**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

Алтайский филиал
Кафедра гуманитарных и естественнонаучных дисциплин

Утверждена
решением заседания кафедры
гуманитарных и
естественнонаучных дисциплин
Протокол № 8
от «17» апреля 2018 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Б1.В.ДВ.03.01 Информационная безопасность в юридической деятельности

по направлению подготовки 40.03.01 Юриспруденция

профиль подготовки: Уголовно-правовой

квалификация: бакалавр

форма обучения: очная

Год набора – 2018

Барнаул, 2018 г.

**Автор–составитель:**
к.т.н., доцент кафедры гуманитарных и естественнонаучных дисциплин В.М.Лопухов

Заведующий кафедрой гуманитарных и естественнонаучных дисциплин, к.с.-х.н., доцент Л.М. Лысенко

# СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы 4
2. Объем и место дисциплины в структуре ОП ВО 5
3. Содержание и структура дисциплины 5
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине 7
5. Методические указания для обучающихся по освоению дисциплины 16
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 22
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 26

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.03.01 «Информационная безопасность в юридической деятельности» обеспечивает овладение следующими компетенциями с учетом этапа:

– компетенции, формирование которых продолжается в течение изучения данной дисциплины:

ПК-11 - способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению (ПК-11.3);

ПК-13 - способность правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации (ПК-13.3).

1.2. В результате освоения дисциплины у обучающихся должны быть сформированы:

Таблица 1.

| **Трудовые или профессиональные действия** | **Код этапа освоения компетенции** | **Результаты обучения** |
|---|---|---|
| предупреждать, выявлять, пресекать и расследовать правонарушения, в том числе коррупционной направленности | ПК - 11.3 Владение основами административного права, юридической психологии, практической психологии в правоприменительной деятельности, информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах, юридической социологии, юридической конфликтологии. | *на уровне знаний:* Знает методы и средства защиты информации, необходимые для предупреждения правонарушений, выявления и устранения причин и условий совершения правонарушений |
| | | *на уровне умений:* Умеет выявлять источники угроз информационной безопасности юридической деятельности; применять знания основ информационной безопасности к практическим ситуациям, связанным с предупреждением правонарушений, выявлением и устранением причин совершения правонарушений |
| | | *на уровне навыков:* Владеет навыками применения подходов для выработки конкретных, научно-обоснованных предложений по решению задач в сфере информационной безопасности. |
| участие в разработке документов правового характера | ПК - 13.3 Владение основами уголовного процесса, информационной безопасности в юридической деятельности, | *на уровне знаний:* Знает основные правила обеспечения информационной безопасности в юридической деятельности. |
| | | *на уровне умений:* Умеет анализировать специальную литературу по вопросам состояния и |

| | | |
|---|---|---|
| | информационных технологий в правоохранительных органах в части составления юридических документов. | проблемам информационной безопасности в юридической деятельности. |
| | | *на уровне навыков:* Владеет навыками соблюдения правил информационной безопасности при ведении юридического документооборота. |

## 2. Объем и место дисциплины в структуре ОП ВО

2.1 Объем дисциплины

Общая трудоемкость дисциплины Б1.В.ДВ.03.01 «Информационная безопасность в юридической деятельности» составляет 72 акад.часа/ 2 з.е.

Из них:

10ч. - лекции, 20ч. – практические занятия, 21,25 ч. – контактная работа с преподавателем, 31,75 ч. – самостоятельная работа, 9 ч. - контроль.

2.2 Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.03.01 «Информационная безопасность в юридической деятельности» является дисциплиной по выбору, относится к вариативной части учебного плана по направлению подготовки 40.03.01 «Юриспруденция» и изучается в 4 семестре на очной форме обучения.

Дисциплина реализуется среди формирующих компетенции:

- ПК-11 «Способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению»;
- ПК-13 «Способность правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации».

## 3. Содержание и структура дисциплины

Таблица 2.

| № п/п | Наименование тем (разделов) | Объем дисциплины , час. | | | | | | | Форма текущего контроля успеваемости, промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|
| | | Всего | Контактная работа обучающихся с преподавателем по видам учебных занятий | | | | | СР | |
| | | | Л | ЛР | ПЗ | Катт | К | | |
| Тема 1 | Основы информационной безопасности | 28 | 6 | | 10 | | | 12 | ДП, Т |
| Тема 2 | Обеспечение информационной безопасности в юридической деятельности | 37,75 | 4 | | 14 | | | 19,75 | ДП, ТЗ, КР |
| Промежуточная аттестация | | 9 | | | | | | | Зач |
| Консультации | | 1 | | | | | 1 | | |

| № п/п | Наименование тем (разделов) | Объем дисциплины , час. | | | | | | | Форма текущего контроля успеваемости, промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|---|
| | | Всего | Контактная работа обучающихся с преподавателем по видам учебных занятий | | | | | СР | |
| | | | Л | ЛР | ПЗ | Катт | К | | |
| Катт | | 0,25 | | | | 0,25 | | | |
| **Всего:** | | **72** | **10** | | **20** | **0,25** | **1** | **31,75** | **9** |

*Примечание: 4 – формы контроля успеваемости: типовое задание (ТЗ), доклад-презентация (ДП), тестирование (Т), контрольная работа (КР), зачет (Зач).*

## Содержание дисциплины

Таблица 3

| № п/п | Наименование тем (разделов) | Содержание тем (разделов) |
|---|---|---|
| Тема 1. | Основы информационной безопасности | Доступ к информации, классификация информации по доступу к ней. Виды информации ограниченного доступа. Актуальность защиты информации. Преступления в сфере компьютерной информации. Система защиты информации. Концептуальная модель информационной безопасности: угрозы информации, объекты угроз, цели злоумышленников, способы защиты информации, источники угроз, основные направления, средства защиты информации, действия, приводящие к неправомерному овладению конфиденциальной информацией. Направления обеспечения информационной безопасности: правовое, организационное и инженерно-техническое. |
| Тема 2. | Обеспечение информационной безопасности в юридической деятельности | Противоправные действия с финансовой информацией. Угрозы информационной безопасности финансовой деятельности. Использование информации в компьютерных сетях для совершения правонарушений и преступлений. Критерии безопасности компьютерных систем. Криптографическая защита. Электронная подпись. Экранирование, персональные и корпоративные межсетевые экраны, их назначение. Разграничение доступа, ролевое управление доступом. Защита компьютерных систем. Идентификация и аутентификация, парольная аутентификация, идентификация/аутентификация с помощью биометрических данных. Правила выбора пароля. Сетевые вирусы. Правила поведения в сети «Интернет» и «компьютерная гигиена». Преступления в «киберпространстве», «кибервойна». |

## 4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.ДВ.03.01 «Информационная безопасность в юридической деятельности» используются следующие методы текущего контроля успеваемости обучающихся:

– при проведении лекционных занятий: традиционные лекции и лекции-презентации;

– при проведении практических занятий и при контроле результатов самостоятельной работы обучающихся: решение типовых практических заданий (ТЗ), тестирование (Т), контрольная работа (КР), доклад с презентацией (ДП).

4.1.2. Зачет проводится с применением следующих методов (средств)

Промежуточная аттестация по дисциплине проводится для очной формы обучения в виде устного опроса на зачете.

4.2. Материалы текущего контроля успеваемости обучающихся

**Типовые оценочные материалы**

**Тема 1 «Основы информационной безопасности»**

*Типовые вопросы теста:*

Вопрос 1. К какой группе средств относятся механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения, и противодействия техническим средствам промышленного шпионажа?

Варианты ответов:

1: аппаратные

2: программные

3: криптографические

4: физические

5: организационное

6: правовое

Вопрос 2. Аппаратные средства защиты информации разделяют по техническим возможностям на

Варианты ответов:

1: средства общего назначения

2: профессиональные комплексы

3: любительские
4: специальные
5: полупрофессиональные

Вопрос 3. Миниатюрное электронное устройство перехвата речевой информации, состоящее из микрофона и радиопередатчика, обеспечивающего передачу подслушанного звукового сигнала на достаточно значительное расстояние с помощью электромагнитных волн, ЭТО?

Варианты ответов:
1: закладное подслушивающее устройство
2: "жучок"
3: "паучок"
4: скремблер
5: дешифратор
6: криптофон
7: радиозакладка

Вопрос 4. Укажите существующие виды закладных устройств

Варианты ответов:
1: акустические
2: вибрационные
3: инфракрасные
4: сетевые
5: телефонные
6: аппаратные

Вопрос 5. Как можно проводить поиск закладных устройств?

Варианты ответов:
1: с помощью визуального осмотра
2: с применением специальной аппаратуры
3: с помощью радиоконтроля (радиомониторинг) помещений
4: визуальным осмотром с применением специальной аппаратуры
5: с помощью "жучков"

Вопрос 6. Укажите, что относится к средствам обнаружения утечки информации

Варианты ответов:
1: индикаторы поля
2: цифровые зонды/мониторы
3: обнаружители видеокамер
4: нелинейные локаторы
5: маскираторы электромагнитных излучений и наводок

Вопрос 7. К какой группе средств относятся устройства, передающие речь в цифровом и зашифрованном виде. Вместо собственно речевого сигнала они передают только значения его определённых параметров, которые на приемной стороне управляют синтезатором речи?

Варианты ответов:
1: маскираторы электромагнитных излучений и наводок

2: скремблеры
3: криптофоны
4: маскираторы речи
5: вокодеры
6: преобразователи голоса

Вопрос 8. Укажите правильные высказывания из области криптографии.

Варианты ответов:

1: сложность написания символов в шифре замены усложняет процесс "вскрытия" зашифрованного сообщения

2: при "вскрытии" сообщения, зашифрованного шифром простой однобуквенной замены, подсчитывают частоты вхожения символов

3: слово-лозунг используют для лёгкого запоминания ключа

4: в шифре разнозначной замены одной букве могут ставится в соответствие один или два символа

Вопрос 9. Укажите, для чего используется криптография.

Варианты ответов:

1: Для защиты конфиденциальности данных;
2: Для защиты целостности данных
3: Для неотказуемости данных
4: Для аутентичности данных

Вопрос 10. Как называется информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Варианты ответов:

1: электронная подпись
2: электронная цифровая подпись
3: электронный документ
4: хеш-функция

*Типовые темы доклада-презентации по подтеме «Методы и средства защиты информации»:*

– Противодействие распространению вредоносных компьютерных программ.

– Противодействие взлому паролей, краже номеров кредитных карточек и других банковских реквизитов (фишинг).

– Противодействие распространению противоправной информации (клеветы, дезинформация, материалов, возбуждающих недобросовестную конкуренцию, ведущих к возникновению социальных «взрывов» и т.п.).

– Противодействие Интернет-мошенничеству.

– Противодействие аферам, связанным с продажей доменных имен.

– Противоправные действия с информацией.

– Угрозы в компьютерных сетях.

– Использование информации в компьютерных сетях для совершения

правонарушений и преступлений.

– Правовое направление обеспечения информационной безопасности.

– Организационное направление обеспечения информационной безопасности.

– Инженерно-техническое направление обеспечения информационной безопасности.

– Криптографическая защита данных в юридически значимом документообороте.

– Электронная подпись.

– Экранирование, персональные и корпоративные межсетевые экраны, их назначение.

– Международные стандарты информационного обмена.

– Защищённые протоколы обмена данными в информационно-телекоммуникационных сетях.

– Разграничение доступа, ролевое управление доступом. Аутентификация. Системы контроля управления доступом.

– Правила выбора пароля.

– Правила поведения в сети «Интернет» и «компьютерная гигиена».

– Преступления в «киберпространстве», «кибервойна».

– Управление доступом.

– Журналирование в ОС Windows.

– Системы предотвращения утечек конфиденциальной информации (DLP-системы).

– Системы обнаружения и предотвращения вторжений (IDS/IPS).

– Анализаторы протоколов.

– Источники бесперебойного питания и Генераторы напряжения.

– Угрозы (виды атак) в компьютерных сетях.

– Иммунизаторы.

**Тема 2. «Обеспечение информационной безопасности в юридической деятельности»**

*Типовое практическое задание «Определение перечня сведений конфиденциального характера»:*

1. Выберите специальность юриста (адвокат, прокурор, юрисконсульт, судья, следователь и др.), деятельность которого будет являться объектом исследования.

2. Дайте общее описание выбранной специальности юриста и его деятельности.

3. Определите перечень сведений конфиденциального характера, с которыми работает юрист выбранной специальности и которую необходимо защищать.

4. Отсортируйте перечень сведений конфиденциального характера по значимости с указанием НПА, регламентирующих их защиту.

5. Определите отношение юриста к защищаемой информации (пользователь, владелец, собственник, др.).

6. Оформите в документе MS Word отчёт о проделанной работе.

*Контрольная работа «Разбор конкретных ситуаций по разработке паспорта на систему защиты информации в деятельности юриста конкретной специальности»:*

1. Дайте общее описание автоматизированной информационной системы (АИС), используемой юристом конкретной специальности, деятельность которого выбрана в качестве объекта исследования при выполнении типового задания «Определение перечня сведений конфиденциального характера».

2. Определите перечень программных, информационных и технических средств, входящих в состав автоматизированного рабочего места данного специалиста. Дайте им краткую характеристику.

3. Перечислите примеры угроз доступности, целостности и конфиденциальности информации, с которой работает данный юрист.

4. В соответствии с угрозами определите возможных нарушителей объекта защиты информации. Классифицируйте их в соответствии с двумя группами: внешние нарушители и внутренние нарушители.

5. Опишите систему защиты информации (СЗИ), которой должен пользоваться юрист в своей профессиональной деятельности (состав, структура и процесс функционирования; средства и методы правовой, организационной и инженерно-технической защиты).

6. Перечислите правила обеспечения информационной безопасности, которые данный юрист должен неукоснительно выполнять.

7. Оформите в документе MS Word отчёт о проделанной работе.

*Типовые темы доклада-презентации по подтеме «НПА о защите информации»:*

1. «Конституция Российской Федерации» от 12.12.1993

2. «Доктрина информационной безопасности Российской Федерации» утверждена Указом Президента РФ от 05.12.2016 № 646

3. «Стратегия национальной безопасности Российской Федерации» утверждена Указом Президента РФ от 31.15.2015 № 683

4. Государственная программа Российской Федерации «Информационное общество (2011-2020 годы)» утверждена распоряжением Правительства Российской Федерации от 15.04.2014 N 313

5. «Гражданский кодекс (ГК) Российской Федерации» N 51-ФЗ от 30.11.1994

6. «Кодекс РФ об административных правонарушениях» № 195-ФЗ от 30.12.2001

7. «Трудовой Кодекс Российской Федерации» № 197-ФЗ от 30.12.2001

8. «Уголовный кодекс Российской Федерации» № 63-ФЗ от 13.06.1996

9. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности». Часть 1. «Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

10. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности.» Часть 5 «Руководство по менеджменту безопасности сети»

11. ГОСТ Р Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

16. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

18. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»

20. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

24. ГОСТ 34.936-91. Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом

25. ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»

26. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

27. ГОСТ Р 51583-2000 «Защита информации. Порядок создания систем в защищенном исполнении»

30. ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения»

31. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации»

39. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»

41. Федеральный закон «Об электронной подписи» №63-ФЗ от 6.04.2011

42. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

44. Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006

45. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» N 436-ФЗ от 29.12.2010

46. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне».

47. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»

51. Приказ ФСТЭК России от 12.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

52. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

53. Документ «Требования к системам обнаружения вторжений» (утвержден Приказом ФСТЭК России от 6 декабря 2011 года № 638)

54. Документ «Требования к средствам антивирусной защиты» (утвержден Приказом ФСТЭК России от 20 марта 2012 г. № 28)

## 4.3. Оценочные средства для промежуточной аттестации.

### 4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Таблица 4.

| Код компетенции | Наименование компетенции | Код этапа освоения компетенции | Наименование этапа освоения компетенции |
|---|---|---|---|
| ПК-11 | Способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению | ПК - 11.3 | Владение основами административного права, юридической психологии, практической психологии в правоприменительной деятельности, информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах, юридической социологии, юридической конфликтологии. |
| ПК - 13 | Способность правильно и полно отражать результаты профессиональной деятельности в юридической и иной документации | ПК - 13.3 | Владение основами уголовного процесса, информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах в части составления юридических документов. |

Таблица 5.

| Этап освоения компетенции | Показатель оценивания | Критерий оценивания |
|---|---|---|
| 3 этап (код этапа – ПК - 11.3.) Владение основами административного права, юридической психологии, практической психологии в правоприменительной деятельности, информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах, юридической социологии, юридической конфликтологии. | Изучает основы информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах. Учится выявлять и анализировать причины и условия, способствующие совершению правонарушений при решении практических задач. | Отлично знает основы информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах. Успешно демонстрирует навыки анализа причин и условий, способствующих совершению правонарушений при решении практических задач. |
| 3 этап (код этапа – ПК - 13.3.) Владение основами уголовного процесса, информационной безопасности в юридической деятельности, информационных технологий в правоохранительных органах в части составления юридических документов. | Изучает основы информационной безопасности в юридической деятельности. | Успешно демонстрирует знания основ информационной безопасности в юридической деятельности. |

4.3.2 Типовые оценочные средства

Промежуточная аттестация по дисциплине проводится для очной формы обучения в виде устного опроса на зачете.

*Типовые вопросы для зачета*

1. Виды информации ограниченного доступа.
2. Тайна.
3. Сведения, отнесённые к государственной тайне.
4. Профессиональная тайна.
5. Служебная тайна.
6. Коммерческая тайна.
7. Тайна личной жизни.

8. Персональные данные.
9. Оформление сведений ограниченного доступа.
10. Источники конфиденциальной информации.
11. Преступления в сфере компьютерной информации.
12. Экспертные группы, занимающиеся изучением инцидентов компьютерной безопасности.
13. Компьютерные преступники.
14. Угрозы в компьютерных сетях.
15. Концепция защиты.
16. Структура защиты.
17. Понятие угрозы.
18. Система защиты информации.
19. Цели и задачи системы защиты информации.
20. Требования к системе защиты информации.
21. Противоправные действия с информацией.
22. Неправомерное овладение конфиденциальной информацией.
23. Способы нарушения информационной безопасности.
24. Компоненты концептуальной модели информационной безопасности.
25. Угрозы.
26. Источники угроз.
27. Цели злоумышленников.
28. Направления защиты информации.
29. Комплексный подход к разработке системы защиты информации.
30. Методы определения требований к защите информации.
31. Структура системы защиты информации.
32. Модели построения системы защиты информации.
33. Классификация угроз и специфические виды угроз для компьютерных сетей.
34. Цели, субъекты и уровни уязвимости информационной безопасности.
35. Каналы утечки информации.
36. Пути несанкционированного доступа к информации.
37. Проектирование системы обеспечения информационной безопасности.
38. Типовой порядок действий по обеспечению информационной безопасности.
39. Правовое направление обеспечения информационной безопасности
40. Организационное направление обеспечения информационной безопасности
41. Инженерно-техническое направление обеспечения информационной безопасности.
42. Криптографическая защита данных в юридически значимом документообороте.
43. Электронная подпись.
44. Экранирование, персональные и корпоративные межсетевые экраны, их назначение.

45. Разграничение доступа, ролевое управление доступом. Аутентификация в Internet.
46. Правила выбора пароля.
47. Правила поведения в сети «Интернет» и «компьютерная гигиена».
48. Преступления в «киберпространстве», «кибервойна».

**Шкала оценивания зачета.**

Таблица 6.

| Шкала оценивания | Критерии оценивания |
|---|---|
| «зачтено» | демонстрируются глубокие или частичные знания информационных технологий, теоретических положений, на основе которых осуществляется использование информационных и коммуникационных технологий при обработке правовой информации, показываются хорошие умения практического использования программных средств; выполнены и защищены значительная часть работ текущего контроль знаний |
| «незачтено» | фрагментарные знания информационных технологий, теоретических положений, на основе которых осуществляется использование информационных и коммуникационных технологий при обработке правовой информации, не показываются умения практического использования программных средств; отсутствует значительная часть работ текущего контроль знаний |

4.4. Методические материалы

Зачет проводится по билетам, в которых по два теоретических вопроса.

Выполнение всех заданий текущего контроля является обязательным для всех обучающихся. Обучающиеся, не выполнившие в полном объеме все эти задания, не допускаются к промежуточной аттестации. В случае наличия задолженности обучающийся отрабатывает пропущенные занятия на консультациях, после полной отработки задолженностей обучающийся может быть допущен к промежуточной аттестации.

Оценка знаний обучающегося носит комплексный характер, является балльной и определяется:

–ответом на зачете;

–учебными достижениями в семестровый период.

## 5. Методические указания для обучающихся по освоению дисциплины

Наряду с посещением семинаров и участием в обсуждении проблем, учебный план предусматривает затрату обучающимися, как правило, большего числа часов для самостоятельной работы.

*Методические рекомендации по подготовке к практическим занятиям*

Практическое занятие подразумевает решение типовых задач, разбор определенных ситуаций. Подготовка к практическому занятию начинается с тщательного ознакомления с условиями предстоящей работы, определившись с вариантом задачи, следует обратиться к рекомендуемой литературе. Задание должно быть охвачено полностью и рекомендованная литература должна быть освоена в большем объеме. Для полноценной подготовки к практическому занятию чтения учебников недостаточно, необходимо использовать Интернет-ресурсы. Тщательная подготовка к практическим занятиям, как и к лекциям, имеет определяющее значение: занятие пройдет так, как обучающийся подготовился к его проведению. Готовясь к практическим занятиям, следует активно пользоваться справочной литературой: энциклопедиями, словарями, и др. По окончании практического занятия к нему следует обратиться еще раз, повторив основные моменты – для этого в течение занятия следует делать пометки об используемых информационных технологиях.

*Методические рекомендации по подготовке докладов-презентаций*

Выбор темы является первым этапом работы и осуществляется в соответствии с направлениями будущей деятельности обучающегося. При этом обучающемуся предоставляется право самостоятельного выбора темы с учетом ее актуальности и практической значимости, фактического или планируемого места работы, научных профессиональных интересов и т.д.

Обучающийся имеет право выполнять работу по теме, отличающейся от предложенных преподавателем. В этом случае обучающийся должен представить обоснование выбора данной темы.

Подготовка к написанию работы включает:

- выбор темы из списка или по согласованию с преподавателем;
- подбор научной литературы и нормативного материала по избранной теме, подготовка библиографического списка;
- составление плана работы;
- изучение учебной, специальной литературы, нормативных правовых актов, материалов практики по выбранной теме;
- составление окончательного варианта плана работы и согласование его с преподавателем.

Работа должна отвечать следующим требованиям:

- наличие в работе всех структурных элементов исследования: теоретической, аналитической и практической составляющих;
- наличие обоснованной авторской позиции;
- использование в аналитической части исследования обоснованного комплекса методов и методик, способствующих раскрытию сути проблемы;
- целостность работы, которая проявляется в связанности теоретической и практической его частей;
- перспективность исследования: наличие в работе материала, который может стать источником дальнейших исследований;

- достаточность и современность использованного библиографического материала.

Работа должна быть оформлена в соответствии с требованиями, предъявляемых к письменным работам обучающихся в Алтайском филиале РАНХИГС при Президенте РФ.

Основные элементы структуры работы:

1. Титульный лист/слайд.
2. Задание.
3. Содержание.
4. Введение.
5. Основной текст работы.
6. Заключение.
7. Список использованных источников.
8. Приложения (при необходимости).

Введение содержит: актуальность выбранной темы; степень её разработанности; цель и задачи; объект и предмет исследования; круг рассматриваемых проблем и в сжатой форме все основные положения, обоснованию которых посвящена работа.

Первичным является объект исследования (более широкое понятие), вторичным - предмет исследования, в котором выделяется определенная проблемная ситуация. Предмет работы чаще всего совпадает с определением ее темы или очень близок к ней.

Работа должна иметь логическую структуру изложения. Формулировки должны быть лаконичны и отражать суть работы.

Сначала приводятся исторические, теоретические и методические аспекты исследуемой проблемы. В ней содержится обзор используемых источников информации по теме бакалаврской работы, описание объекта и предмета исследования, различные теоретические концепции, принятые понятия и их классификации, а также своя аргументированная позиция по данному вопросу. Сведения, содержащиеся в этой главе, должны давать полное представление о состоянии и степени изученности поставленной проблемы. Написание этой части работы проводится на базе предварительно подобранных литературных источников, в которых освещаются вопросы, в той или иной степени раскрывающие тему.

Особое внимание следует обратить на законодательную, нормативную и специальную документацию, посвященную вопросам, связанным с предметом и объектом исследования.

Далее анализируются особенности объекта исследования, а также практические аспекты проблем, рассмотренных ранее. Эта часть работы посвящена анализу практического материала, собранного ранее. В ней содержится:

- анализ конкретного материала по избранной теме желательно за период не менее 5 лет;
- сравнительный анализ вопроса с действующей практикой;

- описание выявленных закономерностей, проблем и тенденций развития объекта и предмета исследования;
- оценка эффективности принятых решений (на конкретном примере);

Далее могут рассматриваться и обосновываться направления решения выявленных проблем, предлагаются пути решения исследуемой (разрабатываемой) проблемы; конкретные практические рекомендации и предложения по совершенствованию исследуемых (разрабатываемых) явлений и процессов. В данной части работы должны быть сделаны самостоятельные выводы.

Заключение содержит выводы и предложения из всего материала с их кратким обоснованием в соответствии с поставленной целью и задачами, раскрывает значимость полученных результатов. При этом выводы общего порядка, не вытекающие из результатов и содержания работы, не допускаются. Выводы также не могут подменяться механическим повторением выводов по отдельным частям работы. Заключение лежит в основе доклада обучающегося на защите.

Список использованных источников должен содержать сведения об источниках, которые использовались при написании работы.

Стиль доклада должен быть деловым, без излишней эмоциональной окраски. Не рекомендуется использовать местоимения и глаголы в первом лице. Так, вместо выражений «я считаю», «по моему мнению», следует излагать «автор считает», «по мнению автора», «полагаем», «на наш взгляд» и т.д.

Доклад готовится в обязательном порядке с презентацией. При этом обучающиеся самостоятельно изучают группу источников по определённой теме, которая, как правило, подробно не освещается на лекциях.

Цель подготовки доклада-презентации – овладение навыками анализа и краткого изложения изученных материалов в соответствии с требованиями, а также создание наглядных информационных пособий, выполненных с помощью мультимедийной компьютерной программы PowerPoint.

Этот вид работы требует координации навыков обучающегося по сбору, систематизации, переработке информации, оформления ее в виде подборки материалов, кратко отражающих основные вопросы изучаемой темы, в электронном виде, то есть создание докладов с презентацией расширяет методы и средства обработки и представления информации и формирует у обучающихся навыки работы на компьютере.

Доклад-презентация готовится обучающимся в виде слайдов с использованием программы Microsoft PowerPoint. Основные этапы подготовки доклада-презентации:

- выбор темы;
- консультации научного руководителя;
- работа с источниками, сбор материала;
- написание текста доклада;
- оформление рукописи, создание презентационного материала;

– выступление с докладом перед аудиторией.

Подготовка доклада-презентации позволяет обучающемуся основательно изучить интересующий его вопрос, изложить материал в компактном и доступном виде, привнести в текст полемику, приобрести навыки научно-исследовательской работы, устной речи, ведения научной дискуссии. В ходе подготовки доклада с презентацией могут быть подготовлены раздаточные материалы.

Преподаватель на консультациях дает рекомендации по улучшению качества предоставляемого материала и в случае необходимости доработки представленных частей.

*Методические рекомендации по подготовке контрольной работе (КР)*

Контрольные работы являются одной из основных форм текущего контроля преподавателем работы обучающегося.

Контрольная работа представляет собой письменный ответ на вопрос, который рассматривается в рамках дисциплины.

Содержание ответа на поставленный вопрос включает:

– показ автором знания теории вопроса и понятийного аппарата,

– понимание механизма реально осуществляемой практики,

– выделение ключевых проблем исследуемого вопроса и их решение.

Структура (план) письменной контрольной работы может иметь соответствующую рубрикацию.

*Критерии оценки контрольной работы:*

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в контрольной работе проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).

3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

4. Качество полученных результатов (степень завершенности исследования, спорность или однозначность выводов).

5. Использование литературных источников.

6. Культура письменного изложения материала.

7. Культура оформления материалов работы.

Контрольные работы должны быть оформлены в соответствии с требованиями Алтайского филиала РАНХиГС. Контрольные работы оцениваются преподавателем дисциплины по пятибалльной шкале (незачтено/удовлетворительно/хорошо/отлично).

*Подготовка к тестам контроля знаний (Т)*

Подготовка к тестированию требует от обучающихся тщательного изучения материала по теме или блоку тем, где акцент делается на изучение причинно-следственных связей, раскрытию природы явлений и событий, проблемных вопросов. Для подготовки необходима рабочая программа дисциплины с примерами тестов, учебно-методическим и информационным обеспечением.

**Оценивание тестовых заданий**

| **Количество правильных ответов теста (%)** | 0-49 | 50-64 | 65-84 | 85-100 |
|---|---|---|---|---|
| **Отметка по 5-ти бальной шкале** | 2 | 3 | 4 | 5 |

*Методические рекомендации по подготовке к зачету*

При подготовке к зачету по дисциплине «Информационная безопасность в юридической деятельности» следует руководствоваться рабочей программой, что позволит четко представить круг вопросов, подлежащих изучению. При изучении дисциплины «Информационная безопасность в юридической деятельности» трудности в усвоении знаний могут возникнуть в связи с большим разнообразим информационных технологий и компьютерных средств. При этом каждое обеспечение информационной системы обладает собственным понятийным аппаратом. Соответственно, в рамках данной дисциплины обучающимся необходимо уяснить специфику программного, информационного, методического, правового, лингвистического и технического обеспечений юридических автоматизированных информационных систем. На настоящий момент имеется огромный массив документов по вопросам применения информационных технологий в юридической деятельности. Для того чтобы сориентироваться в этом массиве обучающимся следует обратиться к перечню рекомендуемой литературы, сформированному для подготовки в рамках курса «Информационная безопасность в юридической деятельности». Еще одной «проблемой» при изучении данной дисциплины является быстрое изменения, происходящие в области информационных технологий. В связи с этим обучающимся следует учитывать, что по указанной причине в учебниках и учебных пособиях не всегда содержится актуальная информация, касающаяся современных компьютерных средств. Поэтому в процессе самостоятельной работы обучающихся , при подготовке к зачету необходимо уточнять актуальность подобранного материала. Необходимым условием успешного изучения данной дисциплины является свободное

владение обучающимися понятиями области информационных и коммуникационных технологий. Приобретение глубоких знаний предполагает эффективное использование различных видов учебной работы: лекционных и практических занятий, самостоятельной работы.

## 6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

### 6.1. Основная литература

| п/п | Автор | Название | Издатель-ство | Год выпуска | Расположение |
|---|---|---|---|---|---|
| 1 | Нестеров, С. А. | Информационная безопасность : учебник и практикум для академического бакалавриата | М.: Юрайт | 2018 | www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 |
| 2 | Под общ. ред. П. У. Кузнецова | Информационная безопасность в юридической деятельности: учебник для академического бакалавриата | М.: Юрайт | 2018 | www.biblio-online.ru/book/2F7C62C5-F95A-409E-B1E7-169E28DA68CF |
| 3 | Под ред. Т. А. Поляковой, А. А. Стрельцова | Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для бакалавриата и магистратуры | М.: Юрайт | 2018 | https://biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847 |

### 6.2. Дополнительная литература

| п/п | Автор | Название | Издатель-ство | Год выпус-ка | Расположение |
|---|---|---|---|---|---|
| 1 | Внуков А.А. | Защита информации: учебное пособие для бакалавриата и магистратуры | М.: Юрайт | 2018 | https://biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1 |

| | | | | | |
|---|---|---|---|---|---|
| 2 | Под ред. С. Г. Чубуковой | Правовая информатика : учебник и практикум для прикладного бакалавриата | М.: Юрайт | 2018 | www.biblio-online.ru/book/BD5768E2-FD23-4B77-8EC6-96951D5D8D3A |
| 3 | Ельчанинова, Н.Б. | Информационные технологии в юридической деятельности: учебное пособие | Таганрог: Издательство Южного федерального университета | 2016 | http://biblioclub.ru/index.php?page=book&id=493039 |
| 4 | Морозов А.В. | Информационное право и информационная безопасность. Часть 2 [Электронный ресурс]: учебник для магистров и аспирантов | Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа | 2016 | http://www.iprbookshop.ru/66771.html |
| 5 | под ред. В. Д. Элькина | Информационная безопасность в юридической деятельности [Электронный ресурс]: учебник и практикум для академического бакалавриата | М.: Юрайт | 2017 | https://biblio-online.ru/book/5B52F04F-E0AF-483F-8AE3-6A9E4B06C3B0 |
| 6 | Крылов Г.О. | Инновационные методики дисциплины "Информационная безопасность в юридической деятельности" [Электронный ресурс] | Информационное право. N 2. С. 20 - 22 | 2014 | Доступ из СПС Консультант Плюс |
| 7 | Кулантаева И.А. | Информационная безопасность в юридической деятельности [Электронный ресурс]: практикум | Оренбург: Оренбургский государственный университет | 2014 | http://www.iprbookshop.ru/33632 |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Бурняшов Б.А. | Информационная безопасность в юридической деятельности [Электронный ресурс]: курс лекций | Саратов: Южный институт менеджмента | 2014 | http://www.iprbookshop.ru/25966 |

## 6.3. Учебно-методическое обеспечение самостоятельной работы

| п/п | Автор | Название | Издательство | Год выпуска | Расположение |
|---|---|---|---|---|---|
| 1 | Данелян, Т.Я. | Информационные технологии в юриспруденции: (ИТ в юриспруденции) : учебно-методический комплекс | Москва : Евразийский открытый институт | 2011 | http://biblioclub.ru/index.php?page=book&id=90553 (27.09.2018) |
| 2 | Горина Е.В. | Коммуникативные технологии манипуляции в СМИ и вопросы информационной безопасности [Электронный ресурс]: учебно-методическое пособие | Екатеринбург: Уральский федеральный университет | 2016 | http://www.iprbookshop.ru/66538.html |
| 3 | Бурня-шов Б.А. | Информационная безопасность в юридической деятельности [Электронный ресурс]: учебно-методическое пособие | Саратов: Южный институт менеджмента | 2014 | http://www.iprbookshop.ru/25967.html |
| 4 | Королев В.Т. | Информационная безопасность в юридической деятельности. WINDOWS [Электронный ресурс]: учебно-методические материалы | М.: Российский государственный университет правосудия | 2015 | http://www.iprbookshop.ru/45222.html |
| 5 | Шань-гин В.Ф. | Информационная безопасность и защита информации [Электронный ресурс]: учебник | М.: ДМК Пресс | 2014 | http://www.iprbookshop.ru/29257 |
| 6 | Артемов А.В. | Информационная безопасность [Электронный ресурс]: курс лекций | Межрегиональная Академия безопас- | 2014 | http://www.iprbookshop.ru/33430 |

| | | | | | |
|---|---|---|---|---|---|
| | | | ности и выживания | | |

## 6.4. Нормативные правовые документы

1. Официальный сайт компании «КонсультантПлюс» http://consultant.ru/
2. Официальный сайт компании «Гарант» http://garant.ru/

## 6.5. Интернет-ресурсы

1. Галатенко В.А. Основы информационной безопасности http://www.intuit.ru/department/security/secbasics/
2. Защита информации в компьютерных системах http://protect.htmlweb.ru/
3. Информационная безопасность http://www.chemisk.narod.ru/html/ib01.html
4. Лекции по информационной безопасности http://uskof.ucoz.ru/index/lekcii_po_informacionnoj_bezopasnosti/0-69
5. Биленко Ж. Виртуальный криминал [электронный ресурс] // Центр исследования компьютерной преступности. http://www.crime-research.ru/articles/MoneXy19/
6. Рынок информационной безопасности. Исследование. 2013 г. [Электронный ресурс]. – Режим доступа: http://www.tsarev.biz/informacionnaya-bezopasnost/zakonchilsya-proekt-pervogo-ekspertnogo-issledovaniya-rossijskogo-rynka-ib/
7. Сабадаш В. Деятельность центров реагирования на компьютерные инциденты как средство противодействия интернет-мошенничеству [электронный ресурс] // Центр исследования компьютерной преступности. http://www.crime-research.ru/articles/sabodssh17/
8. Текущее состояние рынка аппаратных средств аутентификации [Электронный ресурс]. – Режим доступа: http://zlonov.ru/wp-content/uploads/Текущее-состояние-рынка-аппаратных-средств-аутентификации.pdf

## 6.6. Иные источники

| п/п | Автор | Название | Издательство | Год выпуска | Расположение |
|---|---|---|---|---|---|
| 1 | Казанцев С.Я. | Информационные технологии в юридической деятельности (для бакалавров): Учебник | Москва: КНОРУС | 2018 | - |
| 2 | Коноплева И.А. | Информационные технологии: Учебное пособие | Москва: Проспект | 2017 | - |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Гвоздева В.А. | Базовые и прикладные информационные технологии: Учебник | Москва: ИНФРА-М | 2018 | - |
| 4 | Элькин В.Д. | Информационные технологии в юридической деятельности: Учебное пособие | Москва: Юрайт | 2016 | - |

## 7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для обеспечения учебного процесса по дисциплине «Информационная безопасность в юридической деятельности» филиал располагает учебными аудиториями для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещениями для самостоятельной работы и помещениями для хранения и профилактического обслуживания учебного оборудования.

Лекционные аудитории оснащены видеопроекционным оборудованием для проведения презентаций, а также средствами звуковоспроизведения; помещения для практических занятий укомплектованы учебной мебелью; библиотека располагает рабочими местами с доступом к электронным библиотечным системам и сети интернет. Все учебные аудитории оснащены компьютерным оборудованием и лицензионным программным обеспечением