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

ДАЛЬНЕВОСТОЧНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ

УТВЕРЖДЕНО
Директор
Е.С. Меркулов
Электронная подпись

ПРОГРАММА МАГИСТРАТУРЫ
Управление региональным экономическим развитием

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ, реализуемой без применения электронного (онлайн) курса

Б1.В.ДВ.01.01 Механизмы противодействия информационным угрозам государственного и муниципального управления
(индекс, наименование дисциплины, в соответствии с учебным планом)

38.04.04 Государственное и муниципальное управление
(код, наименование направления подготовки)

Очная, заочная
(форма(ы) обучения)

Год набора - 2025

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 43B0028FD23306BCF414031E3FCDC222
Владелец Меркулов Евгений Сергеевич
Действителен с 29.01.2025 по 29.04.2026

Хабаровск, 2025 г.

Авторы-составители

доцент кафедры математических методов и информационных технологий, кандидат технических наук Буняева Е.В.

доцент кафедры математических методов и информационных технологий, кандидат экономических наук Пынько Л.Е.

Актуализацию РПД выполнил: кандидат экономических наук, доцент кафедры экономики и цифровых технологий Дальневосточного института управления – филиала РАНХиГС Пынько Л.Е.

Заведующий кафедрой экономики и цифровых технологий Поливаева О.Г.

РПД «Механизмы противодействия информационным угрозам государственного и муниципального управления» одобрена на заседании кафедры экономики и цифровых технологий. Протокол 21.04.2025 № 12.

СОДЕРЖАНИЕ

1 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
2 Объем и место дисциплины в структуре образовательной программы (ОП ВО) 5
3. Содержание и структура дисциплины 6
4. Материалы текущего контроля успеваемости обучающихся 9
5. Оценочные материалы для промежуточной аттестации 16
6. Методические материалы для освоения дисциплины 19
7 Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет» 23
7.1 Основная литература 23
7.2 Дополнительная литература 23
7.3. Нормативные правовые документы 25
7.4 Интернет-ресурсы 25

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

1.1 Дисциплина Б1.В.ДВ.01.01 Механизмы противодействия информационным угрозам государственного и муниципального управления, обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код компонента	Наименование компонента компетенции
ПКр-8	Способен осуществлять верификацию и структуризацию информации, получаемой из разных источников, формировать базы данных, осуществлять оценку их полноты и качества, применять эти данные для экспертной оценки реальных управленческих ситуаций и консультирования государственных, некоммерческих и хозяйственных организаций	ПКр-8.1	Способен осуществлять верификацию и структуризацию информации, получаемой из разных источников, формировать базы данных, осуществлять оценку их полноты и качества
ПКр-9	Способен представлять официальную информацию о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами	ПКр-9.1	Способен подготовить официальную информацию о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы:

ОТФ/ТФ ***(при наличии профстандарта)*****/ трудовые или профессиональные действия**	**Код компонента компетенции**	**Результаты обучения**
С7 Руководство внешнеэкономической деятельностью в организации В7 Реализация инвестиционного проекта	ПКр-8.1 Способность осуществлять верификацию и структуризацию информации, получаемой из разных источников, формировать базы данных, осуществлять оценку их полноты и качества	на уровне знаний: – основные модели информационной безопасности; – методы планирования реализации моделей информационной безопасности на базе требований к современному уровню информационной безопасности; – методологические основы информационной безопасности. Определять методы верификации и структуризации информации, получаемой из разных источников, способы формирования базы данных
		на уровне умений: – анализировать и выбирать адекватные модели информационной безопасности; – планировать реализацию моделей информационной безопасности на базе требований к современному уровню информационной безопасности; – использовать знания о современной методологии управления информационной безопасности для разработки реальных методов формирования защиты информационной инфраструктуры

ОТФ/ТФ ***(при наличии профстандарта)*****/ трудовые или профессиональные действия**	**Код компонента компетенции**	**Результаты обучения**
		Обобщать и систематизировать требования к верификацию и структуризации информации, получаемой из разных источников, формировать базы данных с учетом требований информационной безопасности.
		на уровне навыков: – методикой построения анализа и применения математических моделей для оценки рисков информационной безопасности; – разрабатывать мероприятия по минимизации угроз в области информационной безопасности; – навыками работы с современными программно-техническими средствами обеспечения информационной безопасности Подготавливать предложения по приоритетам внешнеэкономической деятельности организации
	ПКр-9.1 Способен подготовить официальную информацию о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами	на уровне знаний: - знание правовых актов в области социально-экономического развития территорий, государственного и местного самоуправления, государственной и муниципальной службы, публичных финансов и инвестиций; - знание источников официальной информации о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами;
		на уровне умений: использование информационных систем и баз данных (умения добавлять, удалять, корректировать, представлять информацию); средствами справочно-правовых систем искать и подготавливать официальную информацию о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами;
		на уровне навыков: самостоятельно осуществлять правильную последовательность выполнения действий, правильную самостоятельную подготовку исходных данных о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами.

2 Объем и место дисциплины в структуре образовательной программы (ОП ВО)

Объем дисциплины

На очной форме обучения дисциплина изучается во 2 семестре, на заочной форме на втором курсе. Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 ак. ч./108 астр. ч. На очной форме обучения: контактная работа с преподавателем – 20 ак. ч./ 15 астр. ч., в том числе: лекции – 6 ак. ч./ 4,5 астр. ч., практические занятия – 14 ак. ч./10,5 астр. ч,

интерактивные занятия – 6 ак. ч./ 4,5 астр. ч., самостоятельная работа – 124 ак. ч./ 93 астр. ч. (самостоятельная работа обучающихся в период зачетно-экзаменационной сессии). Дисциплина реализуется как с применением дистанционных образовательных технологий (*далее - ДОТ*), так и в традиционной форме проведения аудиторной занятий;

- для заочной формы обьучения на контактную работу выделено 12 ак. ч./ 9 астр. ч. (из них: 6 ак. ч./ 4,5 астр. ч. лекции (в том числе 4 ак. ч./3 астр. ч. в период установочной сессии); 6 ак. ч./ 4,5 астр. ч. практических занятий); 132 ак. ч./ 99 астр. ч. – самостоятельная работа (в том числе 32 ак. ч. / 24 астр. ч. в период установочной сессии). Дисциплина реализуется как с применением ДОТ, так и в традиционной форме проведения аудиторной занятий.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.01.01 Механизмы противодействия информационным угрозам государственного и муниципального управления входит в структуру программы подготовки магистратуры и относится к вариативной части (1 курс, 2 семестр – очная форма обучения; 2 курс, зимняя сессия – заочная форма обучения).

Форма промежуточной аттестации в соответствии с учебным планом: зачет.

3. Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов),	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1. Ключевые аспекты и вопросы формирования информационной безопасности современной системы управления								
Тема 1.1	Методологические основы управления информационной безопасностью	7	1	-		-	6	Р
Тема 1.2	Направления защиты информации в системах управления	7		-	1	-	6	ОПЗ
Раздел 2. Угрозы безопасности информационных систем и процессов управления								
Тема 2.1	Угрозы безопасности информационных систем и процессов управления	17		-	1	-	16	ОПЗ
Тема 2.2	Компьютерные преступления в сфере государственного управления	18	1	-	1		16	Р
Тема 2.3	Противодействие фейковой информации в социальных сетях	21	1	-	2		18	Р
Раздел 3. Противодействие угрозам государственной целостности в информационном пространстве								
Тема 3.1	Противодействие угрозам государственной целостности в информационном пространстве	18	1	-	1	-	16	ОПЗ
Тема 3.2	Противодействие кибербулингу и информации, порочащей представителей власти	19	1	-	2	-	16	ОПЗ
Раздел 4. Аудит и экономика систем информационной безопасности								
Тема 4.1	Методы противодействия несанкционированному	19	1	-	2	-	16	ОПЗ

№ п/п	Наименование тем (разделов),	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
	доступу к информации при реализации процессов управления. Аудит системы информационной безопасности							
Тема 4.2	Эффективность процессов управления и эффективность систем информационной безопасности	18		-	2	-	16	ОПЗ
Промежуточная аттестация		**-**	**-**	**-**	**-**		**-**	**Зачет**
Всего (ак. ч./ астр. ч.)		**144 / 108**	**6 / 4,5**	**-**	**14 / 10,5**		**124 / 93**	**Зачет**

Используемые сокращения:
Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся);
ЛР – лабораторные работы (вид занятий семинарского типа);
ПЗ – практические занятия (виды занятий семинарского типа за исключением лабораторных работ);
КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации);
ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности;
СРО – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.
Примечание: формы текущего контроля успеваемости: реферат (Р), отчет по практическому занятию (ОПЗ).

Заочная форма обучения

№ п/п	Наименование тем (разделов),	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1. Ключевые аспекты и вопросы формирования информационной безопасности современной системы управления								
Тема 1.1	Методологические основы управления информационной безопасностью	17	1	-		-	16	Р
Тема 1.2	Направления защиты информации в системах управления	17		-	1	-	16	ОПЗ
Раздел 2. Угрозы безопасности информационных систем и процессов управления								
Тема 2.1	Угрозы безопасности информационных систем и процессов управления	17		-	1	-	16	ОПЗ
Тема 2.2	Компьютерные преступления в сфере государственного управления	18	1	-	1		16	Р
Тема 2.3	Противодействие фейковой информации в социальных сетях	17	1	-	-		16	Р
Раздел 3. Противодействие угрозам государственной целостности в информационном пространстве								
Тема 3.1	Противодействие угрозам государственной целостности в информационном пространстве	20	1	-	1	-	18	ОПЗ

№ п/п	Наименование тем (разделов),	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 3.2	Противодействие кибербулингу и информации, порочащей представителей власти	20	1	-	1	-	18	ОПЗ
Раздел 4. Аудит и экономика систем информационной безопасности								
Тема 4.1	Методы противодействия несанкционированному доступу к информации при реализации процессов управления. Аудит системы информационной безопасности	20	1	-	1	-	18	ОПЗ
Тема 4.2	Эффективность процессов управления и эффективность систем информационной безопасности	18		-	-	-	18	ОПЗ
Промежуточная аттестация		**-**	**-**	**-**	**-**		**-**	**Зачет**
Всего (ак. ч./ астр. ч.)		**144 / 108**	**6 / 4,5**	**-**	**6 / 4,5**		**132 / 99**	**Зачет**

Используемые сокращения:
Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся);
ЛР – лабораторные работы (вид занятий семинарского типа);
ПЗ – практические занятия (виды занятий семинарского типа за исключением лабораторных работ);
КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации);
ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности;
СРО – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.
Примечание: формы текущего контроля успеваемости: реферат (Р), отчет по практическому занятию (ОПЗ).

Содержание дисциплины

Раздел 1. Ключевые аспекты и вопросы формирования информационной безопасности современной системы управления

Тема 1.1. Методологические основы управления информационной безопасностью

Основные понятия и определения: безопасность информации, безопасность программного обеспечения, безопасность систем обработки данных, безопасность информации, защита информации в информационных системах, система защиты информации. Основные этапы построения системы защиты информации на предприятии. Управленческая информация, как товар и объект информации.

Тема 1.2. Направления защиты информации в системах управления

Правовое обеспечение информационной безопасности, организационное направление защиты информации, технические (аппаратные) меры и средства защиты информации, физические методы и средства защиты информации, программно-технические (программно-аппаратные) меры защиты

Раздел 2. Угрозы безопасности информационных систем и процессов управления

Тема 2.1. Угрозы безопасности информационных систем и процессов управления

Терминология и классификация угроз, модель угроз информационной безопасности, модель нарушителя, виды нарушителей. Возможные способы противодействия угрозам ИБ

Тема 2.2. Компьютерные преступления в сфере государственного управления

Классификация компьютерных преступлений, субъекты компьютерных преступлений, объекты атак компьютерных преступлений, уголовно-правовой контроль над компьютерной преступностью в РФ

Тема 2.3. Противодействие фейковой информации в социальных сетях

Основные понятия и определения: боты, программы – боты, распространяющие фейковую информацию, фейк, среды распространения фейков в цифровых системах, виды ущерба государственному управлению от распространения фейков. Методы противодействия фейковым новостям в социальных сетях. Противодействие программам – ботам, с недостоверной и лживой информацией. Взаимодействие с населением, по опровержению ложной информации

Раздел 3. Противодействие угрозам государственной целостности в информационном пространстве

Тема 3.1. Противодействие угрозам государственной целостности в информационном пространстве

Вводная терминология, типы угроз, способы психологического, экономического, социального давления в информационных сетях и меры противодействия им в информационном поле. Механизмы снятия анонимности источника информационных угроз. Правовые способы защиты личных данных в информационном поле, защита членов семей государственных служащих в информационном поле.

Тема 3.2. Противодействие кибербулингу и информации, порочащей представителей власти

Понятие кибербулинга. Правовые механизмы привлечения к ответственности лиц, группы лиц, организующих кибербуллинг, механизмы противодействия ботам, распространяющим заведомо ложную и оскорбляющую информацию, равно информацию, угрожающую безопасности физическим, юридическим лицам, социуму в целом

Раздел 4. Аудит и экономика систем информационной безопасности

Тема 4.1. Методы противодействия несанкционированному доступу к информации при реализации процессов управления. Аудит системы информационной безопасности

Аудит информационной безопасности, цели аудита СИБ, этапы аудита безопасности, методы анализа результатов аудита. Методы противодействия несанкционированному доступу к информации при реализации процессов управления.

Тема 4.2. Эффективность процессов управления и эффективность систем информационной безопасности

Задачи экономики защиты информации, подходы к обоснованию стоимости корпоративной системы защиты, оценка эффективности инвестиций в информационную безопасность

4. Материалы текущего контроля успеваемости обучающихся

4.1 Формы и методы текущего контроля успеваемости

В ходе реализации дисциплины Б1.В.ДВ.01.01 «Механизмы противодействия информационным угрозам государственного и муниципального управления» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости	Методы текущего контроля успеваемости с применением ДОТ
Раздел 1. Ключевые аспекты и вопросы формирования информационной безопасности современной системы управления		
1.1 Методологические основы управления информационной безопасностью	Р	Реферат по вопросам практического занятия
1.2 Направления защиты информации в системах управления	ОПЗ	Отчет по результатам выполнения практического занятия
Раздел 2. Угрозы безопасности информационных систем и процессов управления		
2.1 Угрозы безопасности информационных систем и процессов управления	ОПЗ	Отчет по результатам выполнения практического занятия
2.2 Компьютерные преступления в сфере государственного управления	Р	Реферат по вопросам практического занятия
2.3. Противодействие фейковой информации в социальных сетях	Р	Реферат по вопросам практического занятия
Раздел 3. Противодействие угрозам государственной целостности в информационном пространстве		
3.1. Противодействие угрозам государственной целостности в информационном пространстве	ОПЗ	Отчет по результатам выполнения практического занятия
3.2. Противодействие кибербулингу и информации, порочащей представителей власти	ОПЗ	Отчет по результатам выполнения практического занятия
Раздел 4. Аудит и экономика систем информационной безопасности		
4.1. Методы противодействия несанкционированному доступу к информации при реализации процессов управления. Аудит системы информационной безопасности	ОПЗ	Отчет по результатам выполнения практического занятия
4.2. Эффективность процессов управления и эффективность систем информационной безопасности	ОПЗ	Отчет по результатам выполнения практического занятия

– занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.

4.2 Типовые материалы текущего контроля успеваемости обучающихся
Типовые оценочные материалы по практическим занятиям

Практическое занятие по теме 1.2. «Направления защиты информации в системах управления»

Тема занятия: Направления защиты информации в системах управления

Цель: для условного предприятия выполнить анализ существующей информационно-распорядительной документации и нормативных требований, отражающих текущую или желаемую политику безопасности; определить цели и задачи системы ИБ; разработать модель угроз ИБ и модель нарушителя; выбрать нормативно-техническую базу ИБ, разработать основные положения системы управления ИБ, определить требования к комплексу мер и средств обеспечения ИБ.

Занятие проводится посредством интерактивной формы обучения – работа в малых группах над общей задачей.

Составить детальное описание охраняемой информации, «портрета» нарушителя, модели

угроз, выполнить построение модели ИБ.

Практическое занятие №1 по теме 2.1. «Угрозы безопасности информационных систем и процессов управления»

Тема занятия: Угрозы безопасности информационных систем и процессов управления

Цель работы: для ИС условного предприятия выделить уязвимости и дефекты защиты. Выполнить расчет параметров защищенности при помощи модели с полным перекрытием.

Практическое занятие №2 по теме 2.1. «Угрозы безопасности информационных систем и процессов управления»

Тема занятия: Угрозы безопасности информационных систем и процессов управления

Цель работы: изучить нормативно-правовые акты, регулирующие системы аутентификации и идентификации в информационных системах.

Практическое занятие по теме 3.1. «Противодействие угрозам государственной целостности в информационном пространстве»

Тема занятия: Противодействие угрозам государственной целостности в информационном пространстве

Цель: ознакомление с принципами защиты от информационных угроз на уровне государственного и муниципального управления. Изучить правовые механизмы привлечения к ответственности лиц, группы лиц, организующих клевету и сознательные информационные диверсии, механизмы противодействия ботам, распространяющим заведомо ложную и оскорбляющую информацию, равно информацию, угрожающую безопасности физическим, юридическим лицам, социуму в целом.

Практическое занятие по теме 3.2. «Противодействие кибербулингу и информации, порочащей представителей власти»

Тема занятия: Противодействие кибербулингу и информации, порочащей представителей власти

Цель: научиться применять количественный и качественный подходы к оценке рисков информационной безопасности в условном государственном учреждении. Освоить методы противодействия кибербулингу и информации, порочащей представителей власти.

Практическое занятие по теме 4.1. «Методы противодействия несанкционированному доступу к информации при реализации процессов управления. Аудит системы информационной безопасности»

Тема занятия: Методы противодействия несанкционированному доступу к информации при реализации процессов управления. Аудит системы информационной безопасности.

Цель: освоить методы противодействия несанкционированному доступу к информации при реализации процессов управления. Изучить ГОСТы и международные стандарты (ISO) по

аудиту системы информационной безопасности. Освоить методы противодействия психологическому, экономическому, социальному давлению в информационных сетях и меры противодействия им в информационном поле.

Практическое занятие по теме 4.2. «Эффективность процессов управления и эффективность систем информационной безопасности»

Тема занятия: Эффективность процессов управления и эффективность систем информационной безопасности

Цель: научиться использовать для оценки экономической эффективности инвестиций в информационную безопасность следующие показатели: отдача в инвестиционный капитал (ROI), совокупная стоимость владения (TCO).

Типовые вопросы для подготовки рефератов

Тема 1.1 Методологические основы управления информационной безопасностью

1. Страсбургское соглашение о Международной патентной классификации от 24 марта 1971 г.
2. Лиссабонское соглашение о защите указаний места происхождения изделий и их международной регистрации от 31 октября 1958 г.
3. Служба безопасности предприятия: назначение, структура.
4. Источники, объекты и субъекты права защиты против недобросовестной конкуренции.
5. Правовая охрана права на защиту против недобросовестной конкуренции. 6. Виды «вредной» информации деструктивно воздействующей на человека.
6. Понятие информационно-психологической безопасности и особенности ее обеспечения.
7. Государственная система обеспечения информационно-психологической безопасности.
8. Особенности правовой охраны прав на информационные системы.
9. Понятие информационной безопасности РФ. Нормативно-правовые акты в области информационной безопасности.
10. Источники права о сохранении единого информационного пространства. 12. Понятие и признаки информационного общества.
11. Понятие, признаки, структура и потенциальные угрозы для Российской Федерации.
12. Нормативно-правовые акты в области информационной безопасности.
13. Понятие «организационные методы защиты информации».
14. Перечень и содержание организационных мер, направленных на защиту ГТ.
15. Документальное оформление допуска граждан РФ к государственной тайне.
16. Физические мероприятия по обеспечения защиты информации.
17. Технические мероприятия по защите информации.
18. Рекомендации по отнесению сведений к коммерческой тайне. Режим коммерческой тайны.
19. Основные права и обязанности собственника коммерческой тайны.
20. Юридический статус информации «ноу-хау», в режиме коммерческой тайны
21. Система защиты коммерческой тайны.
22. Защита коммерческой тайны в трудовых и гражданско-правовых отношениях.
23. Понятие профессиональной тайны в российском законодательстве. Объекты и субъекты права на профессиональную тайну.

24. Основные цели и задачи информационной безопасности НПА: Закон Российской Федерации от 21 июля 1993 г. N 5485-1 О государственной тайне

25. Основные цели и задачи информационной безопасности НПА: методика от 14 февраля 2008 г. Определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

26. Основные цели и задачи информационной безопасности НПА: методический документ от 1 декабря 2014 г. Профили защиты средств контроля съемных машинных носителей информации

27. Основные цели и задачи информационной безопасности НПА: методический документ от 11 мая 2017 г. Профили защиты операционных систем типов Б и В

28. Основные цели и задачи информационной безопасности НПА: методический документ от 11 февраля 2014 г. Меры защиты информации в государственных информационных системах

29. Основные цели и задачи информационной безопасности НПА: методический документ от 12 сентября 2016 г. Профили защиты межсетевых экранов

30. Основные цели и задачи информационной безопасности НПА: методический документ от 14 июня 2012 г. Профили защиты средств антивирусной защиты

31. Основные цели и задачи информационной безопасности НПА: методический документ от 17 мая 2023 г. Руководство по организации процесса управления уязвимостями в органе (организации)

32. Основные цели и задачи информационной безопасности НПА: методический документ от 2 мая 2024 г. Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктур Российской Федерации

33. Основные цели и задачи информационной безопасности НПА: методический документ от 25 декабря 2022 г. Рекомендации по безопасной настройке операционных систем Linux

34. Основные цели и задачи информационной безопасности НПА: методический документ от 26 июня 2018 г. Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России

35. Основные цели и задачи информационной безопасности НПА: методический документ от 28 октября 2022 г. Методика тестирования обновлений безопасности программных, программно-аппаратных средств

36. Основные цели и задачи информационной безопасности НПА: методический документ от 28 октября 2022 г. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств

37. Основные цели и задачи информационной безопасности НПА: методический документ от 3 февраля 2012 г. Профили защиты систем обнаружения вторжений

38. Основные цели и задачи информационной безопасности НПА: методический документ от 30 декабря 2013 г. Профили защиты средств доверенной загрузки

39. Основные цели и задачи информационной безопасности НПА: методический документ от 5 февраля 2021 г. Методика оценки угроз безопасности информации

40. Основные цели и задачи информационной безопасности НПА: методический документ от 6 марта 2012 г. Профили защиты систем обнаружения вторжений

41. Основные цели и задачи информационной безопасности НПА: методический документ от 8 февраля 2017 г. Профили защиты операционных систем типа А

42. Основные цели и задачи информационной безопасности НПА: Порядок аттестации работников органов по сертификации и испытательных лабораторий. Утвержден приказом ФСТЭК России от 27 июля 2023 г. N 147 «Выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений,

составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа»

43. Основные цели и задачи информационной безопасности НПА: Порядок проведения сертификации. Утвержден приказом ФСТЭК России от 1 декабря 2023 г. N 240 «Процессов безопасной разработки программного обеспечения средств защиты информации»

44. Основные цели и задачи информационной безопасности НПА: Правила выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий. Утверждены приказом ФСТЭК России от 27 июля 2023 г. N 148

45. Основные цели и задачи информационной безопасности НПА: Приказ ФСТЭК России от 10 апреля 2015 г. N 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности»

46. Основные цели и задачи информационной безопасности НПА: Приказ ФСТЭК России от 10 декабря 2024 г. N 227 «Об утверждении Программы профилактики нарушений лицензионных требований, соблюдение которых оценивается при проведении ФСТЭК России лицензионного контроля за деятельностью по технической защите конфиденциальной информации и деятельностью по разработке и производству средств защиты конфиденциальной информации, на 2025 год».

Типовые вопросы для подготовки рефератов

Тема 2.2 Компьютерные преступления в сфере государственного управления

1. Компьютерная информация как объект преступного посягательства в сфере государственного управления.
2. Информация и компьютерная информация: общее и различия.
3. Осмотр средства электронно-вычислительной техники.
4. Изъятие средств электронно-вычислительной техники и компьютерной информации как элемент отдельных следственных действий в сфере защиты информации в государственном управлении.
5. Уголовный кодекс и преступления в сфере компьютерной информации.
6. Объект и объективная сторона.
7. Субъект и субъективная сторона.
8. Квалификационные признаки.
9. Понятие, содержание и основные элементы криминалистической характеристики преступлений в сфере компьютерной информации.
10. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях
11. Классификация компьютерных преступлений, субъекты компьютерных преступлений, объекты атак компьютерных преступлений, уголовно-правовой контроль над компьютерной преступностью в РФ
12. Комплексная компьютерно-техническая и технико-криминалистическая экспертиза документов
13. Специальные структуры в правоохранительных органах в борьбе с преступлениями в сфере компьютерной информации

Типовые вопросы для подготовки рефератов

Тема 2.3 Противодействие фейковой информации в социальных сетях

1. Развитие государственных образовательных программ по медиа- и интернет-грамотности;
2. Развитие государственных образовательных ресурсов в социальных сетях и мессенджерах по медиа- и интернет- грамотности;
3. Развитие официальных государственных ресурсов в социальных сетях и мессенджерах по информированию населения и предоставлению достоверной информации;
4. Распространение платформ по проверке информации для различной аудитории;
5. Системное изучение общественного мнения на уровне государственных институтов власти;
6. Исследование медиарынка и подача объективной информации по медиапотреблению;
7. Факты и их интерпретация в информационной среде;
8. Анализ стиля текста, а не содержания информационного сообщения;
9. Анализ распространения информационного сообщения;
10. Анализ пользовательской активности при просмотре и комментировании информационного сообщения;

Критерии оценивания отчётов по практическим занятиям

8 баллов выставляется студенту, если он предоставил письменный подробно изложенный отчёт с описанием всех его манипуляций при выполнении практического задания, провёл необходимое тестирование результатов, полученных в конце выполнения практического занятия, с использованием встроенных механизмом программного обеспечения проверил результаты расчётов на отсутствие ошибок в них.

6 балла выставляется студенту, если он предоставил письменный, но не подробный отчёт с описанием большинства его манипуляций (но не всех) при выполнении практического задания, провёл необходимое тестирование результатов, полученных в конце выполнения практического занятия, с использованием встроенных механизмом программного обеспечения проверил результаты расчётов на отсутствие ошибок в них.

4 балла выставляется студенту, если он предоставил письменный, но не подробный отчёт с описанием большинства его манипуляций (но не всех) при выполнении практического задания.

2 балла - выставляется студенту, если он сдал письменный отчёт не полным и без проведения необходимых проверок расчётов на ошибки, при этом описание действий в отчёте уже содержит структурные ошибки, при условии, что выводы оформлены верно.

0 баллов - выставляется студенту, если он не сдал письменный отчёт.

Критерии оценивания рефератов

Рефераты оцениваются по следующим критериям:

Защита рефератов осуществляется, как правило, в форме групповой дискуссии, которая предполагает активное взаимодействие обучающегося с другими обучающимися группы и преподавателем. Дискуссия направлена на развитие коммуникативных навыков и формирования собственной позиции по рассматриваемой проблеме. Помимо содержания реферата преподавателем оценивается процедура его представления группе и аргументированность ответов на задаваемые выступающему вопросы.

14 баллов – реферат написан с соблюдением всех требований к письменным работам обучающихся, тема раскрыта полностью, верно определены объект и предмет исследования, представлен широкий перечень источников (не менее 10), проведен сравнительный анализ, использована действующая нормативная правовая база, приведены различные точки зрения, сделаны выводы, обучающийся доступно с использованием профессиональной терминологии, без существенной опоры на текст сделал доклад по теме реферата, обучающийся дал полные и развернутые ответы на вопросы группы и преподавателя, сформировал и отстаивает собственную позицию по рассматриваемой проблеме;

10 баллов – реферат написан с соблюдением всех требований к письменным работам обучающихся, тема раскрыта полностью, представлен широкий перечень источников (не менее 10), использована действующая нормативная правовая база, сравнительный анализ и выводы не представлены, обучающийся доступно, но с существенной опорой на текст, с использованием профессиональной терминологии сделал доклад по теме реферата, обучающийся дал достаточно полные ответы на вопросы группы и преподавателя, сформировал собственную позицию по рассматриваемой проблеме;

5 баллов – реферат написан с соблюдением всех требований к письменным работам обучающихся, тема раскрыта не полностью, объект и предмет исследования определены неверно, обучающийся доступно, но с существенной опорой на текст, с частичным использованием профессиональной терминологии представил доклад по теме реферата, обучающийся дал ответы не на все вопросы группы и преподавателя, не сформировал собственную позицию по рассматриваемой проблеме;

0 баллов – тема не раскрыта, неверно определены объект и предмет исследования, список использованных источников недостаточный, отсутствует сравнительный анализ, не сделаны выводы, обучающийся с существенной опорой на текст, без использования профессиональной терминологии представил доклад по теме, обучающийся не ответил на вопросы группы и преподавателя, не сформировал какую-либо позицию по рассматриваемой проблеме.

Шкала оценивания результатов успеваемости при осуществлении текущего контроля

Вид оценочного средства	Шкала оценивания (баллы)
Практическое занятие (предусмотрены 7 практических занятий)	0-49 (до 7 баллов за один отчет по практическому занятию)
Рефераты (до 3 рефератов) / количество баллов за один реферат	0-21 (до 7 баллов за один реферат)
Итого	***0-70****

* 70 - максимальное количество баллов по результатам текущего контроля

5. Оценочные материалы для промежуточной аттестации

5.1. Зачет проводится с применением следующих средств: в устной форме по заданиям билета зачета.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Промежуточный / Ключевой индикатор оценивания	Критерий оценивания
ПКр-8.1	Демонстрирует способность осуществлять верификацию и структуризацию информации, получаемой из разных источников, формировать базы данных, осуществлять оценку их полноты и качества. / Проводит верификацию и структуризацию информации, получаемой из разных источников, применяет различные способы по формированию баз данных, осуществляет оценку их полноты и качества	Анализирует достаточность и качество предоставляемой информации для осуществления оценочных расчетов; выбирает оптимальные модели оценочных расчетов; проводит верификацию и структуризацию информации, получаемой из разных источников, применяет различные способы по формированию баз данных, осуществляет оценку их полноты и качества; использует инструменты информационных технологий для проведения исследований в области финансовой отчётности, анализирует её показатели и результаты, использует методы финансового планирования и бюджетирования в сфере публичного управления; определяет комплекс аналитических процедур и методов анализа и оценки рисков финансового планирования и бюджетирования в сфере публичного управления; устанавливает ключевые индикаторы рисков и предельно допустимые значения

Компонент компетенции	Промежуточный / Ключевой индикатор оценивания	Критерий оценивания
		рисков финансового планирования и бюджетирования в сфере публичного управления с помощью информационных технологий.
ПКр-9.1	Демонстрирует способность подготовить официальную информацию о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами. / Использует информационные системы и базы данных в целях поиска и обработки официальной информации о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами	Демонстрирует знание правовых актов в области социально-экономического развития территорий, государственного и местного самоуправления, государственной и муниципальной службы, публичных финансов и инвестиций; использует информационные системы и базы данных в целях поиска и обработки официальной информации о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами; самостоятельно осуществлять правильную последовательность выполнения действий, правильную самостоятельную подготовку исходных данных; самостоятельно интерпретировать полученные результаты.

Шкала оценивания ответов на типовые вопросы билета заданий зачета (в баллах)

Вид оценочного средства	Шкала и критерии оценивания (баллы)
Индивидуальное собеседование	0-30
Итого	***0-30****

*30 баллов – обучающийся доступно с использованием профессиональной терминологии представил полные и развернутые ответы на вопросы, сформировал и отстаивает собственную позицию по рассматриваемой проблеме, провел сравнительный анализ, использовал действующую нормативную правовую базу, привел различные точки зрения, сделал выводы;

20 баллов – обучающийся доступно с использованием профессиональной терминологии представил достаточно полные ответы на вопросы, сформировал собственную позицию по рассматриваемой проблеме, использовал действующую нормативную правовую базу, сравнительный анализ и выводы не представлены;

10 баллов – обучающийся доступно с частичным использованием профессиональной терминологии представил ответы не на вопросы, не сформировал собственную позицию по рассматриваемой проблеме;

0 баллов – обучающийся не ответил на вопросы, не сформировал какую-либо позицию по рассматриваемой проблеме.

Шкала оценивания результатов обучения при осуществлении промежуточной аттестации

Показатель оценивания	Критерий оценивания	Оценка
Способен осуществлять верификацию и структуризацию	Анализирует достаточность и качество предоставляемой информации для осуществления оценочных расчетов; выбирает оптимальные модели оценочных расчетов; проводит верификацию и структуризацию информации, получаемой из разных источников,	Зачтено

информации, получаемой из разных источников, формировать базы данных, осуществлять оценку их полноты и качества. Способен подготовить официальную информацию о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами.	применяет различные способы по формированию баз данных, осуществляет оценку их полноты и качества; использует инструменты информационных технологий для проведения исследований в области финансовой отчётности, анализирует её показатели и результаты, использует методы финансового планирования и бюджетирования в сфере публичного управления; определяет комплекс аналитических процедур и методов анализа и оценки рисков финансового планирования и бюджетирования в сфере публичного управления; устанавливает ключевые индикаторы рисков и предельно допустимые значения рисков финансового планирования и бюджетирования в сфере публичного управления с помощью информационных технологий. Демонстрирует знание правовых актов в области социально-экономического развития территорий, государственного и местного самоуправления, государственной и муниципальной службы, публичных финансов и инвестиций; использует информационные системы и базы данных в целях поиска и обработки официальной информации о деятельности органа власти, государственной или муниципальной организации при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами; самостоятельно осуществлять правильную последовательность выполнения действий, правильную самостоятельную подготовку исходных данных; самостоятельно интерпретировать полученные результаты.	
	Не способен самостоятельно анализировать достаточность и качество предоставляемой информации для осуществления оценочных расчетов; выбирает оптимальные модели оценочных расчетов; не проводит верификацию и структуризацию информации, получаемую из разных источников, не способен формировать базы данных или осуществляет это не уверенно с многочисленными ошибками внесения / изменения данных в базе; не использует инструменты информационных технологий для проведения исследований в области финансовой отчётности, не умеет анализировать показатели и результаты, не имеет представления о методах финансового планирования и бюджетирования в сфере публичного управления и не способен искать первичные финансовые показатели в их официальных источниках; не определяет комплекс аналитических процедур и методов анализа и оценки рисков финансового планирования и бюджетирования в сфере публичного управления; не способен оценивать и проводить ранжирование рисков финансового планирования и бюджетирования в сфере публичного управления с помощью информационных технологий. Не уверенно демонстрирует знание правовых актов в области социально-экономического развития территорий, государственного и местного самоуправления, государственной и муниципальной службы, публичных финансов и инвестиций; не использует информационные системы и базы данных в целях поиска и обработки официальной информации о деятельности органа власти и имеет слабое представление об их официальных источниках; не способен самостоятельно осуществлять правильную последовательность выполнения действий, правильную самостоятельную подготовку исходных данных; не умеет интерпретировать полученные результаты; не способен обрабатывать официальную информацию из источников, предоставленной государственной или муниципальной организацией при взаимодействии с государственными, некоммерческими, хозяйственными организациями и физическими лицами.	Не зачтено

Шкала соответствия между баллами (процентами), выставляемыми по многобалльной (процентной) системе, и отметками бинарной системы оценки знаний

Наименование отметки	Сумма баллов (процентов)
«Зачтено»	100 – 60
«Не зачтено»	59 - 0

Типовые вопросы к зачету

1. Концепция информационной безопасности
2. Место информационной безопасности экономических систем в национальной безопасности государства
3. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы
4. Виды возможных нарушений информационной безопасности вычислительной системы
5. Актуальность проблемы защиты информации
6. Модели безопасности и их применение
7. Классификация методов защиты информации от несанкционированного доступа
8. Механизмы защиты информации от несанкционированного доступа
9. Государственные требования к построению системы защиты информации
10. Требования к криптографическим средствам системы защиты информации от несанкционированного доступа
11. Средства активного аудита компьютерных систем
12. Идентификация и аутентификация субъектов и объектов компьютерных систем
13. Основные подходы к защите данных от несанкционированного доступа
14. Цель и задачи правового обеспечения системы защиты информации
15. Аппаратные методы защиты информации
16. Особенности физических методов защиты информации
17. Внешние угрозы компьютерным системам защиты информации
18. Внутренние угрозы корпоративной информации
19. Классификация злоумышленников
20. Классификация ущерба после реализации угрозы в виде атаки
21. Классификация компьютерных преступлений
22. Виды компьютерной преступности
23. Понятие и виды информации, защищаемой законодательством РФ
24. Уголовно-правовая характеристика компьютерных преступлений
25. Понятие компьютерных вирусов и их отличительная особенность
26. Классификация компьютерных вирусов
27. Способы борьбы с компьютерными вирусами. Профилактические мероприятия
28. Алгоритм работы антивирусной программы
29. Электронная подпись, области ее применения
30. Хэш-функция и ее назначение
31. Цель аудита системы информационной безопасности.
32. Этапы аудита системы информационной безопасности
33.

6. Методические материалы для освоения дисциплины

6.1 Методические рекомендации для обучающихся при подготовке к аудиторным занятиям

Методические указания для обучающихся по освоению материала занятий лекционного типа

Лекция представляет собой систематизированное, последовательное изложение преподавателем учебного материала в соответствии с изучаемой темой дисциплины. Занятия лекционного типа дают обучающимся систематизированные знания о наиболее сложных и актуальных проблемах изучаемой дисциплины.

Осуществляя учебные действия на лекционных занятиях, обучающиеся должны внимательно воспринимать материал, подготовленный преподавателем, мыслить, добиваться понимания изучаемого предмета. Обучающимся рекомендуется вести конспект. В случае недопонимания какой-либо части предмета следует в установленном порядке задать вопрос преподавателю.

Для визуального восприятия формулировки темы, учебных вопросов, наиболее важных определений, схем, иллюстраций, таблиц, графиков, дополнительных источников информации и т. п. обучающимся рекомендуется обращать внимание на предлагаемые преподавателем учебные презентации в формате MS PowerPoint (или созданные с помощью иных приложений).

Методические указания для обучающихся по освоению материала занятий семинарского типа

Занятия семинарского типа (практические занятия, лабораторные занятия) являются аудиторными. Для того, чтобы аудиторный материал занятия был освоен обучающимся, ему необходимо предварительно изучить теоретический материал по данной теме, ознакомиться с литературой, рекомендованной преподавателем и найденной самостоятельно; выполнить задания, предложенные преподавателем к занятию; составить перечень вопросов, вызывающих затруднения, неясности или сомнения, обсудить их с преподавателем на занятии.

В ходе подготовки к практическим и лабораторным занятиям обучающемуся рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. При этом следует учесть рекомендации преподавателя и требования рабочей программы. Рекомендуется также дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины.

Следует подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие.

Готовясь к выступлению на занятии, обучающийся может обращаться за методической помощью к преподавателю. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам.

Методические указания для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных вопросов учебной дисциплины. Самостоятельная работа является обязательной для каждого обучающегося, ее объем определяется учебным планом.

Усвоение материала дисциплины в процессе аудиторных занятий и в результате самостоятельной подготовки и изучения отдельных вопросов дисциплины позволят студенту подойти к промежуточной аттестации подготовленным и потребует лишь повторения ранее пройденного материала. Знания, накапливаемые постепенно и в различных ракурсах, с использованием противоположных мнений и взглядов на ту или иную проблему экономики являются глубокими и качественными, и позволяют сформировать соответствующие компетенции как итог образовательного процесса.

Для систематизации знаний по дисциплине первоначальное внимание обучающемуся следует обратить на рабочую программу курса, которая включает основные темы дисциплины, в рамках которых и формируются вопросы для текущего контроля и промежуточной аттестации. Поэтому обучающийся, заранее ознакомившись с программой курса, может лучше сориентироваться в последовательности освоения курса с позиций организации самостоятельной работы.

При организации процесса освоения дисциплины обучающемуся следует учитывать:

1. Планирование времени, отведенного на освоение дисциплины.

При планировании времени на освоение дисциплины следует руководствоваться: а) структурой дисциплины (раздел 3 настоящей рабочей программы), в которой указаны количество

академических часов в разрезе каждой темы, вида занятий (лекции, практические занятия) и часы на самостоятельную работу; б) формой текущего контроля успеваемости (опрос, опорный конспект, тестирование, реферат); в) формой промежуточной аттестации (зачет).

2. Последовательность действий при освоении дисциплины. Изучение каждой темы дисциплины целесообразно начинать со знакомства с содержанием дисциплины в разрезе тем; затем следует этап подбора источников из числа рекомендуемых и подобранных самостоятельно (научные статьи; информация с официальных сайтов государственных органов, др.). Изучение источниковой базы может сопровождаться конспектированием (например, тезисным), составлением глоссария, др. Целесообразно вести перечень проблемных вопросов как по существу темы, обусловленных пробелами в научном и правовом поле и проблемами практического характера, так и в случае затруднений с уяснением смысла изложенного в источниках материала (указанные вопросы могут быть разрешены впоследствии самим студентом во время занятий или на консультации с преподавателем).

3. Использование учебно-методических материалов и работа с литературой. Следует применять следующую последовательность подбора источников для изучения тем дисциплины: а) научная и учебная литература: основная и дополнительная; б) нормативные правовые материалы; в) Интернет-ресурсы и др.

4. Подготовка к текущему контролю успеваемости. При выполнении заданий следует руководствоваться методическими рекомендациями, представленными по каждому виду заданий (опрос/опорный конспект, реферат, тестирование).

При самостоятельной работе обучающиеся работают с рекомендованными материалами при минимальном участии преподавателя. При необходимости обучающемуся рекомендуется записывать вопросы, возникшие у него в ходе работы над темой, для обсуждения их с преподавателем в ходе семинаров или консультаций.

Методические указания по подготовке рефератов

Реферат – результат самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Реферат должен состоять из следующих частей: титульный лист; содержание; введение; основной текст, разбитый на главы и подразделы (вопросы); заключение; библиографический список. Реферат оформляется в соответствии с требованиями, предъявляемыми локальными нормативными актами РАНХиГС к письменным работам.

6.2 Методические рекомендации по изучению дисциплины с применением ДОТ

Данная дисциплина может быть реализована с применением дистанционных образовательных технологий (ДОТ).

Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на образовательном портале института: https://lms.ranepa.ru. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

Страница каждой дисциплины на образовательном портале имеет следующую структуру и содержание:

1. Общая информация содержит:

– РПД – рабочую программу дисциплины, в которой представлены объем и место дисциплины в структуре образовательной программы; содержание и структура дисциплины; материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине; методические указания для обучающихся по освоению дисциплины и т.д);

– Календарно тематический план изучения дисциплины, в котором отражена дата проведения лекционного, семинарского занятий по соответствующей теме и режим проведения занятия;

– Инструкция по работе в СДО и рекомендации по изучению дисциплины посредством

СДО

– Графики индивидуальных и групповых консультаций.

2. Лекционные материалы – в этом разделе представлены текстовыми файлами лекции преподавателя (с разбивкой по темам, разделам и т.п.). В дополнение к лекционному материалу могут быть представлены презентации, нормативно-правовые документы.

3. Задания к занятиям семинарского типа (практич. занятиям, семинарам, лаб. работам и т.п.) – в этом разделе представлены материалы к занятиям семинарского типа отдельными файлами для каждого отдельного занятия (согласно расписанию), в которых в полном объеме отражено содержание занятия по указанной теме, приведены задания с указанием балльной оценки за их выполнение, сроков выполнения и организационных моментов по представлению выполненных заданий преподавателю на проверку (например, сдача заданий старосте группе с последующей их отправкой на почту преподавателя единым письмом или личная отправка задания преподавателю каждым студентом).

4. Самостоятельная работа – в этом разделе представлена информация по организации самостоятельной работы студентов, например, указаны темы для самостоятельного изучения, перечень индивидуальных заданий, тематика докладов, рефератов.

5. Текущий контроль – в этом разделе представлены задания для выполнения их студентами с целью ведения учета текущей успеваемости студента.

6. Промежуточная аттестация – в этом разделе размещается информация по формату промежуточной аттестации, вопросы для подготовки к экзамену (зачету), тесты.

7. Рекомендуемая литература – в этом разделе представлен перечень рекомендуемой литературы для изучения дисциплины, ссылки на ЭБС.

8. Успеваемость – в этом разделе преподаватель размещает еженедельные сведения по успеваемости студентов.

Таким образом, весь материал необходимый для изучения студентом дисциплины представлен на образовательном портале института.

Для активного взаимодействия диалогового характера (лекции, семинары, консультации) со студентами преподаватель по мере освоения режима обучения с применением ДОТ может использовать различные возможности Интернет-пространства, допустимые для института.

Все виды работ проводятся по календарному учебному графику и строго по расписанию. В начале пары преподаватель проверяет присутствующих, дает комментарии по лекции (семинарскому занятию), дает задание, дает рекомендации по его выполнению, комментирует оценку за его выполнение, сроки и процедуру сдачи заданий.

Преподаватель ведет и сохраняет записи текущей успеваемости (выполненные задания, ведомость, студенческий журнал, журнал преподавателя) и видеозаписи и результаты промежуточной аттестации с обязательной идентификацией обучающихся (паспорт).

Доступ к системе дистанционных образовательных технологий (СДО) осуществляется каждым обучающимся самостоятельно с любого устройства на образовательном портале института: https://lms.ranepa.ru. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

Все формы текущего контроля, проводимые в системе дистанционного обучения, оцениваются в системе дистанционного обучения. Доступ к видео и материалам лекций предоставляется в течение всего семестра. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется на ограниченное время согласно регламенту дисциплины, опубликованному в СДО. Преподаватель оценивает выполненные обучающимся работы после окончания срока выполнения согласно установленному графику.

7 Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

7.1 Основная литература

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2022. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/33430.html (дата обращения: 24.10.2023). — Режим доступа: для авторизир. Пользователей

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Г. П. Жигулин. — СПб. : Университет ИТМО, 2022. — 174 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/67451.html (дата обращения: 24.10.2023). — Режим доступа: для авторизир. пользователей

3. Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под редакцией А. В. Морозов. — М. : Всероссийский государственный университет юстиции (РПА Минюста России), 2022. — 78 с. — ISBN 978-5-89172-850-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/47262.html (дата обращения: 24.10.2023). — Режим доступа: для авторизир. Пользователей

4. Петров Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/33857.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. пользователей

5. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/43183.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

6. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77320.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. пользователей

7.2 Дополнительная литература

1. Аверченков, В. И. Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. — Брянск : Брянский государственный технический университет, 2012. — 184 с. — ISBN 978-89838-489-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/7002.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. пользователей

2. Алексеев, В. А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / В. А. Алексеев. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2009. — 16 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17710.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. пользователей

3. Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 95 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17925.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

4. Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17926.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

5. Кармановский, Н. С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — СПб. : Университет ИТМО, 2016. — 169 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/67452.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

6. Кремер, А. С. Нормативно-правовые аспекты обеспечения информационной безопасности инфокоммуникационных сетей : учебное пособие / А. С. Кремер. — М. : Московский технический университет связи и информатики, 2007. — 97 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/61745.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

7. Разработка системы технической защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. — Брянск : Брянский государственный технический университет, 2012. — 187 c. — ISBN 5-89838-358-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/7005.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

8. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — М. : Московский городской педагогический университет, 2011. — 260 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/26486.html (дата обращения: 24.10.2019). — Режим доступа: для авторизир. Пользователей

9. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М. : Издательство Юрайт, 2017. – 261 с. – (Серия : Бакалавр и магистр. Академический курс).– ISBN 978-5-534-01678-9. – Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.

10. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. – 2-е изд., испр. и доп. – М. : Издательство Юрайт, 2017. – 246 с. – (Серия : Бакалавр и магистр. Академический курс).– ISBN 978-5-534-01679-6. – Режим доступа : www.biblio-online.ru/book/2095B353-8AE3-4A0F-987F-00C157F3BDE7.

11. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – М. : Издательство Юрайт, 2017. – 309 с. – (Серия : Бакалавр и магистр. Академический курс).– ISBN 978-5-534-04732-5. – Режим доступа : www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E.

7.3. Нормативные правовые документы

1. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-фз от 27 июня 2006 года [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
2. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: Федеральный закон № 8-фз от 9 февраля 2009 года [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
3. Об организации предоставления государственных и муниципальных услуг: Федеральный закон № 210-фз от 27 июля 2010 года [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
4. Об электронной подписи : Федеральный закон № 63-фз от 6 апреля 2011 года [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
5. О персональных данных: Федеральный закон № 152-фз от 27 июля 2006 года [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
6. Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме: постановление Правительства РФ от 8 июня 2011 г. № 451 [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
7. О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций) : постановление Правительства РФ от 24 октября 2011 г. № 861 [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».

7.4 Интернет-ресурсы

1. Российской государственной библиотеки www.rsl.ru
2. Справочно-информационный портал http://www.gramota.ru
3. ЭБС «ЛАНЬ». – URL.:http://www.e.lanbook.com.
4. ЭБС «Ай пи эр букс». – URL.:http://www.iprbookshop.ru.
5. ЭБС «ЮРАЙТ». – URL.:http://www.biblio-online.ru.

7.5 Иные источники

Статистические сборники.
Аналитические материалы.

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

Адрес	Наименование оборудованных учебных кабинетов	Оснащенность оборудованных учебных кабинетов, перечень программного обеспечения
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), практик, групповых и индивидуальных консультаций, текущего контроля и	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.

	промежуточной аттестации.	
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Специализированные аудитории, оборудованные для проведения занятий по информационным технологиям (компьютерные классы)	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доска маркерная, учебные пособия, тренажеры и другие средства и оборудование. Аудитории обеспечены компьютерной техникой с возможностью подключения к сети «Интернет» и электронной информационно-образовательной среде организации. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение, справочно-правовая система «Консультант плюс», информационно-справочная система «Кодекс», Any Logic University, KNIME (Open Source программное обеспечение с открытым исходным кодом), Gretl, Statgraphics Centurion XV Academic Pro, 1С Предприятие 8 для учебных заведений, Eviews Academic, Adobe Photoshop
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Учебные аудитории для самостоятельной работы обучающихся	Специализированная мебель для организации рабочих мест обучающихся, технические средства обучения, мультимедийное оборудование, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Специализированная аудитория, оборудованная для проведения занятий по криминалистике / кабинет криминалистики	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доска маркерная, макеты, реактивы, раздаточные методические материалы и наглядные пособия, реквизит к осмотру места происшествия, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33, Точка кипения	Центр (класс) деловых игр	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, учебно-наглядные пособия, доска маркерная, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.

680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Специальная библиотека (библиотека ограниченного доступа) /	Помещение для самостоятельной работы обучающихся. Специализированная мебель для организации рабочих мест обучающихся, технические средства обучения, мультимедийное оборудование. Читальный зал научной библиотеки оснащен компьютерной техникой с возможностью подключения к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Кабинет иностранных языков	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доска маркерная, макеты, наглядные учебные пособия, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Научно-исследовательская лаборатория	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доска маркерная, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Помещения для научно-исследовательской работы	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доска маркерная, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д.33	Актовый зал	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доступ к сети «Интернет» и электронной информационно-образовательной среде. Программное обеспечение: Microsoft Windows, пакет Microsoft office, антивирусное программное обеспечение.

Информационные технологии реализуются через электронно-информационную образовательную среду академии.