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

Сибирский институт управления – филиал РАНХиГС
Юридический факультет
Кафедра уголовного права и процесса

Утверждена
кафедрой Уголовного права и процесса
Протокол от «_30_» августа 2019 г.
№ _6_

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Правовые основы борьбы с криминальными угрозами информационной безопасности»
(Б1.Б.24)

ПОБ-КУИБ
краткое наименование дисциплины

по специальности 40.05.01 Правовое обеспечение национальной безопасности

специализация «Уголовно-правовая»
квалификация выпускника: Юрист

Формы обучения: очная, заочная

Год набора – 2020

г. Новосибирск, 2019.

Автор-составитель:
канд., юрид. наук. А.А. Комаров

Заведующий кафедрой Уголовного права и процесса:

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы ……	4
2. Объём и место дисциплины в структуре ОП ВО ……..	5
3. Содержание и структура дисциплины …….	6
4. Материалы текущего контроля успеваемости и фонд оценочных средств промежуточной аттестации по дисциплине ……	10
5. Методические указания для обучающихся по освоению дисциплины …….	19
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине ……..	23
6.1. Основная литература ……..	23
6.2. Дополнительная литература ……..	24
6.3. Учебно-методическое обеспечение самостоятельной работы …….....	24
6.4. Нормативные правовые документы ……..	24
6.5. Интернет-ресурсы ……...	25
6.6. Иные источники ……..	25
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 образовательной программы.

Дисциплина Б1.В.ДВ.06.02 «Правовые основы борьбы с криминальными угрозами 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	Очная форма обучения – ПК-12.2	Способность использовать криминологические знания для выявления причин и условий компьютерной преступности и конкретных преступлений.
		Заочная форма обучения – ПК-12.2	Способность использовать криминологические знания для выявления причин и условий компьютерной преступности и конкретных преступлений.
		Заочная форма обучения с применением технологий ЭО и ДОТ – ПК-12.2	Способность использовать криминологические знания для выявления причин и условий компьютерной преступности и конкретных преступлений.

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; участие в судебном разбирательстве	ПК-12.2	**знания:** научно обоснованных закономерностей развития компьютерной преступности; специфики её причинного комплекса, а равно основных направлений деятельности субъектов профилактики 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; использовать данные судебной статистики и материалы судебной практики при разработке мер по усилению борьбы с преступностью.
		навыки информационно-аналитической работы в целях совершенствования профилактики компьютерной преступности и иных (малозначительных) правонарушений; навыками по составлению и презентации научно-обоснованных рекомендаций по борьбе с преступностью с последующим включением их в аналитические отчеты, записки информационные письма, справки, обзоры; навыками имплементации конкретных мероприятий в ведомственные планы по борьбе с преступностью исходя из объективной оценки оперативной обстановки на конкретном объекте или территории.

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: 14 часов (из них) 6 – лек, 8 – практ.), 94 – самостоятельная работа обучающихся;

Для заочной формы обучения с применением ЭО и ДОТ: 14 часов (из них) 6 – лек, 8 – практ.), 94 – самостоятельная работа обучающихся;

Место дисциплины, – Б1.В.ДВ.06.02 «Правовые основы борьбы с криминальными угрозами информационной безопасности» осваивается студентами уголовно-правовой специализации на:

- четвёртом курсе, седьмом семестре (по очной форме обучения);
- четвёртом курсе, седьмом семестре (по заочной форме обучения);
- четвёртом курсе, восьмом семестре (по заочной форме обучения с применением ЭО и ДОТ).

Дисциплина реализуется после изучения дисциплин:

На очной форме:

Б.1.Б.24. Криминология.

На заочной форме обучения, в т.ч. с применением ЭО и ДОТ:

Б.1.Б.24. Криминология.

3. Содержание и структура дисциплины.

Таблица 3.

№ п/п	Наименование тем (разделов)	Объём 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								
Тема 1.	Компьютерная преступность, как угроза информационной безопасности.	12	2		4		6	Опрос, реферат
Тема 2.	Уголовно-правовая характеристика преступных угроз информационной безопасности.	14	2		4		8	Опрос, реферат
Тема 3.	Качественные и количественные показатели компьютерной преступности в Российской Федерации.	16	2		4		10	Опрос, реферат
Тема 4.	Детерминация компьютерной преступности.	16	2		4		10	Опрос, эссе
Тема 5.	Личностные характеристики преступников, совершающих компьютерные преступления и их жертв.	16	2		4		10	Опрос, реферат
Тема 6.	Предупреждение компьютерной преступности.	16	2		4		10	Опрос, реферат
Тема 7.	Криминологическая характеристика и предупреждение отдельных видов (групп) компьютерных преступлений.	18	2		4		12	Опрос, реферат
								зачёт
Всего:		**108**	**14**		**28**		**66**	акад. час.
		3						зач. ед.
		81						астраном. 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)	Объём 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								
Тема 1.	Компьютерная преступность, как угроза информационной безопасности.	11	1		2		8	Диспут
Тема 2.	Уголовно-правовая характеристика преступных угроз информационной безопасности.	15	1				14	
Тема 3.	Качественные и количественные показатели компьютерной преступности в Российской Федерации.	13	1		2		10	контрольная работа
Тема 4.	Детерминация компьютерной преступности.	19	1				18	
Тема 5.	Личностные характеристики преступников, совершающих компьютерные преступления и их жертв.	19	1				18	
Тема 6.	Предупреждение компьютерной преступности.	11	1		2		8	контрольная работа
Тема 7.	Криминологическая характеристика и предупреждение отдельных видов (групп) компьютерных преступлений.	20			2		18	опрос
								зачёт
Всего:		**108**	**6**		**8**		**94**	акад. час.
		3						зач. ед.
		81						астраном. 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

Таблица 5.

№ п/п	Наименование тем (разделов)	Объём дисциплины, час.						Форма текущего контроля успеваемости[5], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРС	
			л/эо, дот[6]	лр/эо, дот[3]	пз/эо, дот[3]	КСР		
Заочная форма обучения с применением технологий ДО								
Тема 1.	Компьютерная преступность, как угроза информационной безопасности.	11	1		2		8	реферат
Тема 2.	Уголовно-правовая характеристика преступных угроз информационной безопасности.	15	1				14	
Тема 3.	Качественные и количественные показатели компьютерной преступности в Российской Федерации.	13	1		2		10	
Тема 4.	Детерминация компьютерной преступности.	19	1				18	Реферат
Тема 5.	Личностные характеристики преступников, совершающих компьютерные преступления и их жертв.	19	1				18	
Тема 6.	Предупреждение компьютерной преступности.	11	1		2		8	Тестирование
Тема 7.	Криминологическая характеристика и предупреждение отдельных видов (групп) компьютерных преступлений.	20			2		18	
								зачёт
Всего:		**108**	**6**		**8**		**94**	акад. час.
		3						зач. ед.
		81						астраном. час

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

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

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Компьютерная преступность, как угроза информационной безопасности.

Понятие компьютерной преступности. История возникновения и развития данного социального феномена. Уголовно-правовая обусловленность (общественная опасность), современных видов компьютерных преступлений. Место в общей структуре современной преступности.

Типология компьютерной преступности. Понятия информационной и корыстной компьютерной преступности.

Тема 2. Уголовно-правовая характеристика преступных угроз информационной безопасности.

Информационная безопасность, как объект уголовно-правовой защиты. Понятие правовых методов обеспечения информационной безопасности. Уголовно-правовые способы обеспечения информационной безопасности.

Тема 3. Качественные и количественные показатели компьютерной преступности в Российской Федерации.

Объём и распространённость. Динамика. Структура. Цена. География компьютерной преступности. Основные тенденции компьютерной преступности в России и за рубежом.

Латентность отдельных видов (групп) компьютерных преступлений.

Тема 4. Детерминация компьютерной преступности.

Структура причинного комплекса компьютерной преступности. Условия компьютерной преступности. Специальные причины компьютерной преступности. Типичные особенности механизма индивидуального преступного поведения в рамках отдельных видов (групп) компьютерных преступлений.

Тема 5. Личностные характеристики преступников, совершающих компьютерные преступления и их жертв.

Особенности личности преступника, совершившего компьютерное преступление. Структура их личности. Типология компьютерных преступников. Особенности личности жертвы компьютерных преступлений. Типология жертв компьютерных преступлений.

Тема 6. Предупреждение компьютерной преступности.

Содержание деятельности по предупреждению компьютерной преступности. Система мер предупреждения. Субъекты предупреждения компьютерной преступности, основные направления их деятельности и специфика реализуемых мер по предупреждению компьютерной преступности. Участие общественности в предупреждении компьютерной преступности.

Тема 7. Криминологическая характеристика и предупреждение отдельных видов (групп) компьютерных преступлений.

Корыстная компьютерная преступность и её специфические причины на территории Российской Федерации. Специальное предупреждение корыстной компьютерной преступности.

Информационная компьютерная преступность и её специфические причины на территории Российской Федерации. Специальное предупреждение информационной компьютерной преступности.

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.06.02 «Правовые основы борьбы с криминальными угрозами информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся (очная и заочная формы обучения):

Таблица 5.

Для проведения занятий по очной и заочной формам обучения, в т.ч. с применением технологии ЭО и ДО		
Тема (раздел)		**Методы текущего контроля успеваемости**
11	Компьютерная преступность, как угроза информационной безопасности.	Опрос, реферат; диспут;
22	Уголовно-правовая характеристика преступных угроз информационной безопасности.	Опрос, реферат
33	Качественные и количественные показатели компьютерной преступности в Российской Федерации.	Опрос, реферат; контрольная работа
44	Детерминация компьютерной преступности.	Опрос, эссе; реферат
55	Личностные характеристики преступников, совершающих компьютерные преступления и их жертв.	Опрос, реферат
66	Предупреждение компьютерной преступности.	Опрос, реферат; контрольная работа; тестирование
77	Криминологическая характеристика и предупреждение отдельных видов (групп) компьютерных преступлений.	Опрос, реферат

4.1.2. зачёт проводится с применением следующих методов (средств): устное собеседование, либо письменные ответы на вопросы билета. Выбор метода оценивания для традиционной формы обучения осуществляет преподаватель, информировав обучающихся в день проведения консультации к зачёту.

4.2. Материалы текущего контроля успеваемости.

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

Тема 1. Компьютерная преступность, как угроза национальной безопасности.

Примерный перечень вопросов для проведения практического занятия в виде опроса:

1) Дайте понятие информационной безопасности в соответствии с информационным правом.
2) Понятие информационной безопасности согласно Указа Президента РФ «Об утверждении Доктрины информационной безопасности РФ».
3) Обозначьте три направления обеспечения информационной безопасности.
4) Право на информацию (в т.ч. распространяемую посредством информационно-коммуникативных технологий) в конституционном и международном праве.
5) Каким образом (по каким причинам, в силу каких обстоятельств) сложилось понимание компьютерной преступности в «узком» и «широком» смыслах?

Примерный перечень тем для подготовки рефератов:

1) Компьютерная преступность в банковской сфере: основные направления уголовно-правовой политики в Российской Федерации.
2) Безопасность и компьютерная преступность в Германии.
3) Компьютерная преступность как правовая категория и социальное явление.
4) Компьютерная преступность и виды компьютерных преступлений.

Перечень дискуссионных вопросов для проведения диспута по теме практического занятия:

1) Компьютерная преступность в современной России: проблемы определения понятия.
2) Компьютерная преступность как угроза международной безопасности.
3) Подходы к определению компьютерной преступности.
4) Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны.

Тема 2. Уголовно-правовая характеристика преступных угроз информационной безопасности.

Примерный перечень вопросов для проведения практического занятия в виде опроса:

1) Что является объектом преступления в составах преступления, предусмотренных ст.ст. 272, 273, 274 УК РФ?
2) Истолкуйте понятие компьютерной информации, как предмета преступления.
3) Истолкуйте вредоносную программу, как предмет преступления.
4) В каких случаях завладение денежными средствами с использованием банковской карты должно быть квалифицировано как кража?
5) В каких случаях завладение денежными средствами с использованием банковской карты должно быть квалифицировано как мошенничество?
6) Какие спорные вопросы существуют в определении момента окончания хищения с использованием ЭПС, банковских карт?
7) Какие составы преступлений в структуре особенной части УК РФ (1996 г.) можно отнести к корыстным компьютерным преступлениям?
8) Что является объектом корыстных компьютерных преступлений?
9) Какие особенности квалификации завладения денежными средствами полученными посредством банковских карт, через АТМ-банкинг существуют?
10) Какими тремя способами возможно совершить компьютерное мошенничество и мошенничество с использованием электронных средств платежа?

Примерный перечень тем для подготовки рефератов:

1) Компьютерная преступность, или криминальный интернет: особенности уголовной ответственности
2) Способы совершения, предусмотренного ст. 272 УК РФ.
3) Способы совершений, предусмотренного ст. 273 УК РФ.
4) Вредоносные последствия объективной стороны состава преступлений, предусмотренных ст. 272 УК РФ.

Тема 3. Качественные и количественные показатели компьютерной преступности в Российской Федерации.

Примерный перечень вопросов для проведения практического занятия в виде опроса:
1) Охарактеризуйте степень латентности отдельных видов компьютерной преступности.
2) Охарактеризуйте раскрываемость преступлений, совершаемых в сфере высоких технологий (телекоммуникаций).
3) Охарактеризуйте динамику российской компьютерной преступности.
4) Охарактеризуйте структуру российской компьютерной преступности.

Примерный перечень тем для подготовки рефератов:
1) Теоретические основы и социальная обусловленность профилактики латентной компьютерной преступности.
2) География неправомерного доступа к охраняемой законом компьютерной информации.
3) География компьютерного мошенничества.
4) География создания, использования или распространения вредоносных компьютерных программ.

Приблизительная тематика (практических заданий) для выполнения контрольных работ:
1) Дайте определение компьютерной преступности. Каким составом преступления предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации?
2) Проведите типологию компьютерной преступности. Каким составом преступления предусмотрена уголовная ответственность за создание вредоносных компьютерных программ?

Тема 4. Детерминация компьютерной преступности.

Примерный перечень вопросов для проведения практического занятия в виде опроса:
1) Причины компьютерной преступности в современной России.
2) Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации.
3) Социальная зависимость как одна из причин развития компьютерной преступности.
4) Влияние компьютерных игр на насильственную преступность несовершеннолетних.
5) Как подразделяются причины компьютерной преступности по механизму действия?
6) Как подразделяются причины компьютерной преступности по уровню действия?
7) Как соотносятся между собой условия и причины компьютерной преступности?
8) Какими видами социальной связи характеризуются детерминанты компьютерной преступности?

Примерный перечень тем для подготовки рефератов:
1) Специфичные черты и факторы, обуславливающие рост компьютерной преступности (преступности в сфере компьютерной информации).
2) Характеристика направленности компьютерной преступности в условиях современного мира.
3) Структура и состояние компьютерной преступности в Российской Федерации.
4) Причины и условия профессиональной компьютерной преступности.

Примерный перечень тем для написания эссе по дисциплине:
1) Борьба с компьютерной преступностью в Японии.
2) Безопасность и компьютерная преступность в Германии.
3) Современное состояние преступности в сфере компьютерного мошенничества в Чили.
4) Международно-правовое сотрудничество государств - участников СНГ в борьбе с преступностью в сфере компьютерной информации.

Тема 5. Личностные характеристики преступников, совершающих компьютерные преступления и их жертв.

Примерный перечень вопросов для проведения практического занятия в виде опроса:
1) Опишите структуру личности интернет-мошенника.
2) Опишите структуру личности информационного преступника.
3) Какие социально-демографические признаки личности характерны для личности корыстного компьютерного преступника.
4) Какие нравственно-психологические признаки личности характерны для личности корыстного компьютерного преступника.
5) Какие социально-демографические признаки личности характерны для жертвы корыстных компьютерных преступлений.

Примерный перечень тем для подготовки рефератов:
1) Субкультура хакеров и другие факторы компьютерной преступности.
2) Виктимологические проблемы компьютерной преступности.
3) Криминологическая характеристика личности киберпреступника.
4) Должностные лица в качестве субъекта транснационального компьютерного преступления.
5) Криминологическая характеристика лиц, совершающих преступления в сфере компьютерной информации.
6) Кибер-преступность и виктимизация женщин.
7) Криминологический портрет личности кибертеррориста.
8) Организационные аспекты виктимологической профилактики преступлений, совершаемых с использованием информационных технологий.
9) Личность компьютерного преступника в современной России.

Тема 6. Предупреждение компьютерной преступности.

Примерный перечень вопросов для проведения практического занятия в виде опроса:
1) какие основные группы мер предупреждения компьютерной преступности выделяются?
2) какие меры предупреждения относят к деятельности по совершенствованию действующего уголовного законодательства?
3) какие меры предупреждения относят к деятельности по совершенствованию судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации?
4) какие меры предупреждения относят к деятельности по совершенствованию международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбе с ними?
5) какие меры предупреждения относят к деятельности по совершенствованию информационного законодательства?
6) какие меры предлагаются в качестве специальных духовно-культурных в деле предупреждения компьютерной преступности?
7) какие меры предлагаются в качестве организационно-управленческих в деле предупреждения компьютерной преступности?

Примерный перечень тем для подготовки рефератов:

1) Компьютерная преступность в России: состояние и перспективы совершенствования законодательства.
2) Международно-правовое сотрудничество государств - участников СНГ в борьбе с преступностью в сфере компьютерной информации.
3) Безопасность и компьютерная преступность в Германии.
4) Предупреждение компьютерной преступности в российской федерации: интегративный и комплексный подходы.
5) Особенности оперативно-розыскного противодействия компьютерной преступности
6) Некоторые вопросы борьбы с преступностью в сфере телекоммуникаций и компьютерной информации.
7) Правовое обеспечение международной борьбы с преступностью в глобальных компьютерных сетях.
8) Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий.

Приблизительная тематика (практических заданий) для выполнения контрольных работ:
1) Правовое обеспечение международной борьбы с преступностью в глобальных компьютерных сетях.
2) Особенности реализации в России международного опыта по защите от корыстных преступлений, совершаемых в киберпространстве.
3) Деятельность Интерпола по координации сотрудничества в борьбе с преступностью в сфере высоких технологий.
4) Предложения по профилактике совершения правонарушений и преступлений в информационной сфере, отнесенных к предметам ведения законодательства субъектов Российской Федерации.

Примеры тестовых вопросов по указанной теме:

01. Структура компьютерной преступности в «широком смысле» сегодня может быть представлена тремя подвидами (блоками):
☐ Преступления против информационной безопасности;
☐ Преступления, в которых электронная информация является средством совершения другого преступления;
☐ Преступления, где компьютеры используются для донесения «визуализации» информации до жертвы;
(выберите один правильный вариант ответа).

02. Динамика компьютерной преступности последних лет характеризуется двумя противоположными тенденциями:
☐ Отрицательным темпом роста преступлений в сфере компьютерной информации
☐ Отрицательным темпом роста корыстных компьютерных преступлений;
☐ Положительным темпом роста корыстных компьютерных преступлений;
☐ Положительным темпом роста преступлений в сфере компьютерной информации;
(выберите несколько правильных вариантов ответа).

Тема 7. Криминологическая характеристика и предупреждение отдельных видов (групп) компьютерных преступлений.

Примерный перечень вопросов для проведения практического занятия в виде опроса:
1) Предупреждение хищений, совершенных с использованием интернет-технологий.
2) Предупреждение мошенничества в социальных сетях.
3) Криминологические проблемы создания российской системы борьбы с преступлениями в сфере высоких технологий.
4) Проблемы противодействия преступности в сфере цифровой экономики.
5) Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет.

Примерный перечень тем для подготовки рефератов:
1) Профессиональная компьютерная преступность и мошенничество.

2) Компьютерная преступность в банковской сфере: основные направления уголовно-правовой политики в Российской Федерации.
3) Влияние компьютерных игр на насильственную преступность несовершеннолетних.
4) Организованная преступность и информационное пространство глобальных компьютерных сетей.
5) Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества.
6) Этнический аспект в компьютерной преступности.
7) Борьба с преступностью в компьютерных сетях "глубинного" Интернета.

4.3. Оценочные средства 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 7.

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	Очная форма обучения – ПК-12.2	Способность использовать криминологические знания для выявления причин и условий компьютерной преступности и конкретных преступлений.
		Заочная форма обучения – ПК-12.2 Заочная форма обучения с применением ЭО и ДОТ – ПК-12.2	Способность использовать криминологические знания для выявления причин и условий компьютерной преступности и конкретных преступлений.

Таблица 8.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
Очная и заочная форма обучения в т.ч. с применением ЭО и ДОТ		
ПК-12.2. Способность использовать криминологические знания для выявления причин и условий компьютерной преступности и конкретных преступлений.	Объясняет существующие закономерности развития преступности в российском обществе на основе научных фактов.	Способен **внятно изложить** содержание научных фактов, установленных современной криминологией и **объяснить** какой совокупностью методов данный результат был получен.
	Использует эмпирические факты для обоснования собственной позиции в решении проблем предупреждения преступности.	В ответе **обосновывает научную и практическую целесообразность** конкретных профилактических мер по отношению к конкретному виду преступности **исходя из** требований: законности, научности, экономической и социальной целесообразности.
	Использует междисциплинарные методы для решения прикладных задач в деятельности по предупреждению преступности.	**Представляет** самостоятельную качественную и количественную оценку состояния преступности в Российской Федерации на основании принятых в криминологии показателей (индикаторов).
	Владеет методикой прогнозирования индивидуального преступного поведения	**Даёт правильную личностную характеристику** виновному / осуждённому (исходя из смоделированной учебной ситуации).

Критерии оценивания:

Таблица 9. Шкала оценивания ответа на каждый из вопросов экзаменационного билета

Зачет	Экзамен (5-балльная шкала)	Критерии оценки
незачтено	2	Не может привести в пример научно обоснованных закономерностей развития преступности; не владеет криминологической терминологией; не ориентируется в системе курса криминологии при попытке раскрыть конкретный вопрос применительно к какому-либо разделу учебной дисциплины.
зачтено	3	Понимает содержание основных криминологических терминов; способен привести примеры научно обоснованных закономерностей развития преступности; имеет общее представление о теоретических вопросах контрольного задания (билета); затрудняется решить практическую задачу либо делает это поверхностно с использованием бытовых соображений.
	4	Владеет криминологической терминологией в полной мере; способен привести примеры научно обоснованных закономерностей развития преступности; имеет детальное представление о теоретических вопросах контрольного задания (билета); допускает ошибки в решении практической задачи, либо не может объяснить механизм действия избранных профилактических мер применительно к описанной в задании ситуации.
	5	В состоянии выявить все закономерности причинного комплекса конкретного вида преступности и коррелирующих с ней иных (малозначительных) правонарушений в соответствии с имеющимися в правоохранительной практике сведениями о состоянии преступности на объекте или территории; имеет детальное представление о теоретических вопросах контрольного задания (билета); избирает верные, научно обоснованные профилактические методы и обосновывает эффективность и результативность их применения в конкретной ситуации.

4.3.2. Типовые оценочные средства.

Полный перечень вопросов и заданий находится на кафедре Уголовного права и процесса.

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ К ЗАЧЁТУ

1. Кратко охарактеризуйте документальный метод; приведите пример возможного использования этого метода в криминологическом исследовании.
2. Какие показатели характеризуют качественную, а какие количественную стороны компьютерной преступности?
3. Кратко охарактеризуйте метод анкетирования, приведите пример возможного использования этого метода в криминологическом исследовании.
4. Кратко охарактеризуйте метод интервьюирования; приведите пример возможного использования этого метода в криминологическом исследовании.
5. Назовите основные криминологические показатели компьютерной преступности и укажите, как они рассчитываются.
6. Как рассчитывается коэффициент преступности и какие преимущества по сравнению с другими относительными величинами он имеет?
7. Какова научная и практическая значимость установления причин и условий компьютерной преступности?
8. В чем заключается уровневый подход к определению причин и условий компьютерной преступности?
9. Назовите малые социальные группы, в которых формируется личность компьютерного преступника.

4.4. Методические материалы промежуточной аттестации.

Промежуточная аттестация по дисциплине осуществляется в форме зачёта. В этих целях реализованы специальные аттестационные задания (билеты) в которых содержатся конкретные вопросы и задания для проверки усвоения студентами, 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 трёх 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).

Пример.

БИЛЕТ № 1 (ПРИМЕР).

1. Структура личности преступника. *Теоретический вопрос. Направлен на проверку знаний студента относительно выделения основных криминогенных характеристик личности;*

2. Прочтите описание преступного поведения. Проанализируйте криминогенную ситуацию и личность преступника. Возможно ли было предотвратить это преступление?

Трифонов работал на таможне. Он не любил азартные игры. Может быть, потому, что чувствовал: стоит только начать – потом не остановишься. Так оно и произошло. В казино он проиграл 6 тысяч долларов. Необходимо было как можно быстрее заплатить проигрыш, но таких денег у него не было. Выход Трифонову предложили уже на

следующий день: «У нас к вам просьба. Не нужно завтра слишком тщательно осматривать фургон с таким-то гос. номером. А если что-нибудь там увидите «такое», сделайте вид, что все в порядке. Ваша доля – 10 тысяч долларов». Через неделю Трифонову подарили видеофильм. Где был записан этот разговор и факт передачи денег. Так таможенный инспектор стал сотрудничать с наркомафией.

Данный вопрос позволит выявить умение студента правильно оценить криминогенную ситуацию и выбрать наиболее оптимальный и с правовой точки зрения законный способ устранения криминальных рисков;

3. Система мер по предупреждению компьютерной преступности. Позволяет выявить конкретные навыки студента по планированию мер предупреждения компьютерных преступлений в деятельности специальных субъектов предупреждения компьютерной преступности, когда студент показывает экзаменатору навыки применения в конкретной ситуации мер по обеспечению законности и правопорядка.

Для студентов, обучающихся на заочной форме обучения с применением ЭО и ДОТ выполнение письменного контрольного задания позволяет оценить умения и навыки по дисциплине и осуществляется в течении семестра.

Проверка знаний также осуществляется с помощью тестовых заданий. Тестирование проводится в СДО "Прометей" в соответствии с установленными требованиями. Итоговый тест формируется на аппаратном уровне с использованием банка тестовых заданий по дисциплине. Проверка результатов тестирования осуществляется автоматически.

Алгоритм расчета итоговой оценки студентов, обучающихся на заочной форме обучения с применением ЭО и ДОТ, установлен «Регламентом о системе оценивания знаний обучающихся по дисциплинам учебного модуля по образовательным программам с применением электронного обучения на факультете заочного и дистанционного обучения Сибирского института управления-филиала РАНХиГС».

5. Методические указания для обучающихся по освоению дисциплины.

Учебным планом предусмотрено изучение курса «Правовые основы борьбы с криминальными угрозами информационной безопасности» в объеме 108 академических часов. Изучение курса осуществляется в одном семестре и заканчивается экзаменом.

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. 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.

5.2. Устный опрос по разделам дисциплины на практических занятиях.

Криминология по своей сути наука прикладная, призванная решать конкретные вопросы уголовной юстиции и ряд более широких проблем в области организации борьбы с преступностью, вплоть до выработки целостной уголовной политики государства. В этой связи организация практических занятий является неотъемлемой частью образовательного процесса и этапом освоения новых знаний для применения в повседневной деятельности юриста.

Практическое занятие – это хорошая возможность обучить студента не только теоретическим положениям дисциплины, но и элементам правовой социализации, профессиональной подготовленности, деловой коммуникации, умению дискутировать, уверенности достойно держаться в кругу правоведов. И те часы, которые отведены студенту для этого, необходимо использовать с максимальной пользой.

Тематический план дисциплины позволяет проводить практические занятия по целым разделам криминологии, объединяющим в себе несколько лекционных тематик. Тем самым в изучении отдельных вопросов достигается системное единство.

Каждое практическое занятие обусловлено определенной темой. При изучении той или иной темы в обязательном порядке применяется проблемный метод, что ориентирует студента на дискуссию. Проблема – это практический вопрос, требующий ответа. На его поиски и ориентирована работа участников практического занятия.

Любое практическое занятие в соответствии с предлагаемой тематикой имеет ряд ключевых вопросов, составляющих план практического занятия. Вопросы сгруппированы в два последовательных блока: для проверки остаточных знаний используются контрольные (проверочные) вопросы, далее следуют проблемные (дискуссионные) вопросы.

5.3. Тестирование и оценка результатов.

Тестирование как методика контроля качества подготовки специалистов получило признание и широкое распространение в деятельности высшей школы, особенно в последние годы, когда вопрос о выборе объективных критериев контроля качества встал особенно остро.

Кроме собственно знаний, тесты позволяют проверить сформированность умений и навыков студентов по конкретным разделам (темам) криминологии.

Тестовые задания, составленные в целом по всему объему учебной дисциплины, дают возможность получить обобщенный срез знаний по всем аспектам и темам изученного курса, в то время как в традиционной системе проверки знаний студентов по экзаменационным билетам присутствует элемент случайности, выборочности (как правило, билет ограничивается 2–3-мя вопросами).

Наконец, по сравнению с устным опросом, тестирование существенно экономит время, отводимое на контроль знаний студентов. Для заочного обучения в условиях предельного ограничения количества аудиторных часов тестирование часто является единственной возможностью формирования достаточно объективной оценки знаний студентов.

Однако следует учесть, что овладение методикой тестирования требует дополнительной работы со студентами, направленной на формирование умений отвечать на тест. Для успешного прохождения тестирования важно умение концентрироваться, выделять главное, сущностное в вопросе. Кроме того, следует обращать внимание и на формулировку вопроса. Ведь в практике тестирования бывают и вопросы, задаваемые «от противного».

В рамках дисциплины «криминология» тестирование проводится по специально разработанным тематическим тестам (в соответствии с разделами дисциплины), аттестационно-модульным тестам (построенным по модульной схеме изучения дисциплины), итоговым тестам. Итоговые и модульные тесты в случае необходимости

могут быть использованы для проведения промежуточной аттестации студента по дисциплине.

Каждый тест представляет собой совокупность вопросов (15-20) по изученным темам на бланке формата А4. Для ответа на поставленные вопросы студентам даётся 20 минут. Тест является закрытым. На каждый вопрос даётся определённое количество вариантов ответа (2-4) из которых, только один является правильным. Напротив правильного ответа (в специальном квадратике) необходимо проставить знак (галочка, крестик). Записи, отметки делаются в тесте шариковой, гелевой ручкой синего, фиолетового, зеленого цветов. Использование ручек с красной, черной пастой, карандашей, фломастеров, маркеров запрещено.

Исправления в тестах (в т.ч. с помощью корректора) запрещены, ответ на вопрос в таком случае засчитывается как неправильный.

Для оценки результатов тест должен быть подписан студентом. Оценка результатов проводится по следующим критериям: все ответы даны правильно – отлично; 1-2 ошибки в тесте – хорошо; 3-4 ошибки – удовлетворительно; в остальных случаях – неудовлетворительно.

5.4. Методические рекомендации по освоению дисциплины для обучающихся заочной формы с применением ЭО, ДОТ.

Обучающиеся участвуют в вебинаре по дисциплине (режим off-line). В случае, если студент не имеет возможность присутствовать на вебинаре в режиме off-line, он может просмотреть запись вебинара, размещенную в СДО "Прометей".

Студенты осуществляют самостоятельное изучение учебно-методических материалов, размещенных в библиотеке СДО "Прометей", внешних электронных библиотеках или доступных обучающемуся по месту жительства. В процессе изучения выделяют вопросы, вызывающие затруднения. Возникшие у обучающихся вопросы они могут задать преподавателю дисциплины на вебинаре в режиме off-line. Задать вопросы можно также через преподавателя-тьютора, закрепленного за потоком с целью оказания организационно-методической помощи обучающимся. В этом случае преподаватель может ответить на них либо с использованием форума СДО "Прометей", либо передать ответ через преподавателя-тьютора.

Участие в электронном семинаре и тестирование в режиме «самопроверка» позволяет студенту определить степень усвоения необходимого объема материала по дисциплине.

В ходе проверки результатов выполнения заданий текущего контроля успеваемости (электронного семинара) преподаватель обобщает и комментирует работу студента, что позволяет студенту скорректировать самостоятельное изучение дисциплины, обратить внимание на часто допускаемые ошибки и устранить пробелы в знаниях.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине.

6.1. Основная литература.

1. Морозов А.В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс]: учебник для магистров и аспирантов/ А.В. Морозов, Л.В. Филатова, Т.А. Полякова— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 604 с.— Режим доступа: http://www.iprbookshop.ru/66771.html .— ЭБС «IPRbooks».

2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/

С.В. Петров, П.А. Кисляков— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html .— ЭБС «IPRbooks».

3. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html .— ЭБС «IPRbooks».

4. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В. Прохорова— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.html .— ЭБС «IPRbooks».

5. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks».

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