

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное учреждение  
высшего профессионального образования  
"Казанский (Приволжский) федеральный университет"  
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.



20\_\_ г.

подписано электронно-цифровой подписью

### Программа дисциплины

Правовое обеспечение информационной безопасности Б1.В.ОД.4

Направление подготовки: 09.04.03 - Прикладная информатика

Профиль подготовки: Информационная безопасность экономических систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

**Автор(ы):**

Сабирова Л.Л.

**Рецензент(ы):**

Туфетулов А.М.

**СОГЛАСОВАНО:**

Заведующий(ая) кафедрой: Туфетулов А. М.

Протокол заседания кафедры No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_ г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_ г

Регистрационный No 913816

Казань  
2016

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. Сабирова Л.Л. Кафедра теории и истории государства и права Юридический факультет , LLSabirova@kpfu.ru

### 1. Цели освоения дисциплины

Цель изучения дисциплины – формирование у будущих бакалавров теоретических знаний и практических навыков в области правового регулирования общественных отношений в сфере информационной безопасности, формирование и развитие правовой культуры и правового сознания. При этом важно развить у студентов способность применять полученные знания и навыки для решения конкретных задач, возникающих в процессе профессиональной деятельности.

Дисциплина предусматривает решение следующих задач:

- получение системы знаний о таком социальном регуляторе как право, формирование понятийной базы в области юриспруденции;
- ознакомление с основными нормами права, регулирующими правовое обеспечение информационной безопасности;
- изучение правового механизма реализации прямых и косвенных методов государственного управления общественной жизнью в целом и информационной, в частности;
- исследование условий осуществления информационной безопасности в рамках правового поля;
- обучение легитимным способам защиты своих прав и законных интересов.

### 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.В.ОД.4 Дисциплины (модули)" основной образовательной программы 09.04.03 Прикладная информатика и относится к обязательные дисциплины. Осваивается на 1 курсе, 2 семестр.

Данная учебная дисциплина включена в раздел Б1.Б.4 гуманитарного, социального и экономического цикла дисциплин и относится к базовой части. Осваивается на первом курсе (2 семестр).

Изучению дисциплины предшествует изучение ряда дисциплин в рамках школьной программы среднего образования (таких, как: обществознание, русский язык) и предметов гуманитарного блока в рамках высшей школы (таких, как Правоведение). Данная дисциплина способствует освоению многих профессиональных дисциплин.

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-3 (общекультурные компетенции)	способностью к саморазвитию, самореализации, использованию творческого потенциала;
ОПК-1 (профессиональные компетенции)	способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач профессиональной деятельности;
ОПК-2 (профессиональные компетенции)	способностью руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия;

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-3 (профессиональные компетенции)	способностью исследовать современные проблемы и методы прикладной информатики и научно-технического развития информационно-коммуникационных технологий;
ПК-19 (профессиональные компетенции)	способностью организовывать и проводить переговоры с представителями заказчика и профессиональные консультации на предприятиях и в организациях;
ПК-20 (профессиональные компетенции)	способностью в условиях функционирования ИС брать на себя ответственность за выполнение производственных задач ИТ-служб, эффективно использовать современные приемы и методы работы с ИТ-персоналом;
ПК-21 (профессиональные компетенции)	способностью использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС;
ПК-22 (профессиональные компетенции)	способностью использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций;
ПК-23 (профессиональные компетенции)	способностью использовать информационные сервисы для автоматизации прикладных и информационных процессов.

В результате освоения дисциплины студент:

1. должен знать:

существующие подходы к пониманию сущности и содержания базовых отраслей российского права как элемента правового механизма регулирования общественной жизни;

□ место и роль базовых отраслей российского права (конституционного права, административного права, уголовного права, экологического права, информационного права, гражданского права, хозяйственного права, трудового права, семейного права) в российской правовой системе;

□ основные понятия и институты изучаемых базовых отраслей российского права;

□ положения Конституции РФ, постановления и определения Конституционного Суда РФ по проблемам обеспечения прав и законных интересов субъектов, органов государственной власти РФ, субъектов РФ и органов местного самоуправления;

□ нормы Гражданского кодекса РФ, Уголовного кодекса РФ, Кодекса об административных правонарушениях, Трудового кодекса РФ, Семейного кодекса РФ, которые применяются для регулирования правоотношений, возникающих при обеспечении информационной безопасности;

□ специальные нормы федерального законодательства, которые определяют содержание основных институтов базовых отраслей российского права;

□ возможности работы с правовой информацией, размещенной в глобальной компьютерной сети Интернет;

2. должен уметь:

толковать и применять законы и другие нормативно-правовые акты, регламентирующие правовое обеспечение информационной безопасности субъектов, а также приемы, способы, пределы государственного управления в этой сфере;

□ юридически грамотно квалифицировать факты и обстоятельства деятельности субъектов;

□ осуществлять правоприменение на уровне учебных задач по вопросам, возникающим в предметной области изучаемых базовых отраслей российского права;

□ понимать и осуществлять преддоговорную и договорную работу, действия по самозащите прав;

### 3. должен владеть:

специальными (практическими) навыками работы в справочной правовой системе "КонсультантПлюс", позволяющими находить ответы на вопросы правоприменительной практики (общие знания и навыки о функционировании пользовательского интерфейса справочной правовой системы "КонсультантПлюс": устройство системы "КонсультантПлюс"; основные способы поиска документа по заданным реквизитам; работа с документом, редакционные возможности; создание подборки документов по заданной правовой проблеме; работа со встроенными формами документов в форматах MS Word и MS Excel, – формируются у студентов в процессе изучения курса "Информатика");

□ приемами и технологией сбора, систематизации и анализа нормативной и фактической информации, имеющей значение для реализации правовых норм в сфере правового обеспечения информационной безопасности субъектов;

□ методикой осуществления правовой экспертизы нормативно-правовых актов в изучаемой сфере;

□ навыками разработки отдельных документов правового характера.

### 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет во 2 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

#### 4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

##### Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.	2	1	2	0	2	устный опрос
2.	Тема 2. Основные понятия, виды и источники информации, подлежащей защите.	2	2-3	4	0	4	научный доклад

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности.	2	4-5	4	0	4	тестирование устный опрос
4.	Тема 4. Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ. Практика защиты коммерческой тайны за рубежом.	2	6	2	0	2	устный опрос тестирование
5.	Тема 5. Проблемы и угрозы информационной безопасности.	2	7	2	0	2	дискуссия
	Тема . Итоговая форма контроля	2		0	0	0	зачет
	Итого			14	0	14	

## 4.2 Содержание дисциплины

### Тема 1. Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.

#### **лекционное занятие (2 часа(ов)):**

Основные понятия. Общие положения. Типы и виды информационной безопасности. Участники отношений в области информационной безопасности. Федеральные, региональные, местные законы по информационной безопасности. Основные международные акты, регулирующие сферу информационной безопасности. Объективные и субъективные предпосылки создания глобального общества. Роль Интернета в мировом информационном пространстве. Глобальные ожидания и опасения человечества. Негативные последствия глобальной информатизации общества. Конституция РФ о правовом обеспечении информационной сферы. Федеральное законодательство в сфере информационной безопасности. Федеральные законы, Указы Президента РФ и иные нормативно-правовые акты по вопросам информационной безопасности. Организационное обеспечение информационной безопасности. Международное сотрудничество России в области обеспечения информационной безопасности.

#### **лабораторная работа (2 часа(ов)):**

Основы правового регулирования отношений в сфере информационной безопасности. Система нормативно-правовых актов, регулирующих данную проблематику. Международные нормы в области информационной безопасности.

### Тема 2. Основные понятия, виды и источники информации, подлежащей защите.

#### **лекционное занятие (4 часа(ов)):**

Лекция 1. Информация и право. Научно-технический прогресс и условия формирования информационного общества. Информатика и правовые дисциплины. Информационное право.  
Лекция 2. Виды информации, подлежащей защите. Понятие информации с ограниченным доступом. Соотношение тайн и права на информацию.

**лабораторная работа (4 часа(ов)):**

Занятие 1. Информация, подлежащая правовой защите: понятие, виды. Занятие 2. Источники информации, подлежащей правовой защите.

**Тема 3. Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности.**

**лекционное занятие (4 часа(ов)):**

Лекция 1. Методы государственного регулирования информационной безопасности. Программы развития информационной безопасности. Лекция 2. Статистическое наблюдение в области информационной безопасности. Государственная поддержка информационной безопасности в Российской Федерации. Информационное обеспечение информационной безопасности.

**лабораторная работа (4 часа(ов)):**

Занятие 1. Основы и методы государственной политики Российской Федерации обеспечения информационной безопасности. Занятие 2. Формы правового регулирования отношений в области создания и использования информационных систем, информационных технологий и средств их обеспечения. Заказчики, разработчики и эксплуатационники. Лицензирование.

**Тема 4. Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ. Практика защиты коммерческой тайны за рубежом.**

**лекционное занятие (2 часа(ов)):**

Понятие государственной тайны, правовое регулирование. Режим государственной тайны. Понятие коммерческой тайны, правовое регулирование. Режим коммерческой тайны. Практика правового регулирования и защиты коммерческой тайны за рубежом.

**лабораторная работа (2 часа(ов)):**

Понятие и значение государственной тайны и коммерческой тайны. Вопросы правового регулирования. Отечественный и зарубежный опыт в защите государственной и коммерческой тайны.

**Тема 5. Проблемы и угрозы информационной безопасности.**

**лекционное занятие (2 часа(ов)):**

Понятие информационной безопасности. Основные проблемы информационной безопасности и пути их решения. Виды и источники угроз информационной безопасности. Информационные противостояния от древности до Нового времени. Информационные войны XX века. Место информационной безопасности в системе национальной безопасности России.

**лабораторная работа (2 часа(ов)):**

Глобальные ожидания и опасения человечества. Негативные последствия глобальной информатизации общества. Проблемы правового регулирования распространения информации через Интернет. Сущность и современное состояние манипуляции сознанием и поведением людей. Основные методы и средства информационного воздействия на человека. Мифы как инструмент воздействия на людей. Манипулятивные технологии в избирательных кампаниях. Технологии «черного пиара». Дестабилизирующее влияние слухов. Влияние средств массовой информации на мировоззрение людей и духовно-нравственное становление подрастающих поколений. Роль рекламы в манипуляции сознанием людей. Повседневный-бытовой уровень манипуляции сознанием. Средства информационного воздействия и защита здоровья.

#### **4.3 Структура и содержание самостоятельной работы дисциплины (модуля)**

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.	2	1	подготовка к устному опросу	7	устный опрос
2.	Тема 2. Основные понятия, виды и источники информации, подлежащей защите.	2	2-3	подготовка к научному докладу	10	научный доклад
3.	Тема 3. Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности.	2	4-5	подготовка к тестированию	3	тестирование
				подготовка к устному опросу	7	устный опрос
4.	Тема 4. Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ. Практика защиты коммерческой тайны за рубежом.	2	6	подготовка к тестированию	3	тестирование
				подготовка к устному опросу	7	устный опрос
5.	Тема 5. Проблемы и угрозы информационной безопасности.	2	7	подготовка к дискуссии	7	дискуссия
	Итого				44	

### 5. Образовательные технологии, включая интерактивные формы обучения

Освоение дисциплины предполагает использование как традиционных (лекции, практические занятия с использованием методических материалов), так и инновационных образовательных технологий с использованием в учебном процессе активных и интерактивных форм проведения занятий: решение и обсуждение правовых казусов; проведение семинара в форме семинара-дискуссии - решения "проблемной ситуации" по теме дисциплины; подготовка докладов в форме презентаций обучающимися, объединенными преподавателем в подгруппы.

### 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

## **Тема 1. Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.**

устный опрос , примерные вопросы:

Примерные вопросы для обсуждения: 1. Понятие и значение информации. История создания информационного общества, основные этапы развития. 2. Информация и право. Информационное право: понятие, субъекты (участники) и объекты. 3. Источники правового регулирования информационной безопасности. 4. Понятие системы международного информационного права. 5. Научно-технический прогресс и условия формирования информационного общества. Соотношение тайн и права на информацию.

## **Тема 2. Основные понятия, виды и источники информации, подлежащей защите.**

научный доклад , примерные вопросы:

Примерные темы для самостоятельного изучения и подготовки доклада: 1. Место информационной безопасности в системе национальной безопасности России. 2. Правовые основы информационной безопасности РФ. 3. Федеральное законодательство в сфере информационной безопасности. 4. Международное сотрудничество России в области обеспечения информационной безопасности. 5. Информационное общество. Стадии становления. 6. Хартия Глобального информационного общества (Окинава). 7. Государственная политика в области формирования информационного общества. 8. Проблемы правового регулирования отношений в условиях информационного общества. 9. Безопасность в сфере духовной жизни человека и общества. 10. Информационное право РФ. 11. Участник информационных отношений: понятие, правовое положение. 12. Юридическая ответственность за правонарушения, связанные с нарушением информационной безопасности: понятие, виды. 13. Судебная практика по нарушению информационной безопасности.

## **Тема 3. Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности.**

тестирование , примерные вопросы:

Примерные тестовые задания. Вопрос 1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это... 1) политическая разведка; 2) промышленный шпионаж; 3) добросовестная конкуренция; 4) конфиденциальная информация; 5) правильного ответа нет. Вопрос 2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности? 1) любая информация; 2) только открытая информация; 3) запатентованная информация; 4) закрываемая собственником информация; 5) коммерческая тайна. Вопрос 3. Кто может быть владельцем защищаемой информации? 1) только государство и его структуры; 2) предприятия акционерные общества, фирмы; 3) общественные организации; 4) только вышеперечисленные; 5) кто угодно. Вопрос 4. Какие сведения на территории РФ могут составлять коммерческую тайну? 1) учредительные документы и устав предприятия; 2) сведения о численности работающих, их заработной плате и условиях труда; 3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности; 4) другие; 5) любые. Вопрос 5. Какие секретные сведения входят в понятие ?коммерческая тайна?? 1) связанные с производством; 2) связанные с планированием производства и сбытом продукции; 3) технические и технологические решения предприятия; 4) только 1 и 2 вариант ответа; 5) три первых варианта ответа. Вопрос 6. Что называют источником конфиденциальной информации? 1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников; 2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе; 3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники; 4) это защищаемые предприятием сведения в области производства и коммерческой деятельности; 5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

устный опрос , примерные вопросы:

Примерные вопросы для обсуждения: 1. Основы государственной политики Российской Федерации обеспечения информационной безопасности: понятие и виды. 2.

Организационно-правовое регулирование защиты информации. 3. Классификация видов противоправных деяний в отношении информации.

#### **Тема 4. Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ. Практика защиты коммерческой тайны за рубежом.**

тестирование , примерные вопросы:

Примерные тестовые задания. Вопрос 1. Что называют источником конфиденциальной информации? 1) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников; 2) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе; 3) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники; 4) это защищаемые предприятием сведения в области производства и коммерческой деятельности; 5) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации. Вопрос 2. Как называют процессы обмена информацией с помощью официальных, деловых документов? 1) непосредственные; 2) межличностные; 3) формальные; 4) неформальные; 5) конфиденциальные. Вопрос 3. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника? 1) хищение носителей информации; 2) использование технических средств для перехвата электромагнитных ПЭВМ; 3) разглашение; 4) копирование программой информации с носителей; 5) другое. Вопрос 4. Каким образом происходит разглашение конфиденциальной информации? 1) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера; 2) опубликование материалов в печати; 3) сообщение, передача, предоставление в ходе информационного обмена; 4) все вышеперечисленные способы; 5) правильного варианта ответа нет. Вопрос 5. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации? 1) получить, изменить, а затем передать ее конкурентам; 2) размножить или уничтожить ее; 3) получить, изменить или уничтожить; 4) изменить и уничтожить ее; 5) изменить, повредить или ее уничтожить.

устный опрос , примерные вопросы:

Примерные вопросы для обсуждения: 1. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну. 2. Защита информации в экономике, внутренней и внешней политике, науке и технике. Защита интеллектуальной собственности. 3. Информационное обеспечение оборонных мероприятий и боевых действий. Понятие информационной войны. 4. Обеспечение информационной безопасности в правоохранительной сфере и при возникновении чрезвычайных ситуаций. 5. Методы и средства защиты электронной информации.

#### **Тема 5. Проблемы и угрозы информационной безопасности.**

дискуссия , примерные вопросы:

Примерные темы для самостоятельного изучения и подготовки выступления в дискуссии 1. Понятие информационной безопасности. Виды и источники угроз информационной безопасности. 2. Информационные противостояния от древности до Нового времени. Информационные войны XX века. 4. Основные методы и средства информационного воздействия на человека. 5. Манипулятивные технологии в избирательных кампаниях. Технологии ?черного пиара?. 6. Дестабилизирующее влияние слухов. 7. Влияние средств массовой информации на мировоззрение людей и духовно-нравственное становление подрастающих поколений. 8. Роль рекламы в манипуляции сознанием людей. 9. Средства информационного воздействия и защита здоровья. 10. Роль Интернета в мировом информационном пространстве. 11. Негативные последствия глобальной информатизации общества.

#### **Тема . Итоговая форма контроля**

Примерные вопросы к зачету:

Примерные вопросы к зачету.

1. Роль информации в жизни личности, общества, государства.
2. Информационное общество. Стадии становления.
3. Хартия Глобального информационного общества (Окинава).
4. Государственная политика в области формирования информационного общества.
5. Проблемы правового регулирования отношений в условиях информационного общества.
6. Определение понятия "информация" информация как основной объект информационной сферы и правовой системы.
7. Информация в актах законодательства России.
8. Юридические особенности и свойства информации. Классификация информации.
9. Структура информационной сферы, основные и обеспечивающие области информационной сферы.
10. Информационные процессы. Информационные системы.
11. Понятие информационного права. История становления информационного права.
12. Информационные права и свободы - фундамент правового регулирования информационной безопасности.
13. Основные субъекты информационного права: производители информации, обладатели информации, потребители информации, собственники и владельцы информационных объектов.
14. Информационные отношения.
15. Методы правового регулирования информационной безопасности. Особенности применения методов правовой информатики и правовой кибернетики.
16. Принципы правового регулирования информационной безопасности.
17. Информационно-правовые нормы. Общая характеристика, структура, содержание, состав. Специфика информационно-правовых норм.
18. Информационное правоотношение. Понятие, содержание, структура. Классификация информационных правоотношений.
19. Информационное законодательство. Структура и состав отечественного информационного законодательства.
20. Информационно-правовые нормы международно-правовых актов.
21. Информационно-правовые нормы Конституции РФ.
22. Нормы об ответственности за правонарушения в информационной сфере.
23. Конституционная основа осуществления права на поиск, получение и передачу информации. Субъективные права.
24. Правоотношения, возникающие между потребителями информации, с одной стороны, и производителями, обладателями информации - с другой.
25. Правовые гарантии поиска и получения информации. Свобода доступа к информации. Правовой режим доступа к открытой информации.
26. Ограничения доступа к информации на основе закона. Ограничение распространения информации, представляющей угрозу интересам личности, общества, государства.
27. Баланс интересов личности, общества, государства при осуществлении права на доступ к информации.
28. Право на поиск и получение документированной информации из государственных информационных ресурсов.
29. Право каждого на доступ и получение информации о себе.
30. Формы правового регулирования отношений в области производства документированной информации, формирования и использования информационных ресурсов.
31. Обязательный экземпляр документа как разновидность документированной информации.
32. Юридическая модель самостоятельного оборота информации. Гражданский и публичный оборот информации.
33. Правовой режим документированной информации.

34. Электронный документ, электронный документооборот, электронная цифровая подпись в гражданском и публичном оборотах.
35. Правовой статус производителя, обладателя и потребителя информации, производителя информационных услуг. Правовой статус собственника и владельца информационных объектов.
36. Документированная информация в международном информационном обмене.
37. Государственная политика в области формирования и использования информационных ресурсов.
38. Формы правового регулирования отношений в области создания и использования информационных систем, информационных технологий и средств их обеспечения. Заказчики, разработчики и эксплуатационники.
39. Государственная политика в области создания и использования информационных систем, информационных технологий и средств их обеспечения.
40. Формы правового регулирования отношений в области информационной безопасности. Угрозы безопасности в информационной сфере.
41. Защита прав и свобод человека и гражданина в информационной сфере в условиях информатизации.
42. Государственная политика в области информационной безопасности.
43. Доктрина информационной безопасности.
44. Интернет и право. Виртуальная среда обращения информации и информационных отношений.

### **7.1. Основная литература:**

1. Основные положения информационной безопасности: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с. Режим доступа: <http://znanium.com/bookread2.php?book=508381>
2. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. Режим доступа: <http://znanium.com/bookread2.php?book=491597>
3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. Режим доступа: <http://znanium.com/bookread2.php?book=423927>

### **7.2. Дополнительная литература:**

1. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н. Н. Куняев. - М.: Логос, 2010. - 348 с. Режим доступа: <http://znanium.com/bookread2.php?book=469026>
2. Кузнецов, И. Н. Бизнес-безопасность [Электронный ресурс] / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - 416 с. Режим доступа: <http://znanium.com/bookread2.php?book=430343>
3. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. Режим доступа: <http://znanium.com/bookread2.php?book=463061>

### **7.3. Интернет-ресурсы:**

- Сайт Верховного Суда Российской Федерации - <http://www.vsrp.ru/>  
Сайт Государственной Думы Российской Федерации - <http://www.duma.gov.ru/>  
Сайт Конституционного Суда Российской Федерации - <http://www.ksrf.ru>

Справочная правовая система ?ГАРАНТ? - [http:// www.garant.ru](http://www.garant.ru)

Справочная правовая система ?КонсультантПлюс? - [http:// www.consultant.ru](http://www.consultant.ru)

## **8. Материально-техническое обеспечение дисциплины(модуля)**

Освоение дисциплины "Правовое обеспечение информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Программное обеспечение для изучения дисциплины:

– пакет прикладных программ MS Office, в том числе MS Word 2007, PowerPoint 2007.

г) базы данных, информационно-справочные и поисковые системы

– "КонсультантПлюс"

- "ГАРАНТ".

Материально-техническое обеспечение дисциплины:

□ компьютерные классы с выходом в Интернет и доступом к справочным правовым системам "КонсультантПлюс" и (или) "ГАРАНТ";

□ аудитории, оборудованные мультимедийными средствами обучения.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 09.04.03 "Прикладная информатика" и магистерской программе Информационная безопасность экономических систем .

Автор(ы):

Сабирова Л.Л. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Туфетулов А.М. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.