия проектирования
в. Стадия ввода в действие

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Вопросы для устного опроса

1. Информационная безопасность России и задачи по ее обеспечению
2. Уровневый подход
3. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ.
4. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус.

Тест

1. Что такое преступление?
а. Правонарушение
б. Общественно опасное противоправное деяние лица, за совершение которого подлежит наказанию в соответствии с УК РФ.
в. Психическое отношения лица к совершенному им деянию

а. Что такое компьютерная информация?
б. Это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

в. Это информация, зафиксированная в периодических изданиях
г. Это серия и номер паспорта

2. Кем совершаются преступления в сфере компьютерной информации?
а. ЭВМ
б. Компьютерной сетью Интернет
в. Человеком

3. К какой главе УК РФ относятся ст. 272, ст. 273, ст. 274 в области информационной безопасности?
а. 28
б. 36
в. 25
г. 27

4. Преступления в сфере информационных технологий
а. Распространение вредоносных программ
б. Взлом паролей
в. Все перечисленное

5. Фальсификация единого государственного реестра юридических лиц это
а. Преступления в сфере информационных технологий
б. Ошибка разработчика
в. Злоумышленное деяние

6. Расставьте по порядку этапы развития информационного общества:
а. Изобретение электричества
б. Изобретение книгопечатания
в. Изобретение микропроцессора
г. Изобретение письменности

7. Информатизация общества — это процесс:
а. Увеличения объема избыточной информации в социуме
б. Более полного использования накопленной информации во всех областях человеческой деятельности за счет широкого применения средств информационных и коммуникационных технологий
в. Повсеместного использования компьютеров

8. Что называется информационным обществом:
а. Историческая фаза развития общества, главными продуктами производства которого являются знания и информация
б. Историческая фаза развития общества, главными продуктами производства которого являются компьютерные технологии и робототехника
в. Историческая фаза развития общества, в котором 90% численности населения планеты используют в повседневной жизни информационные технологии

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

1. Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ.
2. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности

3. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России.
4. Составы административных правонарушений, посягающих на ИБ страны.

Тест

1. **Что является совокупностью официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности государства?**

а. Конституция Российской Федерации
б. Доктрина информационной безопасности Российской Федерации
в. Доктрина экономической безопасности Российской Федерации

2. **На каком принципе базируется ответственность в информационной** сфере?

а. Законность
б. Обоснованность
в. Справедливость
г. Все перечисленное верно

3. **Согласно Конституции РФ, определяются основные направления внутренней политики государства?**

а. Федеральным собранием
б. Правительством РФ
в. Президентом РФ
г. Государственной Думой РФ

4. **Административно-правовая ответственность за правонарушения в информационной сфере носит**

а. Публичный характер
б. Частный характер
в. Публично-частный характер

5. **Какой характер носит уголовная ответственность за правонарушения в информационной сфере?**

а. Личный характер
б. Групповой характер
в. Может носить и личный и коллективный характер

6. **Кража персональных данных (пароля, логина) с целью похищения средств с банковской карты называется**

а. Фишинг
б. «Нигерийские письма»
в. Махинации с интернет-кошельками

7. **Что являлось предметом регулирования Федерального закона "Об информации, информатизации и защите информации":**

а. Документированная информация;
б. **Конфиденциальные информационные отношения**;
в. Служебная тайна;

Дискуссия.

Основной целью проведения «дискуссии» является выработка у студентов профессиональных умений излагать мысли, аргументировать свои соображения, обосновывать предлагаемые решения и отстаивать свои убеждения.
Построение дискуссии:

- Выдвижение одной-двух проблемных ситуаций по заданной теме
- Формулируется вопросы, обсуждение которых позволят более подробно рассмотреть с разных сторон проблемную ситуацию
- Вопросы распределяются по подгруппам для более тщательной проработки
- Определяется очередность выступающих
- Разные точки зрения фиксируются на информационных носителях
- Устанавливаются временные отрезки на уточняющие вопросы
- Приведение к семантическому однообразию
- Устанавливаются правила этики коммуникационного процесса

Пример:
Тема для дискуссии:

1. Проблемы реализации информационных правоотношений в Интернете.
2. Правовое обеспечение информационной безопасности в сфере Интернета.
3. Интеллектуальная собственность как институт информационного права
4. Персональные данные как особый институт охраны прав на неприкосновенность частной жизни. Ограничения информационной сферы налогового контроля.
5. Обеспечение права на информацию налогоплательщика.
6. Классификация угроз информационной безопасности.
7. Кадровое обеспечение организации в области информационной безопасности.
8. Особенности внутриобъектового режима.
9. Особенности пропускного режима
10. Аудит подсистемы защиты информации

2.2 Промежуточная аттестация

Практические задачи
Тема 1. 2. Составить словарь терминов по теме Правовое Информационная безопасность (ИБ) РФ
Студенты должны представить по 5-7 терминов, с раскрытием смысла и частотой употребления.
Тема 3.4
Составить таблицу классификации информационных носителей. Способ эксплуатации.
Тема 5.6.
Составить таблицу по статистическим данным совершенных преступлений в информационной сфере за 5 лет. Дать характеристику, связанную с изменением и расширением фактов нарушения.
Тема 9. Составит список объектов интеллектуальной собственности, в отношении которых происходят правонарушения. Выписать способы, которыми совершаются данные правонарушения.
Тема 10.11. Создать модель системы по обеспечению сохранности персональных данных.

2.2.2. Вопросы для подготовки к зачету

1. Понятие ИБ и информационного общества.

2. Цели, задачи и принципы обеспечения ИБ.
3. Угроза национальной безопасности и их виды.
4. Информационные войны и информационное оружие.
5. Информационный терроризм.
6. Информационное общество в РФ и его характеристики.
7. Информационная сфера и ее области.
8. Национальные интересы России в информационной сфере.
9. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.
10. Причины и условия преступлений в сфере компьютерной информации в современных условиях.
11. Характеристика личности преступника в сфере компьютерной информации.
12. Основы предупреждения преступлений в сфере компьютерной информации.
13. Правовое регулирование борьбы с преступлениями в сфере компьютерной информации.
14. Понятие преступления в сфере компьютерной информации.
15. Классификация преступлений, совершаемых с использованием
16. компьютерных технологий.
17. Особенности объекта и предмета преступлений в сфере компьютерной информации
18. Проблемы квалификации преступлений в сфере компьютерной
19. информации.
20. Место совершения преступлений как признак преступлений в сфере компьютерной информации.
21. Общая характеристика международного законодательства в сфере борьбы с киберпреступностью.
22. Основные направления международного сотрудничества в борьбе
23. с киберпреступностью
24. сфере ИБ
25. Виды деятельности, подлежащие лицензированию в сфере ИБ.
26. Система государственного лицензирования в сфере ИБ и ее функции.
27. Субъекты лицензирования в сфере ИБ и их правовой статус.
28. Цели создания системы ССЗИ
29. Объекты сертификационной деятельности и режимы сертификации
30. Юридическая ответственность за нарушением правил лицензирования и сертификации
31. Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере.
32. Конституционные гарантии правовой охраны прав личности в информационной сфере.
33. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни.
34. Правовой механизм защиты права на неприкосновенность частной жизни
35. Врачебная тайна как институт защиты интересов личности.
36. Защита права на личную информацию с ограниченным доступом.
37. Персональная тайна и ее виды.
38. Обработка и правовая охрана персональных данных.
39. Правовая база обеспечения защиты личности от воздействия «вредной» информации.
40. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации
41. Организационно-управленческие меры обеспечения защиты информации в сфере
42. высоких технологий.
43. Компьютерные преступления и особенности их идентификации и предупреждения.

44. Правовые основы применения «электронной цифровой подписи» (ЭЦП).
45. Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств.
46. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.
47. Понятие интеллектуальной собственности и ее правовой статус.
48. Законодательство РФ об авторских и смежных правах.
49. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС.
50. Правовой механизм обеспечения защиты авторских и смежных прав.
51. Государственная регистрация ПИС.
52. Особенности правовой защиты программ для электронных вычислительных машин и баз данных.
53. Патентное право и патентные правоотношения. Правовой статус участников.
54. Сфера действия патентного законодательства.
55. Показатели и условия патентоспособности.

3. Описание системы оценивания, шкала оценивания

3.1 Показатели и критерии оценивания для текущего контроля.

Оценочные средства (формы текущего и промежуточного контроля)	Показатели оценки Критерии оценки
Доклад	Соблюдение регламента (15 мин.); характер источников (более трех источников); подача материала (презентация); ответы на вопросы (владение материалом). Каждый критерий оценки доклада оценивается в 0,25 балла, максимум 1 балл за доклад. Допускается не более одного доклада в семестр, десяти докладов в год (всего до 10 баллов)
Тестирование	Процент правильных ответов на вопросы теста Менее 60% – 0 баллов; 61 - 75% – 6 баллов; 76 - 90% – 8 баллов; 91 - 100% – 10 баллов.
Устный опрос	Корректность и полнота ответов Сложный вопрос: полный, развернутый, обоснованный ответ – 10 баллов Правильный, но не аргументированный ответ – 5 баллов Неверный ответ – 0 баллов Обычный вопрос: полный, развернутый, обоснованный ответ – 4 балла Правильный, но не аргументированный ответ – 2 балла Неверный ответ – 0 баллов. Простой вопрос: Правильный ответ – 1 балл; Неправильный ответ – 0 баллов
Выполнение проблемных заданий	Правильность решения; корректность выводов обоснованность решений баллы начисляются от 1 до 3 в зависимости от сложности задачи/вопроса (не более 38 баллов за семестр)

3.2 Показатели и критерии оценивания для промежуточного контроля

Компонент компетенции (с указанием кода)	**Индикаторы достижения компетенций**	**Критерии оценивания (в баллах для специалитета, в оценках)**
ПКр ОС-1 Способность Принимать правовые меры по нейтрализации угроз безопасности личности, общества, государства	Принимает правовые меры по нейтрализации угроз безопасности личности, общества, государства	В соответствии с балльно-рейтинговой системой на промежуточную аттестацию отводится 30 баллов. Зачет проводится по тестам. Менее 60% – 0 баллов; 61 - 75% – 10 баллов; 76 - 90% – 20 баллов; 91 - 100% – 30 баллов.

Шкала перевода оценки из многобалльной в систему «зачтено»/«не зачтено»:

от 0 по 50 баллов	«не зачтено»
от 51 по 100 баллов	«зачтено»