Приложение 1

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
Кафедра безопасности

Утверждены
решением учебно-методической
комиссии по специальности
40.05.01 Правовое обеспечение
национальной безопасности

Протокол № 1

от «31» августа 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Б1.В.03.05 Правовое обеспечение информационной безопасности

УРвТД

Гражданско-правовая
Специализация

40.05.01 «Правовое обеспечение национальной безопасности»

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
2. Оценочные средства по дисциплине

   2.1 Текущий контроль

   2.2 Промежуточная аттестация
3. Описание системы оценивания, шкала оценивания.

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	Обеспечивает безопасность личности, общества, государства правовыми средствами;

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.

Темы докладов:

1. Предметная область теории информационной безопасности
2. Базовые термины в теории защиты информации.
3. Основные термины и определения правовых понятий в области информационных отношений и защиты информации
4. Основные понятия в области защиты информации
5. Что относится к целям защиты информации и что такое эффективность защиты информации
6. Информационный терроризм. Динамика изменения данного явления в мире.
7. Основные технические угрозы. Промышленный шпионаж.
8. Влияние низкой квалификации пользователей на информационную безопасность
9. Меры по обеспечению информационной безопасности

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

Темы докладов:

1. Международный пакт о гражданских и политических правах
2. Федеральный закон «Об информации, информационных технологиях и о защите информации (2006) Основные положения.
3. Указ президента Российской Федерации №250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"
4. Национальные интересы в сфере информационной безопасности
5. Формирования государственной политики в области обеспечения информационной безопасности РФ
6. Что такое доктрина информационной безопасности
7. Основные функции государственной системы обеспечения информационной безопасности РФ
8. Основные функции стандартов в области 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

Темы докладов:

1. Информация как объект познания.
2. Роль человека по отношению к информации.
3. Вещественные информационные носители. Способы защиты данного объекта.
4. Основные способы защиты информации на энергетическом носителе.
5. Информация как объект познания и объект защиты
6. Жизненный цикл информации
7. Классификация информационных ресурсов
8. Предметные сферы тайны, как вида ограниченного доступа
9. Формирование состава информации ограниченного доступа. Документы ограниченного доступа.
10. Юридические нормы правового режима информационных ресурсов.

Тесты

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

а. Владелец;

б. Пользователь;

в. Собственник

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. 2012 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

Темы докладов:

1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации
2. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи
3. Структура государственной системы защиты информации
4. Ведомства, регулирующие отношения в области защиты информации
5. ФСТЭК как основной орган управления государственной системы защиты информации
6. Роль различных министерств и ведомств в вопросах защиты информации
7. Основные цели защиты информации
8. Обеспечение информационной безопасности в системе основных функций государства
9. Федеральные органы исполнительной власти в обеспечении информационной безопасности
10. Компетенция органов государственной власти в области обеспечения информационной безопасности

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

Темы докладов:

1. Понятие «информационная преступность». Основные отличия от «компьютерной преступности»
2. Основные группы информационных преступлений
3. Нормативно-правовые документы, регулирующие неправомерный доступ и распространение охраняемой законом информации
4. Нормативно-правовые документы, регулирующие неправомерное сокрытие информации
5. Нормативно-правовые документы, регулирующие неправомерное использование информации, полученной законным путем
6. Экономические киберпреступления
7. «Темная сеть» и преступления против общественной безопасности
8. Киберэкстремизм

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

9. **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

8. Передача ложной информации относится к

а. Манипуляционному воздействию
б. К инструменту принуждения
в. К ослаблению критического мышления

Темы докладов:

1. Регулирование телемедицинских технологий
2. Окинавская Хартия глобального информационного общества
3. Информационные права и свободы личности, закрепляемые в Конституции РФ
4. Профессиональная тайна: признаки и виды, выделяемые законодательством
5. Защита права на личную информацию с ограниченным доступом
6. Политика обработки персональных данных
7. Понятие и виды персональных данных
8. Основные положения о защите неприкосвенности частной жизни (ОЭСР)
9. Обязанности оператора по обеспечению безопасности персональных данных

10. Федеральный закон от 29 декабря 2010 г. N436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

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

Темы докладов:

1. Понятие и признаки государственной тайны
2. Порядок определения размеров ущерба, нанесенного раскрытием государственной тайны
3. Основные нормативно-правовые документы, регулирующие информационные отношения по защите государственной тайны
4. Кластер, входящие в понятие государственная тайна
5. Засекречивание сведений, относящихся к государственной тайне
6. Носители сведений, составляющих государственную тайну
7. Органы государственной власти, наделенные полномочиями по отнесению к государственной тайне
8. Межведомственные комиссии по защите государственной тайны
9. Ответственность за нарушение законодательства о государственной тайны

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.

Темы для докладов:

1. Электронно-цифровая подпись.
2. Основные алгоритмы шифрования данных: ГОСТ.
3. Защита данных в автономном компьютере.
4. Правовая охрана программ для электронных вычислительных машин и баз данных
5. Правовая охрана программ для электронных вычислительных машин и баз данных
6. Обзор и классификация методов шифрования информации

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

Темы докладов:

1. Классификация объектов интеллектуальной собственности
2. Система международной объектов объектов промышленной собственности
3. Объекты авторского права
4. ИС научно-технической сферы
5. Требования единства по российскому законодательству группы изобретений
6. Базовые международные договоры в сфере ИС
7. Основные способы защиты интеллектуальных прав
8. Патентное право. Понятие «Автор». Патентообладатель

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. Любые объекты;
г. 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;

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

Темы докладов
Признаки информации, составляющие коммерческую тайну
1. Содержание мер по охране конфиденциальности информации
2. Права и обязанности обладателя информации, составляющей КТ
3. Нормативно-правовая основа регулирующая ответственность за нарушение КТ
4. Источники права о коммерческой тайне.
5. Порядок установления режима коммерческой тайны
6. Уровни промышленного шпионажа, его объекты и субъекты, силы и средства, формы и методы деятельности
7. Современные возможности проведения операций промышленного шпионажа.
8. Принципы взаимодействия государства и национального бизнеса в области похищения промышленных секретов.

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 не рассматривает споры о нарушении пав на КТ**

а. Арбитражный суд
б. Третейский суд
в. Суд

3. **Что такое коммерческая тайна?**

конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

4. **К внутренним нарушителям в информационной среде относится**

а. Конкуренты
б. Хакеры
в. Контраагенты

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.

Темы докладов

1. ФЗ "О лицензировании отдельных видов деятельности" № 99 от 4.05.2011 г
2. Лицензионные требования, предъявляемыми к соискателю лицензии
3. Перечень видов деятельности, на которые требуются лицензии
4. Этапы создания систем защиты информации
5. Правовая регламентация лицензионной деятельности в области защиты информации
6. Органы лицензирования и их полномочия. К
7. В чем заключаются особенности проведения специальных экспертиз?
8. Система государственной аттестации руководителей и специалистов в области защиты информации

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.

Темы докладов

1. Внешние и внутренние источники угроз в информационной сфере
2. Разработка и создание механизмов формирования и реализации государственной информационной политики России
3. Современные угрозы в сфере информационных технологий
4. Государственная политика в области создания информационных систем, технологий и средств их обеспечения
5. Формирование информационного общества

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
г. Распространение противоправной информации

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.

Темы докладов

1. Субъекты и объекты правоотношений в области обеспечения информационной безопасности
2. Элементы информационного правонарушения
3. Особенности юридической ответственности за нарушения законодательства, регулирующего отношения в информационной сфере
4. Дисциплинарная ответственность за информационные правонарушения
5. Административная ответственность за правонарушения в информационной сфере
6. Оперативно-розыскная деятельность, связанная с расследованием преступлений в информационной сфере
7. Использование Интернета с целью хищения или мошенничества
8. Проблемы противодействия правонарушения в информационной сфере
9. Уголовно-правовые санкции, связанные с нарушением информационной безопасности

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;
г. Использование интернет-технологий.

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.

Основная литература

6.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

6.2. Дополнительная литература

1. Белопушкин В.И., Кириллычев А.Н. Правовые аспекты обеспечения информационной безопасности. М., МГТУ, 2003 г.;

2. В.П. Петров, С.В. Петров «Информационная безопасность в истории и современной жизнедеятельности.»: учебно-методическое пособие / М.: ЮОУО ДО г. Москвы , 2007.
3. Верещагин Д. Влияние: Система дальнейшего энергоинформационного развития. -Спб: Изд-во «Невский проспект».
4. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-016789. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.
5. Волчинская Е.К. О стратегии и проблемах развития законодательства в сфере обеспечения информационной безопасности. Материалы конференции «Инфофорум». - 2004
6. Государственная тайна в Российской Федерации: учебно-методическое пособие / Под ред. чл.-кор. Международной академии информатизации М.А.Вуса. - Издательство С.-Пб. Университета, 1999
7. Доктрина информационной безопасности Российской Федерации. 2004 г. 48 с;
8. Замятин А., Замятин В., Юсупов Р. Опасности информационно психологической войны. // «ОБЖ. Основы безопасности жизни» №6 2002
9. Извеков Н.Н. Исторические традиции как средство укрепления национального иммунитета в информационных войнах III тысячелетия. // Информационный сборник «Безопасность». №№7-12 2001
10. Информационная безопасность. Information Security. Издательство: Оружие и технологии России, 2009 г. 256 с;
11. Информационные технологии в юридической деятельности : учебник и практикум для СПО / Т. М. Беляева, А. Т. Кудинов, Н. В. Пальянова, С. Г. Чубукова ; отв. ред. С. Г. Чубукова. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 314 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-00565-3. — Режим доступа : www.biblio-online.ru/book/0CC76DA0-57FF-4471-A4E6-6E60C43C36B7.
12. Кавеладзе И.Т. Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации). - М.: Изд-во «ЭКО -консалтинг», 1992
13. Кара-Мурза С.Г. Манипуляция сознанием в России сегодня. - М.: Изд-во «Эксмо», 2001
14. Лепехин А. Н.. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. Издательство: Тесей, 2008 г. 176 с;
15. Лопатин В.Н. Концептуальные основы развития российского законодательства в области обеспечения информационной безопасности // Компьютерная преступность и информационная безопасность / Под общ. Ред. А.П.Леонова. - Минск : АРИЛ, 2000
16. Мельников В. П., Клейменов С. А., Петраков А. М.. Информационная безопасность и защита информации. Издательство: Академия, 2009 г. 336 с;
17. Минаев В. А., Фисун А. П.. Правовое обеспечение информационной безопасности. Издательство: Маросейка, 2008 г.;
18. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа : www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7.
19. Одинцов А. А.. Защита предпринимательства (экономическая и информационная безопасность). Учебное пособие. Издательство: Международные отношения, 2003 г. 328 с;
20. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017.

— 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Режим доступа : www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847.
21. Панарин И.Н., Панарина Л.Г. Информационная война и мир. - М.: Изд-во «ОЛМА-ПРЕСС», 2003
22. Петров В. П., Петров С. В. Информационная безопасность человека и общества. Издательство: НЦ ЭНАС, 2007 г.;
23. Расторгуев С. П. Основы информационной безопасности. Издательство: Академия, 2007 г. 192 с;
24. Родионов М.А. Информационное противоборство: история и современность. // Информационный сборник «Безопасность».№№7-8 2002
25. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с;
26. С.Н.Семкин А.Н. Семкин Основы правового обеспечения защиты информации. М.:Горячая линия -Телеком, 2007
27. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия. - М.: “Дашков и К”, 2006 г.
28. Семененко В.А. Информационная безопасность. Учебное пособие. - М.: МГИУ, 2006. - 277 с;
29. Семкин С.Н., Семкин А.Н. Основы правового обеспечения информационной безопасности. - М.: Труд, 2003
30. Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. 2005 г. 304 с;
31. Тихонов В. А., Райх В. В. Информационная безопасность. Концептуальные, правовые, организационные и технические аспекты. Издательство: Гелиос АРВ, 2007 г.;
32. Уманский С.В. Психологическое воздействие: манипуляция или психотерапия. В кн. «Психологическая теория и практика в изменяющейся России» (Тезисы окладов Всероссийской научной конференции). - Челябинск: Изд-во ЮУрГУ, 2006
33. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2017. — 209 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01740-3. — Режим доступа : www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83.
34. Шершнев Л.И. Четвертая мировая война и ее особенности. // «ОБЖ. Основы безопасности жизни». №7,9 2005.
35. Яковец Е.Н. Правовые основы информационной безопасности. М.: Юрлитинформ, 2010
36. Ярочкин В. И.. Информационная безопасность. Учебник для вузов. Издательства: Академический проект, Мир, 2008

6.3. Нормативные правовые документы и иная правовая информация

1. Окинавская хартия глобального информационного общества: Принята на о. Окинава 22.07.2000 // Дипломатический вестник. 2000. № 8. С. 51-56.
2. Конституция Российской Федерации: Принята всенародным голосованием 12.12.1993 (в посл. ред.) // СЗ РФ. 1996. № 5. Ст. 410.
3. Гражданский кодекс Российской Федерации (часть вторая) от26.01.1996 № 14-ФЗ (в посл. ред.) // Российская газета. 1996. 6 февраля.
4. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (в посл. ред.) // Российская газета. 2006. 22 декабря.

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в посл. ред.) // СЗ РФ. 1996. № 25. Ст. 2954.
6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (посл. ред.) // Российская газета. 2001. 31 декабря.
7. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в посл. ред.) // Российская газета. 2006. 29 июля.
8. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (в посл. ред.) // Российская газета. 2004. 5 августа.
9. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ (в посл. ред.) // Российская газета. 2011. 6 мая.
10. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в посл. ред.) // Российская газета. 2006. 29 июля.
11. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (в посл. ред.) // Российская газета. 1995. 18 августа.
12. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184- ФЗ (в посл. ред.) // Российская газета. 2002. 31 декабря.
13. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (в посл. ред.) // Российская газета. 2003. 10 июля.
14. Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ (в посл. ред.) // Российская газета. 2002. 12 января.
15. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1(в посл. ред.) // Российская газета. 1996. 10 февраля.
16. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (в посл. ред.) // СЗ РФ 1997. № 41. Стр. 8220-8235.
17. Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30.11.1995 № 1203 (в посл. ред.) // Российская газета. 1995. 27 декабря.
18. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 06.03.1997 № 188 (в посл. ред.) // Российская газета. 1997. 14 марта.
19. Указ Президента РФ «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» от 30.05.2005 № 609 (в посл. ред.) // Российская газета. 2005. 7 июня.
20. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационнотелекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 (в посл. ред.) // СЗ РФ. 2008. № 12. Ст. 1110.
21. Указ Президента РФ «О Доктринt информационной безопасности Российской Федерации» от 05.12.2016 № 646 // СПС «КонсультантПлюс»
22. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СПС «КонсультантПлюс»
23. Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // Российская газета. 2008. 24 сентября.
24. Постановление Правительства РФ «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 № 781 // Российская газета. 2007. 21 ноября.
25. Постановление Правительства РФ «О порядке проведения проверки наличия в заявках на выдачу патента на изобретение или полезную модель, созданные в Российской Федерации,

сведений, составляющих государственную тайну» от 24.12.2007 № 928 (в посл. ред.) // Российская газета. 2007. 28 декабря.
26. Постановление Правительства РФ «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» от 06.02.2010 № 63 // СЗ РФ. 2010. № 7. Ст. 762.
27. Постановление Правительства РФ «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» от 15.04.1995 № 333 (в посл. ред.) // Российская газета. 1995. 5 мая.
28. Постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 № 79 // СЗ РФ. 2012. № 7. Ст. 863.
29. Приказ Минкомсвязи РФ «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования» от 25.08.2009 № 104 // Российская газета. 2009. 7 октября.
30. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем» от 24.06.2009 № 286 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 38.
31. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» от 24.06.2009 № 287 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 38.
32. Приказ ФСТЭК РФ «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации» от 28.08.2007 № 181 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 45.
33. Приказ ФСТЭК РФ «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации» от 28.08.2007 № 182 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2007. № 45.
34. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации» от 01.04.2009 № 123 (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 29.
35. Приказ ФСБ РФ «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг

по защите государственной тайны» от 27.02.2009 № 75 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 20.
36. Приказ МВД РФ № 368, ФСБ РФ № 185, ФСО РФ № 164, ФТС РФ № 481, СВР РФ № 32, ФСИН РФ № 184, ФСКН РФ № 97, Минобороны РФ № 147 от 17.04.2007 «Об утверждении Инструкции о порядке представления результатов оперативнорозыскной деятельности дознавателю, органу дознания, следователю, прокурору или в суд» // Российская газета. 2007. 16 мая.
37. Приказ ФСС РФ «О внедрении защищенного обмена документами в электронном виде с применением электронной цифровой подписи для целей обязательного социального страхования» от 12.02.2010 № 19 (в посл. ред.) // СПС «КонсультантПлюс».
38. Приказ ФНС РФ «Об утверждении Унифицированного формата транспортного контейнера при информационном взаимодействии с приемными комплексами налоговых органов по телекоммуникационным каналам связи с использованием электронной цифровой подписи» от 09.11.2010 № ММВ-7-6/535@ (в посл. ред.) // СПС «КонсультантПлюс».
39. Приказ ФНС РФ «Об утверждении Требований к сертификату ключа подписи и списку отозванных сертификатов для обеспечения единого пространства доверия сертификатам ключей электронной цифровой подписи» от 02.07.2009 № ММ-7- 6/353@ (в посл. ред.) // СПС «КонсультантПлюс».
40. Приказ Минкомсвязи РФ «Об утверждении Административного регламента предоставления Федеральным агентством по информационным технологиям государственной услуги по подтверждению подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей» от 10.07.2009 № 92 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 45.
41. Приказ ФНС РФ «Об утверждении Порядка ведения единого пространства доверия сертификатам ключей ЭЦП» от 17.12.2008 № ММ-3-6/665@ // СПС «КонсультантПлюс».
42. Приказ ФСТЭК РФ «Об утверждении Положения о методах и способах защиты информации в информационных системах
43. персональных данных» от 05.02.2010 № 58 // Российская газета. 2010. 5 марта.
44. Приказ Минкомсвязи РФ «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных» от 30.01.2010 № 18 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2010. № 16.
45. Приказ ФСТ РФ «Об утверждении Положения о работе с персональными данными государственного гражданского служащего ФСТ России и ведении его личного дела» от 07.11.2008 № 441-к (в посл. ред.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2009. № 2.
46. Приказ Минкомсвязи РФ «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» от 14.11.2011 № 312 // СПС «КонсультантПлюс».

3. Описание системы оценивания, шкала оценивания

3.1 Показатели и критерии оценивания.

Оценочные средства	Показатели оценки	Критерии оценки
Устный опрос	Устный опрос проводится на практических занятиях. Обучающиеся участвуют в дискуссии, отвечают на вопросы преподавателя. Оценивается уровень домашней подготовки по теме, способность системно и логично излагать материал, анализировать, формулировать собственную позицию, отвечать на дополнительные вопросы.	**Сложный вопрос:** полный, развернутый, обоснованный ответ – 5 баллов Правильный, но не аргументированный ответ – 3 балла Неверный ответ – 0 баллов **Обычный вопрос:** полный, развернутый, обоснованный ответ – 2 балла Правильный, но не аргументированный ответ – 1 балла Неверный ответ – 0 баллов. **Простой вопрос:** Правильный ответ – 1 балл; Неправильный ответ – 0 баллов
Доклад	Обучающиеся выступают с докладами, сообщениями, дополнениями. Оцениваются проработка источников, изложение материала, формулировка выводов, своевременность выполнения, ораторские способности.	Доклад оценивается в 2 балла. Допускается не более трех докладов в семестр.
Тестирование	Тестирование проходит с использованием LMS Moodl или в письменной форме. Обучающийся получает определённое количество тестовых заданий. На выполнение выделяется фиксированное время в зависимости от количества заданий. Оценка выставляется в зависимости от процента правильно выполненных заданий.	За 10 правильных вопросов 3 балла.
Ситуационная задача	Студенты получают формулировку	Полнота раскрытия темы задания и владение терминологией, ответы на

	проблемной ситуации профессиональной деятельности, для которой нужно найти решения с позиции участников ситуации. Оцениваются применение методов решения проблемных ситуаций, способность анализировать элементы ситуации, навыки, необходимые для профессиональной деятельности.	дополнительные вопросы – до 5 баллов.
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной форме по билетам, в которых содержатся вопросы по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии – 40 баллов

3.2 Шкала перевода баллов для уровней образования бакалавриата и специалитета
Согласно приказу № 306 от 06.09.2019 г. «О применении балльно-рейтинговой системы оценки знаний обучающихся» в институте установлена следующая шкала перевода оценки из многобалльной системы в зачет:

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

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