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

Нижегородский институт управления – филиал РАНХиГС
(наименование института (факультета))
Кафедра правового обеспечения национальной безопасности
(наименование кафедры)

УТВЕРЖДЕНО
Директор Нижегородского института управления – филиала РАНХиГС

Парамонов Александр Васильевич
Подписано цифровой подписью: Парамонов Александр Васильевич
Дата: 2024.07.02 16:06:40 +03'00'

ПРОГРАММА МАГИСТРАТУРЫ

«Информационные технологии в государственном и муниципальном управлении»
(наименование образовательной программы)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ, реализуемой с применением электронного (онлайн) курса

Б1.В.ДВ.04.02 ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(индекс и наименование дисциплины, в соответствии с учебным планом)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)
очная, заочная
(форма обучения)

Год набора – 2024

Нижний Новгород, 2024 г.

Авторы-составители:

Доцент кафедры правового обеспечения национальной безопасности, канд. полит. наук, доцент — И.А. Кононов

(ученая степень и(или) ученое звание, должность, наименование кафедры) — *(Ф.И.О.)*

Заведующий кафедрой правового обеспечения национальной безопасности, канд. юрид. наук, доцент — М.В. Балалаева

(ученая степень и(или) ученое звание, должность, наименование кафедры) — *(Ф.И.О.)*

РПД Б1.В.ДВ.04.02 Правовые основы информационной безопасности одобрена на заседании кафедры правового обеспечения национальной безопасности.

Протокол № 7 от 09 февраля 2024 г.

Содержание

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы 4

2. Объем и место дисциплины в структуре ОП ВО 5

3. Содержание и структура дисциплины 5

4. Материалы текущего контроля успеваемости обучающихся 8

5. Оценочные материалы промежуточной аттестации по дисциплине 11

6. Методические материалы по освоению дисциплины с применением ЭК 16

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 19

7.1 Основная литература 19

7.2 Дополнительная литература 20

7.3 Учебно-методическое обеспечение самостоятельной работы. 20

7.4 Нормативно-правовые документы 20

7.5. Интернет-ресурсы, справочные системы. 23

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 24

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

1.1 Дисциплина «Правовые основы информационной безопасности» обеспечивает овладение следующими компетенциями:

Таблица 1.

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента освоения компетенции
ПК-12	Способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств, адаптировать современные ИКТ к задачам прикладных ИС	ПК-12.2	Способен применять технологии подбора современных ИКТ в соответствии с решаемыми прикладными задачами с учетом действующих правовых норм.
ПК-20	Способен использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций	ПК-20.2	Способен использовать международные стандарты и информационные ресурсы на практике, внедряя их в производственно-технологический процесс

1.2 В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2.

ОТФ/ТФ/ профессиональные действия	Код компонента компетенции	Планируемые результаты обучения
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D); ТФ: • разработка инструментов и методов адаптации бизнес-процессов заказчика к возможностям ИС (D/09.7).	ПК-12.2	На уровне знаний: – устройство и функционирование современных ИС; – источники информации, необходимой для профессиональной деятельности; – современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM). На уровне навыков: • владения технологией подбора современных ИКТ в соответствии с решаемыми прикладными задачами.
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (D); ТФ: • разработка инструментов и методов проектирования бизнес-процессов заказчика (D/08.7); • организационное и технологическое обеспечение разработки баз данных ИС (D/17.7).	ПК-20.2	На уровне знаний: – современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); – программные средства и платформы инфраструктуры информационных технологий организаций; – ссовременные стандарты информационного взаимодействия систем; – отраслевая нормативная техническая документация. На уровне навыков: – работы с отечественными и международными базами данных, прикладными программами и приложениями, в рамках осуществления профессиональной деятельности.

2. Объем и место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.04.02 «*Правовые основы информационной безопасности*» входит в число дисциплин по выбору части, формируемой участниками образовательных отношений, Блока 1 Дисциплины (модули) в соответствии с учебным планом.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 академических часа / 54 астрономических часа.

Освоение дисциплины опирается на необходимый объем теоретических знаний и практических навыков в области права и информационных технологий.

Дисциплины, на которых базируется данная дисциплина: Тенденции развития Web-пространства (Б1.О.07); Технологии межведомственного электронного взаимодействия (Б1.В.01.05).

Дисциплины, для которых данная дисциплина является предшествующей: Организационные основы обеспечения информационной безопасности (Б1.В.ДВ.03.01); Программно-техническое обеспечение компьютерной безопасности (Б1.В.ДВ.03.02).

При ***очной форме обучения*** на контактную работу с преподавателем выделено 32 ч, в том числе на лекционные занятия – 8 ч, на практические (семинарские) занятия – 24 ч; контроль – 4 ч; на самостоятельную работу обучающихся выделено 36 ч.

При ***заочной форме обучения*** на контактную работу с преподавателем выделено 12 ч, в том числе на лекционные занятия – 4 ч, на практические (семинарские) занятия – 8 ч;контроль – 4 ч; на самостоятельную работу обучающихся выделено 56 ч.

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Таблица 3.

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, и промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО ДОТ*	ПЗ/ ЭО ДОТ*	КСР		
Очная форма обучения								
Тема 1	Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.	8	2	-	2	-	4	О
Тема 2	Основные понятия, виды и источники информации, подлежащей защите.	8	-	-	2	-	6	О
Тема 3	Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности	12	2	-	4	-	6	ПЗ
Тема 4	Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ.	8	-	-	4	-	4	О
Тема 5	Проблемы и угрозы информационной безопасности.	12	2	-	4	-	6	О

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, и промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО, ДОТ*	ЛР/ ЭО ДОТ*	ПЗ/ ЭО ДОТ*	КСР		
Тема 6	Особенности работы с персоналом, владеющим конфиденциальной информацией	8	-	-	4	-	4	ПЗ
Тема 7	Защищенный документооборот	12	2		4		6	Д
Промежуточная аттестация		4						зачет
Всего (в з.е./акад.часах/астр.часах):		**2/72/54**	**8/6**		**24/18**		**36/27**	4/3
Заочная форма обучения								
Тема 1	Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.	9	1	-	1	-	7	О
Тема 2	Основные понятия, виды и источники информации, подлежащей защите.	9	-	-	1	-	8	О
Тема 3	Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности	10	1	-	1	-	8	ПЗ
Тема 4	Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ.	10	-	-	1	-	9	О
Тема 5	Проблемы и угрозы информационной безопасности.	10	1	-	1	-	8	О
Тема 6	Особенности работы с персоналом, владеющим конфиденциальной информацией	9	-	-	1	-	8	ПЗ
Тема 7	Защищенный документооборот	11	1		2		8	Д
Промежуточная аттестация		4						зачет
Всего (в з.е./акад.часах/астр.часах):		**2/72/54**	**4/3**		**8/6**		**56/42**	**4/3**

Примечание:
** – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом*
*** – формы текущего контроля успеваемости: опрос (О), отчет о выполнении практического задания (ПЗ), оценка доклада (Д)*

3.2. Содержание дисциплины

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

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.

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

Информация и право. Научно-технический прогресс и условия формирования информационного общества. Информатика и правовые дисциплины. Информационное право.

Виды информации, подлежащей защите. Понятие информации с ограниченным доступом.

Виды конфиденциальной информации: тайна частной жизни, коммерческая тайна, банковская тайна,

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

Методы государственного регулирования информационной безопасности. Программы развития информационной безопасности. Статистическое наблюдение в области информационной безопасности. Государственная поддержка информационной безопасности в Российской федерации. Информационное обеспечение информационной

Тема 4 Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ.

Понятие государственной тайны, правовое регулирование. Режим государственной тайны. Перечень сведений, запрещенных к засекречиванию:

- ✓ о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- ✓ о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- ✓ о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- ✓ о фактах нарушения прав и свобод человека и гражданина;
- ✓ о размерах золотого запаса и государственных валютных резервов Российской Федерации;
- ✓ о состоянии здоровья высших должностных лиц Российской Федерации;
- ✓ о фактах нарушения законности органами государственной власти и их должностными лицами.

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

Тема 5 Проблемы и угрозы информационной безопасности.

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 XXI века. Место информационной безопасности в системе национальной безопасности России.

Тема 6 Особенности работы с персоналом, владеющим конфиденциальной информацией

Угрозы безопасности информации от персонала и направления ее защиты. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.

Доступ персонала к конфиденциальным сведениям, документам и базам данных

Принципы, организационные формы и методика обучения сотрудников правилам обеспечения безопасности информации.

Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией. Правовая ответственность персонала за разглашение информации ограниченного доступа.

Тема 7 Защищенный документооборот

Понятие и задачи, основные требования к защищённому документообороту. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.

Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.

Принципы учёта документов, содержащих сведения ограниченного доступа.

Технология обработки подготовленных документов, содержащих сведения ограниченного доступа.

Порядок работы персонала с документами, содержащих сведения ограниченного доступа. Проверка наличия документов, дел и носителей информации.

Формирование и хранение дел, содержащих информацию ограниченного доступа.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.В.ДВ.04.02 «*Правовые основы информационной безопасности*» используются следующие **методы текущего контроля** успеваемости обучающихся:

Таблица 4.

Тема (раздел)	**Методы текущего контроля успеваемости**
Тема 1 Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности.	Опрос
Тема 2 Основные понятия, виды и источники информации, подлежащей защите.	Опрос
Тема 3 Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности	Решение задач
Тема 4 Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ.	Опрос
Тема 5 Проблемы и угрозы информационной безопасности.	Опрос
Тема 6 Особенности работы с персоналом, владеющим конфиденциальной информацией	Решение задач
Тема 7 Защищенный документооборот	Доклады

4.2. Типовые материалы текущего контроля успеваемости обучающихся

По теме 1. «Правовое регулирование отношений в области информационной безопасности. Международные стандарты безопасности».

Примерный перечень вопросов для опроса

1. Понятие и виды информации, её роль в жизни личности, общества, государства.
2. Информационно-правовые нормы и информационные правоотношения: содержание, основания возникновения, классификация.
3. Информационная безопасность как элемент национальной безопасности.
4. Система нормативно-правовых актов, регулирующих вопросы информационной безопасности.
5. Основные задачи и уровни реализации информационной безопасности.

По теме 2 «Основные понятия, виды и источники информации, подлежащей защите».

Примерный перечень вопросов для опроса

1. Основные понятия в области обеспечения безопасности информации определены в ГОСТ Р 50922-2006 – Защита информации. Основные термины и определения (взамен ГОСТ Р 50922-96).
2. Назовите особенности современного информационного общества.
3. Какие элементы информационной инфраструктуры Вы знаете?
4. Что понимается под угрозой безопасности информации?
5. Дайте определение информационной безопасности на предприятии.
6. Назовите объекты информационной безопасности на предприятии.
7. Какие обеспечивающие подсистемы включает система защиты информации?
8. Назовите особенности экономической информации.
9. В чем отличия понятий информационный ресурс, продукт и услуга?
10. Как определяется цена информационного продукта?
11. Что такое конфиденциальность, целостность и доступность информации?
12. Какая информация компании не может быть отнесена к коммерческой тайне?
13. Что такое персональные данные?

По теме 3. «Основы государственной политики Российской Федерации обеспечения информационной безопасности. Организационно-правовые методы обеспечения финансово-информационной безопасности»

Примерные варианты практико-ориентированных заданий
для проведения текущего контроля успеваемости обучающихся

Задача 1.

Волков С.А. сделал резервную копию для личного пользования с подаренного ему CD-диска с компьютерной игрой.

Дайте юридическую оценку действиям Волкова. Назовите нормативные акты, регулирующие описанные правоотношения.

Задача 2.

Михайлов О.Ф. приобрел в магазине в качестве подарка на день рождения другу Семенову М.Н. лицензионный DWD-диск с записью концерта любимой группы последнего, сделал с него копию и оставил себе.

Дайте правовую оценку действиям Михайлова. Охарактеризуйте юридические полномочия Семёнова как собственника данного DWD-диска.

Задача 3.

Соколов А.Н. приобрёл на радиорынке диск с нелицензионным экземпляром программного продукта, который не работал из-за встроенных в него модулей,

защищающих от несанкционированной активации. Тогда Соколов скопировал с компьютера своего знакомого Орлова Н.С. специальную компьютерную программу, запуск которой обеспечил нейтрализацию средств защиты и работу программного продукта.

Квалифицируйте действия Соколова и Орлова. Подлежат ли они юридической ответственности?

По теме 4. «Понятие и режим государственной тайны. Понятие и режим коммерческой тайны в РФ».

Примерный перечень вопросов для опроса

1 Что составляет базу функционирования специализированных организаций в сфере информационной безопасности?

2 Назовите характерные черты организационной работы специализированных организаций в сфере информационной безопасности.

3 Что представляют собой альянсы крупных технологических компаний?

4 Перечислите типичные приемы организационной работы альянсов крупных технологических компаний.

5 Сделайте доклад о деятельности одной из специализированных организаций в сфере информационной безопасности.

6 Чем занимается Альянс по смарт-картам?

7 Какие задачи решает Альянс по безопасности сети Интернет?

8 Сделайте доклад о деятельности одной из международных организаций в сфере информационной безопасности.

9 О чем Доктрина информационной безопасности РФ (5 декабря 2016 г.)?

10 Дайте характеристику Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»?

11 О чем Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» (с изм. на 2022 г.)?

12 Охарактеризуйте содержание статей 159(1-6), 272, 273, 274 УК.

По теме 5. «Проблемы и угрозы информационной безопасности».

Примерный перечень вопросов для опроса

1 Назовите основные принципы политики безопасности.

2 Что означает принцип эшелонированной обороны?

3 Какие вопросы отражаются в Концепции информационной безопасности?

4 Что включает политика безопасности верхнего уровня?

5 Как организован удаленный доступ к сервису?

6 Что включает политика управления паролями?

7 Как оценить риски реализации угроз информации?

8 Какие этапы выделяются в жизненном цикле информационного сервиса?

9 На каких принципах базируется системный подход к защите информации?

10 Как обеспечивается управление доступом?

11 Какие программные средства используются для ИБ?

12 В чем отличия метода принуждения от метода побуждения?

13 Чем занимается криптография?

14 Что такое электронная подпись и для чего она используется?

По теме 6. «Особенности работы с персоналом, владеющим конфиденциальной информацией»

Примерные варианты практико-ориентированных заданий для проведения текущего контроля успеваемости обучающихся

Задача 1.

В ООО «Дельта» планируется ввести режим коммерческой тайны. Доступ к сведениям, составляющим коммерческую тайну данной организации, для выполнения своих функциональных обязанностей необходим коммерческому директору Остапову Ф.Ю., переведённому из другого подразделения на должность менеджера по рекламе Комарову С.О. и поступающей на должность делопроизводителя Лапиной А.Н.

Помимо этого, ООО «Дельта», для выполнений обязательств по находящемуся в стадии разработки договору с ООО «Гамма» должно будет использовать сведения, составляющие коммерческую тайну последнего.

Каким образом следует организовать доступ указанных лиц к сведениям, составляющим коммерческую тайну ООО «Дельта» и «Гамма» с точки зрения обеспечения информационной безопасности? Составьте проекты необходимых документов.

Задача 2.

Служба безопасности ООО «Спарта» разрабатывает систему мер по обеспечению информационной безопасности при производстве наукоёмкой высокотехнологической продукции. Административные и производственные помещения ООО «Спарта» расположены на отдельной территории, огороженной забором.

Сотрудники ООО «Спарта» активно представляют разработки предприятия на промышленных выставках и научных симпозиумах.

Назовите приоритетные направления обеспечения информационной безопасности ООО «Спарта».

Задача 3.

Выпускник ВУЗа, обучающийся по направлению от органа исполнительной власти, при заключении служебного контракта о замещении должности, для выполнения должностных обязанностей по которой ему необходимо будет работать с документами под грифом «секретно», отказался проходить проверку на допуск к сведениям, составляющими государственную тайну.

Назовите, какие действия в данном случае должен предпринять представитель нанимателя.

по теме 7. «Защищенный документооборот»

Примерный перечень тем докладов

1. Характеристика нормативно-правовой базы, регулирующей отношения в области оборота документированной информации ограниченного пользования.

2. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.

3. Основы технологии обработки и хранения конфиденциальных документов.

4. Направления и методы защиты документов на различных видах носителей.

5. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

6. Порядок работы персонала с документами, содержащих сведения ограниченного доступа.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет проводится с применением следующих методов (средств): проведение устного (письменного) зачет, включающего теоретическую часть и практико-ориентированное задание, требующее демонстрации уровня владения умениями/навыками.

5.2. Оценочные материалы промежуточной аттестации

Таблица 5.

Показатели и критерии оценивания

Компонент компетенции	Промежуточный индикатор оценивания	Критерий оценивания
ПК-12.2 Способен применять технологии подбора современных ИКТ в соответствии с решаемыми прикладными задачами с учетом действующих правовых норм.	ИПК-12.2 Применяет технологии подбора современных ИКТ в соответствии с решаемыми прикладными задачами с учетом действующих правовых норм.	Использует технологии подбора современных ИКТ в соответствии с решаемыми прикладными задачами с учетом действующих правовых норм.
ПК-20.2 Способен использовать международные стандарты и информационные ресурсы на практике, внедряя их в производственно-технологический процесс.	ИПК-20.2 Применяет международные стандарты и информационные ресурсы на практике, внедряя их в производственно-технологический процесс.	Демонстрирует навыки использования международных информационных ресурсов и стандартов

Примерные вопросы к зачёту

1. Понятие информации, ее юридические особенности, свойства, виды.
2. Понятие информации, ее юридические особенности, свойства, виды.
3. Информационно-правовые нормы и информационные правоотношения.
4. Понятие и система источников, регулирующих вопросы информационной безопасности.
5. Документированная информация как объект информационных правоотношений.
6. Обязательный экземпляр документа как разновидность документированной информации.
7. Электронный документ и электронный документооборот. Электронная подпись.
8. Информационные ресурсы: понятие, виды, правовой режим информационных ресурсов.
9. Использование международных информационных ресурсов и стандартов в информатизации предприятий и организаций.
10. Информационные системы: понятие, назначение, признаки. Программы для ЭВМ и базы данных как модули информационной системы.
11. Информационно-телекоммуникационные сети: понятие, значение.
12. Понятие и виды информационных технологий, порядок их создания и основные направления внедрения.
13. Правовые основы использования инновационных инструментальных средств для проектирования информационных процессов и систем, адаптации современных ИКТ к задачам прикладных ИС.
14. Правовые формы организации деятельности СМИ.
15. Информация как объект гражданских правоотношений: особенности информации как объекта собственности.
16. Особенности регулирования информационных отношений институтом интеллектуальной собственности.
17. Особенности информационных правоотношений в Интернете.
18. Правовые режимы информации: общая характеристика.
19. Режим свободного доступа к информации.
20. Институт тайны как правовой режим информации ограниченного доступа.
21. Правовое регулирование информационных отношений в области государственной тайны.
22. Правовое регулирование информационных отношений в области коммерческой

тайны.

23. Особенности информационных правоотношений, возникающих при производстве, передаче и распространении персональных данных.

24. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.

25. Понятие информационной безопасности и национальные интересы Российской Федерации в информационной сфере.

26. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.

27. Принципы, задачи, функции и стандарты обеспечения информационной безопасности.

28. Понятие и виды вредной информации.

29. Правовая защита информации от угроз несанкционированного и неправомерного воздействия.

30. Информационная безопасность личности.

31. Вопросы компьютерной безопасности. Методы защиты от компьютерных вирусов.

32. Информационная безопасность в глобальном информационном пространстве.

33. Цели и задачи ведения кибервойн.

34. Правовые основы и государственная система лицензирования и сертификации в области защиты информации.

35. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.

36. Понятие и виды правонарушений в информационной сфере.

37. Уголовная ответственность за совершение информационных преступлений.

38. Понятие компьютерных преступлений и особенности борьбы с ними.

39. Административная ответственность за совершение правонарушений в информационной сфере.

40. Гражданско-правовая ответственность за информационные правонарушения.

41. Дисциплинарная ответственность за информационные правонарушения.

42. Ответственность в области массовой информации.

43. Особенности ответственности за информационные правонарушения в сети Интернет.

44. Аналитическая работа по выявлению угроз информационной безопасности.

45. Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации.

46. Компьютерные технологии и формирование основ системы защиты информации.

47. Формирование и актуализация системы защиты информации в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом организации и видами угроз.

48. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

49. Службы безопасности в организациях различных типов.

50. Взаимодействие службы безопасности и службы персонала.

51. Анализ и оценка надежности и эффективности применяемой системы защиты.

52. Угрозы безопасности информации от персонала и направления ее защиты.

53. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.

54. Доступ персонала к конфиденциальным сведениям, документам и базам данных

55. Понятие и задачи, основные требования к защищённому документообороту.

56. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.

57. Технологические системы защиты и обработки документов, содержащих сведения ограниченного доступа.

58. Принципы учёта и технология обработки документов, содержащих сведения ограниченного доступа.

59. Контроль за оборотом документов, содержащих информацию ограниченного доступа.

Примеры практико-ориентированных (практических) заданий к зачету

ПК-12.2 - способен применять технологии подбора современных ИКТ в соответствии с решаемыми прикладными задачами с учетом действующих правовых норм:

Задание 1.

ООО «Огонёк», специализирующееся на электронных публикациях литературных произведений в сети Интернет, при размещении материалов использует специальный плагин, препятствующий копированию текста.

Вопрос: Нормы какого правового акта должен был соблюдать разработчик описанного программного средства защиты авторских прав?

Задание 2.

ООО «Альфа» получило по электронной почте платёжное поручение на оплату оказанных услуг от ООО «Омега».

Вопрос: Каким образом с использованием программных средств можно удостоверить подлинность информации, полученной ООО «Альфа»?

Задание 3.

Бухгалтер ООО «Презент» Ласточкина О.Н., заканчивающая обучение в ВУЗе на заочном отделении, загрузила с личной флеш-карты в служебный компьютер фотографии, сделанные на отдыхе в отпуске, распечатала несколько писем от контрагентов ООО «Презент», присланных на служебный адрес электронной почты, нашла в сети «Интернет» и скачала материал, необходимый для своей дипломной работы. При запуске компьютерной базы данных с бухгалтерскими документами ООО «Каскад» выяснилось, что она повреждена вирусом.

Вопрос: Какие меры следует предпринять при проектировке и внедрении системы электронного документооборота ООО «Презент» для профилактики заражения компьютерными вирусами?

Задание 4.

Менеджер по работе с персоналом акционерного общества «Каскад» Сидоров К.Н. установил на служебный компьютер программу для создания презентаций, скачанную из сети «Интернет». В процессе установки программы произошёл сбой в работе компьютера и была повреждена база данных сотрудников АО «Каскад». Специалист отдела компьютерной техники установил, что нарушения в работе компьютера были вызваны вирусом, попавшим на компьютер в момент скачивания программы.

Какие меры следует предпринять при создании и функционировании локальной сети ООО «Каскад» и организации доступа в интернет в данной организации для профилактики заражения компьютерными вирусами?

ПК-20.2 - способен использовать международные стандарты и информационные ресурсы на практике, внедряя их в производственно-технологический процесс:

Задание 5.

ООО «Эпсилон» осуществляет регулярный обмен персональными данными клиентов при коммерческом взаимодействии с зарубежными контрагентами. Назовите требования

каких международных правовых актов должны соблюдаться при электронном обмене персональными данными.

Задание 6.

ООО «Эребус» занимается разработкой программного обеспечения. Назовите международные правовые акты, регулирующие создание и использование программ для ЭВМ.

Задание 7.

ООО «Старт» занимается разработкой и внедрением криптографических средств защиты информации. Назовите международные правовые акты, регулирующие осуществление данного вида деятельности.

Задание 8.

ООО «Браво» специализируется на создании сайтов для коммерческих организаций.

Требования каких международных стандартов необходимо соблюдать при осуществлении данной деятельности?

Шкала оценивания

Промежуточная аттестация проводится в форме зачета без применения балльно-рейтинговой системы оценивания - посредством аттестационных испытаний в форме традиционного зачета.

Результаты промежуточной аттестации оцениваются: по бинарной системе оценивания («зачтено», «не зачтено»).

Наряду с оцениванием учебных достижений обучающихся по принятой образовательной организации системе оценок и использованием ее при оформлении официальных дипломов Академии о высшем образовании, вводят повышенный («Excellent» и «Good») и базовый («Very good» и «Satisfactory») уровень оценок «отлично» и «хорошо» для использования при оформлении ЕПД, согласно Положению об оформлении и выдаче ЕПД.

Таблица 6.

Соответствие академической оценке

Академическая оценка		Оценка по шкале ESTS	
зачтено	отлично	Passed	A (Excellent)
			B (Very Good)
	хорошо		C (Good)
			D (Satisfactory)
	удовлетворительно		E (Sufficient)
не зачтено	неудовлетворительно	-	-

Критерии оценивания на зачете

Оценка **«зачтено»** выставляется обучающемуся, если он твердо знает материал, четко и логически стройно излагает его на зачете, умеет тесно увязывать теорию с практикой, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами заданий, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение.

Оценка «**не зачтено**» выставляется обучающемуся, если он не знает значительной части программного материала, допускает неточности, недостаточно правильные формулировки, выполнение практических заданий неуверенно, с большими затруднениями

6. Методические материалы по освоению дисциплины с применением ЭК

Обучение по дисциплине «Правовые основы информационной безопасности» предполагает изучение курса на аудиторных занятиях (лекции, практические/семинарские) и самостоятельной работы обучающихся.

Практические/семинарские занятия дисциплины «Правовые основы информационной безопасности» предполагают их проведение в различных формах с целью выявления полученных знаний, умений, навыков и компетенций.

Подготовка к лекции студентами заключается в следующем:

– повторить материал предыдущей лекции, прочитав его повторно;

– ознакомиться с темой предстоящей лекции (в рабочей программе учебной дисциплины);

– ознакомиться с учебными материалами по данной теме в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины или с электронными материалами, предложенными лектором;

– записать возможные вопросы, которые можно будет задать лектору.

Подготовка к практическим (семинарским) занятиям:

– внимательно прочитать материал лекций относящихся к данному занятию, ознакомиться с учебными материалами, включая электронные в соответствии с предложенным списком литературы в рабочей программе учебной дисциплины;

– подготовить развернутые ответы на вопросы, предложенные в рабочей программе дисциплины для обсуждения;

– выполнить задания, если они предусмотрены в письменной форме;

– понять, что для вас осталось неясными и постараться получить на них ответ заранее;

– готовиться к практическим/семинарским занятиям можно как индивидуально, так и в составе малой группы;

– рабочую программу учебной дисциплины необходимо использовать в качестве основного ориентира в организации обучения;

– электронной версии рабочей программы по дисциплине размещена на сайте Нижегородского института управления и предоставлен авторизованный доступ.

Самостоятельная работа студентов призвана закрепить теоретические знания и практические навыки, полученные студентами на лекциях, практических и семинарских занятиях.

Самостоятельная работа обучающихся проводится с целью:

– систематизации и закрепления полученных теоретических знаний и практических умений студентов;

– углубления и расширения теоретических знаний;

– формирования умений использовать справочную документацию и специальную литературу;

– развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формированию самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развития исследовательских умений.

Эффективность лекционных, семинарских и практических занятий по дисциплине во многом зависит от качества самостоятельной работы студентов, от их самоподготовки. Часть времени, отведенного на самостоятельную работу должна использоваться на

подготовку к аудиторным занятиям, другая часть на выполнение домашней работы, осмысление и оформление результатов практических занятий.

При подготовке к занятиям студенту полезно:

– изучить теоретический материал по данной теме (конспект занятия);
– ознакомиться с литературой, рекомендованной преподавателем;
– выполнить задания, предложенные преподавателем, к занятию;
– составить перечень вопросов, вызывающих затруднения, неясности или сомнения, обсудить их с преподавателем или на занятии;
– заниматься самостоятельным поиском дополнительной литературы по изучаемой теме.

Вопросы для самостоятельной подготовки к лекционным и практическим занятиям

ТЕМА 1.

1. Понятие и виды информации, её роль в жизни личности, общества, государства.
2. Информационно-правовые нормы и информационные правоотношения: содержание, основания возникновения, классификация.
3. Субъекты информационных правоотношений: правовой статус, классификация.
4. Объекты информационных правоотношений.
5. Информационная безопасность как элемент национальной безопасности.
6. Международные договоры и программные документы Российской Федерации в области информационной безопасности.
7. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг.
8. Законодательство о безопасности и защите информации, его структура и содержание.
9. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание.
10. Основные задачи и уровни реализации информационной безопасности.

ТЕМА 2.

1. Определение, цели, задачи, направления исследования и практической реализации информационной безопасности.
2. Основные угрозы жизненно важным интересам личности, общества, государства, предпринимательства в информационной сфере.
3. Информационная безопасность и компьютеризация информационной среды.
4. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации.
5. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг.
6. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации.
7. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения.
8. Понятие и цели защиты информации. Соотношение понятий информационной безопасности, безопасности информации, защиты информации.

ТЕМА 3.

1. Правовой режим информационных ресурсов. Документирование информации как обязательное условие включения информации в информационные ресурсы.
2. Классификация информационных продуктов и услуг.

3. Риски угроз информационным ресурсам.
4. Защита информации институтом интеллектуальной собственности.
5. Законодательные акты, охраняющие вещную собственность на документированную информацию.
6. Правовое регулирование деятельности средств массовой информации.
7. Институт тайн в законодательстве Российской Федерации.
8. Информация ограниченного доступа и ее виды.
9. Понятие и виды правонарушений в информационной сфере.
10. Ответственность за совершение информационных преступлений.

ТЕМА 4..

1. Аналитическая работа по выявлению угроз информационной безопасности.
2. Понятие, цели, задачи, принципы построения, элементы системы защиты конфиденциальной информации.
3. Компьютерные технологии и формирование основ системы защиты информации.
4. Формирование и актуализация системы в реальных обстоятельствах, изменения в соотношении элементов системы в соответствии с типом организации и видами угроз.
5. Сертификация систем и средств защиты информационных систем и информационных ресурсов.

ТЕМА 5.

1. Службы безопасности в организациях различных типов.
2. Задачи и функции различных подразделений служб безопасности.
3. Взаимодействие службы безопасности и службы персонала.
4. Профессиональные и психологические требования к сотрудникам службы безопасности.
5. Назначение и взаимосвязь плановой и контрольной работы службы безопасности, их место в построении и функционировании комплексной системы защиты информации организации.
6. Анализ и оценка надежности и эффективности применяемой системы защиты.

ТЕМА 6.

1. Угрозы безопасности информации от персонала и направления ее защиты.
2. Задачи и стадии работы с персоналом, обладающим конфиденциальными сведениями.
3. Доступ персонала к конфиденциальным сведениям, документам и базам данных
4. Принципы, организационные формы и методика обучения сотрудников правилам обеспечения безопасности информации.
5. Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией.
6. Правовая ответственность персонала за разглашение информации ограниченного доступа.

ТЕМА 7.

1. Понятие и задачи, основные требования к защищённому документообороту.
2. Виды угроз традиционным и электронным документопотокам, задачи защиты документопотоков.
3. Основные принципы категорирования защищаемых ресурсов, принятые в Российской Федерации.
4. Технологические системы защиты и обработки документов, содержащих

сведения ограниченного доступа.

5. Принципы учёта документов, содержащих сведения ограниченного доступа.

6. Технология обработки подготовленных документов, содержащих сведения ограниченного доступа.

7. Порядок работы персонала с документами, содержащих сведения ограниченного доступа.

8. Формирование и хранение дел, содержащих информацию ограниченного доступа.

Подготовка к промежуточной аттестации по дисциплине. К промежуточной аттестации по дисциплине необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем и тематикой письменных работ, а также методическими рекомендациями по их выполнению;
- перечнем вопросов к зачёту.

Систематическое выполнение всех видов заданий на лекциях, практических/семинарских занятиях, а также самостоятельная работа позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачёта.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1 Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 17.04.2024). – Режим доступа: по подписке.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239 (дата обращения: 17.04.2024). - Режим доступа: по подписке.

3. Крылов, Г.О. Базовые понятия информационной безопасности : монография / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина. - Москва : Русайнс, 2020. - 257 с. - Internet access. - ISBN 978-5-4365-1557-1. - Текст : электронный // ЭБС "BOOK.RU" : [сайт]. - URL: http://www.book.ru/book/932492 (дата обращения: 02.03.2024). - Режим доступа: по подписке.

7.2 Дополнительная литература

1. Архипов, В. В. Интернет-право : учебник и практикум для вузов / В. В. Архипов. — Москва : Издательство Юрайт, 2023. — 249 с. — (Высшее образование). — ISBN 978-5-534-03343-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511640 (дата обращения: 17.04.2024). - Режим доступа: по подписке.

2. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510644 (дата обращения: 17.04.2024). - Режим доступа: по подписке.

7.3 Учебно-методическое обеспечение самостоятельной работы.

1. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1861659 (дата обращения: 17.04.2024). – Режим доступа: по подписке.

2. Электронные информационно-образовательные ресурсы Нижегородского института управления – филиала РАНХиГС - http://sdo.niu.ranepa.ru/

7.4 Нормативно-правовые документы

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ.

2. Приказ Министерства науки и высшего образования Российской Федерации от 06.04.2021 №245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»

3. Всеобщая декларация прав человека (принята 10 декабря 1948 г. Генеральной Ассамблеей ООН) // Международное публичное право: Сборник документов. Т. 1. М.: БЕК, 1996.

4. Международный пакт о гражданских и политических правах от 19 декабря 1966 г.

5. Резолюция № 428 (1970) Консультативной ассамблеи Совета Европы «Относительно Декларации о средствах массовой информации и правах человека (принята 23 января 1970 г. на 21-й сессии Консультативной ассамблеи Совета Европы).

6. Заключительный акт Совещания по безопасности и сотрудничеству в Европе от 1 августа 1975 г.

7. Декларация об основных принципах, касающихся вклада средств массовой информации в укрепление мира и международного взаимопонимания, в развитие прав человека и борьбу против расизма и апартеида и подстрекательства к войне (принята 28 ноября 1978 г.).

8. Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS N 108 (Страсбург, 28 января 1981 г.).

9. Декларация основных принципов правосудия для жертв преступлений и злоупотреблений властью (принята 29 ноября 1985 г. Резолюцией 40/34 Генеральной Ассамблеи ООН).

10. Директива «О правовой охране компьютерных программ (91/250/ЕЭС) (Брюссель, 14 мая 1991 г.).

11. Декларация о правах и свободах человека и гражданина Российской Федерации от 22 декабря 1991 г.
12. Всеобщая декларация о геноме человека и правах человека (принята 11 ноября 1997 г. на 29-й сессии Генеральной конференции ЮНЕСКО) // Международное публичное право: Сборник документов. Т. 1. М.: БЕК, 1996.
13. Окинавская хартия глобального информационного общества от 22 июля 2000.
14. Типовой закон ЮНСИТРАЛ об электронных подписях (принят ЮНСИТРАЛ 5 июля 2001 г.)
15. Коммюнике глав государств и правительств «Группы восьми» (Генуя, 22 июля 2001 г.).
16. Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г.,
17. Декларация «Партнерство во имя будущего» (Бангкок, 21 октября 2003 г.)
18. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // «Собрание законодательства РФ», 04.08.2014, N 31, ст. 4398.
19. Федеральный конституционный закон от 30 мая 2001 г. № 3-ФКЗ «О чрезвычайном положении» (с послед. изм. и доп.) // СЗ РФ. 2001. № 23. Ст. 2277.
20. Федеральный конституционный закон от 30 января 2002 года № 1-ФКЗ «О военном положении» // СЗ РФ. 2002. № 5. Ст. 375.
21. Гражданский кодекс Российской Федерации (с послед изм. и доп.) // СЗ РФ. 1994. № 32. Ст. 3301; 1996. N 5. Ст. 410; 2001. N 49. Ст. 4552; 2006. N 52. Ст. 5496.
22. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с послед. изм. и доп.) // СЗ РФ. 1996. № 25. Ст. 2954.
23. Налоговый кодекс РФ.Ч. 1. от 31 июля 1998 года № 146 (с послед. изм. и доп.) // СЗ РФ. 1998. № 31. Ст. 3824.
24. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с послед. изм. и доп.) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.
25. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (с послед. изм. и доп.) // СЗ РФ. 2002. № 1 (ч. 1). Ст. 3.
26. Арбитражно-процессуальный кодекс РФ от 24 июля 2002 года № 95-ФЗ (с послед. изм. и доп.) // СЗ РФ. 2002. № 30. Ст. 3012.
27. Федеральный закон от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (с послед. изм. и доп.) // СЗ РФ. 1994. № 35. Ст. 3648.
28. Федеральный закон от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» (с послед. изм. и доп.) // СЗ РФ. 1995. № 1. Ст. 1.
29. Федеральный закон от 29 декабря 1994 г. № 78-ФЗ «О библиотечном деле» (с послед. изм. и доп.) // СЗ РФ. 1995. № 1. Ст. 2.
30. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «Об органах федеральной службы безопасности в Российской Федерации» (с послед. изм. и доп.) // СЗ РФ. 1995. № 15. Ст. 1269.
31. Федеральный закон от 19 мая 1995 г. № 82-ФЗ «Об общественных объединениях» (с послед. изм. и доп.) // СЗ РФ. 1995. № 21. Ст. 1930.
32. Федеральный закон от 18 июля 1995 г. № 108-ФЗ «О рекламе» (с послед. изм. и доп.) // СЗ РФ. 1995. № 30. Ст. 2864.
33. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с послед. изм. и доп.) // СЗ РФ. 1995. № 33. Ст. 3349.
34. Федеральный закон от 17 ноября 1995 г. № 168-ФЗ «О прокуратуре Российской Федерации» (с послед. изм. и доп.) // СЗ РФ. 1995. № 47. Ст. 4472.
35. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с послед. изм. и доп.) // СЗ РФ. 2002. № 30. Ст. 3031.

36. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (с послед. изм. и доп.) // СЗ РФ. 2003. № 28. Ст. 2895.
37. Федеральный закон от 10 января 2003 г. № 20-ФЗ «О государственной автоматизированной системе РФ «Выборы» (с послед. изм. и доп.) // СЗ РФ. 2003. № 2. Ст. 172.
38. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с послед. изм. и доп.) // СЗ РФ. 2004, № 32, ст. 3283
39. Федеральный закон от 22 октября 2004 г. № 125-ФЗ; «Об архивном деле в Российской Федерации» (с послед. изм. и доп.) // СЗ РФ. 2004. № 43. Ст. 4169.
40. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (с послед. изм. и доп.) // СЗ РФ. 2006. № 11. ст. 1146.
41. Федеральный закон от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // СЗ РФ. 2006. № 19. Ст. 2060.
42. Федеральный закон от 13 марта 2006 г. № 38-ФЗ; «О рекламе» (с послед. изм. и доп.) // СЗ РФ. 2006. № 12. ст. 1232.
43. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с послед. изм. и доп.) // СЗ РФ. 2006. № 31. ст. 3448.
44. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с послед. изм. и доп.) // СЗ РФ. 2006. № 31. ст. 3451.
45. Федеральный закон от 28 февраля 2010 г. № 390-ФЗ «О безопасности» (с послед. изм. и доп.) // СЗ РФ. 2011. № 1. Ст. 2.
46. Федеральный закон от 07 февраля 2011 г. № 3-ФЗ «О полиции» (с послед. изм. и доп.) // СЗ РФ. 2011. № 7. Ст. 900.
47. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СЗ РФ. 2011. № 15. Ст. 2036.
48. Федеральный закон от 29.12.2012 N 273-ФЗ "Об образовании в Российской Федерации" (с послед. изм. и доп.) // СЗ РФ. 2012. № 53 (ч.1). Ст. 7598.
49. Закон РФ от 21 июля 1993 № 5485-I «О государственной тайне» (с послед. изм. и доп.) // СЗ РФ. 1997. N 41.
50. Закон Российской Федерации от 11 марта 1992 г. № 2487-I «О частной детективной и охранной деятельности в Российской Федерации» (с послед. изм. и доп.) // ВСНД и ВС РФ. 1992. № 17. Ст. 888.
51. Закон РФ от 9 октября 1992 г. № 3612-1 «Основы законодательства Российской Федерации о культуре» (с послед. изм. и доп.) // Ведомости СНД РФ и ВС РФ. 1992. № 46. Ст. 2615.
52. Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (с послед. изм. и доп.) // Ведомости СНД РФ и ВС РФ. 1992. № 7. Ст. 300.
53. Указ Президента РФ от 17 февраля 1995 г. № 161 «О гарантиях права граждан на охрану здоровья при распространении рекламы» (с послед. изм. и доп.) // СЗ РФ. 1956. № 8. Ст. 659.
54. Указ Президента РФ от 30 ноября 1995 г. №1203; «О перечне сведений, отнесенных к государственной тайне» (с послед. изм. и доп.) // СЗ РФ. 1998. №5. Ст.561; 2001. №24. Ст.2418.
55. Указ Президента РФ от 06 марта1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с послед. изм. и доп.) // СЗ РФ. 1997. N 10. Ст. 1127.
56. Указ Президента РФ от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» (с послед. изм. и доп.) // СЗ РФ. 2006. № 8. Ст. 897.
57. Указ Президента РФ от 18 мая 2009 г. № 559 «О представлении гражданами, претендующими на замещение должностей федеральной государственной службы, и федеральными государственными служащими сведений о доходах, об имуществе и

обязательствах имущественного характера» (с послед. изм. и доп.) // СЗ РФ. 2009. № 21. Ст. 2544.

58. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1. (часть II) Ст. 212.

59. Указ Президента РФ от 05 декабря 2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

60. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // СЗ РФ. 2017. № 20. Ст. 2901.

61. «Положение о Межведомственной комиссии по защите государственной тайны» утверждено Указом Президента РФ от 20 января 1996 г. №71 // СЗ РФ. 1996. № 4. Ст. 268.

62. Постановление Правительства РФ от 04 сентября 1995 г. № 870 «Правила отнесения сведений составляющих государственную тайну, к различным степеням секретности» (с послед. изм. и доп.) // СЗ РФ. 1995. № 37. Ст. 3619.

63. Постановление Правительства РФ от 28 февраля 1999 г. № 226 «О государственном учете и регистрации баз и банков данных» (с послед. изм. и доп.) // СЗ РФ. 1999 №12. Ст.1114.

64. ГОСТ 6.10.4-84. Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, созданным средствами вычислительной техники. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/9010879 свободный. - Загл. с экрана.

65. ГОСТ 6.10.5-87 Унифицированные системы документации. Требования к построению формуляра-образца. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/1200012305 свободный. - Загл. с экрана.

66. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/1200007350 свободный. - Загл. с экрана.

67. ГОСТ Р 50922-96. Защита информации: Основные термины и определения. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006 свободный. - Загл. с экрана.

68. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/1200071688свободный. - Загл. с экрана.

69. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/gost-r-51275-2006. - Загл. с экрана.

70. ГОСТ Р 7.0.97-2016 Система стандартов по информации, библиотечному и издательскому делу (СИБИД). Организационно-распорядительная документация. Требования к оформлению документов. [Электронный ресурс] - Режим доступа: http://docs.cntd.ru/document/1200142871. - Загл. с экрана.

7.5. Интернет-ресурсы, справочные системы.

1. Официальный сайт Президента РФ [Электронный ресурс]. Режим доступа: www.kremlin.ru.
2. Официальный сайт Правительства РФ [Электронный ресурс]. Режим доступа: www.government.ru.
3. Официальный Интернет-портал правовой информации [Электронный ресурс]. Режим доступа: www.pravo.gov.ru.
4. Институт развития информационного общества в России [Электронный ресурс]. Режим доступа: http://www.iis.ru/index.html.

5. "Вводный научный комментарий к части четвертой Гражданского кодекса Российской Федерации" (Павлова Е.А., Калятин В.О., Корнеев В.А.) (Подготовлен для системы КонсультантПлюс, 2015).

6. "Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и защите информации" (постатейный) (Савельев А.И.) ("Статут", 2015).

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

8.1. Материально-техническая база

Перечень материально-технического обеспечения:

1. Учебные аудитории, оборудованные для проведения учебных занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, коллоквиумов, мероприятий текущего контроля и промежуточной аттестации, в том числе мультимедийным оборудованием для демонстрации электронных презентаций и аудио- и видеоматериалов.
2. Компьютерные классы для выполнения групповых тестовых и иных заданий, а также для самостоятельной работы обучающихся оснащенные компьютерной техникой и обеспечением доступа к сети «Интернет» и доступа в электронную информационно-образовательную среду организации.
3. Специализированные аудитории и лаборатории.
4. Библиотека с обеспечением печатными изданиями или электронно-библиотечная система обеспечивающая доступ к электронным изданиям (электронная библиотека).
5. Читальный зал.
6. Технические средства обучения: персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV и др.

8.2. Информационные технологии, программное обеспечение:

При осуществлении образовательного процесса по дисциплине используется информационные технологии и программное обеспечение:

1. Современная операционная система.
2. Kaspersky Endpoint Security (или аналог).
3. Средство просмотра файлов формата pdf.
4. Современные офисные средства (текстовые и табличные редакторы, средства работы с презентационными материалами и т.д.).
5. Архиватор 7-Zip.
6. Система дистанционного обучения.
7. Автоматизированная библиотечная система.

8.3. Информационные справочные системы:

1. https://www.urait.ru –Электронно-библиотечная система [ЭБС] Юрайт;
2. http://www.iprbookshop.ru – Электронно-библиотечная система [ЭБС] «IPR SMART» (ранее – IPRBooks)
3. https://e.lanbook.com - Электронно-библиотечная система [ЭБС] «Лань».
4. https://znanium.com - Электронно-библиотечная система [ЭБС] «Znanium.com».
5. https://www.book.ru - Электронно-библиотечная система [ЭБС] «Book.ru».
6. https://ibooks.ru - Электронно-библиотечная система [ЭБС] «ibooks.ru».
7. https://www.ezproxy.ranepa.ru:2443/login?url=https://dlib.eastview.com/ – East

View. Полные тексты российских научных и практических журналов, а также газет центральной прессы России.

8. https://www.ezproxy.ranepa.ru:2443/login?url=https://grebennikon.ru/ - Полные тексты 38 научно-практических журналов по маркетингу, менеджменту, финансам и управлению персоналом ИД «Гребенников»
9. http://www.consultant.ru/ - Справочно-правовая система «Консультант».
10. http://www.garant.ru/ Справочно-правовая система «Гарант».