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

Сибирский институт управления – филиал РАНХиГС
Факультет юридический
Кафедра: Уголовного права и процесса

Утверждена кафедрой
Уголовного права и процесса
Протокол от «_25_» августа 2017 г.
№ _6_

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Правовое обеспечение информационной безопасности
(Б1.В.ДВ.7.1)

не устанавливается
краткое наименование дисциплины

по специальности/направлению подготовки 40.05.01 Правовое обеспечение национальной безопасности
Направленность (профиль/специализация): «Уголовно-правовая»
квалификация выпускника: Юрист
формы обучения: очная, заочная
год набора: 2018.

г. Новосибирск, 2017.

Автор-составитель:
канд. юрид. наук, доцент кафедры уголовного права и процесса
Комаров Антон Анатольевич.

Заведующий кафедрой Уголовного права и процесса:
канд. юрид. наук, доцент, доцент кафедры уголовного права и процесса
Крупницкая Валерия Игоревна.

СОДЕРЖАНИЕ

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

Дисциплина Б1.В.ДВ.7.1 «Правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями:

Таблица 1.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-12	способностью осуществлять профилактику, предупреждение правонарушений, коррупционных проявлений, выявлять и устранять причины и условия, способствующие их совершению	*ПК 12.2. – очная и заочная формы обучения*	Способность осуществлять специально-криминологическое предупреждение компьютерной преступности на профессиональном уровне.

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

Таблица 2.

Профессиональные действия	**Код этапа освоения компетенции**	**Результаты обучения**
выявление, пресечение преступлений, расследование и разрешение уголовных дел, в том числе с применением специальных познаний	*ПК 12.2.*	**Знаний:** научно обоснованных закономерностей развития компьютерной преступности в Российской Федерации.
		Умения: выявить закономерности причинного комплекса компьютерной преступности и коррелирующих с ней иных (малозначительных) правонарушений (исходя из подведомственности) в соответствии с имеющимися в правоохранительной практике сведениями о состоянии преступности на объекте или территории;.
		Навыками: навыками по составлению и презентации научно-обоснованных рекомендаций по борьбе с преступностью с последующим включением их в аналитические отчёты, записки, информационные письма, справки, обзоры.

2. Объём и место дисциплины в структуре образовательной программы высшего образования.

Объём дисциплины:

общая трудоёмкость дисциплины в зачётных единицах составляет **3** З.Е.;

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся составляет

для очной формы обучения: 42 часа (из них 14 – лек, 28 – практ.,), 66 – самостоятельная работа обучающихся;

для заочной формы обучения: 26 часа (из них 6 – лек, 20 – практ.,), 78 – самостоятельная работа обучающихся;

Место дисциплины, – Б1.В.ДВ.7.1 *«Правовое обеспечение информационной безопасности»* осваивается студентами уголовно-правового профиля на:

- пятом курсе, девятом семестре (по очной форме обучения);
- шестом курсе, одиннадцатом и двенадцатом семестре (по заочной форме обучения);

Дисциплина реализуется после изучения дисциплин:

На очной форме обучения:	
Б.1.Б.27.	Криминология
На заочной форме обучения:	
Б.1.Б.27.	Криминология

3. Содержание и структура дисциплины.

Таблица 3.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[1], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРС	
			л/эо, дот[2]	лр/эо, дот[3]	пз/эо, дот[3]	КСР		
Очная форма обучения								
Раздел 1.	**Основы международного сотрудничества по вопросам противодействия компьютерной преступности**							Написание эссе по итогам изучения раздела
Тема 1	*Международные стандарты безопасности глобального информационного общества*		2	-	2		12	Устный опрос
Тема 2	*Основы организации работ по защите информации при сотрудничестве с зарубежными странами*		2		10		14	Устный опрос
Раздел 2.	**Проблемы обеспечения информационной безопасности в Российской Федерации**							Написание эссе по итогам изучения раздела
Тема 3	*Правовые режимы информации*		2	-	2		12	Устный опрос
Тема 4	*Специально-криминологическое предупреждение компьютерной преступности.*		6	-	4		14	Устный опрос
Тема 5	*Правовые вопросы защиты информации с использованием технических средств. Лицензирование и сертификация в информационной сфере*		2		10		14	Устный опрос
Промежуточная аттестация								Зачёт.
Всего:		**108**	**14**		**28**	**-**	**66**	Акад. час.
		3						Зач. ед.
		81						Астр. час

1 Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э),реферат (Р), диспут (Д) и др.

[2] При применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом

Таблица 4.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[3], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРС	
			л/эо, дот[4]	лр/эо, дот[3]	пз/эо, дот[3]	КСР		
Заочная форма обучения								
Раздел 1.	**Основы международного сотрудничества по вопросам противодействия компьютерной преступности**							Написание эссе по итогам изучения раздела
Тема 1	*Международные стандарты безопасности глобального информационного общества*		1		4		14	Устный опрос
Тема 2	*Основы организации работ по защите информации при сотрудничестве с зарубежными странами*		1		4		16	Устный опрос
Раздел 2.	**Проблемы обеспечения информационной безопасности в Российской Федерации**							Написание эссе по итогам изучения раздела
Тема 3	*Правовые режимы информации*		2		4		16	Устный опрос
Тема 4	*Специально-криминологическое предупреждение компьютерной преступности.*		1		4		16	Устный опрос
Тема 5	*Правовые вопросы защиты информации с использованием технических средств. Лицензирование и сертификация в информационной сфере*		1		4		16	Устный опрос
Промежуточная аттестация						4		Зачёт.
Всего:		**108**	**6**		**20**	**4**	**78**	Акад. час.
		3						Зач. ед.
		81						Астр. час

3 Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э),реферат (Р), диспут (Д) и др.

4 При применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом

Содержание дисциплины.

Тема 1. *Международные стандарты безопасности глобального информационного общества.*

Электронная торговля. Электронное образование, дистанционные образовательные технологии. Болонское соглашение от 19 сентября 2003 года (бакалавр, магистр, доктор философии). Электронное правительство. Рекомендации Совета Европы № 2 и № 3 от 28 февраля 2001 года (безвозмездный доступ к правовым актам, земельный кадастр и регистр населения, судебный процесс через Интернет). Информационная безопасность (информационное оружие, информационная война). Окинавская хартия глобального информационного общества от 22 июля 2000 года.

Тема 2. *Основы организации работ по защите информации при сотрудничестве с зарубежными странами.*

Требования нормативных актов, регламентирующих посещение режимных предприятий иностранными специалистами; проведение международных мероприятий научно-технического и экономического сотрудничества.

Импортозамещение программного обеспечения.

Тема 3. *Правовые режимы информации.*

Информация как объект правового регулирования. Конституционные гарантии прав на информацию и механизм их реализации. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности.

Тема 4. *Специально-криминологическое предупреждение компьютерной преступности.*

Понятие правового режима защиты государственной тайны. Перечень и содержание организационных мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

Персональные данные. Служебная тайна. Коммерческая тайна. Банковская тайна. Тайна следствия и судопроизводства. Профессиональная тайна. Правовые режимы конфиденциальной информации: содержание и особенности.

Тема 5. *Правовые вопросы защиты информации с использованием технических средств. Лицензирование и сертификация в информационной сфере.*

Понятие лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области защиты информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации.

Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие сертификации по российскому законодательству.

Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).

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.7.1 «Правовое обеспечение информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся очной и заочной формы обучения:

Таблица 5.

Тема (раздел)		Методы текущего контроля успеваемости
Р 1.	**Основы международного сотрудничества по вопросам противодействия компьютерной преступности**	Написание эссе по итогам изучения раздела
Т.1	*Международные стандарты безопасности глобального информационного общества.*	Устный опрос
Т.2.	*Основы организации работ по защите информации при сотрудничестве с зарубежными странами*	Устный опрос
Р 2.	**Правовые проблемы обеспечения информационной безопасности в Российской Федерации**	Написание эссе по итогам изучения раздела
Т. 3.	*Законодательство Российской Федерации в области информационной безопасности*	Устный опрос
Т.4.	*Правовые режимы информации*	Устный опрос
Т.5.	*Правовые вопросы защиты информации с использованием технических средств. Лицензирование и сертификация в информационной сфере*	Устный опрос

4.1.2. Зачёт проводится с применением следующих методов (средств): устное собеседование по вопросам билета, либо письменные ответы на вопросы билета. Выбор метода оценивания для традиционной формы обучения осуществляет преподаватель, информировав обучающихся.

4.2. Материалы текущего контроля успеваемости.

Полный перечень материалов текущего контроля находится на кафедре Уголовного права и процесса. Далее приведены типовые оценочные средства.

4.2.1. Вопросы и задания для устного опроса:

Тема № 1. Международные стандарты безопасности глобального информационного общества.

Вопросы:

1. Информационная безопасность Российской Федерации.
2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
3. Виды угроз информационной безопасности Российской Федерации.
4. Источники угроз информационной безопасности Российской Федерации.
5. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

Тема № 2. Основы организации работ по защите информации при сотрудничестве с зарубежными странами.

Вопросы:

1. Методы обеспечения информационной безопасности Российской Федерации.
2. Общие методы обеспечения информационной безопасности Российской Федерации.
3. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.
4. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.
5. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации.
6. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.
7. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.
8. Организационная основа системы обеспечения информационной безопасности Российской Федерации.
9. Основные функции системы обеспечения информационной безопасности Российской Федерации.
10. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

Тема № 3. Законодательство Российской Федерации в области информационной безопасности

Вопросы:

1. Назовите основные признаки информации.
2. Какие признаки информации являются существенными для правового регулирования отношений, складывающихся по поводу информации?
3. Перечислите основания классификации информации в правовой сфере.
4. Дайте определение нормативной правовой информации. Каким образом она классифицируется в юридических науках?
5. Что можно отнести к ненормативной правовой информации?

6. На какие категории классифицируют информацию по уровню доступа?
7. В каком нормативном правовом акте даётся определение информационной сферы, информационных процессов и информационных отношений?
8. Перечислите методы правового регулирования, используемые в информационном праве.
9. Какие методы могут быть использованы при изучении науки информационного права?
10. Какие информационные революции произошли в истории развития цивилизации? В чём особенность последней революции?
11. Перечислите основные черты информационного общества.
12. Назовите субъектов информационного права.
13. С какой целью была принята Хартия глобального информационного общества?
14. Какие принципы информационного права, на ваш взгляд, являются наиболее значимыми?
15. Что представляет собой информационное право как наука, как учебная дисциплина и как отрасль права?
16. Почему информационное право следует относить к комплексной отрасли права?
17. Расскажите историю становления информационного права.

Тема № 4. Правовые режимы информации.

Вопросы:

1. В чём состоят особенности информационных отношений в области коммерческой тайны?
2. В чём состоит правовой режим коммерческой тайны?
3. Как охраняется коммерческая тайна в трудовых отношениях?
4. В чём состоят особенности информационных отношений в области персональных (конфиденциальных) данных?
5. Каковы правовые основания работы с персональными данными?
6. В чём заключается государственное регулирование в области персональных данных?
7. Что собой представляет понятие «частная жизнь»?
8. Какова юридическая ответственность за нарушения правового режима конфиденциальной информации?
9. В чём состоят особенности информационных отношений в области государственной тайны?
10. В чём состоит правовой режим государственной тайны?
11. Каков порядок отнесения сведений к государственной тайне?
12. Какие степени секретности устанавливаются для сведений, составляющих государственную тайну?
13. Что является основанием для рассекречивания сведений?
14. Каков срок засекречивания сведений, составляющих государственную тайну?
15. В чём заключается проблема собственности в связи с информацией, составляющей государственную тайну?
16. Какие органы осуществляют защиту государственной тайны?
17. Как осуществляется допуск должностных лиц и граждан Российской Федерации к государственной тайне?
18. Как осуществляется контроль за обеспечением защиты государственной тайны?

Тема № 5. Правовые вопросы защиты информации с использованием технических средств. Лицензирование и сертификация в информационной сфере.

Вопросы:

1. Каково понятие лицензирования по российскому законодательству?
2. Какие виды деятельности в информационной сфере подлежат лицензированию.

3. Назовите основные правовые акты, регламентирующие лицензионную деятельность в области защиты информации.
4. Какие объекты лицензирования в сфере защиты информации вы знаете?
5. Каковы правовые основы защиты информации с использованием технических средств?
6. Что представляет собой правовая регламентация сертификационной деятельности в области защиты информации?
7. Каковы правовые основы применения электронно-цифровой подписи?
8. Каковы правовые аспекты оказания услуг, связанных с электронной цифровой подписью?

4.2.2. Тематика эссе по дисциплине:

1. Субъекты законодательной инициативы. Процесс превращения законопроекта в закон.
2. Болонское соглашение от 19 сентября 2003 года. Процесс подготовки бакалавра, магистра, доктора философии.
3. Рекомендации Совета Европы № 2 и № 3 от 28 февраля 2001 года.
4. Указы Президента Российской Федерации «О концепции национальной безопасности», «Перечень сведений, отнесенных к государственной тайне», «Вопросы Межведомственной комиссии по защите государственной тайны». Нормативные документы Межведомственной комиссии по защите государственной тайны в Российской Федерации, ФСТЭК, МВД, ФСБ и др.
5. Отнесение сведений к государственной тайне, их засекречивание и рассекречивание, доступ к государственной тайне, контроль за состоянием ее защиты, юридическая ответственность за нарушение режимных требований. Нормативно-техническая документация по порядку учета, хранения, транспортировки и эксплуатации.
6. Трудовой договор (контракт) как особый вид договорных отношений. Предмет и стороны контракта. Содержание и основы для прекращения трудовых договорных отношений.
7. Требования нормативных актов, регламентирующих посещение режимных предприятий иностранными специалистами.
8. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 года.
9. Порядок проведения экспертизы, аттестации и сертификации в сфере информационной безопасности. Органы, уполномоченные на ведение лицензионной деятельности.
10. Уголовный кодекс Российской Федерации (глава 28).
11. Гражданский кодекс РФ (часть 4). Защита интеллектуальной собственности средствами авторского права.
12. Кодекс РФ об административных правонарушениях. Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).
13. Кодекс РФ об административных правонарушениях. Статья 13.12. Нарушение правил защиты информации.
14. Основные положения Закона «О частной детективной и охранной деятельности».
15. Криминалистическая характеристика преступлений в сфере компьютерной информации, методика расследования, механизмы следообразования.
16. Виды «вредной» информации. Спам, диффамация и клевета.
17. Информационно-психологическая безопасность. Правовое регулирование в сфере информационно-психологической безопасности.
18. Правовые основы электронного документооборота. Порядок и механизмы его реализации.
19. Правовое обеспечение информационной безопасности межбанковских расчетов юридических лиц.

20. Конституция Российской Федерации (статьи 24 и 29). Законодательное регулирование вопросов обеспечения информационной безопасности.
21. Электронная торговля. Электронное образование, дистанционные образовательные технологии. Электронное правительство.
22. Доступ к правовым актам, земельный кадастр и регистр населения, судебный процесс через Интернет.
23. Конфиденциальная информация: персональные данные, служебная тайна, профессиональная тайна, коммерческая тайна, тайна следствия и другие виды тайн.
24. Государственная тайна как особый вид защищаемой информации. Система защиты государственной тайны.
25. Основы трудового права. Регулирование вопросов обеспечения сохранности информации с ограниченным доступом.
26. Требования нормативных актов, регламентирующих проведение международных мероприятий научно-технического и экономического сотрудничества.
27. Угрозы информационной безопасности из Доктрины информационной безопасности Российской Федерации от 9 сентября 2000 года.
28. Правовые основы и государственная система лицензирования и сертификации в области защиты информации.
29. Уголовный кодекс Российской Федерации. Статья 146. Нарушение авторских и смежных прав.
30. Экономические аспекты защиты информации и охраны интеллектуальной собственности. Критерии эффективности «затраты – надежность». Особенности страхования информационных рисков.
31. Кодекс РФ об административных правонарушениях. Статья 7.12. Нарушение авторских и смежных прав, изобретательских и патентных прав.
32. Кодекс РФ об административных правонарушениях. Статья 13.13. Незаконная деятельность в области защиты информации.
33. Правовые основы деятельности служб безопасности. Источники права, объекты и субъекты. Задачи и элементы структуры служб безопасности.
34. Криминалистические аспекты проведения расследований. Информация как криминалистический объект.
35. Основы психологической устойчивости при работе в экстремальных условиях.
36. Основы психофизиологического тестирования.
37. Государственная автоматизированная система «Выборы».
38. Государственная автоматизированная система «Правосудие».
39. Правовое обеспечение информационной безопасности кредитных пластиковых карточек физических лиц.

4.3. Оценочные средства промежуточной аттестации.

Таблица 6.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-12	способностью осуществлять профилактику, предупреждение правонарушений, коррупционных проявлений, выявлять и устранять причины и условия, способствующие их совершению	*ПК 12.2. – очная и заочная формы обучения*	Способность осуществлять специально-криминологическое предупреждение компьютерной преступности на профессиональном уровне.

Таблица 7.

Этап освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
Очная и заочная формы обучения		
ПК 12.2. Способность осуществлять специально-криминологическое предупреждение компьютерной преступности на профессиональном уровне.	Выявляет обстоятельства, способствующие совершению компьютерных преступлений в России Сопоставляет результаты собственного исследования с уже имеющимися в криминологии результатами. Самостоятельно использует статистические методы для определения состояния преступности – количественной оценки функциональных связей отдельных элементов социальной структуры (преступности) и анализирует качественные характеристики её причинного комплекса.	**Проявляет знание** особенностей причинного комплекса компьютерных преступлений и учитывает их в процессе подбора способов предупреждения преступности. **Понимает** специфические закономерности развития компьютерной преступности в Росси и за рубежом. **Самостоятельно** может указать **на наиболее достоверные источники информации** о состоянии компьютерной преступности в России и мире. **Выдвигает научно-обоснованные** предложения по совершенствованию мер предупреждения компьютерной преступности из числа имеющихся в арсенале криминологической науки. **Знает** специфику деятельности специальных субъектов предупреждения преступности конкретного вида; правила составления ведомственных планов по борьбе с отдельными видами преступности. **Использует** данные судебной статистики и материалы судебной практики при разработке мер по усилению борьбы с преступностью.

Критерии оценивания:

Таблица 8. Шкала оценивания ответа на вопросы зачета

Зачет	Экзамен (5-балльная шкала)	Критерии оценки
незачтено	2	Не знает принципов на основе которых осуществляется сотрудничество правоохранительных органов по борьбе с компьютерной преступностью и иными информационными правонарушениями Не знает принципов построения общественных отношений в информационном обществе. Не знает ни одного нормативного документа специально посвященного регулированию информационных правоотношений в Российской Федерации. Не умеет правильно разграничить правовые режимы оборота электронной информации. Не знает ни одного юридически обоснованного метода обеспечения безопасности оборота информации.
зачтено	3	Может перечислить нормативно-правовые акты составляющие систему информационного права. Умеет правильно выделить надлежащий правовой режим оборота конкретной информации, правильно установить меру юридической ответственности за нарушение принципов такого оборота.
	4	Знает правовые основы международного сотрудничества в деле построения информационного общества и проблемы связанные с реализацией единого правового поля, относительно компьютерных технологий. Умеет правильно выделить надлежащий правовой режим оборота конкретной информации, правильно установить меру юридической ответственности за нарушение принципов такого оборота.
	5	Способен правильно избрать форму международного сотрудничества и обосновать эффективность подобного рода взаимодействия в деле профилактики информационных правонарушений на международном уровне. В состоянии показать пути имплементации международного правоприменительного опыта во внутрироссийский.

4.3.2. Типовые оценочные средства.
Полный перечень вопросов и заданий находится на кафедре Уголовного права и процесса.

Примерный перечень вопросов для подготовки к зачёту.

1. Охарактеризуйте основные положения Закона Российской Федерации «О персональных данных».
2. Опишите все элементы состава преступления: Статья 274 УК РФ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
3. Изложите основные положения Доктрины информационной безопасности Российской Федерации.
4. Приведите примеры способов реализации Рекомендации Комитета Министров Совета Европы № 2 и № 3 от 28 февраля 2001 года по правовому обеспечению информационных технологий.
5. Дайте краткую характеристику элементов состава преступления: статья 272 УК РФ. Неправомерный доступ к компьютерной информации.
6. Прокомментируйте основные положения Закона Российской Федерации «Об информации, информационных технологиях и о защите информации».
7. Опишите все элементы состава преступления: статья 273 УК РФ. Создание, использование и распространение вредоносных программ для ЭВМ.
8. Дайте краткую характеристику элементов состава преступления: статья 274 УК РФ. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
9. Определите правовой статус ЭЦП и задачи удостоверяющих центров в соответствии с ФЗ «Об электронной подписи».
10. Прокомментируйте основные положения Окинавской хартии глобального информационного общества от 22 июля 2000 года.

4.4. Методические материалы промежуточной аттестации.

Промежуточная аттестация по дисциплине осуществляется в форме зачёта. В этих целях реализованы специальные аттестационные задания в которых содержатся конкретные вопросы и задания для проверки усвоения магистрантами, предусмотренных рабочей программой компетенций. Далее даётся несколько примеров типовых заданий, которые предусматривают возможность контроля конкретных «знаний», «умений» и «навыков владения».

Каждое аттестационное задание состоит из двух вопросов, первый из которых раскрывает знания студента по избранной теме, второе задание позволяет выявить степень владения этим материалом, для решения конкретных деловых (профессиональных) задача. И, наконец, последний вопрос (задание) сформулирован так, чтобы появилась возможность утвердительно или отрицательно охарактеризовать умение применять знания к конкретной проблемной ситуации, логически связанной с предыдущими вопросами.

В целом, весь этот комплекс заданий направлен на решение одной конкретной проблемы, что показывает системность полученных знаний или невозможность комплексно и последовательно реализовывать соответствующие элементы конкретной формируемой компетенции (в случае неудовлетворительного ответа).

5. Методические указания для обучающихся по освоению дисциплины

Учебным планом подготовки студентов предусмотрено изучение курса «Предупреждение (профилактика) криминальных угроз национальной безопасности» в объеме 108 академических часов. Изучение курса осуществляется в одном семестре и заканчивается зачётом.

Основными формами получения знаний по данному курсу будут лекции, практические занятия, лабораторные работы, консультации, научно-исследовательская и самостоятельная работа.

Теоретические занятия (лекции). На лекциях преподавателем используются аудиторные доски для представления схем, формул, графиков и иного подсобного материала, проекторы для демонстрации слайдов и иных материалов через соответствующую аппаратуру. В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на семинарское занятие и указания на самостоятельную работу.

Практические занятия проводится по группам. В процессе рассмотрения вынесенных на обсуждение вопросов могут использоваться такие формы проведения занятий, как сообщение, дискуссия, и т.д. Могут применяться ТСО для демонстрации проблемного видеосюжета или условия задачи, мультимедийные средства для презентации выступлений и т.п. Семинарские занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, рефератов, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине. Семинар предполагает свободный обмен мнениями по избранной тематике. Он начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам семинара, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения и объявляет оценки выступавшим студентам. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе семинарских занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке к семинару студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Самостоятельная работа. Самостоятельная работа студентов включает в себя изучение учебной, учебно-методической и специальной литературы, нормативных актов, их конспектирование, обобщение положительной практики органов внутренних дел, суда, прокуратуры и других органов в сфере борьбы с преступностью и подготовку письменных контрольных работ. Кроме того, студентам рекомендуется завести папку с подборками сообщений, публикуемых в специальных юридических журналах и СМИ, касающихся самых последних решений Правительства и иных органов власти в сфере борьбы с преступностью, сообщений о реализованных операциях правоохранительных органов и т.п. Главная задача самостоятельной работы – приобретение научных знаний путём изучения рекомендованной литературы, поисков дополнительной информации для ответов на контрольные вопросы,

формирование интереса к творчеству и решению профессиональных вопросов, изучение тематики курса в полном объёме.

Написание эссе по дисциплине. Эссе представляет собой малый художественный жанр литературы. Объем его не велик, но выполняется оно на строго заданную тему. Криминология, безусловно, является наукой. Но это не отрицает того факта, что научно-публицистические материалы по данному предмету также существуют. Поскольку студентам далеко не всегда удается изучение криминологии (тем паче – научное исследование) эссе может стать весьма востребованным методом обучения.

Принципы, заложенные в написание эссе.

1. Эссе, как сочинение. Подразумевает, что это творческая работа студента, который представляет свое видение проблемы. Следовательно, оригинальность текста (отсутствие заимствований) должна быть велика – не менее 85% по системе «Антиплагиат». Самостоятельно проверить качество работ можно по ссылке: https://www.antiplagiat.ru/

2. Научная обоснованность. Сродни тому, как исполняют свой долг научные корреспонденты, представители пресс-служб правоохранительных органов, так и студент в своих рассуждениях должен опираться на положения криминологической науки, которую он изучает. Следовательно, в тексте статьи должны использоваться ссылки на работы ученых. Чем больше, тем лучше. Стоит только помнить о правилах оформления библиографических ссылок в соответствии с ГОСТ. Все ссылки должны быть затекстовыми, а сноска на источник внутри текста проставляется в квадратных скобках как, например, сейчас [4, С.11]. Нумерация и последовательность источников в списке литературы может производиться по любому основанию: первый раз встречается в тексте или по алфавиту. Стоит помнить, что ссылка на конкретную страницу дается внутри текста, в самом списке указывается полное количество страниц.

Пример:

1. Комаров, А.А. Интернет-мошенничество: проблемы детерминации и предупреждения. – М.: Юрлитинформ, 2013. – 184 с.

(Пример ссылки на монографию (книгу)

2. Комаров, А.А. Правонарушения в сети Интернет: сравнительный анализ наднациональных концепций / А.А. Комаров // Право и кибербезопасность. – 2014. – №2(5). – С. 66-72.

(пример ссылки на печатный журнал)

3. Комаров, А.А. Краткий анализ государственных мер по декриминализации и девиктимизации несовершеннолетних пользователей Интернет / А.А. Комаров // Проблемы профилактики девиантного (делинквентного) поведения несовершеннолетних: пути их преодоления: сб. научных трудов кафедр уголовно-правовых дисциплин и уголовного процесса и криминалистики Юридического института МГПУ (г. Москва). – Саратов, Изд-во «Саратовский источник», – М. 2015. – С. 118-130. (пример ссылки на сборник научных трудов)

4. Комаров, А.А. К вопросу о целесообразности расчёта цены интернет-мошенничества / А.А. Комаров // Политика, государство и право. – 2015. – № 5 [Электронный ресурс]. URL: http://politika.snauka.ru/2015/05/2859 (дата обращения: 24.09.2015).

(пример ссылки на сетевой журнал)

5. Комаров, А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дисс. … канд. юрид. наук. – Пятигорск, 2011. – 262 с.

(пример ссылки на диссертацию)

3. Краткость (лаконичность). Объём сочинения не должен быть менее 6000 знаков с учётом пробелов и, как правило, не более 9000 знаков. Стоит учитывать, что список

литературы, приведённый в конце не должен составлять искомый объём. Учитывается лишь само сочинение.

4. Форма отчётности. Первоначально эссе предоставляется в электронном варианте в формате *.doc (MS Word) на электронную почту преподавателя: reise83@mail.ru После того, как эссе одобрено к печати и будут исправлены все указанные в переписке недочеты, оно считается сданным. После этого стоит принести распечатанный вариант или сразу несколько одобренных работ на кафедру, поставив под ними свою подпись.

Оформление следует начать с Ф.И.О. курса, группы, и обратного адреса электронной почты, далее заголовок.

Пример:

Иванов Иван Иванович
Стдудент 3-го курса СИУ-РАНХиГС
Юр. Фак-та, группа: 00000
e-mail.ru

Динамика похищений людей в Российской Федерации за последнее десятилетие

Текст, текст [1, С. 78] текст, текст[2], текст[3, С.11-12], текст, текст

(выравнивание по ширине)

Список литературы.

1. Источник №1
2. Источник № 2.

5.1. Методические указания по освоению дисциплины для студентов заочной формы обучения.

Преподавание дисциплины «Правовое обеспечение информационной безопасности» имеет свои особенности применительно к заочной форме обучения. Обусловлено это тем обстоятельством, что лекционных курс на заочном отделении, как правило, значительно сокращен и большее внимание в процессе преподавания дисциплины отводится самостоятельной работе. Поэтому некоторые темы студенты должны исследовать самостоятельно по указанию и рекомендациям преподавателя. Для этого необходимо разобраться с учебной и научной литературой, законспектировать её содержание.

Основные вопросы, предусмотренные тематическим планом, будут рассмотрены в ходе лекций, в процессе которых помимо изложения теоретического материала, рассмотрения положений соответствующих нормативных актов и материалов практики предполагается постановка проблемных вопросов, обсуждение которых выносится на практическое занятие. Главным приёмом усвоения знаний, в таком случае, выступает конспектирование лекций. Конспектирование представляет собой процесс мыслительной

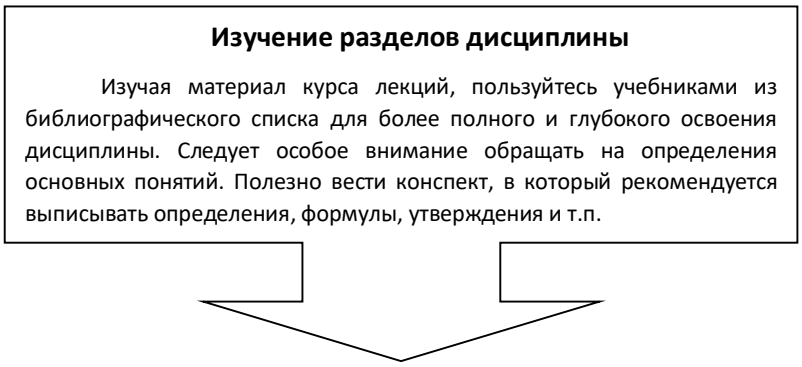
переработки и письменной фиксации основных положений читаемого или воспринимаемого на слух текста. При конспектировании происходит свертывание, компрессия первичного текста. Результатом конспектирования является запись в виде конспекта. Следует учитывать, что конспектирование является универсальным приёмом фиксации изучаемых источников (лекций преподавателя, учебников, дополнительной, справочной литературы). Поэтому при изучении предмета конспектирование представляет собой отдельный вид как аудиторной, так и самостоятельной работы. Например, аудиторная работа, зачастую подразумевает под собой плановый конспект: составляется при помощи предварительного плана, каждому его пункту соответствует определенная часть конспекта.

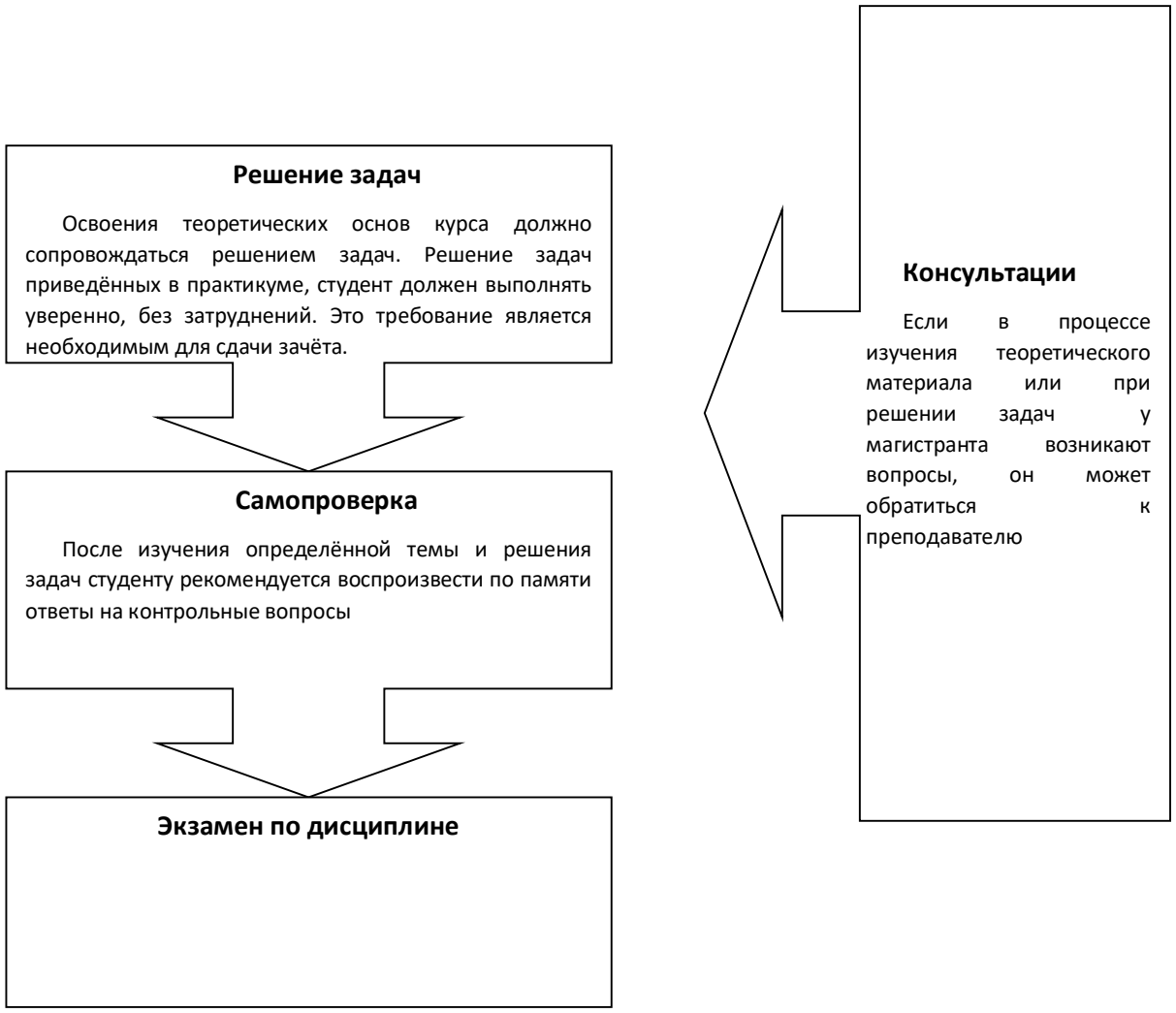
Далее приводится таблица, кратко отражающая методологию конспектирования.

Таблица 9. – Этапы подготовки конспекта.

Этап 1.	Выделяются смысловые части – вся информация, относящаяся к одной теме, группируется в один блок.
Этап 2.	В каждой смысловой части формулируется тема в опоре на ключевые слова и фразы.
Этап 3.	В каждой части выделяется главная и дополнительная по отношению к теме информация.
Этап 4.	Главная информация фиксируется в конспекте в разных формах: в виде тезисов, выписок (текстуальный конспект), в виде вопросов, выявляющих суть проблемы, в виде назывных предложений (конспект-план и конспект-схема).
Этап 5.	Дополнительная информация приводится при необходимости.

В целом работа студента заочной формы обучения должна строиться по следующей схеме:




Решение задач
Освоения теоретических основ курса должно сопровождаться решением задач. Решение задач приведённых в практикуме, студент должен выполнять уверенно, без затруднений. Это требование является необходимым для сдачи зачёта.
Самопроверка
После изучения определённой темы и решения задач студенту рекомендуется воспроизвести по памяти ответы на контрольные вопросы
Экзамен по дисциплине
Консультации
Если в процессе изучения теоретического материала или при решении задач у магистранта возникают вопросы, он может обратиться к преподавателю

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

6.1. Основная литература.

1. Спектор, Е. И. Лицензирование в Российской Федерации: правовое регулирование [Электронный ресурс] : учеб. пособие / Е. И. Спектор. — Электрон. дан. — Москва : Юстицинформ , 2007. — 197 с. — Доступ из ЭБС изд-ва «Лань». - Режим доступа : http://e.lanbook.com/books/element.php?pl1_id=10682, требуется авторизация (дата обращения : 24.04.2016) — Загл. с экрана.
2. Лапина, М. А. Информационное право [Электронный ресурс] : учеб. пособие / М. А. Лапина, А. Г. Ревин, В. И. Лапин ; под ред. И. Ш. Килясханов. - Электрон. дан. – Москва : Юнити-Дана, 2015. - 336 с. – Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=118624, требуется авторизация (дата обращения : 11.04.2016). - Загл. с экрана.
3. Ловцов, Д. А. Информационное право [Электронный ресурс] : учеб. пособие / Д. А. Ловцов. – Электрон. дан. - Москва : Рос. акад. правосудия, 2011. - 228 с. – Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=140621, требуется авторизация (дата обращения : 11.04.2016). - Загл. с экрана
4. Геращенко, М. М. Информационные технологии в юридической деятельности : учеб. пособие : [в 2 ч.]. Ч. 2 / М. М. Геращенко, Е. А. Печенкина, В. Н. Храпов ; Рос. акад. нар. хоз-ва и гос. службы при Президенте РФ, Сиб. ин-т. - Новосибирск : Изд-во СибАГС, 2012. - 190 с. - То же [Электронный ресурс]. - Доступ из Б-ки электрон. изд. / Сиб. ин-т упр. – филиал РАНХиГС. – Режим доступа : http://www.sapanet.ru, требуется авторизация (дата обращения : 23.04.2016). - Загл. с экрана.
5. Килясханов, И. Ш. Информационное право в терминах и понятиях [Электронный ресурс] : учеб. пособие / И. Ш. Килясханов, Ю. М. Саранчук. - Электрон. дан. - Москва : Юнити-Дана, 2015. - 135 с. – Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=115167, требуется авторизация (дата обращения : 11.04.2016). - Загл. с экрана.

6.2. Дополнительная литература.

1. Бачило, И. Л. Государство и право XXI в. Реальное и виртуальное / И. Л. Бачило ; Ин-т государства и права РАН. - Москва : Юркомпани, 2013. - 277 с.
2. Куняев, Н. Н. Обеспечение национальных интересов Российской Федерации в информационной сфере: правовой аспект : монография / Н. Н. Куняев. - Москва : Юрлитинформ, 2012. – 331 с.
3. Информационные технологии в юридической деятельности : учебник / Урал. гос. юрид. акад. ; под общ. ред. П. У. Кузнецова. - Москва : Юрайт, 2012. - 422 с.
4. Ефимова, Л. Л. Информационное право [Электронный ресурс] : учеб.-метод. комплекс / Л. Л. Ефимова. - Электрон. дан. – Москва : Евраз. открытый ин-т, 2011. - 336 с. – Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=90541, требуется авторизация (дата обращения : 11.04.2016). - Загл. с экрана.

6.3. Учебно-методическое обеспечение самостоятельной работы.

1. Уголовное право. Общая часть : метод. рекомендации / сост. Т. А. Черткова ; Рос. акад. нар. хоз-ва и гос. службы при Президенте РФ, Сиб. ин-т упр. - Новосибирск : Изд-во СибАГС, 2015. - 52 с. - То же [Электронный ресурс]. – Доступ из Б-ки электрон. изданий / Сиб. ин-т упр. – филиал РАНХиГС. – Режим доступа : http://siu.ranepa.ru, требуется авторизация (дата обращения : 14.04.2016). – Загл. с экрана.

6.4. Нормативные правовые документы.

1. Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. // Офиц. интернет-портал правовой информации. – Режим доступа: http://pravo.gov.ru/ (дата обращения: 16.02.2016).
2. Уголовный кодекс РФ от 13 июня 1996 г. №63-ФЗ // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.
3. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федеральный закон от 07.08.2001 №115-ФЗ (ред. от 29.06.2015) // Собр. законодательства Рос. Федерации. – 2001. – №33, Ч. 1. – Ст. 3418.
4. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. —
5. 2006. — 31 (ч. 1).
6. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // Рос. газ. — 2006. — 29 июл.
7. О государственной тайне : Закон РФ от 21.07.1993 № 5485-I // СЗ РФ. — 1997. — № 41. — Ст. 8220.

6.5. Интернет-ресурсы.

1. Президент РФ: http://president.kremlin.ru
2. Правительство РФ: http://www.governmrnt.ru
3. Государственная Дума РФ: http://www.duma.ru
4. Конституционный Суд РФ: http://www.rfnet.ru
5. Гарант: законодательство РФ: http://garant.ru
6. Консультант +: законодательство РФ: http://www.consultant.ru
7. Журнал «Информационное право»: www.infolaw.ru
8. Интернет и право: http://www.internet-law.ru

6.6. Иные источники.

1. Данелян, Т. Я. Информационные технологии в юриспруденции: [Электронный ресурс] : учеб.–метод. комплекс / Т. Я. Данелян ; - Электрон. дан. - Москва : Евраз. открытый ин-т, 2011. - 284 с. - Доступ из ЭБС «Унив. б-ка ONLINE». - Режим доступа : http://biblioclub.ru/index.php?page=book&id=90553, требуется авторизация (дата обращения : 22.04.2016). - Загл. с экрана.

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

7.1. Программное обеспечение

1. Единая электронная справочно-правовая система «Консультант Плюс»
2. Единая электронная справочно-правовая система «Гарант»
3. Электронная библиотека НОУ "ИНТУИТ"
4. пакет MS Office
5. Microsoft Windows
6. сайт филиала
7. СДО Прометей
8. корпоративные базы данных
9. iSpring Free Cam8.

7.2. Технические средства и материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа	экран, компьютер с подключением к локальной сети института, и выходом в Интернет, звуковой усилитель, антиподавитель, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Учебный зал судебных заседаний (зал деловых игр)	Столы аудиторные, телевизор, компьютер, доска, судейский молоток, имитационная камера заключения, мультимедиапроектор
Лаборатория личностного и профессионального развития	полиграф «Фемида», компьютер с подключением к локальной сети института и выходом в Интернет, телевизор, колонки, DVD-проигрыватель, музыкальные центры, видеокамера, видеомагнитофоны, методические материалы (тесты, методики и т.п.), столы письменные, стулья, шкаф, трибуна настольная, стеллаж, доска аудиторная, ковровое покрытие; стекло для одностороннего просмотра для проведения фокус-групп
Юридическая клиника	Телевизор, компьютер с выходом в локальную сеть филиала и Интернет, столы аудиторные, стулья, правовые системы, отечественные и зарубежные интернет-ресурсы
Учебные аудитории для проведения занятий семинарского типа	экран, компьютер с подключением к локальной сети и выходом в Интернет, звуковой усилитель, столы аудиторные, стулья, трибуна, доска аудиторная
Аудитория для самостоятельной работы обучающихся. Центр Интернет-ресурсов.	Мультимедийный проектор, Экран проекционный, принтер, ПК с подключенным интернетом и к локальной сети института (включая правовые системы) и Интернет, столы аудиторные, стулья, доски аудиторные, экран.

Библиотека.Центр интернет-ресурсов	компьютеры с выходом в Интернет, автоматизированную библиотечную информационную систему и электронные библиотечные системы: «Университетская библиотека ONLINE», «Электронно-библиотечная система издательства ЛАНЬ», «Электронно-библиотечная система издательства «Юрайт», «Электронно-библиотечная система IPRbooks»,«Университетская Информационная Система РОССИЯ», «Электронная библиотека диссертаций РГБ», «Научная электронная библиотека eLIBRARY», «EBSCO», «SAGE Premier». Система федеральных образовательных порталов «Экномика. Социология. Менеджмент», «Юридическая Россия», Сервер органов государственной власти РФ, Сайт Сибирского Федерального округа и др. Экран, компьютер с подключением к локальной сети филиала и выходом в Интернет, звуковой усилитель, мультимедийный проектор, столы аудиторные, стулья, трибуна, доска аудиторная. Наборы виртуального демонстрационного оборудования, наглядные учебные пособия.
Библиотека (имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет	компьютеры с подключением к локальной сети филиала, Центру интернет-ресурсов и Интернет, Wi-Fi, столы аудиторные, стулья
Специализированный кабинет для занятий с маломобильными группами (студенты с ограниченными возможностями здоровья)	Экран, компьютеры с подключением к локальной сети института, Центру интернет-ресурсов и выходом в Интернет, звуковой усилитель, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная, офисные кресла