МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

СОГЛАСОВАНО
Руководитель ОП

Р.И. Дремлюга

«17» июня .2019 г.

УТВЕРЖДАЮ
Директор Школы цифровой экономики

_____ И.Г. Мирин

«17» ____06_____ 2019 г.

«ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»
направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

курс 1 семестр 2
лекции 18 час.
практические занятия 36 час.
лабораторные работы 0 час.
всего часов аудиторной нагрузки 54 час.
самостоятельная работа 54 час.
контрольные работы программой не предусмотрены
курсовая работа/проект – не предусмотрено
зачет с оценкой 2 семестр
экзамен – не предусмотрено учебным планом

Рабочая программа составлена в соответствии составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки/специальности 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918.

Рассмотрена и утверждена на заседании Дирекции Школы цифровой экономики «17» июня 2019 года (протокол № 124-01-07-05).

Составитель: доц., к.ю.н. Р.И. Дремлюга

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № ___

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании Дирекции Школы цифровой экономики:
Протокол от «_____» _____ 20___ г. № ___

Заместитель директора ШЦЭ
по учебной и воспитательной работе _____ _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ
Б1.В.ДВ.01.02 ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Рабочая программа дисциплины «Правовые основы кибербезопасности» предназначена для студентов, обучающихся по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры), профиль «Кибербезопасность».

Дисциплина «Правовые основы кибербезопасности» входит в часть, формируемую участниками образовательных отношений, блока «Дисциплины (модули) Б1» (Б1.В.ДВ.01) учебного плана подготовки магистров, модуль элективных дисциплин

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы или 108 часов. Дисциплина реализуется на 1 курсе в 1 семестре.

Семестр	Аудиторные Занятия			Самостоятельная работа	Контроль	Форма контроля	Всего по дисциплине	
	Лекции	Лабораторные занятия	Практические занятия				Часы	з.е.
1 семестр	18	-	18	72	-	Зачет	108	3

Цель освоения дисциплины - подготовка высококвалифицированных специалистов, способных ориентироваться в актуальных проблемах правового регулирования рынка информационных ресурсов и обеспечить информационную безопасность государства, общества и личности, а также представлять интересы в области обмена в международном информационном пространстве

К числу основных задач курса относятся:

• получение знаний о правовом понятии «информационное общество в условиях глобализации» в целях его применения в правотворческой деятельности как на международном, так и на национальном уровне;

• получение знаний об общественных отношениях, которые связаны с созданием, хранением, обработкой, распространением и использованием

информационных ресурсов;

• получение знаний о существующих подходах к решению актуальных проблем использования сети «Интернет»;

• получение знаний и навыков о приоритетных направлениях совершенствования правового обеспечения информационного пространства (интернет-технологий и интернет-среды);

• получение знаний о правовых проблемах, влияющих на формирование государственной политики Российской Федерации при интеграции в глобальное информационное общество

Успешное решение данных задач зависит от соблюдения Положений Конституции Российской Федерации, федеральных конституционных законов, федеральных законов, правовых актов Президента Российской Федерации и Правительства Российской Федерации, нормативных правовых актов федеральных органов исполнительной власти и иных органов, субъектов Российской Федерации, а также уголовно-процессуального кодекса РФ.

В результате освоения курса обучающиеся будут знать:

•краткие основы информационной безопасности для тех, кто использует ИТ в бизнесе;

•как обезопасить данные организации и свои собственные данные от злоумышленников;

•современные угрозы безопасности данных и приложений, которые используются в бизнесе ;

•ключевые правила обеспечения безопасности данных в организации;

•подходы к эксплуатации уязвимостей и этапы действия злоумышленников;

•как определить для себя приоритеты в вопросах безопасности данных и составить план действий, направленный на снижение рисков и защиту бизнеса.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные и профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-2.1 Знает: модели безопасности компьютерных сетей; виды политик безопасности компьютерных систем и сетей; нормативно-правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации; организационные меры по защите информации ПК-2.2 Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем ПК-2.3 Владеет: навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработки руководящих документов по защите информации в организации
ПК-5 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-5.1 Знает: форматы хранения информации в анализируемой компьютерной системе; особенности хранения конфигурационной и системной информации в компьютерных системах; уязвимости компьютерных систем и сетей; порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; нормы уголовного и административного права в сфере компьютерной информации; характеристики правонарушений в области связи и информации; виды преступлений в сфере компьютерной информации; порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов ПК-5.2 Умеет: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства

	события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; выявлять возможные траектории состояний функционирования системы и несоответствия имеющейся информации ее расположению в системе ПК-5.3 Владеет: технологиями поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; навыками прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов; способами обнаружения и нейтрализации последствий вторжений в компьютерные системы; методами анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов; методами анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Тема № 1. Глобальное информационное пространство

Роль информации в жизни личности, общества и государства. Информационные революции. Понятие глобального информационного пространства. Структура глобального информационного пространства. Виды правового регулирования глобального информационного пространства. Международное правовое регулирование глобального информационного пространства. Национальное законодательство в сфере отношений, связанных с применением интернет-технологий в условиях развития глобального информационного общества. Риски, возникающие в связи с активным развитием информационно-телекоммуникационных технологий. Ограничение деструктивного и противоправного воздействия в целях нарушение территориальной целостности государств, актов экстремизма, агрессии.

Тема № 2. Информационные ресурсы, информационные технологии и информационные системы как объекты права

Понятие и содержание документирования информации. Электронный документ и электронная подпись. Понятие и виды информационных ресурсов. Порядок формирования информационных ресурсов и предоставления информационных услуг.

Понятие и виды информационных технологий. Понятие средств обеспечения информационных технологий. Информационно-телекоммуникационные сети. Лицензирование деятельности в области оказания услуг связи. Особенности правового регулирования общественных отношений в области создания и применения информационных технологий и средств их обеспечения в Интернете.

Понятие и правовое регулирование создания и использования информационных систем. Правовое положение персонала и пользователей информационных систем. Структура информационных систем в Российской Федерации.

Тема № 3. Информационный рынок

Структура и инфраструктура информационного рынка. Правовое регулирование информационного рынка. Законодательное регулирование

информационного обеспечения торговой деятельности. Специфика обращения коммерческих (деловых) секретов при заключении внутренних и внешнеторговых сделок и исполнения обязательств. Система сбора и распространения коммерческой информации.

Понятие и особенности электронной кооперации. Государственное регулирование области правового регулирования рынка в России. Полномочия международных организаций в области правового регулирования информационного рынка.

Тема № 4. Правовой статус субъектов правоотношений, возникающих в глобальном информационном пространстве

Правовой статус субъектов правоотношений в системе «Интернет». Проблемы множественной юрисдикции субъектов правоотношений в системе интернет-технологий и интернет-среды. Режим свободного доступа к информации. Режим ограниченного доступа к информации. Понятие допуска и доступа к информации.

Тема № 5. Информационная безопасность в глобальном информационном пространстве

Понятие и виды информационной безопасности. Обеспечение информационной безопасности личности в глобальном информационном пространстве. Обеспечение информационной безопасности государства с точки зрения пространства доверия, безопасного развития от информационных войн, кибертерроризма и киберпреступности. Обеспечение информационной безопасности общества, вытекающей из «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утверждённых 24 июля 2013 года Президентом РФ.

Тема № 6. Проблемы обеспечения безопасности при использовании интернет-технологий и интернет-среды

Международно-правовое регулирование обеспечения информационной безопасности при использовании систем интернет-технологий и интернет-среды. Внутригосударственное правовое регулирование обеспечения информационной безопасности при использовании систем интернет-технологий и интернет-среды. Правовой механизм реализации конституционного права на информацию. Виды угроз обеспечения информационной безопасности. Несанкционированное использование или распространение информации в сети Интернет. Установления оснований и процедур ограничения доступа к информации, размещенной в сети Интернет.

Виды информации с ограниченным доступом. Государственная тайна. Конфиденциальная информация. Служебная тайна. Коммерческая тайна. Банковская тайна. Профессиональная тайна. Инсайдерская информация. Персональные данные.

Тема № 7. Проблемы обеспечения авторских и смежных прав в глобальном информационном пространстве

Обеспечения авторских и смежных прав на информационные технологии, ресурсы и системы. Правовое регулирование обеспечения авторских и смежных прав на информационные технологии, ресурсы и систем интернет-технологий и интернет-среды. Международно-правовое обеспечение авторских и смежных прав на информационные технологии, ресурсы и системы.

Тема № 8. Проблемы обеспечения права собственности на информацию и права интеллектуальной собственности в глобальном информационном пространстве

Понятие обеспечение права собственности на информацию и права интеллектуальной собственности. Обеспечение права собственности и права интеллектуальной собственности на информационные технологии, ресурсы и систем интернет-технологий и интернет-среды. Международно-правовое регулирование обеспечения права собственности на информацию и права интеллектуальной собственности. Способы защиты права собственности на информацию и права интеллектуальной собственности.

Тема № 9. Проблемы правомерного использования информации в глобальном информационном пространстве

Правовое регулирование распространения коммерческой рекламной информации в глобальном информационном пространстве. Правомерность применения политических технологий в глобальном информационном пространстве. Правовое регулирование порядка создания и функционирования средств массовой информации в интернет-среде.

Правовое регулирование о конфиденциальности в договорах на выполнение маркетинговых исследований, на передачу ноу-хау или технологии, передачу коммерческой информации и ее переработку, на оказание возмездных информационных услуг, коммерческой концессии.

Тема № 10. Проблемы ответственности за правонарушения, совершённые в глобальном информационном пространстве

Ответственности за нарушение правил ведения электронной коммерции. Электронное мошенничество. Ответственность за неправомерное распространение коммерческой и политической рекламной информации. Ответственность за нарушение авторских и смежных прав.

Уголовная ответственность за преступления в информационной сфере. Административная и дисциплинарная ответственность за правонарушения в информационной сфере. Гражданско-правовая ответственность за правонарушения в информационной сфере.

II. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы принятия решений» представлено в Приложении 1 и включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- характеристика заданий для самостоятельной работы студентов и методические рекомендации по их выполнению;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

III. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Контрольные и методические материалы, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

IV. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основные нормативные правовые акты

1. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) // Российская газета. 1993. 25 декабря. № 237.

2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ (в действ. ред.)..
3. Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности» (в действ. ред.).
4. Federal Cloud Computing Strategy.
5. Unleashing the potential of cloud computing in Europe.
6. Cloud and Interoperability Centre, CIC.
7. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895).
8. Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)».
9. Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» (в действ. ред.).
10. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (в действ. ред.).
11. «Модельный закон об основах регулирования Интернета» (Принят в г. Санкт-Петербурге 16.05.2011 Постановлением 36-9 на 36-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ)

Научная и учебно-методическая литература

Основная литература

1. Бачило И.Л. Государство и право XXI в. Реальное и виртуальное. М.: Юркомпани, 2012. -280 с.
2. Бачило И.Л. Информационное право РФ. 4-е изд. Учебник для вузов. М.: Издательство Юрайт, 2013.
3. Зенин И.А. Право интеллектуальной собственности: Учебник для магистров. 8-е изд. М.: Юрайт, 2012.
4. Кузык Б.Н., Яковец Ю.В. Россия – 2050. Стратегия инновационного прорыва. М.: Экономика, 2005.
5. Северин В.А. Правовая защита информации в коммерческих организациях. Учебное пособие для вузов. М.: Изд-во «Академия». 2009.
6. Северин В.А. Профессиональная переподготовка юристов для нужд инновационной экономики //Вестн. Моск. ун-та, серия 11, Право. 2011, № 5.

Дополнительная литература

1. Абрамова М.Г., Попов А.В. К вопросу о содержании понятий «информация», «информационные технологии» и «информационное право» // Образование и право. 2012. № 3.
2. Бачило И.Л. Правовая платформа построения электронного государства // Информационное право. 2008. № 4.
3. Глобальная безопасность в цифровую эпоху: стратагемы для России. Под общ. ред. Смирнова А.И. – М. : ВНИИгеосистем, 2014. – 394 с. 16
4. Голованов С.Ю. Новые угрозы. Spyware. HackingTeam // Право и кибербезопасность. 2013. № 1. С. 24 - 35.
5. Губин М.А. Проблема регулирования глобального информационного пространства // Научное сообщество студентов: междисциплинарные исследования: сб. ст. по мат. II Междунар. студ. науч.-практ. конф. № 3. URL: sibac.info/sites/default/files/conf/file/stud_3_2.pdf
6. Дятлова Е. В., Юсупов Т. З. Правовое регулирование отношений в условиях информационного общества. // Молодой ученый. — 2017. — №15. — С. 244-246.
7. Ефремов А.А.. Тенденции развития правового регулирования информационного пространства //Вестник ЮУрГУ. Серия «Право». 2017. Том 17, №2. С.80-82.
8. *Карев Я.А.* Электронные документы и сообщения в коммерческом обороте: правовое регулирование. М.: Статут, 2006.
9. Королев А.Н., Плешакова О.В. Комментарий к Федеральному закону "Об информации, информационных технологиях и о защите информации" (постатейный). М.: Юстицинформ, 2007.
10. Лопатин В.Н. Информационная безопасность России: человек, общество, государство. СПб: Изд.-во «Юридический центр Пресс», 2000.
11. Максуров А.А. Интернет как новое правовое пространство // Право и экономика. 2010. № 3.
12. Мухопад В.И. Коммерциализация интеллектуальной собственности. М.: Магистр: ИНФРА-М, 2010.
13. Паненков А.А. Кибертерроризм как реальная угроза национальной безопасности России // Право и кибербезопасность. 2014. № 1. С. 12 - 19.
14. Пилипенко Ю.С. Особенности профессиональных тайн //Законодательство и экономика. 2008, № 3.
15. Полякова Т.В. Проблемы правового обеспечения доступа к информации //Бизнес и безопасность в России, 2004, № 38.
16. Рассолов И.М. Право и Интернет. Теоретические проблемы. 2-е изд., доп. М.: Норма, 2009.
17. Северин В.А. Правовое регулирование информационных отношений //Вестн. Моск. ун-та, сер. 11, Право, № 5, 2000.
18. Северин В.А. Правовые проблемы обеспечения информационной безопасности в Российской Федерации //Вестник Моск. ун-та, сер. 11, Право, № 4, 2000.

19. Северин В.А. Услуги информационного характера, обеспечивающие коммерческую деятельность //Законодательство, № 1, 2000.
20. Северин В.А. Эволюция законодательства о коммерчески значимой информации в России //Вестн. Моск. ун-та. Серия 11 «Право», № 4, 2005.
21. Северин В.А. Формирование условий конфиденциальности при выполнении НИОКР //Законодательство. 2007. № 1.
22. Северин В.А**.** Проблемы конфиденциальности при передаче информации и оказании услуг //Законодательство. 2007. № 4.
23. Северин В.А. Правовой институт коммерческой тайны //Коммерческое право. 2008. № 2(3).
24. Северин В.А. Коммерческая тайна в России. 2-е изд. М.: ИКД «Зерцало-М», 2009.
25. Северин В.А. Договорное регулирование отношений в инновационной сфере //Коммерческое право. № 2(9). 2011.
26. Северин В.А. Допуск к информации в коммерческих организациях // Законодательство. Право для бизнеса. № 10. 2012. Северин В.А. Роль информации в модернизации экономики России //Правовая политика и развитие российского законодательства в условиях модернизации: Сб. докл. /Под ред. А.В. Малько, В.М. Шафирова, А.В. Усса. Красноярск: Издательский центр СФУ, 2012.
27. Северин В.А. Инновационное развитие российской экономики через коммерциализацию новшеств и образование //Научные труды. Российская академия юридических наук. Вып.12: в 2 т. Т. 2. М., Издательство «Юрист», 2012.
28. Северин В.А. Присоединение России к ВТО и защита коммерческой тайны // Коммерческое право. № 1(12). 2013.
29. Семилетов С.И. Информация как особый нематериальный объект права //Государство и право. М., 2000, №5.
30. Стрельцов А.А. Предмет правового обеспечения информационной безопасности //Российский юридический журнал, 2003, №2.
31. Сумин А.А. Комментарий к Закону Российской Федерации «О государственной тайне». М.: 2001.
32. Сушкова О.В. Гражданско-правовой режим инноваций в научно-технической сфере. М.: РПА Минюста России, 2011.
33. Сушкова О.В. Договоры, опосредующие инновационную деятельность. М.: РПА Минюста России, 2012.
34. Тедеев А.А. Проблемы и условия регулирования интернет отношений // Информационное право. 2008. № 4.
35. Тарасов А.М. Киберугрозы, прогнозы, предложения // Информационное право. 2014. N 3. С. 11 - 15.
36. Услинский Ф.А. Кибертерроризм в России: его свойства и особенности // Право и кибербезопасность. 2014. № 1. С. 6 - 11.

37. Химченко А.И. Информационное общество: правовые проблемы в условиях глобализации: диссертация ... кандидата юридических наук. М., 2014. –174с.
38. Химченко А.И., Полякова Т.А. Правовые проблемы обеспечения информационной безопасности при использовании облачных технологий. / // Правовая информатика. Периодический научный журнал. Выпуск № 2 - 2013. – М.: ФБУ НЦПИ при Минюсте России, 2013. С. 12-17.
39. Химченко А.И., Полякова Т.А. Реализация государственной политики в сфере организационно-правового обеспечения информационной безопасности. Федеральный справочник. Связь и массовые коммуникации в России: информационно-аналитическое издание; Т.12/ НП «Центр стратегического партнёрства». – М.: НП «Центр стратегического партнёрства», 2013. С. 73-77.
40. Цибуля А.Н., Гордин В.А. К вопросу о состоянии информационной безопасности государства в условиях современных вызовов и угроз // Военно-юридический журнал. 2014. № 3. С. 20 - 24.
41. Чеботарев В.Е., Забелина О.Г. Обеспечение информационной безопасности детей в сети Интернет // Право и кибербезопасность. 2014. № 1. С. 32 - 37.
42. Черешнев Е. Пособие по выживанию в социальных сетях // Право и кибербезопасность. 2013. № 1. С. 59 - 64.
43. Шаньгин В.Я. Защита информации в компьютерных системах и сетях. М: ДМК Пресс, 2012. 592 с.
44. Яблоков В.В., Елисеев Е.Ю. «Лаборатория Касперского» и мобильные угрозы // Право и кибербезопасность. 2013. № 1. С. 52 – 54.
45. Яровенко В.В., Корчагин А.Г., Трушова И.В. Проблемы правового регулирования криптовалюты в России // Полицейская деятельность – 2018. – № 1. – С. 9 - 21. DOI: 10.7256/2454-0692.2018.1.25526 URL: http://nbpublish.com/library_read_article.php?id=25526
46. Яровенко В.В., Полещук О.В., Шаповалова Г.М. Облачные вычисления (cloud computing) – новая парадигма в криминалистике // Полицейская и следственная деятельность. – 2018. - № 2. DOI: 10.25136/2409-7810.2018.2.26409. URL: http://e-notabene.ru/pm/article_26409.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.gosuslugi .ru / Единый портал государственных услуг РФ
2. http://www.consultant.ru / СПС Консультант Плюс
3. http://www.garant.ru / СПС Гарант
4. http://pravo.gov.ru - Официальный интернет-портал правовой информации/
5. http://zakon.scli.ru – Федеральный регистр НПА
6. http://law.edu.ru – Юридическая Россия. 17

7. http://www.constitution.ru – Фонд распространения правовых знаний
8. http://www.hro.org – «Права человека в России».
9. http://www.pravo.eup.ru – «Юридическая электронная библиотека».
10.Научная электронная библиотека «Elibrary.ru» // URL: http://elibrary.ru/defaultx.asp

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для организации выполнения практических заданий и самостоятельной работы с целью получения первичных профессиональных умений и навыков материально-техническое обеспечение дисциплины, обеспечивающей методическое сопровождение, включает:

а) программное обеспечение: MS Office: Word, PowerPoint, СПС «Гарант», «Консультант плюс», Система «Антиплагиат»;

б) неограниченный доступ к Интернет ресурсам, доступ к электронным библиотекам, персональные компьютеры-терминалы расположенные в читальном зале Библиотеки, специальная юридическая библиотека, Лаборатория «Юридическая клиника»;

в) техническое и лабораторное обеспечение: лаборатория криминалистика, располагающая необходимыми материалами, технико-криминалистическими средствами, приборами для выполнения практических заданий.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебная аудитория для занятий семинарского типа 690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10 Здание ФЭК корпус А, лит О, ауд. G371	Комплект специализированной мебели: доска аудиторная – 1 шт.; парты – 30 шт.; стул -30 шт.; Проектор DLP, 4000 ANSI Lm, 1920x1080, 2000:1 FD630u Mitsubishi; Проектор DLP, 2800 ANSI Lm, 1920x1080, 2000:1 GT1080 Optoma; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi; Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS).

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине

«ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

направления 09.04.01 Информатика и вычислительная техника
Магистерская программа «Кибербезопасность»
Форма подготовки очная

Владивосток
2019

№ п/п	Дата / сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1.	8 неделя 14 неделя	Выполнение реферата	12	Защита реферата
2.	10 неделя 16 неделя	Подготовка к К/Р	12	К/Р
3.	В течение семестра	Выполнение Индивидуальных заданий	12	Сдача расчётно-графических ИДЗ
4.	4 неделя 6 неделя 9 неделя 12 неделя 15 неделя 18 неделя	Подготовка к зачету	18	Зачет, Письменные ответы и устное собеседование
ИТОГО			54	

Рекомендации по самостоятельной работе студентов

Самостоятельная работа магистрантов выполняется во внеаудиторное время по заданию и при методическом руководстве преподавателя. Она состоит в подготовке и выполнении заданий по темам курса, а также написание рефератов, подготовке докладов и презентаций.

В процессе изучения курса «Правовые основы кибербезопасности» предполагается изучение материалов следственной практики, периодической печати, научной и учебной литературы.

Значительный вклад в самостоятельную работу магистрантов должны вносить преподаватели, ведущие занятия по дисциплине. Для подготовки к практическим занятиям, на предыдущих занятиях и в процессе консультации следует объяснить обучающимся, где и как они должны проводить свою самостоятельную работу, а также обратить их внимание на наиболее сложные вопросы, требующие дополнительного изучения.

Решающим элементом организации самостоятельной работы магистрантов является ее целенаправленное осуществление самими обучающимися

Наиболее глубокие знания показывают те магистранты, которые много и эффективно работают самостоятельно по изучению дисциплин учебного плана. Поэтому об уровне самостоятельной работы можно судить по показателям их участия в учебном процессе.

Разновидностью самостоятельной работы является научно-исследовательская работа магистрантов, которая состоит из нескольких этапов:

1. Сбор имеющегося по данной теме материала (первоисточников, монографий, статей из периодических изданий и т.д.);

2. Анализ обнаруженных источников с точки зрения полноты охвата изучаемой темы, использования тех или иных методов исследования, достоверности полученных автором выводов и их актуальности;

3. Обобщение научной информации по теме;

4. Постановка цели, конкретных задач и начало собственного исследования. Преподавателем может формулироваться тематика индивидуальных научно-практических исследований. План такой работы и их конкретная тематика формулируется индивидуально. Индивидуальные научно-практические исследования направлены на формирования высокоуровневого освоения теоретико-практических компетенций магистрантов и направлено на повышения их эффективности персонального обучения.

В докладе должны быть точно отражены взгляды автора. Следует соблюдать научный стиль изложения, допустимо использование точного, краткого, литературного языка. Доклад представляет собой аналитический текст, оценивающий и сравнивающий различные научные позиции, оценки правоприменителей, с последующим авторским обобщающим выводом. Доклад излагается в устной форме публично (в рамках учебной аудитории).

Самостоятельная работа по подготовке и написанию аналитического реферата

Методические указанию к выполнению реферата. Цели и задачи реферата

Реферат (от лат. *refero* – докладываю, сообщаю) представляет собой краткое изложение проблемы практического или теоретического характера с формулировкой определенных выводов по рассматриваемой теме.

Целями написания реферата являются:

– развитие у студентов навыков поиска актуальных проблем товароведения;

– развитие навыков краткого изложения материала с выделением лишь самых существенных моментов, необходимых для раскрытия сути проблемы;

– развитие навыков анализа изученного материала и формулирования собственных выводов по выбранному вопросу в письменной форме, научным, грамотным языком.

Задачами написания реферата являются*:*

– научить студента максимально верно передать мнения авторов, на основе работ которых студент пишет свой реферат;

– подготовить студента к дальнейшему участию в научно-практических конференциях, семинарах и конкурсах;

– помочь студенту определиться с интересующей его темой, дальнейшее раскрытие которой возможно осуществить при написании курсовой работы или выпускной квалификационной работы.

–

Основные требования к содержанию реферата

Реферат должен быть написан каждым студентом самостоятельно. Студент должен использовать только те литературные источники (научные статьи, монографии, пособия и т.д.), которые имеют прямое отношение к избранной им теме. Не допускаются отстраненные рассуждения, не связанные с анализируемой проблемой. Оглавление должно четко отражать основное содержание работы и обеспечивать последовательность изложения. Студенту необходимо строго придерживаться логики изложения – начинать с определения и анализа понятий, перейти к постановке проблемы, проанализировать пути ее решения и сделать соответствующие выводы. Работа должна быть достаточно краткой, но раскрывающей все вопросы содержания и тему.

По своей структуре реферат должен иметь титульный лист, оглавление, введение (где студент формулирует проблему, подлежащую анализу и исследованию), основной текст (где последовательно раскрывается избранная тема), заключение (где студент формулирует выводы, сделанные на основе основного текста работы), список использованных источников (10-15 наименований). В список использованных источников вносятся не только источники, на которые студент ссылается при подготовке реферата, но и иные, которые были изучены им при подготовке реферата.

Порядок сдачи реферата и его оценка

Реферат пишется студентами в сроки, устанавливаемые преподавателем по реализуемой дисциплине, и сдается преподавателю, ведущему дисциплину.

При оценке реферата учитываются соответствие содержания выбранной теме, четкость структуры работы, умение работать с научной литературой и нормативными и техническими документами, логически мыслить, владеть профессиональной терминологией, грамотность оформления.

По результатам проверки реферата и его защиты студенту выставляется определенное количество баллов, которое учитывается при общей оценке промежуточной аттестации.

Критерии оценки реферата

– 100-86 баллов выставляется студенту, если студент выразил свое мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно;

– 85-76 баллов – работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации

приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы;

– 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы;

– 60-50 баллов – если работа представляет собой пересказанный или полностью переписанный исходный текст, без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Примерные темы рефератов

Тема № 1. Глобальное информационное пространство

Роль информации в жизни личности, общества и государства. Информационные революции. Понятие глобального информационного пространства. Структура глобального информационного пространства. Виды правового регулирования глобального информационного пространства. Международное правовое регулирование глобального информационного пространства. Национальное законодательство в сфере отношений, связанных с применением интернет-технологий в условиях развития глобального информационного общества. Риски, возникающие в связи с активным развитием информационно-телекоммуникационных технологий. Ограничение деструктивного и противоправного воздействия в целях нарушение территориальной целостности государств, актов экстремизма, агрессии.

Тема № 2. Информационные ресурсы, информационные технологии и информационные системы как объекты права

Понятие и содержание документирования информации. Электронный документ и электронная подпись. Понятие и виды информационных ресурсов. Порядок формирования информационных ресурсов и предоставления информационных услуг.

Понятие и виды информационных технологий. Понятие средств обеспечения информационных технологий. Информационно-телекоммуникационные сети. Лицензирование деятельности в области оказания услуг связи. Особенности правового регулирования общественных отношений в области создания и применения информационных технологий и средств их обеспечения в Интернете.

Понятие и правовое регулирование создания и использования информационных систем. Правовое положение персонала и пользователей информационных систем. Структура информационных систем в Российской Федерации.

Тема № 3. Информационный рынок

Структура и инфраструктура информационного рынка. Правовое регулирование информационного рынка. Законодательное регулирование информационного обеспечения торговой деятельности. Специфика обращения коммерческих (деловых) секретов при заключении внутренних и внешнеторговых сделок и исполнения обязательств. Система сбора и распространения коммерческой информации.

Понятие и особенности электронной кооперации. Государственное регулирование области правового регулирования рынка в России. Полномочия международных организаций в области правового регулирования информационного рынка.

Тема № 4. Правовой статус субъектов правоотношений, возникающих в глобальном информационном пространстве

Правовой статус субъектов правоотношений в системе «Интернет». Проблемы множественной юрисдикции субъектов правоотношений в системе интернет-технологий и интернет-среды. Режим свободного доступа к информации. Режим ограниченного доступа к информации. Понятие допуска и доступа к информации.

Тема № 5. Информационная безопасность в глобальном информационном пространстве

Понятие и виды информационной безопасности. Обеспечение информационной безопасности личности в глобальном информационном пространстве. Обеспечение информационной безопасности государства с точки зрения пространства доверия, безопасного развития от информационных войн, кибертерроризма и киберпреступности. Обеспечение информационной безопасности общества, вытекающей из «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», утверждённых 24 июля 2013 года Президентом РФ.

Тема № 6. Проблемы обеспечения безопасности при использовании интернет-технологий и интернет-среды

Международно-правовое регулирование обеспечения информационной безопасности при использовании систем интернет-технологий и интернет-среды. Внутригосударственное правовое регулирование обеспечения информационной безопасности при использовании систем интернет-технологий и интернет-среды. Правовой механизм реализации конституционного права на информацию. Виды угроз обеспечения информационной безопасности. Несанкционированное использование или распространение информации в сети Интернет. Установления оснований и процедур ограничения доступа к информации, размещенной в сети Интернет.

Виды информации с ограниченным доступом. Государственная тайна. Конфиденциальная информация. Служебная тайна. Коммерческая тайна. Банковская тайна. Профессиональная тайна. Инсайдерская информация. Персональные данные.

Тема № 7. Проблемы обеспечения авторских и смежных прав в глобальном информационном пространстве

Обеспечения авторских и смежных прав на информационные технологии, ресурсы и системы. Правовое регулирование обеспечения авторских и смежных прав на информационные технологии, ресурсы и систем интернет-технологий и интернет-среды. Международно-правовое обеспечение авторских и смежных прав на информационные технологии, ресурсы и системы.

Тема № 8. Проблемы обеспечения права собственности на информацию и права интеллектуальной собственности в глобальном информационном пространстве

Понятие обеспечение права собственности на информацию и права интеллектуальной собственности. Обеспечение права собственности и права интеллектуальной собственности на информационные технологии, ресурсы и систем интернет-технологий и интернет-среды. Международно-правовое регулирование обеспечения права собственности на информацию и права интеллектуальной собственности. Способы защиты права собственности на информацию и права интеллектуальной собственности.

Тема № 9. Проблемы правомерного использования информации в глобальном информационном пространстве

Правовое регулирование распространения коммерческой рекламной информации в глобальном информационном пространстве. Правомерность применения политических технологий в глобальном информационном

пространстве. Правовое регулирование порядка создания и функционирования средств массовой информации в интернет-среде.

Правовое регулирование о конфиденциальности в договорах на выполнение маркетинговых исследований, на передачу ноу-хау или технологии, передачу коммерческой информации и ее переработку, на оказание возмездных информационных услуг, коммерческой концессии.

Тема № 10. Проблемы ответственности за правонарушения, совершённые в глобальном информационном пространстве

Ответственности за нарушение правил ведения электронной коммерции. Электронное мошенничество. Ответственность за неправомерное распространение коммерческой и политической рекламной информации. Ответственность за нарушение авторских и смежных прав.

Уголовная ответственность за преступления в информационной сфере. Административная и дисциплинарная ответственность за правонарушения в информационной сфере. Гражданско-правовая ответственность за правонарушения в информационной сфере.

Рекомендации по работе с литературой

При самостоятельной работе с рекомендуемой литературой студентам необходимо придерживаться определенной последовательности:

– при выборе литературного источника теоретического материала лучше всего исходить из основных понятий изучаемой темы курса, чтобы точно знать, что конкретно искать в том или ином издании;

– для более глубокого усвоения и понимания материала следует читать не только имеющиеся в тексте определения и понятия, но и конкретные примеры;

– чтобы получить более объемные и системные представления по рассматриваемой теме необходимо просмотреть несколько литературных источников (возможно альтернативных);

– необходимо выделить и законспектировать основные положения, определения и понятия, позволяющие выстроить логику ответа на изучаемые вопросы.

Рекомендации по подготовке к зачету

Подготовку к зачету лучше начинать с распределения предложенных контрольных вопросов по разделам и темам курса. Затем необходимо выяснить наличие теоретических источников (конспекта учебных материалов, учебников, учебных пособий).

При изучении материала следует выделять основные положения, определения и понятия, можно их конспектировать. Выделение опорных положений даст возможность систематизировать представления по дисциплине и, соответственно, результативнее подготовиться к экзамену.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЦИФРОВОЙ ЭКОНОМИКИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

«ПРАВОВЫЕ ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

направления 09.04.01 Информатика и вычислительная техника

Магистерская программа «Кибербезопасность»

Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

Код и формулировка компетенции	Этапы формирования компетенции
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-2.1 Знает: модели безопасности компьютерных сетей; виды политик безопасности компьютерных систем и сетей; нормативно-правовые акты, национальные, межгосударственные и международные стандарты в области защиты информации; организационные меры по защите информации ПК-2.2 Умеет: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем ПК-2.3 Владеет: навыками определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети; разработки руководящих документов по защите информации в организации
ПК-5 Способен проводить экспертизу при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-5.1 Знает: форматы хранения информации в анализируемой компьютерной системе; особенности хранения конфигурационной и системной информации в компьютерных системах; уязвимости компьютерных систем и сетей; порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; нормы уголовного и административного права в сфере компьютерной информации; характеристики правонарушений в области связи и информации; виды преступлений в сфере компьютерной информации; порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов ПК-5.2 Умеет: применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа; анализировать структуру механизма возникновения и обстоятельства события; определять причину и условия изменения программного обеспечения; выделять свойства и признаки информации, позволяющие установить ее

	принадлежность определенному источнику; определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой; применять действующую законодательную базу в области обеспечения защиты информации; выявлять возможные траектории состояний функционирования системы и несоответствия имеющейся информации ее расположению в системе ПК-5.3 Владеет: технологиями поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов; навыками прогнозирования возможных путей развития новых видов компьютерных преступлений, правонарушений и инцидентов; способами обнаружения и нейтрализации последствий вторжений в компьютерные системы; методами анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов; методами анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении

Контроль достижений целей курса

№ п/п	Контролируемые модули/ разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства – наименование	
				текущий контроль	промежуточная аттестация
1	Тема 1-4	ПК-2, ПК-5	знает	2, 4, 6 недели – блиц-опрос на занятии (УО); дискуссия (УО-2)	Зачет. Вопросы к экзамену 1-18
			умеет		
			владеет	6 неделя – выполнение первой части реферата	
2	Тема 5-7	ПК-2, ПК-5	знает	3, 5, 8 недели – блиц-опрос на лекции (УО)	Зачет. Вопросы к экзамену 19-30
			умеет		
			владеет	8, 10, 12 неделя – выполнение практических заданий (ПР-11)	
3	Тема 8-10	ПК-2, ПК-5	знает	14, 16 недели – блиц-опрос на занятии (УО)	Зачет. Вопросы к
			умеет		

			владеет	16-18 неделя – выполнение второй части реферата (ПР-3)	экзамену 31-42

Вопросы к экзамену

1. Понятие глобального информационного пространства.
2. Структура глобального информационного пространства.
3. Виды правового регулирования глобального информационного пространства.
4. Международно-правовое регулирование глобального информационного пространства.
5. Государственное регулирование глобального информационного пространства.
6. Понятие и содержание документирования информации.
7. Понятие и виды информационных ресурсов.
8. Понятие и виды информационных технологий.
9. Понятие информационных систем.
10. Правовое регулирование создания и использования информационных систем.
11. Понятие и структура информационного рынка.
12. Правовое регулирование информационного рынка.
13. Правовое регулирование информационного рынка в России.
14. Полномочия международных организаций в регулировании информационного рынка.
15. Понятие и особенности электронной кооперации.
16. Правовой статус субъектов правоотношений в системе «Интернет».
17. Режим свободного доступа к информации.
18. Режим ограниченного доступа к информации.
19. Понятие допуска и доступа к информации.
20. Понятие и виды информационной безопасности.
21. Обеспечение информационной безопасности личности в глобальном информационном пространстве.
22. Виды угроз обеспечения информационной безопасности.
23. Несанкционированное использование или распространение информации в сети Интернет.
24. Виды информации с ограниченным доступом.
25. Государственная и служебная тайна.
26. Конфиденциальная информация.
27. Коммерческая и банковская тайна.
28. Профессиональная тайна.
29. Инсайдерская информация.
30. Обеспечения авторских и смежных прав на информационные технологии, ресурсы и системы.
31. Понятие обеспечение права собственности на информацию и права интеллектуальной собственности.

32. Обеспечение права собственности и права интеллектуальной собственности на информационные технологии, ресурсы и систем интернет-технологий и интернет-среды.
33. Способы защиты права собственности на информацию и права интеллектуальной собственности.
34. Правовое регулирование распространения коммерческой рекламной информации в глобальном информационном пространстве.
35. Правомерность применения политических технологий в глобальном информационном пространстве.
36. Правовое регулирование порядка создания и функционирования средств массовой информации в интернет-среде.
37. Ответственности за нарушение правил ведения электронной коммерции.
38. Электронное мошенничество.
39. Ответственность за неправомерное распространение коммерческой и политической рекламной информации.
40. Уголовная ответственность за преступления в информационной сфере.
41. Административная и дисциплинарная ответственность за правонарушения в информационной сфере.
42. Гражданско-правовая ответственность за правонарушения в информационной сфере.

Критерии выставления оценки студенту на зачете по дисциплине

Баллы (рейтинговой оценки)	**Оценка зачета/ экзамена**	**Требования к сформированным компетенциям**
100-86	*«зачтено» / «отлично»*	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение.
85-76	*«зачтено»/ «хорошо»*	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

75-61	*«зачтено» / «удовлетворительно»*	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
60-50	*«не зачтено» / «неудовлетворительно»*	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.