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 истории и теории государства и права
(наименование кафедры)

УТВЕРЖДЕНО
Директор Нижегородского института управления – филиала РАНХиГС

Парамонов Александр Васильевич
Подписано цифровой подписью: Парамонов Александр Васильевич
Дата: 2024.07.02 16:05:26 +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.03.01 ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ 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.

Автор-составитель:

Доцент кафедры истории и теории государства и права канд. ист. наук, доцент	Е.А. Акимова
(ученая степень и(или) ученое звание, должность, наименование кафедры)	*(Ф.И.О.)*
Заведующий кафедрой истории и теории государства и права, доктор ист. наук, профессор	А.А. Халин
(ученая степень и(или) ученое звание, должность, наименование кафедры)	*(Ф.И.О.)*

РПД Б1.В.ДВ.03.01 Организационные основы обеспечения информационной безопасности одобрена на заседании кафедры истории и теории государства и права.
Протокол №6 от 07.02.2024 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 7

5. Оценочные материалы промежуточной аттестации по дисциплине 16

6. Методические материалы по освоению дисциплины с применением ЭК 19

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет 21

7.1 Основная литература 21

7.2 Дополнительная литература 22

7.3 Учебно-методическое обеспечение самостоятельной работы. 22

7.4 Нормативные правовые документы. 22

7.5. Интернет-ресурсы, справочные системы. 23

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 23

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

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

Таблица 1.

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента освоения компетенции
ПК-6	Способен выбирать методологию и технологию проектирования ИС с учетом проектных рисков	ПК-6.2	Способен применять методы оценки и управления рисками ИТ-проектов.
ПК-11	Способен проектировать архитектуру и сервисы информационных систем предприятий и организаций в прикладной области	ПК-11.2	Способен использовать инструментарий проектирования архитектуры и сервисов ИС.
ПК-19	Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных информационных систем	ПК-19.2	Способен использовать методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.

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);	ПК-6.2	На уровне навыков: – оценки и управления рисками проектов проектирования ИС.
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); • организационное и технологическое обеспечение разработки баз данных ИС (D/17.7).	ПК-11.2	На уровне знаний: – возможности ИС; – архитектура, устройство и функционирование вычислительных систем; – инструменты и методы моделирования бизнес-процессов организации. На уровне навыков: – проектирования и разработки сервисов ИС в прикладных областях.
ОТФ: управление работами по сопровождению и проектами создания (модификации) ИС,	ПК-19.2	На уровне навыков: – проведения анализа основных концептуальных подходов к проблеме

ОТФ/ТФ/ профессиональные действия	Код компонента компетенции	Планируемые результаты обучения
автоматизирующих задачи организационного управления и бизнес-процессы (D);		обеспечения информационной безопасности.

2. Объем и место дисциплины в структуре ОП ВО

Индекс дисциплины Б1.В.ДВ.03.01 «Организационные основы обеспечения информационной безопасности» входит в число дисциплин по выбору части, формируемой участниками образовательных отношений 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 информационной безопасности.

Дисциплины, на которых базируется данная дисциплина:

Философские проблемы науки и техники (Б1.О.01)

Информационные технологии в образовании (Б1.О.04)

Управление внедрением IT-проектов (Б1.О.06)

Тенденции развития Web- пространства (Б1.О.07)

Дисциплины, для которых данная дисциплина является предшествующей:

Актуальные проблемы информационного права (Б1.В.ДВ.04.01)

Правовые основы информационной безопасности (Б1.В.ДВ.04.02)

Проектирование Web-сервисов информационных систем (Б1.В.01.04)

Технологии межведомственного электронного взаимодействия (Б1.В.01.05)

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	Введение в проблему информационной безопасности	17	2		6		9	О, Д, Т, М
Тема 2	Информационное противоборство и безопасность.	17	2		6		9	О, Д, Т, М

№ 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		
	Информационная война.							
Тема 3	Нормативно-правовая база обеспечения информационной безопасности.	17	2		6		9	О, Д, Т, М
Тема 4	Информационная безопасность в практике международных отношений.	17	2		6		9	О, Д, Т, М
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	Введение в проблему информационной безопасности	16	1		2		13	О, Д, Т, М
Тема 2	Информационное противоборство и безопасность. Информационная война.	18	1		2		15	О, Д, Т, М
Тема 3	Нормативно-правовая база обеспечения информационной безопасности.	18	1		2		15	О, Д, Т, М
Тема 4	Информационная безопасность в практике международных отношений.	16	1		2		13	О, Д, Т, М
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), тестирование (Т), оценка доклада (Д), оценка работы с документами в микрогруппе (М).*

3.2. Содержание дисциплины

Тема 1 Введение в проблему информационной безопасности

Понятие «информация». Информационное общество. Интернет. Критерии информационного общества. Современные тенденции и влияние на общество и государства процессов глобальной информатизации. Развитие информационного общества в России. Понятия «безопасность», «информационная безопасность». Транснациональные вызовы и угрозы безопасности, связанные с развитием информационных технологий. Субъекты международной информационной безопасности. Информатизация процесса производства и управления, глобальные сети и глобальное управление, расширение экономической географии, революция в военном деле. СМИ и глобальное медиа-пространство. Интернет как фактор формирования глобальной социально-экономической информационной среды.

Тема 2 Информационное противоборство и безопасность. Информационная война.

Противоборство и конфликты в информационной сфере. Понятия «информационная безопасность» и «кибер-безопасность». Новые объекты безопасности в информационной сфере. Информационные средства воздействия. Информационное оружие. Информационный терроризм и трансформация международного терроризма. Использование интернета в преступных целях.

Интересы государств и иных факторов мировой политики в информационной сфере. Применение общих принципов международного права к борьбе в информационной сфере. Включение информационной войны в международно-правовое понимание войны как вооруженного противоборства.

Тема 3 Нормативно-правовая база обеспечения информационной безопасности.

Государственная политика в сфере обеспечения информационной безопасности. Государственные органы РФ, контролирующие деятельность в области защиты информации. Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом. Доктрина информационной безопасности Российской Федерации (2016). Стратегия национальной безопасности Российской Федерации (2021). Основы государственной политики Российской Федерации в области международной информационной безопасности (2021). Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 гг. (2017). Государственная программа Российской Федерации «Информационное общество (2020). Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (2014). Конвенция Совета Европы «О компьютерных преступлениях» (Будапешт, 2001). Концепция Конвенции ООН об обеспечении международной информационной безопасности (2017). Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации (2017). Проблема устаревания официальных документов.

Тема 4 Информационная безопасность в практике международных отношений.

Российские инициативы в области международной информационной безопасности, история их выдвижения и продвижения. Российско-американские отношения по вопросу международной информационной безопасности. Позиция Китая. Расстановка сил на мировой арене в связи с российскими инициативами по международной информационной безопасности. Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.

Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Евросоюза, ШОС в области международной информационной безопасности.

Изменение расстановки сил на международной арене в 2014 г. после воссоединения Крыма с Россией – информационный аспект. Информационная война США и Великобритании против России. Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом. Роль информационных войн в трансформации международных отношений в 2022 г.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.В.ДВ.03.01 «Организационные основы обеспечения информационной безопасности» используются следующие **методы текущего контроля** успеваемости обучающихся:

Таблица 4.

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1 Введение в проблему информационной безопасности	Опрос, тестирование, оценка доклада, оценка работы с документами в микрогруппе..
Тема 2 Информационное противоборство и безопасность. Информационная война.	Опрос, тестирование, оценка доклада, оценка работы с документами в микрогруппе..
Тема 3 Нормативно-правовая база обеспечения информационной безопасности.	Опрос, тестирование, оценка доклада, оценка работы с документами в микрогруппе..

Тема (раздел)	Методы текущего контроля успеваемости
Тема 4 Информационная безопасность в практике международных отношений.	Опрос, тестирование, оценка доклада, оценка работы с документами в микрогруппе..

4.2. Типовые материалы текущего контроля успеваемости обучающихся

Материалы текущего контроля успеваемости по теме 1.

Вопросы для подготовки к семинарским занятиям

Семинар №1. Введение в проблему информационной безопасности

1. Понятия «информация», «безопасность», «информационная безопасность», их сущность, измерения.
2. Информационное общество в России. Роль Интернета в современном обществе.
3. Вызовы и угрозы безопасности, связанные с развитием информационных технологий.
4. Субъекты международной информационной безопасности.

Опрос: ключевые понятия: Информация, безопасность, национальная безопасность, информационная безопасность, защита информации, безопасность данных, информационное общество.

Темы докладов:

- Информационная безопасность: сущность, основные измерения.
- Этапы становления и совершенствования обеспечения информационной безопасности в СССР и РФ.
- Информационное общество: сущность, основные измерения.
- Основные модели информационного общества.
- Международная информационная безопасность.

Тестовые задания:

1. Термин «национальная безопасность» появился в политическом лексиконе России:

- в начале XX века;
- со времени возникновения Российского государства;
- **в конце XX века;**
- после Второй мировой войны.

2. Составными частями национальной безопасности России являются:

- безопасность регионов России;
- безопасность от внешних и внутренних угроз;
- безопасность каждого гражданина России;
- **экономическая, политическая, военная, социальная, экологическая, информационная безопасность.**

3. Национальная безопасность должна определяться:

- интересами крупного бизнеса;
- интересами отдельных социальных групп;
- **долгосрочными интересами страны в целом;**
- интересами государственного аппарата.

4. В какой области обеспечение безопасности должно достигаться с помощью патентной защиты, таможенного регулирования

- **интеллектуальная безопасность;**
- информационная безопасность;
- внешнеэкономическая безопасность;
- промышленной безопасности.

5. Существуют следующие уровни безопасности:

- местная, межрегиональная, глобальная;

- национальная, региональная, глобальная;
- межнациональная, региональная, всеобщая;
- национальная, межрегиональная, всеобщая.

Работа с документами индивидуальная и в рамках микрогруппы:
Белл Д. Грядущее постиндустриальное общество.
Опыт социального прогнозирования.

«Постиндустриальное общество [...] не является проекцией или экстраполяцией современных тенденций западного общества; это новый принцип социально-технологической организации и новый образ жизни, вытесняющий индустриальную систему, точно так же, как она сама вытеснила когда-то аграрную. В первую очередь, оно воплощается в утрате промышленностью, организованной на основе стандартизации и массового производства, своей центральной роли.

Это не означает, что производство товаров прекратится; ведь производство продуктов земледелия в западном мире продолжается и сегодня (причем продовольствия производится больше, чем когда бы то ни было ранее). Прежде всего понятие «постиндустриальное общество» представляет собой не эмпирическое описание, а «теоретическое построение», позволяющее увидеть главное в новых социальных формах. Постиндустриальные тенденции не заменяют прежние социальные формы как некие «стадии» общественного развития. Они часто сосуществуют (как порой сосуществуют на пергаменте старые полустертые письмена и нанесенные поверх них новые), усложняя общество и природу его социальной структуры».

«Мир можно представить себе разделенным на три типа социальной организации. Первый из них – доиндустриальный. Это, прежде всего, добывающие виды хозяйственной деятельности: земледелие, извлечение полезных ископаемых, рыболовство, заготовка леса. До сих пор это удел большей части стран Африки, Латинской Америки и Юго-Восточной Азии, где этими видами хозяйственной деятельности занято 60 или более процентов рабочей силы. Я определяю это в целом как «взаимодействие человека с природой», которое подвержено капризам погоды и усложняется вследствие истощения почв, исчерпания лесных ресурсов и более высокой себестоимости добычи минералов и руд.

Второй тип социальной организации – индустриальный. Это фабричное хозяйство, основанное на приложении энергии к машинам для массового производства товаров.

К индустриальному типу относятся страны, расположенные на берегах Атлантики: Западная Европа, Соединенные Штаты и далее – Советский Союз и Япония. Труд здесь представляет собой взаимодействие с искусственной природой: соединение людей с машинами, организация ритмичной работы с высочайшей степенью координации.

Третий тип – постиндустриальное общество. Это деятельность, связанная в первую очередь с обработкой данных, управлением и информацией.

Это образ жизни, который во все возрастающей степени сводится к «взаимодействию людей друг с другом». Еще более важно то, что возникает новый принцип обновления, прежде всего знаний в их отношении к технологии».

«...Основные изменения в постиндустриальном обществе происходят прежде всего в технико-экономической сфере. Однако тот факт, что постиндустриальные перемены, в отличие от всех предшествующих технологических изменений, связаны с кодификацией теоретического знания, делает науку отличительный чертой этого общества».

«...Мне кажется полезным выделить некоторые новые черты постиндустриального общества.

1) *Центральная роль теоретического знания.* Каждое общество всегда опиралось на знания, но только в наши дни систематизация результатов теоретических исследований и материаловедения становится основой технологических инноваций. Это заметно, прежде всего, в новых, наукоемких отраслях промышленности – в производстве компьютеров, электронной, оптической техники, полимеров, – ознаменовавших своим развитием

последнюю треть столетия.

2) *Создание новой интеллектуальной технологии.* Новые математические и экономические методы, такие, как компьютерное линейное программирование, цепи Маркова, стохастические процессы и т.п., служат технологической основой моделирования, имитации и других инструментов системного анализа и теории решений, позволяющих находить более эффективные, "рациональные" подходы к экономическим, техническим и даже социальным проблемам.

3) *Рост класса носителей знания.* Наиболее быстрорастущая группа общества – класс технических специалистов и профессионалов. В Соединенных Штатах эта группа, вместе с менеджерами, составляла в 1975 г. 25 процентов рабочей силы – восемь миллионов человек. К 2000 году класс технических специалистов и профессионалов будет самой многочисленной социальной группой.

4) *Переход от производства товаров к производству услуг.* В настоящее время в Соединенных Штатах примерно 65 человек из каждых 100 занято в сфере услуг. К 1980 г. это число возрастет до 70. Значительный сектор услуг существует в любом обществе. В доиндустриальный период это в основном класс тех, кто оказывает личные услуги по дому (в Англии это был самый многочисленный из всех классов до 1870 г.). В индустриальном обществе сфера услуг включает транспорт, финансы, которые играют вспомогательную роль в производстве товаров, а также бытовые услуги (косметические кабинеты, рестораны и т.д.). В постиндустриальном обществе появляются новые виды услуг, прежде всего в гуманитарной области (главным образом в здравоохранении, образовании и социальном обслуживании), а также услуги профессионалов и технических специалистов (например, проведение исследований и оценок, работа с компьютерами, осуществление системного анализа). Развитие этих служб [...] становится сдерживающим фактором экономического роста и источником постоянной инфляции.

5) *Изменения в характере труда.* В доиндустриальном мире жизнь представляет собой взаимодействие человека с природой, когда люди, объединившись в малые группы, тяжким трудом добывают себе пропитание на земле, в воде или в лесу и полностью зависят от капризов внешней среды. В индустриальном обществе труд – это взаимодействие человека с преобразованной природой, когда в процессе производства товаров люди становятся придатками машин.

Но в постиндустриальном мире труд является, прежде всего, взаимодействием между людьми (между чиновником и посетителем, врачом и пациентом, учителем и учащимся или между членами исследовательских групп, сотрудниками контор или работниками бригад обслуживания).

Тем самым из процесса труда и повседневной практики исключаются природа, искусственно созданные предметы, а остаются лишь люди, которые учатся взаимодействовать друг с другом. В истории человеческого общества это совершенно новая, не имеющая аналогов ситуация.

6) *Роль женщин.* В индустриальном секторе (в частности, на фабрике) трудились в основном мужчины. Постиндустриальный сектор (например, услуги в гуманитарной области) предоставляет широкие возможности занятости и для женщин. Можно сказать, что впервые женщины получили надежную основу для экономической независимости. Этот факт находит подтверждение в постоянно растущей доле женщин в общей численности работающих, в увеличении числа семей (в настоящее время 60 процентов от их общего количества), в которых более одного человека занято на постоянной работе, и в росте числа разводов по инициативе женщин, ощущающих себя все менее экономически зависимыми от мужчин.

7) *Наука достигает своего зрелого состояния.* Возникшее в XVII веке научное сообщество явилось уникальным социальным институтом.

Оно обладало харизмой, поскольку в своих поисках истины всегда шло революционным путем и открывало доступ к своим методам и технологиям; его сила

заключена в убеждении, что цель науки заключается в получении знания как такового, а не каких-либо способов его утилитарного применения. В отличие от других харизматических сообществ (главным образом религиозных групп и мессианских политических движений) оно не "рутинизирует" свои убеждения и не возводит их в ранг официальных догм. Однако до последнего времени научному сообществу не приходилось сталкиваться с такими явлениями, как бюрократизация научно-исследовательского процесса, подчинение научных поисков целям, устанавливаемым государством, оценка результатов исследований в зависимости от конкретной отдачи. В настоящее же время не только укрепилась связь науки и технологий; она вошла также составной частью в военную сферу и во многом определяет социальные потребности.

Все это составляет основную черту постиндустриального общества, и характер новых научных институтов имеет решающее значение для возможности свободного осуществления исследований и получения знаний в будущем. [...]

9) *Меритократия.* В постиндустриальном обществе, которое по своему характеру есть прежде всего общество технологическое, человек может занять престижное положение не столько по праву наследования или собственности (хотя оно может давать богатство или культурное преимущество), сколько вследствие образования и квалификации. Неизбежно, что вопрос о меритократии становится решающим нормативным вопросом. [...]".

Задание: Ответьте на вопросы:

1. Какую характеристику Д.Белл дает постиндутриальному обществу?
2. Какие три типа социальной организации выделяет Д.Белл? Как можно охарактеризовать каждый тип социальной организации?
3. Какие черты постиндустриального общества выделяет Д.Белл?
4. Можно ли считать, что концепция Д.Белла отражает реальное состояние современного общества? Аргументируйте свой ответ.

Материалы текущего контроля успеваемости по теме 2.
Вопросы для подготовки к семинарским занятиям
Семинар № 2. Информационное противоборство и безопасность. Информационная война.

1. Противоборство и конфликты в информационной сфере. Понятие «кибер-безопасность».
2. Новые объекты безопасности в информационной сфере.
3. Информационные средства воздействия. Информационное оружие.
4. Информационный терроризм и трансформация международного терроризма.
5. Интересы государств и иных факторов мировой политики в информационной сфере.
6. Информационные войны. Методы борьбы с ними.

Опрос: ключевые понятия: Информационное противоборство, информационное поражение, неприемлемый ущерб, информационные ресурсы, информационно-психологический ресурс нации, информационное воздействие, информационно-психологическое воздействие, информационно-психологический ущерб, информационно-психологическое противоборство, информационная война, кибербезопасность, «мягкая сила», «цветная революция».

Темы докладов:

- «Мягкая сила» как метод ведения информационной войны.
- Дж. Най и его концепции «мягкой» и «умной» сил.
- Дж.Ассанж и Э.Сноуден – разоблачители или игроки в стратегии информационных войн?
- «Цветные революции» как элемент информационных войн в мировой политике.
- Информационный терроризм в международной политике.

Тестовые задания:

1. Государственная тайна - это:

- защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны;

- ограничения доступа в отдельные отрасли экономики или на конкретные производства;

- защищаемые банками и иными кредитными организациями сведения о банковских операциях;

- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей.

2. Информационное оружие – это:

- комплекс индивидуального и общественного сознания;

- комплекс нормативно-правовой документации;

- комплекс технических, программных и других средств, методов и технологий предназначенных для распространения выгодной информации и дезинформации в системе формирования общественного мнения.

3. Что не относится к угрозам информационной безопасности:

- сбои и отказы оборудования (технических средств);

- классификация информации;

- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов).

4. К открытым источникам информация относятся.

- Газеты, Радио, Новости;

- информация украденная у спецслужб;

- из вскрытого сейфа;

- украденная из правительственной организации.

Работа с документами индивидуальная и в рамках микрогруппы:

Тема работы в микрогруппах: «Цветные революции на постсоветском пространстве».

Цель: выявить общее и особенное в проведении «цветных революций» на постсоветском пространстве и продумать варианты их предотвращения.

Предварительная работа:

1. Изучить работу Джин Шарп «От диктатуры к демократии» - http://www.aeinstein.org/wp-content/uploads/2013/10/FDTD_Russian.pdf

2. Изучить раздел «Цветные революции» в учебнике Василенко И.А. Геополитика современного мира: учеб. пособие для бакалавров / И. А. Василенко. - 4-е изд., испр. и доп. - Москва: Юрайт, 2021

3. Изучить материал по теме «Цветные революции» в СМИ (печатных, сети Интернет)

Студенческая группа разбивается на 4 микрогруппы. На основе лекционного материала, докладов на семинарском занятии и самостоятельной работы необходимо подготовить материалы по следующей схеме:

1. Государство до начала «цветной революции» (политический строй, социально-экономическая ситуация);
2. Причины расшатывания политической ситуации;
3. Повод «цветной революции»;
4. Этапы развития «цветной революции»;
5. Итоги и последствия «цветной революции»;
6. Оценка: изменилась ли в лучшую/худшую сторону ситуация в государстве?

Государства, где произошли «цветные революции»:

- Грузия (2003 г.);
- Украина (2004 г.);
- Киргизия (2005 г.);
- Украина (2014 г.);

Отчет по работе в микрогруппе делается в виде презентации.

Материалы текущего контроля успеваемости по теме 3.

Вопросы для подготовки к семинарским занятиям

Семинар № 3. Нормативно-правовая база обеспечения информационной безопасности.

1. Государственная политика в сфере обеспечения информационной безопасности.
2. Государственные органы РФ, контролирующие деятельность в области защиты информации.
3. Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом.

Опрос: ключевые понятия: Комитет Государственной Думы по безопасности, Совет безопасности России, ФСТЭК России; ФСБ России; СВР России; Минобороны России; МВД России; Роскомнадзор.

Темы докладов:

См. раздел «Работа с документами индивидуальная и в рамках микрогруппы».

Тестовые задания:

1. Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Министерство юстиции Российской Федерации;
- **Служба внешней разведки Российской Федерации;**
- **Федеральная служба безопасности;**
- **Комитет Государственной думы по безопасности;**
- Министерство иностранных дел;
- **Министерство внутренних дел Российской Федерации;**
- **Совет безопасности России.**

2. Правовое обеспечение информационной безопасности – это:

- документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
- широкое использование технических средств защиты информации;
- **нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.**

3. В число уровней, на которых группируются меры обеспечения информационной безопасности, входят:

- **Законодательный;**
- Исполнительный;
- судебный.

Работа с документами индивидуальная и в рамках микрогруппы

В рамках практического занятия проводится подробный анализ существующих документов по информационной безопасности, оценивается степень их современности, приводятся примеры использования положений документов в современной мировой политике России и зарубежных стран.

Предусматривается разработка докладов по следующим темам:

1. Анализ деятельности государственных органов, контролирующих деятельность в области защиты информации.
2. Анализ Доктрины информационной безопасности
3. Анализ Стратегии национальной безопасности РФ
4. Анализ Стратегии развития информационного общества в РФ на 2017-2030гг.

5. Анализ Основ государственной политики РФ в области международной информационной безопасности на период до 2020 г.

6. Анализ Основных направлений научных исследований в области обеспечения информационной безопасности РФ.

7. Анализ Конвенции об обеспечении международной информационной безопасности (концепция)

8. Проблема устаревания официальных документов.

Документы, участвующие в разработке исследовательских проектов:

1. Доктрина информационной безопасности Российской Федерации. Утверждена 05.12.2016

2. Стратегия национальной безопасности Российской Федерации. Утверждена 02.07.2021

3. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы. Утверждена 09.05.2017.

4. Основы государственной политики РФ в области международной информационной безопасности. Утверждена 12.04.2021 г.

5. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации. Утверждены 31.08.2017.

6. Государственная программа Российской Федерации «Информационное общество Утверждена 31.03.2020 г.

7. Конвенция Совета Европы «О киберпреступности» от 23.11.2001 (Конвенция о компьютерных преступлениях / Конвенция совета Европы о киберпреступности, Будапешт, 23 ноября 2001 года)

8. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации Утверждена 12.12.2014 г.

9. Концепция Конвенции ООН об обеспечении международной информационной безопасности (проект, крайняя редакция 2021).

План выступления на представлении доклада

1. Обоснование актуальности выбранной темы.
2. Определение цели и задач.
3. Анализ источниковой базы исследования.
4. Выявление достоинств и недостатков документа, анализ степени соответствия документа современным политическим реалиям.
5. Предложения по корректировке данного документа.
6. Обзор аспектов реализации документа в политической жизни России и зарубежных стран.

Материалы текущего контроля успеваемости по теме 4.
Вопросы для подготовки к семинарским занятиям

Семинар № 4. Информационная безопасность в практике международных отношений.

1. Российские инициативы в области международной информационной безопасности.

2. Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.

3. Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Группы семи, Евросоюза, ШОС в области международной информационной безопасности.

4. Изменение расстановки сил на международной арене в 2014 г. после воссоединения Крыма с Россией – информационный аспект (2014-2022 гг.).

5. Информационная война США и Великобритании против России (2014 – 2022 гг.)

6. Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом.

Опрос: Ключевые понятия:

Международная информационная безопасность, ИКТ, МСЭ, ЕС, ШОС, ОДКБ, БРИКС.

Темы докладов:

- Деятельность России в ООН по обеспечению международной информационной безопасности.
- Деятельность ОДКБ и ШОС по обеспечению международной информационной безопасности.
- Деятельность ЕС и США по обеспечению международной информационной безопасности.
- Информационная война США и Великобритании против России.

Тестовые задания:

1. Сложность обеспечения информационной безопасности является следствием:

- злого умысла разработчиков информационных систем;
- **объективных проблем современной технологии программирования;**
- происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы.

2. Меры информационной безопасности направлены на защиту от:

- нанесения любого ущерба;
- **нанесения неприемлемого ущерба;**
- попыток похищения любого вида информации.

3. Сложность обеспечения информационной безопасности является следствием:

- невнимания широкой общественности к данной проблематике;
- все большей зависимости общества от информационных систем;
- **быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним.**

4. Компьютерная преступность в мире

- остается на одном уровне;
- *снижается;*
- ***растет.***

Работа с документами индивидуальная и в рамках микрогруппы:

Тема работы в микрогруппах: «Вхождение Крыма в состав Российской Федерации и его геополитические последствия (информационный аспект)».

Цель: Изучить геополитические последствия вхождения территории полуострова Крым в состав Российской Федерации, а также изучить интерпретацию данного события в мировых СМИ.

Предварительная работа:

1. Изучить материал по теме «Вхождение Крыма в состав России» в СМИ (печатных, сети Интернет).

2. Изучить практику международных прецедентов включения в состав /выхода из состава государств административных территорий (образования самостоятельных государств) по результатам проведенных референдумов (в СМИ – печатных, сети Интернет).

Студенческая группа разбивается на 4 микрогруппы. На основе лекционного материала, докладов на семинарском занятии и самостоятельной работы необходимо подготовить материалы по следующей схеме:

1. Проанализировать юридические основания вхождения территории полуострова Крым в состав Российской Федерации.
2. Проанализировать юридические основания вхождения (выхода) указанной территории в состав (из состава) другого государства.
3. Сравнить международную практику с событиями в Крыму в 2014 г.
4. Проанализировать геополитические последствия обоих событий.
5. Оценить информационную составляющую данного события: освещение в СМИ в РФ и за рубежом.

Международные прецеденты включения в состав /выхода из состава государств административных территорий (образования самостоятельных государств) по результатам проведенных референдумов:

- вхождение области Саар в состав ФРГ (1957 г.);
- выход Черногории из состава Государственного союза Сербии и Черногории (ГССЧ) (2006г.);
- выход из состава Сербии и образование частично признанной Республики Косово (2008 г.);
- образование частично признанных государств Южной Осетии и Абхазии (2008 г.);

Отчет по работе в микрогруппе делается в виде презентации.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет проводится с применением следующих методов (средств): проведение устного зачета, 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-6.2 Способен применять методы оценки и управления рисками ИТ-проектов.	ИПК-6.2 Применяет методы оценки и управления рисками ИТ-проектов.	Использует методы оценки и управления рисками ИТ-проектов.
ПК-11.2 Способен использовать инструментарий проектирования архитектуры и сервисов ИС.	ИПК-11.2 Использует инструментарий проектирования архитектуры и сервисов ИС.	Демонстрирует навыки проектирования архитектуры и сервисов информационных систем
ПК-19.2 Способен использовать методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.	ИПК-19.2 Использует методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.	Применяет методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности.

Перечень теоретических вопросов к зачету

1. Понятия «информация», «безопасность», «информационная безопасность», их сущность, измерения.
2. Информационное общество в России. Роль Интернета в современном обществе.
3. Вызовы и угрозы безопасности, связанные с развитием информационных технологий.
4. Субъекты международной информационной безопасности.
5. Противоборство и конфликты в информационной сфере. Понятие «кибер-безопасность».
6. Новые объекты безопасности в информационной сфере.

7. Информационные средства воздействия. Информационное оружие.

8. Информационный терроризм и трансформация международного терроризма.

9. Интересы государств и иных факторов мировой политики в информационной сфере.

10. Информационные войны. Методы борьбы с ними. Использование передовых методов информационной безопасности в процессе эксплуатации прикладных ИС как элемент борьбы с информационными войнами.

11. Государственная политика в сфере обеспечения информационной безопасности.

12. Государственные органы РФ, контролирующие деятельность в области защиты информации. Обеспечение защиты информации в области проектирования архитектуры и сервисов ИС предприятий и организаций.

13. Нормативно-правовая база обеспечения информационной безопасности в России и за рубежом.

14. Российские инициативы в области международной информационной безопасности.

15. Переговорный процесс и международное сотрудничество в области обеспечения информационной безопасности.

16. Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, Группы восьми, Группы семи, Евросоюза, ШОС в области международной информационной безопасности.

17. Изменение расстановки сил на международной арене в 2014 г. после воссоединения Крыма с Россией – информационный аспект. Информационная война США и Великобритании против России.

18. Перспективы установления международного контроля над информационными видами оружия и формирования глобального режима международной информационной безопасности и управления интернетом.

Примеры практико-ориентированных (практических) заданий к зачету

ПК-6.2 - способен применять методы оценки и управления рисками ИТ-проектов:

Провести оценку рейтинга рискообразующих факторов. В соответствии с полученными оценками сгруппировать рискообразующие факторы по следующим категориям критичности:

- рискообразующие факторы, требующие немедленного реагирования;
- рискообразующие факторы, реагирование на которые можно выполнить позже;
- рискообразующие факторы, требующие дополнительного рассмотрения (включая количественный анализ);
- рискообразующие факторы, за которыми в дальнейшем должно проводиться наблюдение.

ПК-11.2 - способен использовать инструментарий проектирования архитектуры и сервисов ИС:

Дайте исходную характеристику сетевой файловой системы, используемой на предприятии. Предложите мероприятия по улучшению имеющейся сетевой ФС и докажите необходимость и эффективность предложенных мер.

ПК-19.2 - способен использовать методы анализа основных концептуальных подходов к проблеме обеспечения информационной безопасности:

Выполните аналитическое задание[1]: В начале 2013 г. Американский технический специалист, бывший сотрудник ЦРУ и Агентства национальной безопасности (АНБ) США Э.Сноуден передал газетам «Гардиан» и «Вашингтон пост» секретную информацию, касающуюся тотальной слежки американских спецслужб

[1] Современные международные отношения: учебник и практикум / под ред. А.И.Позднякова, В.К.Белозёрова, М.М.Васильевой. – М.: Издательство Юрайт, 2016. С.223-224

посредством телефона и Интернета в 60 странах за более чем миллиардом человек, в том числе правительствами 35 стран. По его словам, ежедневно системы сбора информации АНБ перехватывали и записывали около 1,7 млрд телефонных разговоров и электронных сообщений и около 5 млрд записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру. По существу, речь идет о глобальной системе информационно-психологического противоборства (можно предположить, что США не являются единственным субъектом этой деятельности). В связи с этим в США 14 июня 2013 г. Э.Сноудену заочно были предъявлены обвинения в шпионаже и похищении государственной собственности. Он бежал из США сначала в Гонконг, а затем в Россию, где получил временное убежище. Разоблачения Сноудена вызвали жаркие споры (как в США, так и в других странах) о допустимости массового негласного наблюдения, пределах государственной тайны и обеспечения национальной безопасности. Оцените международные, правовые и этические основания подобного рода деятельности, обоснуйте собственную точку зрения.

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 *«Организационные основы обеспечения информационной безопасности»* предполагает изучение курса в ходе контактной работы обучающихся с преподавателем по видам учебных занятий (лекции, семинарские занятия) и самостоятельной работы магистров. Семинарские занятия дисциплины *«Организационные основы обеспечения информационной безопасности»* предполагают их проведение в различных формах, в том числе в виде защиты исследовательских проектов, с целью выявления полученных знаний, умений, навыков в рамках заявленных компетенций.

Подготовка к лекции:

– повторение материала предыдущей лекции;

– определение с темы предстоящей лекции (в рабочей программе учебной дисциплины);

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

– подготовить возможные вопросы, которые можно будет задать лектору.

Подготовка к семинарским занятиям:

– внимательно прочитать материал лекций, относящихся к данному занятию, ознакомиться с материалами по данной теме, содержащимся в перечне основной литературы в п.6 рабочей программы дисциплины;

– подготовить развернутые ответы на вопросы семинарского занятия,

– подготовить доклады по предложенным темам;

– изучить материалы для работы в микрогруппах;

– выполнить предусмотренные задания в письменной форме;

Рабочую программу учебной дисциплины необходимо использовать в качестве основного ориентира в организации обучения. Электронная версия рабочей программы по дисциплине размещена на сайте Нижегородского института управления, и предоставлен авторизованный доступ.

Самостоятельная работа магистров призвана закрепить теоретические знания и практические навыки, полученные магистрантами на лекциях, практических и семинарских занятиях. Самостоятельная работа магистрантов проводится с целью:

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

– углубления и расширения теоретических знаний;

– формирования умений использовать справочную документацию и специальную литературу;

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

– формирования 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 магистрантов, 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 магистранту 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.

Подготовка к зачету.

К зачету необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомиться со следующими учебно-методическими материалами:

– рабочей программой данной дисциплины и содержащимися в ней
  – перечнем знаний и умений, которыми магистр должен владеть;
  – тематическими планами лекций, семинарских занятий;
  – списком рекомендованной литературы и электронных материалов;
– содержанием тем лекционных и семинарских занятий, а также методическими рекомендациями по освоению дисциплины;
– учебником, учебными пособиями по дисциплине, а также электронными ресурсами;
– перечнем вопросов для подготовки к зачету.

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

Вопросы для самостоятельной подготовки к занятиям

1. Перечислите основные этапы построения КСЗИ.
2. Назовите ГОСТ с учётом которых должны быть разработаны требования к системе защиты информации.
3. Перечислите основные понятия которые будут определены при проектировании КСЗИ.
4. Перечислите основное содержание эксплуатационной документации КСЗИ.
5. Перечислите этапы внедрения системы защиты информации.
6. Перечислите процессы выполняемые при обеспечении защиты информации в ходе эксплуатации аттестованной информационной системы.
7. Какие существуют виды обследования защищённости?
8. Назовите порядок проведения аттестации объектов информатизации по требованиям безопасности информации?
9. Какие документы предоставляет заявитель для проведения испытаний органу по аттестации?
10. Какие функции осуществляет ФСТЭК в рамках системы аттестации?
11. Назовите закон о защите персональных данных.
12. Каким документом определяются требования к защите персональных данных?
13. Назовите перечень документов используемых для защиты персональных данных.
14. Назовите документ регламентирующий использование криптографических средств защиты в информационных системах.
15. Какие показатели необходимо рассчитать для построения модели угроз ПДн?
16. Что обозначает коэффициент реализуемости угрозы?
17. Какие угрозы являются актуальными?
18. В соответствии с каким нормативным документом строится модель угроз?
19. В соответствии с каким нормативным документом, и в каких случаях строится модель нарушителя?

20. Назовите структуру нормативных документов предприятия.

21. Какой документ по защите информации является первичным нормативным актом на предприятии?

22. Перечислите законы, регулирующие порядок работы с конфиденциальной информацией.

23. Что регулирует закон об архивном деле?

24. Что регулирует Федеральный закон "О защите персональных данных"?

25. Что регулирует Федеральный закон "О коммерческой тайне"?

26. Что регулирует Федеральный закон "О связи"?

27. Перечислите общий список внутренних нормативных документов, которые должны быть на любом объекте информатизации?

28. Какими документами должен руководствоваться специалист по защите информации при составлении плана мероприятий по улучшению защищённости объекта информатизации?

29. Дайте определение политики информационно безопасности.

30. Из каких основных документов состоит политика информационной безопасности?

31. Назовите общее содержание политики разрешения доступа к технологическим ресурсам.

32. Что включает в себя политика пользования электронной почтой?

33. Назовите общее содержание антивирусная политика.

34. Назовите общее содержание политика подготовки, обмена и хранения документов.

35. Что включает в себя политика информационно-технической поддержки?

36. Что включает в себя политика серверной безопасности?

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: 16.04.2024). – 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: 16.04.2024). - Режим доступа: по подписке.

3. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341267 (дата обращения: 16.04.2024). — Режим доступа: для авториз. пользователей.

7.2 Дополнительная литература

1. 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.

2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2023. — 602 с. — (Среднее профессиональное образование). — DOI 10.12737/1942679. - ISBN 978-5-16-018253-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1942679 (дата обращения: 16.04.2024). – Режим доступа: по подписке.

7.3 Учебно-методическое обеспечение самостоятельной работы.

1. Смоленский, М. Б. Информационное право : учебник / М. Б. Смоленский.. - Ростов-на-Дону : Феникс, 2015. - 221 с.ISBN 978-5-222-25467-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/910963 (дата обращения: 16.04.2024). – Режим доступа: по подписке.

2. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии / М. В. Тумбинская, М. В. Петровский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-507-45046-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256133 (дата обращения: 16.04.2024). — Режим доступа: для авториз. пользователей.

3. Понятийный аппарат информационной безопасности финансово-экономических систем : словарь / составители Г.О. Крылов, В.Л. Никитина. — Москва : Прометей, 2020. — 372 с. — ISBN 978-5-907244-63-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165988 (дата обращения: 02.03.2024). — Режим доступа: для авториз. пользователей.

4. 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: 16.04.2024). – Режим доступа: по подписке.

5. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва : Директ-Медиа, 2020. - 270 с. - ISBN 978-5-4499-0496-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1908082 (дата обращения: 02.03.2024). – Режим доступа: по подписке.

6. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91449 (дата обращения: 02.03.2024). — Режим доступа: для авториз. пользователей.

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

7.4 Нормативные правовые документы.

1.Федеральный закон «Об образовании в Российской Федерации» от 29 декабря 2012 года №273-ФЗ // http://zakon-ob-obrazovanii.ru/

2. Стратегия национальной безопасности Российской Федерации http://www.scrf.gov.ru/security/docs/document133/

3. Доктрина информационной безопасности Российской Федерации - http://www.scrf.gov.ru/security/information/document5/

4. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 гг.// http://www.garant.ru/products/ipo/prime/doc/71570570/

5. Конвенция Совета Европы "О киберпреступности" // http://mvd.gov.by/main.aspx?guid=4603

6. Конвенция об обеспечении международной информационной безопасности Организации Объединенных Наций (проект) // http://www.scrf.gov.ru/security/information/document112/

7. Основы государственной политики РФ в области международной информационной безопасности // http://www.scrf.gov.ru/security/information/document114/

8. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации // http://www.scrf.gov.ru/security/information/document155/

9. 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»

7.5. Интернет-ресурсы, справочные системы.

1. Конституция Российской Федерации. – http://www.constitution.ru/index.htm
2. ЭБС издательства «ЛАНЬ» http://e.lanbook.com
3. ЭБС издательства «ЮРАЙТ» http://biblio-online.ru/
4. ЭБС издательства «IPRbooks» http://www.iprbookshop.ru
5. ЭБС «BOOK.RU» (издательства КноРус) https://www.book.ru/

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».