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 гражданского права и процесса

УТВЕРЖДЕНА
кафедрой гражданского права и процесса
Протокол от 29.08.2017 г.№1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ ТОРГОВЛИ

М.В.ДВ.1.1.

ОБЭТ
краткое наименование дисциплины

по направлению подготовки: 40.04.01 Юриспруденция

Направленность (профиль): «Правовое обеспечение предпринимательской деятельности»

квалификация выпускника: Магистр

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 гражданского права и процесса:
канд.юрид.наук, доцент, доцент кафедры гражданского права и процесса,
Войтович Елена Павловна

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 ……	9
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 ……..	24
6.1. Основная литература ……..	24
6.2. Дополнительная литература ……..	25
6.3. Учебно-методическое обеспечение самостоятельной работы …….....	26
6.4. Нормативные правовые документы ……..	27
6.5. Интернет-ресурсы ……...	27
6.6. Иные источники ……..	27
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы ……	28

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

Дисциплина М.В.ДВ.1.1. «Обеспечение безопасности электронной торговли» обеспечивает овладение следующими компетенциями:

Таблица 1.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-3	Готовностью к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства	Очная форма обучения – ПК-3.2.	Способность обеспечить противодействие правонарушениям в рамках своей профессиональной деятельности
		Заочная форма обучения – ПК 3.3.	Способность обеспечить противодействие правонарушениям в рамках своей профессиональной деятельности
ПК-4	Способность выявлять, пресекать, раскрывать и расследовать правонарушения и преступления	Очная форма обучения – ПК-4.2.	Способность устанавливать применимые меры по выявлению, пресечению и раскрытию различных видов правонарушений и преступлений, определять методики расследования отдельных видов правонарушений и преступлений
		Заочная форма обучения – ПК-4.3.	Способность определять методики расследования отдельных видов правонарушений и преступлений
ПК-5	Способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению	Очная форма обучения – ПК-5.2.	Способность к профилактике преступлений и правонарушений.
		Заочная форма обучения – ПК-5.3.	Способность к профилактике преступлений и правонарушений.

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

Таблица 2.

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	ПК-3.2.	умение определять оптимальные способы обеспечения законности и правопорядка, применимые в конкретной ситуации
	ПК-3.3.	умение определять оптимальные способы обеспечения законности и правопорядка, применимые в конкретной ситуации

	ПК-4.2.	умение определять методики расследования отдельных видов преступлений и иных правонарушений
	ПК-4.3.	умение определять методики расследования отдельных видов преступлений и иных правонарушений
	ПК-5.2.	Знаний основных должностных обязанностей субъектов профилактики правонарушений, лиц, участвующих в профилактике правонарушений, и принимаемых ими мер профилактики правонарушений; Умения определять оптимальные меры правового, организационного, информационного и иного характера, направленные на выявление и устранение причин и условий, способствующих совершению экономических преступлений и правонарушений; Навык применения мер по внесению представлений об устранении причин и условий, способствующих совершению правонарушения
	ПК-5.3.	Знаний основных должностных обязанностей субъектов профилактики правонарушений, лиц, участвующих в профилактике правонарушений, и принимаемых ими мер профилактики правонарушений; Умения определять оптимальные меры правового, организационного, информационного и иного характера, направленные на выявление и устранение причин и условий, способствующих совершению экономических преступлений и правонарушений; Навык применения мер по внесению представлений об устранении причин и условий, способствующих совершению правонарушения

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

Объём дисциплины:

общая трудоемкость дисциплины в зачётных единицах составляет **3** З.Е.

Количество академических часов, выделенных:

для очной формы обучения: 16 часов (из них 4 – лек, 12 – практ.), 92 – самостоятельная работа обучающихся;

для заочной формы обучения: 24 часа (из них 4 – лек, 20 – практ.), 84 – самостоятельная работа обучающихся.

Возможно изучение дисциплины по всем формам обучения с применением электронного обучения и дистанционных образовательных технологий. При этом сохраняется объем контактной и самостоятельной работы по дисциплине в соответствии с учебным планом.

Место дисциплины, – М.В.ДВ.1.1. *«Обеспечение безопасности электронной торговли»* осваивается магистрантами на:

- втором курсе, третьем семестре (по очной форме обучения);
- втором курсе, четвёртом семестре; заканчивается на третьем курсе, пятом семестре (по заочной форме обучения);

Дисциплина реализуется после изучения дисциплин:

	На очной форме обучения:
М2.Б.4	Актуальные проблемы теории права
М3.П.2	Юридическое консультирование
	На заочной форме обучения:

М2.Б.4	Актуальные проблемы теории права
М3.П.2	Юридическое консультирование

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	**Криминальные риски электронной торговли**							Написание эссе по итогам изучения раздела
Тема 1.1	*Классификация и содержание рисков электронной торговли*	24	1	-	2	-	20	Устное обсуждение отдельных вопросов из перечня самоконтроля.
Тема 1.2.	*Правоохранительная деятельность в сфере обеспечения законности в электронной торговле*	24	1	-	2	-	22	Устное обсуждение отдельных вопросов из перечня самоконтроля.
Раздел 2	**Стратегия обеспечения законности и противодействия правонарушениям в сфере электронной торговли**							Написание эссе по итогам изучения раздела
Тема 2.1	*Обеспечение законности предпринимательской деятельности в условиях пробельности российского законодательства в сфере электронной торговли*	24	1	-	2	-	22	Разбор ситуационных задач.
Тема 2.2.	*Организация предупреждения правонарушений в сфере электронной торговли в правоохранительной деятельности*	36	1	-	6	-	28	Разбор ситуационных задач.
	Промежуточная аттестация							**Зачёт**
	Всего:	**108**	**4**	**-**	**12**	**-**	**92**	акад. 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

		3						зач. ед.
		81						астр. час

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	**Криминальные риски электронной торговли**							Написание эссе по итогам изучения модуля
Тема 1.1	*Классификация и содержание рисков электронной торговли*	**26**	2	-	6	-	18	Устное обсуждение отдельных вопросов из перечня самоконтроля.
Тема 1.2.	*Правоохранительная деятельность в сфере обеспечения законности в электронной торговле*	**24**	-	-	4	-	20	Устное обсуждение отдельных вопросов из перечня самоконтроля.
Раздел 2	**Стратегия обеспечения законности и противодействия правонарушениям в сфере электронной торговли**							Написание эссе по итогам изучения модуля
Тема 2.1	*Обеспечение законности предпринимательской деятельности в условиях пробельности российского законодательства в сфере электронной торговли*	**24**	-	-	4	-	20	Разбор ситуационных задач.
Тема 2.2.	*Организация предупреждения правонарушений в сфере электронной торговли в правоохранительной деятельности*	**30**	2	-	6	-	22	Разбор ситуационных задач.
	Промежуточная аттестация	**4**					4	**Зачёт**
	Всего:	**108**	**4**	**-**	**20**	**-**	**84**	акад. час
		3						зач. ед.

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

		81						астр. час

Содержание дисциплины.

Тема 1. Классификация и содержание рисков электронной торговли.

Понятие криминальных рисков электронной торговли. Типология. Компьютерное мошенничество: «identity theft» с использованием электронных платежных систем. Традиционные мошеннические схемы в Интернет, совершаемые при помощи социального инжиниринга. Коммерческий шпионаж и незаконный доступ к компьютерной информации. Спекуляция на клиентоориентированности или «потребительский экстремизм». DDOS-атаки на коммерческую инфраструктуру интернет-торговли. Киберсквоттинг (англ. cybersquatting).

Незаконные организация и проведение азартных игр в Интернет как «сфера услуг». Незаконное предпринимательство в электронной торговле. Сбыт товаров и продукции без маркировки и (или) нанесения информации, предусмотренной законодательством Российской Федерации. Проблемы использования криптовалют в электронной торговле и государственная денежная эмиссия. Криминогенные особенности регулирования дистанционной торговли в РФ.

Причины и условия, существования указанных явлений и преступности в сфере электронной торговли в целом.

Тема 2. *Правоохранительная деятельность в сфере обеспечения законности в электронной торговле.*

Применение норм об уголовной ответственности к интернет-мошенникам. (ст. 159, 159.3, 159.6 УК). Иные хищения с использованием компьютерных технологий. Преступления против информационной инфраструктуры субъектов электронной торговли: ст. 272, 273, 274 УК. Нормы двойной превенции в административном законодательстве: разграничение недобросовестной рекламы и обмана потребителей в соответствии со ст. 14.3 КоАП РФ.

Тема 3. Обеспечение законности предпринимательской деятельности в условиях пробельности российского законодательства в сфере электронной торговли. .

Субъекты предупреждения правонарушений в сфере электронной торговли и их полномочия. Контроль и надзор в сфере электронной торговли. Самоорганизация интернет-сообщества в противодействии интернет-преступности.

Тема 4. Организация предупреждения правонарушений в сфере электронной торговли в правоохранительной деятельности.

Принципы безопасного использования облачных сервисов и построения офисной инфраструктуры коммерческой организации в целях предотвращения хищений компьютерной информации.

Проблемы правового регулирования деятельности интернет-агрегаторов в целях предупреждения обмана потребителей.

Кампания по реформе авторского права в цифровую эпоху в целях создания легального рынка электронного контента и борьбы с «пиратством».

Правовое регулирование импортозамещения программного обеспечения. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных.

Перспективы регулирования деятельности электронных платежных систем в целях противодействия легализации средств добытых преступным путем и финансирования терроризма.

Механизм реализации положений ФЗ «О персональных данных» в электронной торговле.

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 М.В.ДВ.1.1. «Обеспечение безопасности электронной торговли» используются следующие методы текущего контроля успеваемости обучающихся (очная, заочная формы обучения):

Таблица 5.

Тема (раздел)		Методы текущего контроля успеваемости
Р.1.	**Криминальные риски электронной торговли**	Написание эссе по итогам изучения модуля
Т.1.	*Классификация и содержание рисков электронной торговли*	Устное обсуждение отдельных вопросов из перечня самоконтроля.
Т.2.	*Правоохранительная деятельность в сфере обеспечения законности в электронной торговле*	Устное обсуждение отдельных вопросов из перечня самоконтроля.
Р.2.	**Стратегия обеспечения законности и противодействия правонарушениям в сфере электронной торговли**	Написание эссе по итогам изучения модуля
Т.3.	*Обеспечение законности предпринимательской деятельности в условиях пробельности российского законодательства в сфере электронной торговли*	Разбор ситуационных задач.
Т.4.	*Организация предупреждения правонарушений в сфере электронной торговли в правоохранительной деятельности*	Разбор ситуационных задач.

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

4.2. Материалы текущего контроля успеваемости.

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

4.2.1. Примерные вопросы для устного ответа на семинарских (практических) занятиях.

Раздел 1. «Криминальные риски электронной торговли».

Тема № 1.1. Классификация и содержание рисков электронной торговли.

Вопросы:

1. Раскройте содержание понятия: риски электронной торговли.
2. Приведете наиболее распространённые основания для классификации рисков во внутрироссийской и международной электронной торговле.
3. Проанализируйте содержание понятия «компьютерное мошенничество», характер и степень вреда, причиняемого им экономическим интересам.
4. Перечислите основные риски, существующие в области использования электронных платёжных систем и криптовалют при расчётах в электронной коммерции.

5. Дайте оценку состоянию и перспективам развития коммерческого шпионажа путём незаконного доступа к охраняемой законом компьютерной информации.
6. Проанализируйте эффект действия: положительные и отрицательные стороны «потребительского экстремизма» в сфере дистанционной розничной торговли.
7. Дайте правовую оценку современному состоянию рынка незаконных азартных игр в Интернет, с участием граждан Российской Федерации.

Тема № 1.2. Правоохранительная деятельность в сфере обеспечения законности в электронной торговли.

Вопросы:

1. Проведите анализ состава преступления, предусмотренного ст. 159.3 УК РФ.
2. Проведите анализ состава преступления, предусмотренного ст. 159.6 УК РФ.
2. Проведите анализ судебной практики по уголовным делам о мошенничестве (на примере Постановления Пленума Верховного Суда РФ от 27.12.2007 №51 "О судебной практике по делам о мошенничестве, присвоении и растрате").
3. Классифицируйте все известные в следственной практике способы совершения компьютерных хищений.
4. Осуществите разграничение составов правонарушений: недобросовестной рекламы и обмана потребителей в соответствии со ст. 14.3 КоАП РФ.
5. Проведите анализ состава преступления, предусмотренного ст. 272 УК РФ.
6. Проведите анализ состава преступления, предусмотренного ст. 273 УК РФ.
7. Проведите анализ состава преступления, предусмотренного ст. 274 УК РФ.

Раздел 2. «Стратегия обеспечения законности и противодействия правонарушениям в сфере электронной торговли».

Тема № 2.1. Обеспечение законности предпринимательской деятельности в условиях пробельности российского законодательства в сфере электронной торговли.

Вопросы:

1. Назовите причины и условия существования правонарушений в сфере электронной торговли в целом.
2. Перечислите основных субъектов предупреждения правонарушений в сфере электронной торговли.
3. Определите полномочия прокуратуры в сфере координации правоохранительной деятельности по обеспечению законности и предупреждению правонарушений в Интернет
4. Определите основные полномочия Бюро специальных технических мероприятии и его территориальных подразделений в сфере противодействия компьютерной преступности.
5. Перечислите основные принципы эффективного контроля в сфере электронной торговли.
6. Перечислите субъектов общей профилактики, непосредственно связанных с организацией и регулированием деятельности субъектов электронной торговли в России.
7. Приведите примеры самоорганизации интернет-сообщества в противодействии интернет-преступности.

Тема № 2.2. Организация предупреждения правонарушений в сфере электронной торговли в правоохранительной деятельности.

Вопросы:

1. Перечислите принципы безопасного использования облачных сервисов и построения офисной инфраструктуры коммерческой организации в целях предотвращения хищений компьютерной информации.
2. Обозначьте проблемы и возможные пути правового регулирования деятельности интернет-агрегаторов в целях предупреждения обмана потребителей.
3. Перечислите основные рекомендации по совершенствованию авторского права в цифровую эпоху в целях создания легального рынка электронного контента и борьбы с «пиратством».

4. Сформулируйте основные принципы деятельности по импортозамещению программного обеспечения.
5. Обозначьте перспективы регулирования деятельности электронных платежных систем в целях противодействия легализации средств добытых преступным путем и финансирования терроризма.
6. Какие профилактические меры должны быть реализованы в рамках положения ФЗ «О персональных данных» в электронной торговле.
7. Перечислите профилактические особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных.

4.2.2. Тематика эссе по дисциплине:

Раздел 1. «Криминальные риски электронной торговли».

1. Роль информационных технологий в развитии общества.
2. Использование информационных технологий в деятельности федеральных органов государственной власти.
3. Правовое регулирование создания и использования информационных технологий.
4. Информатизация судебной системы.
5. Борьба с информационным неравенством.
6. Нарушение порядка применения информационных технологий.
7. Возникновение и развитие среды глобальных компьютерных сетей.
8. Правовые пробелы в регулировании отношений по массовому распространению информации в российском сегменте сети Интернет.
9. Правонарушения, связанные с содержанием данных.

Раздел 2. «Стратегия обеспечения законности и противодействия правонарушениям в сфере электронной торговли».

1. Правовые проблемы налогообложения субъектов электронной экономической деятельности.
2. Электронная банковская деятельность.
3. Понятие и значение расчетных отношений в информационной среде.
4. Способы гражданско-правовой защиты авторских прав в Интернет.
5. Защита прав на доменные имена.
6. Государственная политика в области информационной безопасности.
7. Правовая защита личности от воздействия недостоверной информации.
8. Кибертерроризм, как один из способов ведения информационной войны.
9. Ответственность за нарушение законодательства о рекламе.
10. Особенности и свойства компьютерной информации в правовом смысле.
11. Международные правовые акты, регулирующие отношения в информационной сфере
12. Основные ограничения в рекламе.
13. Правовая охрана программ для ЭВМ и баз данных.
14. Особенности электронного документа
15. Преимущества и недостатки электронного документооборота.
16. Проблемы, связанные со спецификой передачи электронной почты.
17. Применение электронной цифровой подписи.
18. Вопросы юридической силы электронных документов и ее обеспечения.
19. Правовое обеспечение информационных систем по обработке персональных данных.
20. Правовое регулирование Интернет: проблемы и перспективы.
21. Виды правонарушений, совершаемых в электронной среде.

4.2.3. Примеры ситуационных (типовых) задач.

Задание 1. «Центр информационных услуг и технологий» разработал программный продукт для коммерческого банка «Нижний город». Затем передал этот продукт банку в соответствии с заключенным договором. Через некоторое время один из

авторов-разработчиков Николай Сударушкин был приглашен в банк для консультаций и доводки программы. Во время исполнения этих работ Николай решил усовершенствовать данную программу, для чего, пользуясь своими знаниями о ней, ввел некоторые изменения. Неожиданным побочным эффектом введения дополнительных команд стало то, что информация о каждой 5000-й операции, проводимой банком, не фиксировалась системой. В результате несколько физических лиц – клиентов банка, взяв деньги по электронным карточкам, обнаружили, что сумма на их электронных счетах осталась прежней, и взяли деньги повторно. Совокупный ущерб, причиненный банку (суммы, взятые клиентами, меры безопасности, изменение программного продукта), составил около 500 тыс. руб. Определите правонарушителей. Дайте квалификацию описанным действиям.

Задание 2. Организованной группой граждан были открыты 23 сайта, тематика которых связана с консалтингом экономического характера. На данных сайтах размещались информационные и аналитические материалы, обсуждался курс акции компании малой капитализации, давались советы, по поводу того, продавать или приобретать те или иные ценные бумаги. Авторы указанных материалов позиционировали себя в качестве авторитетных, независимых экспертов-экономистов. При этом они сами скупали акции, курс которых анализировали в своих статьях. По договоренности они одновременно начинали рекомендовать покупку акций определенных компаний с целью увеличения спроса, затем, когда инвесторы поднимали цену, перепродавали акции. Затем некоторые из виртуальных экономистов вступили в сговор с руководством компаний и рекомендовали их акции за определенную плату, но не упоминали об этих отношениях. Оцените ситуацию с точки зрения действующего законодательства. Можно ли привлечь к ответственности экономистов-консультантов?

Задание 3. В ходе приоритетной регистрации в доменной зоне: «РФ» регистратору поступили две заявки на регистрацию доменного имени компарк. РФ. Первая заявка поступила 26 ноября 2009 г от одноименной компании, оказывающей дизайнерские услуги владельцам садовых и парковых участков в течение 5 лет. Вторая заявка принадлежит фирме «Компарк», владеющей соответствующим товарным знаком и занимающейся продажей компьютеров и цифровой техники в течение 8 лет. Эта заявка поступила 9 декабря 2009 года. Какое решение должен принять регистратор?

Задание 4. В научной литературе, посвященной внедрению информационных технологий в сферу государственного и муниципального управления и их применению, высказывались следующие точки зрения:

1) информационные технологии представляют собой эффективный инструмент, с помощью которого можно повысить оперативность работы государственных органов, сократить издержки на содержание управленческого аппарата, осуществлять государственные услуги в более удобной для граждан форме. При этом принципы и содержание государственного управления остаются прежними;

2) применение информационных технологий необратимо влияет на процессы, в которых эти технологии используются. В случае использования информационных технологий для решения задач государственного и муниципального управления качественно изменяется взаимодействие общества и государства – вплоть до изменения соответствующих правоотношений. Как отмечают некоторые авторы, операции обмена информацией оптимизируются настолько, что происходит не просто экономия ресурсов и времени, а изменение даже принципов и традиций управления обществом.

С какой из них вы согласны? Аргументируйте свой ответ.

Задание 5. Блогер Сергей Петров на официальном сайт госзакупок обнаружил сведения о том, что директор одного из филиалов К-ского Технического университета собирается приобрести автомашину «Порше Кайенна» стоимостью 3 миллиона рублей. Посчитав, что такие траты учебного заведения являются необоснованными, Петров сообщил об этом на сайт Президенту РФ. Администрация Президента РФ направила указание Правительству региона проверить этот факт. Из управления по работе с обращениями граждан областного Правительства эту жалобу направили ректору технического

университета и по месту работы Сергея. Технический университет признал жалобу обоснованной и отказался от покупки автомобиля, о чем сообщил на своем сайте. Работодатель Петрова предложил ему уволиться по собственному желанию, пригрозив, что тот не пройдет ближайшую переаттестацию. Оцените действия должностных лиц. Было ли кем-то из них совершено правонарушение? Какая мера ответственности может быть применена? Окажите правовую помощь Петрову.

Задание 6. Андреев создал программу для ЭВМ, предназначенную для копирования компьютерной информации с одного машинного носителя на другие. После чего он на своем персональном компьютере, желая убедиться в работоспособности созданной им программы, ввел данные, позволяющие произвести рассылку 10 нецензурных текстовых сообщений одинакового содержания абоненту сети «Мегафон», привел программу в действие. Убедившись в работоспособности компьютерной программы, Андреев решил осуществить массовую рассылку сообщений нецензурного содержания всем абонентам Челябинского фрагмента сети «Мегафон» ЗАО «Уральский Джи Эс Эм».

Затем Андреев, пытаясь скрыть следы своей деятельности, используя известную ему информацию, с помощью своего персонального компьютера и модема зашел на свой сайт, размещенный в г. Санкт-Петербурге, и разместил там программу, в которую заложил текст сообщения нецензурного содержания. Затем он, не уведомляя собственника компьютерной информации о характере выполненных программой функций и не получив согласия на реализацию программой своего назначения, привел в действие программу, в которой была заложена функция автоматической рассылки сообщений. В результате 11261 абонент Челябинского фрагмента сети «Мегафон» ЗАО «Уральский Джи Эс Эм» получили сообщения нецензурного содержания, что привело нарушению сети ЭВМ ЗАО «Уральский Джи Эс Эм».

Квалифицируйте действия Андреева. Какое наказание ему может быть назначено?

Задание 7. На ряде сайтов в сети Интернет размещались ссылки на сайт muztelega.ru, на котором располагались «пиратские» копии чужих музыкальных произведений. В ходе следствия удалось установить личности только владельцев сайтов, где были размещены указанные ссылки. Но они заявили, что не имеют никакого отношения к сайту с «пиратскими» копиями, а ссылки размещали для привлечения внимания пользователей к своим сайтам. Совершили ли данные лица правонарушение? Являются ли действия лица, разместившего ссылку, воспроизведением, использованием, распространением, или обнародованием произведения?

Задание 8. Оператор ЭВМ одной из коммерческих организаций Ложкина, используя многочисленные сменные носители информации, получаемые от сотрудников других организаций, не всегда проверяла их на наличие «вирусов», доверяясь заверениям поставщиков о том, что «они чистые». В результате в компьютер Тройкиной была внесена программа-«вирус», что привело к утрате важнейшей информации и поставило на грань срыва важное мероприятие.

Задание 9. Бураков приобрел в магазине «Информтех» комплект дисков с пиратской игровой программой и, проверив ее на наличие «вирусов» (они обнаружены не были), установил на свой персональный компьютер. Спустя некоторое время работа компьютера была полностью заблокирована. Придя к выводу, что причиной тому новейший «вирус», которым поражена купленная им программа, Дударов продал комплект дисков через Интернет, утаив от него о некачественности «игрушки».

4.3. Оценочные средства для промежуточной аттестации.

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

Таблица 6.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-3	Готовностью к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства	Очная форма обучения – ПК-3.2.	Способность обеспечить противодействие правонарушениям в рамках своей профессиональной деятельности
		Заочная форма обучения – ПК 3.3.	Способность обеспечить противодействие правонарушениям в рамках своей профессиональной деятельности
ПК-4	Способность выявлять, пресекать, раскрывать и расследовать правонарушения и преступления	Очная форма обучения – ПК-4.2.	Способность устанавливать применимые меры по выявлению, пресечению и раскрытию различных видов правонарушений и преступлений, определять методики расследования отдельных видов правонарушений и преступлений
		Заочная форма обучения – ПК-4.3.	Способность определять методики расследования отдельных видов правонарушений и преступлений
ПК-5	Способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению	Очная форма обучения – ПК-5.2.	Способность к профилактике преступлений и правонарушений.
		Заочная форма обучения – ПК-5.3.	Способность к профилактике преступлений и правонарушений.

Таблица 9.

Этап освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
Очная форма обучения		
ПК 3.2. Способность обеспечить противодействие правонарушениям в рамках своей профессиональной деятельности	Разграничивает административные правонарушения и преступления	Правильно разграничивает административные правонарушения и преступления
ПК 4.2. Способность устанавливать применимые меры по выявлению, пресечению и раскрытию различных видов правонарушений и преступлений, определять методики расследования отдельных видов правонарушений и преступлений	Определяет перечень средств для раскрытия и расследования, предупреждения и пресечения готовящихся и совершаемых преступлений и иных правонарушений	Самостоятельно и обоснованно определяет перечень средств для раскрытия и расследования, предупреждения и пресечения готовящихся и совершаемых преступлений и иных правонарушений

ПК 5.2. Способность к профилактике преступлений и правонарушений.	Определяет содержание представления о принятии мер по устранению обстоятельств, способствовавших совершению преступления. Составляет план профилактических мероприятий в чётком соответствии с требованиями закона.	Верно определяет содержание представления о принятии мер по устранению обстоятельств, способствовавших совершению преступления. Составляет обоснованный план профилактических мероприятий в чётком соответствии с требованиями закона.
Заочная форма обучения		
ПК 3.3. Способность обеспечить противодействие правонарушениям в рамках своей профессиональной деятельности, самостоятельно сформулировать и предложить новые решения по совершенствованию правоприменительной практики	Квалифицирует деяние в соответствии с законом. Разграничивает административные правонарушения и преступления	Правильно квалифицирует деяние в соответствии с законом. Правильно разграничивает административные
ПК 4.3. Способность определять методики расследования отдельных видов правонарушений и преступлений и результаты деятельности по выявлению, пресечению, раскрытию и расследованию отдельных видов правонарушений и преступлений.	Определяет перечень средств для раскрытия и расследования, предупреждения и пресечения готовящихся и совершаемых преступлений и иных правонарушений	Самостоятельно и обоснованно определяет перечень средств для раскрытия и расследования, предупреждения и пресечения готовящихся и совершаемых преступлений и иных правонарушений
ПК 5.3. Способность на научной основе самостоятельно сформулировать и предложить новые решения по совершенствованию профилактической деятельности лиц, участвующих в профилактике преступлений и правонарушений наряду со специальными субъектами профилактики.	Определяет содержание представления о принятии мер по устранению обстоятельств, способствовавших совершению преступления.	Верно определяет содержание представления о принятии мер по устранению обстоятельств, способствовавших совершению преступления.

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

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ К ЭКЗАМЕНУ

1. Дайте понятие криминальных рисков электронной торговли.
2. Раскройте типологию криминальных рисков электронной торговли.
3. Охарактеризуйте риски интернет-мошенничества для существования электронной коммерции.
4. Охарактеризуйте проблему потребительского «экстремизма» в качестве угрозы нормальному развитию общественных отношений в сфере электронной коммерции.
5. Охарактеризуйте риски хакерских атак на коммерческую инфраструктуру.
6. Охарактеризуйте риски киберсквоттинга.

7. Охарактеризуйте общественную опасность незаконного предпринимательства в глобальной сети Интернет.
8. Перечислите основные криминальные риски использования криптовалют в расчётах.
9. Приведите примеры реализации принципов безопасного использования облачных сервисов и построения офисной инфраструктуры коммерческой организации в целях предотвращения хищений компьютерной информации.
10. Охарактеризуйте проблемы правового регулирования деятельности интернет-агрегаторов в целях предупреждения обмана потребителей.
11. Кампания по реформе авторского права в цифровую эпоху в целях создания легального рынка электронного контента и борьбы с «пиратством».
12. Каким образом целесообразно осуществлять правовое регулирование импортозамещения программного обеспечения в целях обеспечения информационной безопасности РФ.
13. Обозначьте научно-обоснованные перспективы регулирования деятельности электронных платежных систем в целях противодействия легализации средств добытых преступным путем и финансирования терроризма.

ШКАЛА ОЦЕНИВАНИЯ

Таблица 7. Шкала оценивания

Зачет	Критерии оценки
незачтено	Неспособен самостоятельно выбрать наиболее эффективные меры противодействия правонарушениям в сфере электронной торговли из существующих в российской и международной практике. Неспособен указать конкретные причины правонарушения в сфере электронной торговли исходя из представленной ситуации. Не может представить обоснование эффективности реализуемых и предлагаемых самим студентом мер по защите электронной торговли от преступлений. Не знает содержания нормативно-правовых источников, устанавливающих права и обязанности должностных лиц, обеспечивающих законность и правопорядок, безопасность личности, общества, государства. Не знает современных методов предупреждения преступности, разработанных криминологической наукой.
зачтено	Умеет самостоятельно выбрать одну или более мер противодействия правонарушениям в сфере электронной торговли из существующих в российской и международной практике. Способен обосновать их целесообразность и эффективность применительно к конкретной практической ситуации. Способен сформулировать основные принципы и наметить пути реализации ведомственной и целевой территориальной программы по предупреждению преступности в сфере высоких технологий и преступности в сфере электронной торговли в частности. Свободно ориентируется в научных положениях по программно-целевому подходу в предупреждении на современном этапе. Способен раскрыть основные положения координационной деятельности правоохранительных структур под началом Прокуратуры РФ.

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 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).

ЗАДАНИЕ № 1 (ПРИМЕР).

1. Теоретический вопрос: **Контроль и надзор в сфере электронной торговли**. Направлен на проверку знаний магистранта относительно обязанностей должностных лиц, обеспечивающих законность и правопорядок в сфере электронной торговли ($З_1$ – ПК-3);

2. Оцените криминальные риски коммерческого шпионажа посредством электронных систем связи в сфере электронной торговли в связи правоприменительной практикой Роскомнадзора. Каким мерам предупреждения: правовым или организационно-техническим стоит отдать в связи с этим приоритет? Данный вопрос позволит выявить умение студента правильно оценить криминогенную ситуацию и выбрать наиболее оптимальный и с правовой точки зрения законный способ устранения криминальных рисков для организации и потребителей ($У_1$ – ПК-3);

3. Система мер по предупреждению коммерческого шпионажа в онлайн-магазине. Позволяет выявить конкретные навыки студента по планированию мер предупреждения правонарушений в деятельности субъектов электронной торговли, что соответствует элементу $В_1$, когда магистрант показывает экзаменатору навыки применения в конкретной ситуации мер по обеспечению законности и правопорядка.

*(Таким образом, компетенция государственного стандарта **(ПК-3)** применительно к нашей дисциплине может считаться сформированной).*

ЗАДАНИЕ №2 (ПРИМЕР).

1. Теоретический вопрос: **Риски интернет-мошенничества**. Здесь магистрант проводит типологию мошенничеств, совершаемых посредством глобальной компьютерной сети Интернет применительно к сфере электронной торговли, выявляет ключевые признаки и способы совершения рассматриваемых преступлений, что формирует у него способность выявления и раскрывать данные правонарушения опираясь на свои знания о них ($З_1$ – ПК-4);

2. Практическое задание №1. Организованной группой граждан были открыты 23 сайта, тематика которых связана с консалтингом экономического характера. На данных сайтах размещались информационные и аналитические материалы, обсуждался курс акции компании малой капитализации, давались советы, по поводу того, продавать или приобретать те или иные ценные бумаги. Авторы указанных материалов позиционировали себя в качестве авторитетных, независимых экспертов-экономистов. При этом они сами скупали акции, курс которых анализировали в своих статьях. По договоренности они одновременно начинали рекомендовать покупку акций определенных компаний с целью увеличения спроса, затем, когда инвесторы поднимали цену, перепродавали акции. Затем некоторые из виртуальных экономистов вступили в сговор с руководством компаний и рекомендовали их акции за определенную плату, но не упоминали об этих отношениях. Оцените ситуацию с точки зрения действующего законодательства. Можно ли привлечь к ответственности экономистов-консультантов? Данное задание позволяет оценить умение студента по правильной юридической оценке деяния (квалификации), т.е. умения разграничивать преступления и иные правонарушения ($У_1$).

3. Практическое задание №2. **Перечислите основные способы пресечения правонарушений с использованием интернет-технологий, используемые в деятельности оперативных подразделений Бюро специальных технических мероприятий.** Данный вопрос позволяет определить уяснил ли магистрант основные

практические приёмы деятельности оперативных сотрудников по предупреждению пресечению правонарушений. Может ли он определить правильную последовательность этих мер ($В_1$).

*(Таким образом, компетенция государственного стандарта **(ПК-4)** применительно к нашей дисциплине может считаться сформированной).*

ЗАДАНИЕ №3 (ПРИМЕР).

1. Теоретический вопрос: **Принципы безопасного использования облачных сервисов и построения офисной инфраструктуры коммерческой организации в целях предотвращения хищений компьютерной информации**. Позволяет проверить знания студента относительно наличествующих методов предупреждения правонарушений в сфере электронной торговли ($З_1$).

2. Практическое задание №1. Оператор ЭВМ одной из коммерческих организаций Ложкина, используя многочисленные сменные носители информации, получаемые от сотрудников других организаций, не всегда проверяла их на наличие «вирусов», доверяясь заверениям поставщиков о том, что «они чистые». В результате в компьютер Тройкиной была внесена программа-«вирус», что привело к утрате важнейшей информации и поставило на грань срыва важное мероприятие. Выявите условия и причины, которые привели к совершению данного правонарушения. Позволяет проверить умение выявлять и устранять причины и условия, способствующие совершению правонарушений ($У_1$).

3. Практическое задание №2. **Система мер по предупреждению неправомерного доступа к компьютерной информации участников (субъектов) электронной торговли: механизм реализации. (Применительно к вышеозначенной в билете ситуации).** Позволяет выявить конкретные навыки студента по планированию мер предупреждения правонарушений в деятельности субъектов электронной торговли, что соответствует элементу ($В_1$), когда магистрант показывает экзаменатору навыки реализации методов предупреждения правонарушений в конкретной ситуации.

*(Таким образом, компетенция государственного стандарта **(ПК-5)** применительно к нашей дисциплине может считаться сформированной).*

При дистанционном формате изучения дисциплины промежуточная аттестация может проводиться в формате тестирования, выполнения письменного контрольного задания или опроса по вопросам билета или защиты выполненной работы в режиме онлайн видеоконференций. Все вопросы и задания, выносимые на промежуточную аттестацию, находятся в рамках тематического содержания дисциплины, представленного в РПД. Прокторинг является обязательным при проведении промежуточной аттестации с использованием ЭО и ДОТ.

5. Методические указания для обучающихся по освоению дисциплины.

5.1. Методические указания по освоению дисциплины для магистрантов очной формы обучения.

Учебным планом подготовки магистров предусмотрено изучение курса «Обеспечение безопасности электронной торговли» 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, 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.

Порядок выполнения заданий и упражнений:

Все предложенные в методических рекомендациях задачи должны быть решены магистрантами письменно в ходе самостоятельной работы. Записи необходимо осуществлять в своих конспектах. Необходимо переписывать условие задачи в тетрадь. Решение каждой задачи должно начинаться с ответа на поставленный вопрос. Затем студент должен дать точный юридический анализ явления, подкрепляя свои выводы ссылками на уголовный закон, другие нормативные акты, постановления Пленума Верховного Суда РФ. Для решения задач рекомендуется использовать одну тетрадь объемом 48 страниц, подписанную студентом с указанием его группы, фамилии и имени. Проверка решенных задач осуществляется на практическом занятии, соответствующем данной теме методом случайной выборки. Таким образом, все задачи данной темы должны быть решены до начала практического занятия, в ходе которого будет проверяться правильность решения и коллективно анализироваться допущенные ошибки.

Типовой вариант решения задач по темам курса.

1. Тим Майер – гражданин иностранного государства прибыл на территорию России в составе туристической группы. Зарегистрировав на свое имя sim-карту одного из российских мобильных операторов, он понял, что номером до него пользовалась некая Лаврентьева, поскольку на телефон постоянно поступали сообщения то от коллекторов, то от банка с предложением получить новый кредит. Используя технологии дистанционного банковского обслуживания Майеру удалось зачислить на счёт теперь уже собственного телефона значительную сумму средств со счёта жертвы, которые он потратил на оплату услуг связи в Москве. Проходя таможенный контроль через месяц (выезжая из России) он был задержан. Подлежит ли Гирлянд уголовной ответственности по УК РФ?

Решение

Тим Майер – гражданин иностранного государства подлежит уголовной ответственности по УК РФ. При решении данной задачи должен быть использован территориальный принцип, установленный в ст. 11 УК РФ. Согласно ч. 1 ст. 11 УК лицо, совершившее преступление на территории Российской Федерации, подлежит уголовной ответственности по УК РФ.

Как вытекает из условий задачи, Т. Майер совершил преступление в Москве, на территории РФ.

Не менее важно – установление личности Т. Майера, его государственно-политического положения. Как видно из условий задачи, он не относится к категории лиц, пользующихся правом иммунитета. В условиях задачи сказано, что Т. Майер прибыл на территорию России в составе туристической группы, т.е. как частное лицо.

Т. Майер совершил уголовно наказуемое деяние на территории РФ, поэтому в соответствии с ч. 1 ст. 11 УК РФ должен быть привлечён к уголовной ответственности за хищение чужого имущества.

Шкала оценивания решения задачи:

Количество баллов		Критерии оценивания
Зачтено	5 баллов	оформление решения задачи с выделением описательной (юридически значимые действия и события), мотивировочной (конкретные статьи нормативно-правовых актов) и резолютивной (принятое решение) частей, полные аргументированные ответы на все поставленные в задаче вопросы;
	4 балла	незначительные погрешности в оформлении решения задачи, неполные (не полностью аргументированные) ответы на поставленные в задаче вопросы;
	3 балла	существенные погрешности в оформлении решения задачи, ответы не на все из поставленных в задаче вопросов;
Не зачтено	2 балла	оформление решения без выделения описательной, мотивировочной и резолютивной частей, неумение аргументировано объяснить предложенное решение;
	1 балл	отсутствие решения задачи (отсутствие ответов на все из поставленных в задаче вопросов); неправильное решение задачи.

5.2. Методические указания по освоению дисциплины для магистрантов заочной формы обучения.

Преподавание дисциплины «Обеспечение безопасности электронной торговли» имеет свои особенности применительно к магистрантам заочной формы 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 магистранта. Поэтому некоторые темы магистранты должны исследовать самостоятельно по указанию и рекомендациям преподавателя. Для этого необходимо самостоятельно разобраться с учебной и научной литературой, законспектировать её содержание.

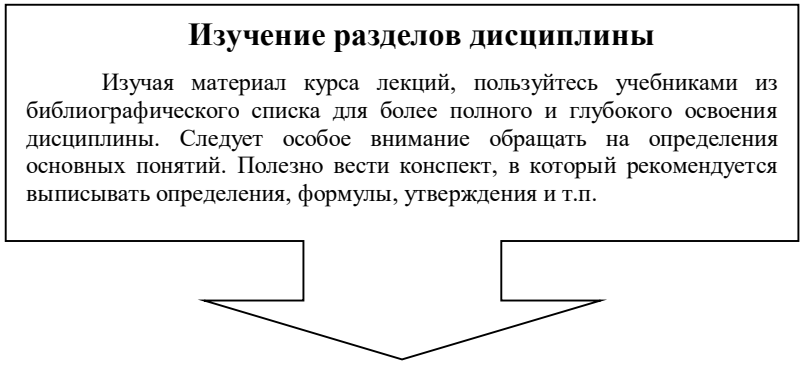
Основные вопросы, предусмотренные тематическим планом, будут рассмотрены в ходе лекций, в процессе которых помимо изложения теоретического материала, рассмотрения положений соответствующих нормативных актов и материалов практики предполагается постановка проблемных вопросов, обсуждение которых выносится 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 криминологии 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.

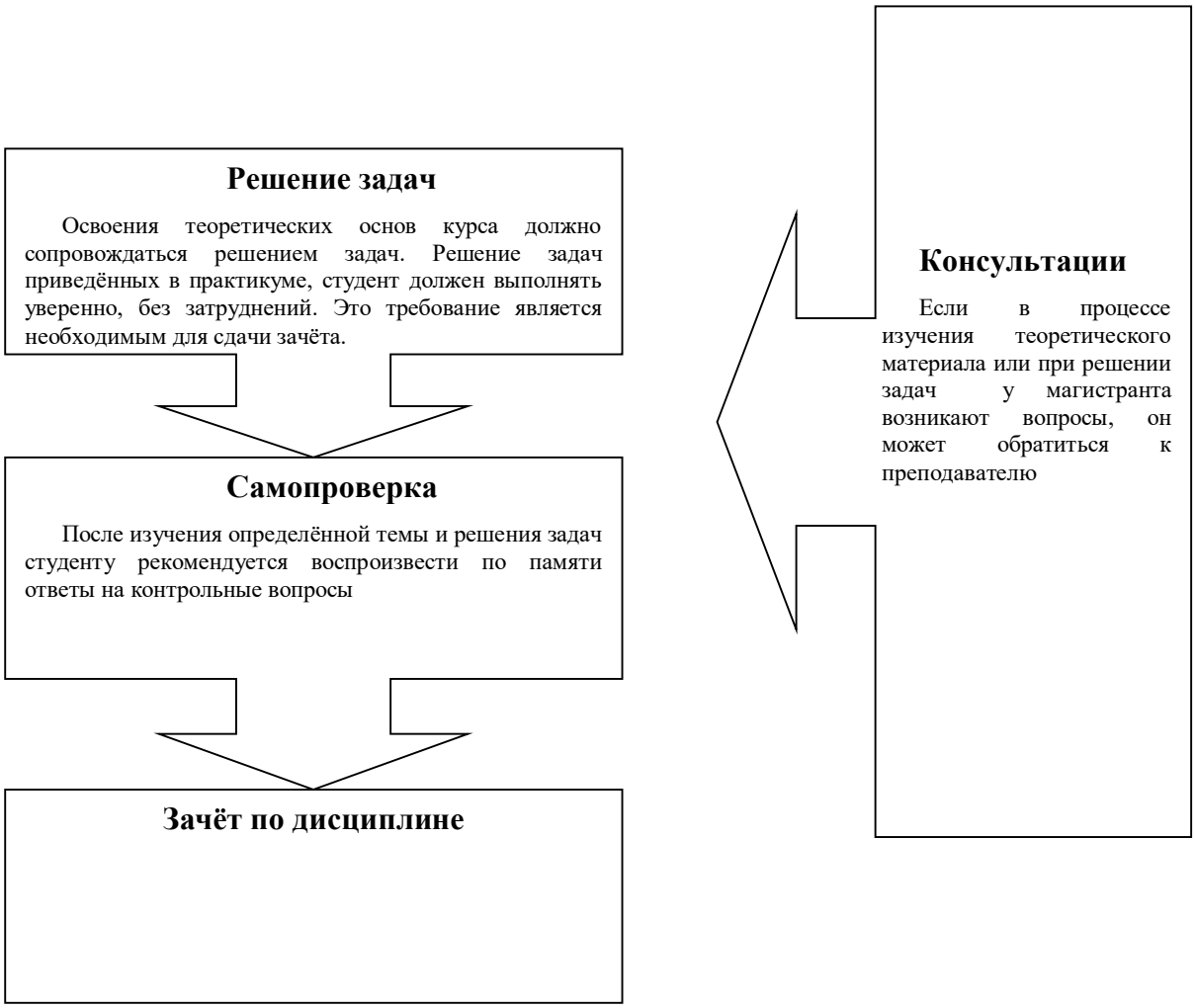
Далее приводится таблица, кратко отражающая методологию конспектирования.

Таблица 5. – 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 магистранта заочной формы обучения должна строиться по следующей схеме:





При применении дистанционной технологии обучения по очной, очно-заочной, заочной (традиционной) форм обучения учебный материал[5], который необходимо обучающимся проработать по конкретной лекции размещается в СДО «Прометей». Все

[5] Материалы конкретных лекционных занятий, с которыми должен ознакомиться обучающийся в рамках данной «лекции»: текст (конспект) лекции, демонстрационные и дополнительные материалы к ним (презентации, учебные фильмы или ссылки на них, материалы для чтения: статьи, документы, хрестоматийный материал), включая ЭБС, ссылки на публичные онлайн-курсы и т.п. с указанием конкретных страниц учебников, конспекта, отрезков видео или фрагментов онлайн-курса, которые должен освоить обучающийся в рамках данного «лекционного» занятия.

обучающиеся имеют доступ в СДО «Прометей» из личного кабинета студента через сайт Сибирского института управления – филиала РАНХиГС.

Дополнительно, при наличии технической возможности, лекционные занятия могут проводятся в соответствии с расписанием в режиме онлайн видеоконференций, для организации которых используются сервисы Zoom, Microsoft Teams, Youtube. В СДО «Прометей» для обучающихся заранее размещаются соответствующие ссылки и идентификаторы конференции. Может быть использована синхронная или асинхронная аудио/видео-конференция посредством вебинара.

Для контроля освоения темы обучающимся выдаются вопросы и задания в соответствии с РПД. Задания размещаются в СДО «Прометей» и /или доводятся до обучающегося любым доступным способом (посредством электронной почты, соц. сетей и др.). Устанавливается срок выполнения и представления заданий, в том числе способ представления.

Материалы, предназначенные для обеспечения семинарских/практических занятий размещаются в СДО «Прометей» и /или доводятся до обучающегося любым доступным способом (посредством электронной почты, соц сетей и др.). в привязке к конкретным занятиям, запланированным в учебном расписании это:

вопросы для обсуждения на семинарских занятиях, планы практических занятий, материалы для подготовки к ним;

тестовые материалы, привязанные к конкретному занятию и предназначенные для автоматической оценки степени освоения обучающимся материалов темы;

варианты письменных работ и методических указаний по их выполнению.

По каждой теме преподаватель осуществляет оперативное консультирование обучающихся, отвечая письменно на их вопросы в СДО «Прометей» и /или в формате чатов в процессе аудио/видео-конференций.

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

6.1. Основная литература.

1. Информационная безопасность России : учеб. пособие / А. П. Барановский [и др.] ; М-во образования и науки РФ, Сиб. гос. технол. ун-т [и др.]. – Красноярск : СибГТУ, 2011. – 123 с.
2. Кобелев, О.А. Электронная коммерция [Электронный ресурс] : учеб. пособие / О.А. Кобелев ; под ред. С.В. Пирогова. - Электрон. текстовые данные. – 4-е изд. перераб. и доп. – Москва : Дашков и Ко, 2012. – 684 с. – Доступ из ЭБС «IPRbooks». – Режим доступа: http://www.iprbookshop.ru/24850, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
3. Кочергин, Д.А. Электронные деньги : учебник / Д. А. Кочергин. – Москва : Маркет ДС, 2011. – 422 с. – То же [Электронный ресурс]. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=209588, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
4. Лапина, М.А. Информационное право [Электронный ресурс] : учеб. пособие / М.А. Лапина, А.Г. Ревин, В.И. Лапин ; под ред. И.Ш. Килясханов. – Электрон. данные. – Москва : Юнити-Дана, 2015. – 336 с. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=118624, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
5. Савельев, А.И. Электронная коммерция в России и за рубежом: правовое регулирование : [монография] / А. И. Савельев. – Москва : Статут, 2014. – 542 с.

6.2. Дополнительная литература.

1. Балабанов, И.Т. Электронная коммерция : учеб. пособие для вузов / И. Т. Балабанов. – Санкт-Петербург : Питер, 2001. – 336 с.
2. Васильев, Г.А. Электронный бизнес и реклама в Интернете [Электронный ресурс] : учебное пособие / Г.А. Васильев, Д.А. Забегалин. – Электрон. данные. – Москва : Юнити-Дана, 2012. – 184 с. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=118558, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
3. Гайдук, А.С. Оценка платежных систем на базе электронных денег : автореф. дис. ... канд. экон. наук : 08.00.10 / А. С. Гайдук; Новосиб. гос. ун-т экономики и упр. – «НИНХ». – Новосибирск, 2011. – 20 с.
4. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] / В. А. Галатенко. – Электрон. текстовые данные. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 266 с. – Доступ из ЭБС «IPRbooks». – Режим доступа: http://www.iprbookshop.ru/22424, требуется авторизация (дата обращения: 18.01.16). – Загл. с экрана.
5. Еляков, А.Д. Проблемы информационной безопасности в использовании электронных компьютерных технологий / А. Д. Еляков // Социол. исслед. – 2013. – № 10. – С. 120-129.
6. Илюхин, О. Интернет-банкинг: безопасность превыше всего / О. Илюхин // Консультант. – 2010. – № 15. – С. 72-76.
7. Ищенко, Е.П. Виртуальный криминал / Е. П. Ищенко. – Москва : Проспект, 2015. – 229 с.
8. Кияев, В. Безопасность информационных систем [Электронный ресурс] : курс / В. Кияев, О. Граничин. – Электрон. данные. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=429032, требуется авторизация (дата обращения: 25.02.2016). – Загл. с экрана.
9. Кобелев, О.А. Электронная коммерция [Электронный ресурс] : учебное пособие / О.А. Кобелев ; под ред. С.В. Пирогов. – Электрон. данные. – 4-е изд. перераб. и доп. – Москва : Дашков и Ко, 2012. – 684 с. – Доступ из ЭБС «IPRbooks». – Режим доступа: http://www.iprbookshop.ru/24850, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана. – То же [Электронный ресурс]. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=112231, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
10. Кришталюк, А.Н. Правовые аспекты системы безопасности [Электронный ресурс] : курс лекций / А.Н. Кришталюк ; Межрегиональная академия безопасности и выживания. – Электрон. данные. – Орел : МАБИВ, 2014. – 204 с. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428612, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
11. Курицкий, А.Б. Проблемы обеспечения информационной безопасности в Интернет-экономике / А. Б. Курицкий // Инновации. – 2003. – № 10. – С. 34-35.
12. Мазуров, В.А. Компьютерные преступления: Классификация и способы противодействия : учеб.-практ. пособие / В. А. Мазуров. – Москва : Палеотип : Логос, 2002. – 148 с.
13. Олиндер, Н.В. Преступления, совершенные с использованием электронных платежных средств и систем: криминалист. аспект : монография / Н. В. Олиндер. – Москва : Русайнс, 2016. – 120 с.
14. Правовое обеспечение информационной безопасности : учеб. пособие / под ред. С. Я. Казанцева. – 2-е изд., испр. и доп. – Москва : Академия, 2007. – 238 с.
15. Расследование неправомерного доступа к компьютерной информации : учеб. пособие / Моск. ун-т МВД России ; под ред. Н.Г. Шурухнова. – 2 изд., доп. и перераб. – Москва, 2004. – 352 с.
16. Ревенков, П.В. Финансовый мониторинг в условиях интернет-платежей [Электронный ресурс] / П.В. Ревенков. – Электрон. данные. – Москва : КНОРУС, 2016. – 64 с. – Доступ из Унив. б-ки ONLINE. - Режим доступа:

http://biblioclub.ru/index.php?page=book&id=430953, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
17. Талимончик, В.П. Международно-правовое регулирование отношений информационного обмена [Электронный ресурс] : учебное пособие / В. П. Талимончик. – Электрон. текстовые данные. – Санкт-Петербург : Юрид. центр Пресс, 2011. – 382 с. – Доступ из ЭБС «IPRbooks». – Режим доступа: http://www.iprbookshop.ru/9251, требуется авторизация (дата обращения: 18.01.16). – Загл. с экрана
18. Тедеев, А.А. Электронная коммерция (электронная экономическая деятельность): Правовое регулирование и налогообложение / А. А. Тедеев. – Москва : Приор-издат, 2002. – 224 с.
19. Терещенко, С.Н. Информационная безопасность компьютерных систем : учеб. пособие / С. Н. Терещенко; Федер. агентство по образованию, Сиб. акад. гос. службы. – Новосибирск : Изд-во СибАГС, 2010. – 169 с. – То же [Электронный ресурс]. – Доступ из Б-ки электрон. изданий / Сиб. Ин-т упр. – филиал РАНХиГС. – Режим доступа: http://www.sapanet.ru, требуется авторизация (дата обращения: 14.01.16). – Загл. с экрана.
20. Уткин, В.Б. Информационные системы и технологии в экономике [Электронный ресурс] : учебник / В.Б. Уткин, К.В. Балдин. – Электрон. данные. – Москва : Юнити-Дана, 2015. – 336 с. – Доступ из Унив. б-ки ONLINE. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=119550, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
21. Хилюта, В. Б. «Компьютерные» хищения / В.Б. Хилюта // Законность. – 2009. – № 1. – С. 36-38.
22. Хмаладзе, Д.З. Особенности электронных денежных средств в открытых и закрытых циркулярных системах / Д. З. Хмаладзе // Нац. безопасность. – 2015. – № 3. – С. 359-363.
23. Чекунов, И.Г. Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества / И. Г. Чекунов // Российский следователь. – 2015. – № 17. – С. 29-33.
24. Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – Санкт-Петербург : Наука и техника, 2004. – 384 с.
25. Электронные деньги и мобильные платежи : энциклопедия / [авт.: В. Г. Мартынов и др.]. – Москва : КноРус : Центр исслед. платеж. систем и расчетов, 2009. – 366 с. – То же [Электронный ресурс]. – Доступ из Унив. б-ки ONLINE. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=209591, требуется авторизация (дата обращения: 15.02.2016). – Загл. с экрана.
26. XI Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Бангкок, 18-25 апреля 2005 г.) : сб. документов / [сост. А. Н. Сухаренко]. – Москва : Юрлитинформ, 2008. – 614 с.

6.3. Учебно-методическое обеспечение самостоятельной работы.

1. Уголовное право : учеб. пособие / Т. А. Черткова ; Рос. акад. нар. хоз-ва и гос. службы при Президенте РФ, Сиб. ин-т упр. - 2-е изд., перераб. - Новосибирск : Изд-во СибАГС, 2013. - 309 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 : 25.04.2016). – 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. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 №14-ФЗ (ред. от 29.06.2015) // Собр. законодательства Рос. Федерации. – 1996. – №5. – Ст. 410.

4. Гражданский кодекс Российской Федерации. Часть четвертая от 18.12.2006 №230-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 52. (ч. 1). – Ст. 5496.
5. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – № 1. (ч.1). – Ст. 1.
6. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 № 149-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31 (ч.1). – Ст. 3448.
7. Об электронной подписи: федеральный закон от 06.04.2011 №63-ФЗ (ред. от 28.06.2014) // Собр. законодательства Рос. Федерации. – 2011. – №15. – Ст. 2036.
8. О деятельности по приёму платежей физических лиц, осуществляемой платежными агентами: федеральный закон от 03.06.2009 №103-ФЗ (ред. от 05.05.2014) // Собр. законодательства Рос. Федерации. – 2009. – №23. – Ст. 2758.
9. О защите прав потребителей: закон РФ от 07.02.1992 №2300-1 (ред. от 05.05.2014) // Собр. законодательства Рос. Федерации. – 1996. – №3. – Ст. 140.
10. Об обязательном экземпляре документов: федеральный закон от 29 декабря 1994 г. № 77-ФЗ // Собр. законодательства Рос. Федерации. – 1995. - № . – Ст. 1.
11. О государственной тайне: Закон РФ от 21 июля 1993 г. №5485-1 // Собр. законодательства Рос. Федерации. – 1997. – № 1. – Ст. 8220-8231.
12. О национальной платёжной системе: федеральный закон от 27.06.2011 №161-ФЗ (ред. от 29.12.2014) // Собр. законодательства Рос. Федерации. – 2011. – №27. – Ст. 3872.
13. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федеральный закон от 9 февраля 2009 г. №8-ФЗ. // Рос. газ. – 2009. – № 4849.
14. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: федеральный закон от 22 декабря 2008 года № 262-ФЗ // Рос. газ. – 2008. – № 4822.
15. 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.
16. О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собр. законодательства Рос. Федерации. – 2006. – № 31 (ч.1). – Ст. 3451.
17. О коммерческой тайне: федеральный закон от 29 июля 2004 г. № 98-ФЗ // Собр. законодательства Рос. Федерации. – 2004. – № 32. – Ст. 3283.
18. О средствах массовой информации: закон РФ от 27.12.91. № 2124-I // Рос. газ. – 1992. – № 32.
19. О рекламе: федеральный закон от 13.03.2006 №38-ФЗ (ред. от 08.03.2015) // Собр. законодательства Рос. Федерации. – 2006. – №12. – Ст. 1232.

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. Журнал «Информационное право»: www.infolaw.ru
6. Интернет и право: http://www.internet-law.ru

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 (модуля).

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, 2 музыкальных центра, видеокамера, 2 видеомагнитофона, 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 -2шт.
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
Видеостудия для вебинаров	компьютеры с выходом в Интернет, оснащенные веб-камерами и гарнитурами (наушники+микрофон), столы, стулья