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

ДАЛЬНЕВОСТОЧНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ - филиал РАНХиГС

УТВЕРЖДЕНО
И.о. директора Дальневосточного института управления – филиала РАНХиГС
М.Ю. Боев

Электронная подпись

ПРОГРАММА СПЕЦИАЛИТЕТА

Прокурорская деятельность

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

Б1.В.24 Информационная безопасность

40.05.04 Судебная и прокурорская деятельность

Очная, заочная

Год набора – 2024

Хабаровск, 2024 г.

Автор(ы)–составитель(и):
кандидат экономических наук, доцент кафедры экономики и цифровых технологий Пынько Л.Е.
кандидат технических наук, доцент кафедры экономики и цифровых технологий Буняева Е.В.

Заведующий кафедрой экономики и цифровых технологий Поливаева О.Г.

РПД «Информационная безопасность» одобрена на заседании кафедры экономики и цифровых технологий. Протокол от 06.05.2024 № 9.

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…….. 5
3. Содержание и структура дисциплины…… 6
4. Материалы текущего контроля успеваемости обучающихся…….. 10
5. Оценочные материалы промежуточной аттестации по дисциплине…….. 20
6. Методические материалы для освоения дисциплины…… 25
7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"…….. 29
7.1 Основная литература…… 29
7.2 Дополнительная литература…… 30
7.3 Нормативные правовые документы и иная правовая информация……. 32
7.4 Интернет-ресурсы……. 32
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы……. 33

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

1.1 Дисциплина Б1.В.24 «Информационная безопасность» обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
УК ОС -8	Способность создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	УК ОС -8.1	Оценивает эффективность основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
		УК ОС -8.2	Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

1.2. В результате освоения дисциплины у обучающихся должны быть сформированы:

Профессиональные действия	Код компонента компетенции	Результаты обучения
Координация деятельности по борьбе с преступностью органов внутренних дел, органов федеральной службы безопасности, органов таможенной службы и других правоохранительных органов	УК ОС -8.1 Оценивает эффективность основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	**На уровне знаний:** обладать знаниями алгоритмов поведения в целях предотвращения угроз безопасности в информационной среде, в т. ч. при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов; имеет представления о методах целенаправленного и эффективного предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества;
		На уровне умений: осуществлять успешную работу с алгоритмами противодействия угроз безопасности в информационной среде, в т. ч. при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов;
		На уровне навыков: владеть навыками предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого

	развития общества, в т. ч. навыками обеспечения безопасности в информационной среде.
УК ОС -8.2 Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	**На уровне знаний:** обладать знаниями работы с правовыми системами; успешного и систематического решения стандартных задач профессиональной деятельности; методов целенаправленного и эффективного предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов;
	На уровне умений: осуществлять успешную работу с правовыми системами; получать юридически значимую информацию; решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности;
	На уровне навыков: владеть навыками предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

В соответствии с учебным планом на дисциплину Б1.В.24 «Информационная безопасность» отведено 3 ЗЕ, что составляет 108 ак.ч./81 астр.ч,:

- для очной формы обучения на контактную работу выделено 48 ак.ч. / 36 астр.ч. (из них: 16 акад. часов / 12 астр. часов лекционных занятий, 32 акад. часов / 24 астр. часов практических занятий), на самостоятельную работу - 60 ак.ч. / 45 астр. часов – на самостоятельную работу.

- для заочной формы обучения на контактную работу выделено 10 ак.ч. / 7,5 астр.ч. (из них: 2 акад. часа / 1,5 астр. часа лекционных занятий, 6 акад. часа / 4,5 астр. часа практических занятий), на самостоятельную работу - 96 ак.ч. / 72 астр. часов – на самостоятельную работу (4 акад. часов / 3 астр. часов самостоятельная работа обучающихся в период зачетно-экзаменационной сессии).

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.24 «Информационная безопасность» входит в структуру программы подготовки специалитета и относится к дисциплинам вариативной части учебного плана (5 курс, 9 семестр для очной формы обучения; 5 курс 9 семестр для заочной формы обучения).

Дисциплина реализуется после изучения дисциплин Б1.Б.04 «Безопасность жизнедеятельности», Б1.В.ДЭ.01.01 «Цифровое общество, введение в искусственный интеллект и разговорные боты», Б1.В.ДЭ.01.02 «Цифровое общество и управление цифровой репутацией».

Форма промежуточной аттестации в соответствии с учебным планом – зачёт.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости[2], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
1.	Методологические основы дисциплины	7	1		2		4	ВК, ОПЗ
2.	Направления защиты информации	8	2*		2		4	О, ОПЗ
3.	Угрозы безопасности информационных систем	12	2		4*		6	ОПЗ, О
4.	Компьютерные преступления	12	2*		2		8	О, ОПЗ
5.	Вредоносные программы и основы защиты от них	9	1		2		6	О, ОПЗ
6.	Криптографические методы защиты информации	12	2		4*		6	ОПЗ, О, КР
7.	Электронная цифровая подпись и особенности ее применения	16	2*		8		6	ОПЗ, О
8.	Нормативно-правовые основы информационной безопасности РФ, правовые основы обеспечения информационной безопасности экономической деятельности	18	2		6		10	ОПЗ, О
9.	Стандарты информационной безопасности. Общие критерии	14	2*		2		10	ОПЗ, О
Промежуточная аттестация								Зачет
Всего (акад.час./астр.час.)		**108**	**16**		**32**		**60**	**Зачет**

Примечание:

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.

** занятие проводится в интерактивной форме*

*** формы текущего контроля успеваемости: входной контроль знаний (ВК), опрос (О), контрольная работа (КР), письменный отчет по практическому занятию (ОПЗ).*

Заочная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
1.	Методологические основы дисциплины	10					10	ВК, ОПЗ
2.	Направления защиты информации	12					12	О
3.	Угрозы безопасности информационных систем	12			2*		10	ОПЗ, О
4.	Компьютерные преступления	12					12	О
5.	Вредоносные программы и основы защиты от них	1					10	О
6.	Криптографические методы защиты информации	12			2*		10	ОПЗ, О, КР
7.	Электронная цифровая подпись и особенности ее применения	10					10	О
8.	Нормативно-правовые основы информационной безопасности РФ, правовые основы обеспечения информационной безопасности экономической деятельности	14			2		12	О
9.	Стандарты информационной безопасности. Политика информационной безопасности предприятия	12	2*				10	О
Промежуточная аттестация							4	Зачет
Всего (акад.час./астр.час.)		**108**	**2**		**6**		**100**	**Зачет**

Примечание:

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.

** занятие проводится в интерактивной форме*

*** формы текущего контроля успеваемости: входной контроль знаний (ВК), опрос (О), контрольная работа (КР), письменный отчет по практическому занятию (ОПЗ).*

Содержание дисциплины

Раздел 1. Ключевые аспекты и вопросы формирования информационной безопасности современного предприятия

Тема 1.1. Методологические основы дисциплины

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. Информация как объект защиты. Современная постановка задачи защиты информации. Информационная безопасность. Принципы информационной безопасности. Объекты информационной безопасности РФ. Задачи обеспечения информационной безопасности. Информационная политика. Информация для экономики. Открытая информация – деловые СМИ. Массовые и специализированные издания для специалистов экономического профиля. Информационные процессы: этапы и закономерности формирования и развития. Принципы и методы анализа и управления состояниями и процессами информационной безопасности

Тема 1.2. Направления защиты информации

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. Правовое регулирование сегментов информационной сферы экономической деятельности. Правовые акты информационной безопасности экономической деятельности. ФЗ «Об информации, информационных технологиях и защите информации». ФЗ «О предпринимательской деятельности». ФЗ «Об информации, информационных технологиях и защите информации».

Стратегия «Национальной безопасности», Стратегия «Экономической безопасности», Доктрина «Информационной безопасности» - их взаимосвязь, взаимное проникновение целей и задач, структурные элементы безопасности нации.

Раздел 2. Безопасность информационных систем

Тема 2.1. Угрозы безопасности информационных систем

Угрозы и оценка уязвимости информации. Терминология и классификация угроз, модель угроз информационной безопасности, модель нарушителя, виды нарушителей. Возможные способы противодействия угрозам ИБ. Модели оценки ущерба от угроз информационной безопасности. Криминогенная обстановка в кредитно-финансовой сфере. Роль человеческого фактора. Основные цели корпоративного управления безопасностью. Тенденции, связанные с обеспечением безопасности информационных ресурсов. Подходы к обеспечению безопасности информационных ресурсов. Документация в области обеспечения безопасности информационных ресурсов. Модели зрелости организации.

Тема 2.2. Компьютерные преступления

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

преступностью в РФ. Обеспечение информационной безопасности в ведущих зарубежных странах мира

Тема 2.3. Вредоносные программы и основы защиты от них

Основные понятия и определения: вирус, свойства компьютерных вирусов, среды распространения в компьютерной системе, виды ущерба компьютерным системам. Классификация вредоносных программ, методы обнаружения и удаления компьютерных вирусов. Классификация антивирусных программ. Алгоритм работы антивирусной программы

Раздел 3. Криптографические методы защиты информации

Тема 3.1. Криптографические методы защиты информации

Вводная терминология, классификация алгоритмов шифрования, реализация криптографических методов.

Тема 3.2. Электронная цифровая подпись и особенности ее применения

Назначение и применение электронной подписи, виды электронной подписи, ее юридическая правомочность, технология формирования электронной подписи, электронный обмен данными

Раздел 4. Правовые основы защиты информации

Тема 4.1. Нормативно-правовые основы информационной безопасности РФ, правовые основы обеспечения информационной безопасности экономической деятельности.

Нормативно-правовые основы информационной безопасности, основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Правовые основы обеспечения информационной безопасности экономической деятельности. Понятие информационной экономики. Теория информационализма М. Кастельса как нового способа развития экономики и общественных отношений. Создание, основные положения теории асимметричной информации. Основные идеи ИЭ в трудах Дж. Стиглица. Развитие основных направлений информационной экономики в России. Формирование инфраструктуры электронного бизнеса. Основные задачи обеспечения эффективного функционирования электронной экономики. Проблемы безопасности электронного бизнеса в России

Тема 4.2. Стандарты информационной безопасности. Политика информационной безопасности предприятия.

Основное содержание оценочного стандарта ISO/IEC 15408. Принципы иерархии: класс-семейство-компонент-элемент; функциональные требования; требования доверия. Политика информационной безопасности предприятия: основные НПА по сопровождению информационной безопасности предприятия. Профилактические мероприятия информационной безопасности организации. Управление системой обеспечения информационной безопасности. Циклическая модель управления Дёминга. Информационные риски. Политика управления информационными рисками. Универсальная модель политики использования ПК интернета. Цель и основные положения политики. Информационные активы и ресурсы. Безопасность и составляющая собственность информация. Правила общего использования и владения интернетом. Недопустимое использование интернета. Работа с системами и сетями. Работа с электронной почтой.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.В.24 Информационная безопасность используются следующие методы текущего контроля успеваемости обучающихся:

Тема №	Тема (раздел)	Методы текущего контроля успеваемости в аудитории
Методологические основы дисциплины	Входной контроль в форме тестирования, отчет по результатам практического занятия	ВК, ОПЗ
Направления защиты информации	Проверка конспектов лекций, обратная связь с преподавателем в форме устного опроса по терминам и основным положениям предыдущих лекций; отчет по результатам практического занятия	О, ОПЗ
Угрозы безопасности информационных систем	Отчет по результатам практического занятия, проверка конспектов лекций, устный опрос на практическом занятии	ОПЗ, О
Компьютерные преступления	Проверка конспектов лекций, обратная связь с преподавателем в форме устного опроса по терминам и основным положениям предыдущих лекций; отчет по результатам практического занятия	О, ОПЗ
Вредоносные программы и основы защиты от них	Отчет по результатам практического занятия, устный опрос на практическом занятии	ОПЗ, О
Криптографические методы защиты информации	Проверка конспектов лекций, обратная связь с преподавателем в форме устного опроса по терминам и основным положениям предыдущих лекций; отчет по результатам практического занятия, контрольная работа в письменной форме	ОПЗ, О, КР
Электронная цифровая подпись и особенности ее применения	Отчет по результатам практического занятия, устный опрос на практическом занятии	ОПЗ, О
Нормативно-правовые основы информационной безопасности РФ, правовые основы обеспечения информационной	Отчет по результатам практического занятия, проверка конспектов лекций, устный опрос на практическом занятии	ОПЗ, О

безопасности экономической деятельности		
Стандарты информационной безопасности. Политика информационной безопасности предприятия	Отчет по результатам практического занятия, проверка конспектов лекций, устный опрос на практическом занятии	ОПЗ, О

формы текущего контроля успеваемости: входной контроль знаний (ВК), опрос (О), контрольная работа (КР), письменный отчет по практическому занятию (ОПЗ).

4.2. Материалы текущего контроля успеваемости обучающихся

Типовые вопросы входного контроля

1. Сущность и понятие информационной безопасности, характеристика её составляющих.
2. Современное состояние развития теории информационной безопасности.
3. Безопасность в информационном обществе.
4. Информация в современном мире и её свойства.
5. Понятие безопасности.
6. Информационная безопасность: понятие и составляющие
7. Место информационной безопасности в системе национальной безопасности России.
8. Информационная война как угроза национальной безопасности.
9. Место информационной безопасности в системе национальной безопасности.
10. Значение информационной безопасности для субъектов информационных отношений.
11. Нормативные правовые акты

Типовые задания и оценочные материалы для проведения практических занятий и типовые вопросы для проведения опросов

Тема №1 «Методологические основы дисциплины»

Подготовка предварительного варианта концепции информационной безопасности (ИБ) предприятия

Цель: ознакомиться с основными структурными элементами концепции информационной безопасности (ИБ) предприятия.

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

Задание: для условного предприятия выполнить анализ существующей информационно-распорядительной документации и нормативных требований, отражающих текущую или желаемую политику безопасности; определить цели и задачи системы информационной безопасности (далее, 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.

Вопросы для проведения опроса:

1. Сущность и содержание понятия «информационная безопасность». Ее место и роль в системе обеспечения национальной безопасности.

2. Цели и задачи обеспечения информационной безопасности.

3. Переход к информационному обществу и возрастание отрицательного воздействия угроз экономического характера.

4. Возможности органов власти и управления, общественных институтов по предотвращению, локализации и нейтрализации угроз информационной безопасности.

Тема №2 «Направления защиты информации»

Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, построение модели ИБ.

Цель: изучить концепцию ИБ для условного предприятия, закрепить знания по видам и классам охраняемой информации, уметь моделировать «портрет» нарушителя, модель угроз, научиться строить модель ИБ.

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

Задание: на основе предварительного варианта концепции ИБ предприятия, полученного в результате практического занятия №1 составить детальное описание охраняемой информации, «портрета» нарушителя, модели угроз, выполнить построение модели ИБ.

Вопросы для проведения опроса:

1) Дайте определения информации, назовите ее основные типы, виды, свойства.

2) Охарактеризуйте экономическую информацию.

3) Выделите информационные составляющие в функционировании экономического сектора народно-хозяйственного комплекса страны.

Примерные темы для написания контрольной работы.

1) Управление информационными процессами как элемент государственной информационной политики.

2) Массовая информационная сфера как объект управления.

Тема №3 «Угрозы безопасности информационных систем»

Разработка параметров защищенности программных информационных систем (ИС) компании и программы ИБ

Цель: рассмотреть для условного предприятия возможные уязвимости и дефекты защиты внутренней производственной информационной системы. Освоить методы расчета параметров защищенности при помощи модели с полным перекрытием.

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

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

Вопросы для проведения опроса:

1) Содержание, структура, правила использования информационных ресурсов экономической деятельности
2) Информационные ресурсы для легальной и теневой экономики
3) Профессиональные периодические издания для экономистов
4) Примерные темы для написания контрольной работы.
5) Идеология как теоретическая основа управления информационными процессами.
6) Цели, стратегия, проект, план, программа, технологии управления информационными процессами.
7) Место и роль социологических, политических, психологических исследований в системе обеспечения информационной безопасности.

Тема №4 «Компьютерные преступления»

Цель: рассмотреть виды основных компьютерных преступлений, вопросы кибербезопасности личности, вопросы кибербезопасности предприятий и организаций.

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

Задание: подготовить доклад, по теме занятия, в тексте доклада должно быть изложение современных тенденций развития компьютерных преступлений на основе анализа правовой статистики в сфере информационной безопасности в РФ, нормативных документов и норм закона, регулирующих ответственность за преступления в сфере информационной безопасности.

Вопросы для проведения опроса:

1. Мошенничество в сфере компьютерной информации: проблемы противодействия.
2. Мошенничество в сфере компьютерной информации: проблемы аппаратного и программного противодействия.
3. Мошенничество в сфере компьютерной информации: проблемы квалификации.
4. Дистанционные мошенничества: способы и меры противодействия.
5. Цифровые картели, как новая разновидность киберпреступлений.
6. Электронные средства платежа как предмет преступлений против собственности.
7. Несовершеннолетнее лицо как субъект преступлений в сети Интернет.
8. Роль формирования цифрового права в системе российского законодательства как фактора предупреждения киберпреступности.

Тема №5 «Вредоносные программы и основы защиты от них»

Криптографические методы защиты информации. Шифры перестановки

Цель: рассмотреть виды основных антивирусных комплексов, систему антивирусной защиты для предприятий и организаций.

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

Задание: используя антивирусные комплексы проверить систему на наличие вирусов, по журналу антивирусной программы определить найденные уязвимости в системе, рассмотреть инструменты помещения угроз «на карантин», удаления угроз в системе, тестирование системы на безопасность после устранения в ней вирусов и нежелательного ПО.

Вопросы для проведения опроса:

1. Классификация вредоносных программ
2. Компьютерные вирусы
3. Сетевые черви
4. Троянские программы
5. Шпионское ПО (Spyware)
6. Хакерские утилиты (RootKit)
7. Основы работы антивирусных программ
8. Сигнатурный анализ
9. Проактивные методы обнаружения
10. Эвристические анализаторы
11. Поведенческие блокираторы
12. Дополнительные модули
13. Режимы работы антивирусов
14. Проверка в режиме реального времени
15. Проверка по требованию
16. Антивирусные комплексы

Тема №6 «Криптографические методы защиты информации»

Криптографические методы защиты информации. Шифры замены, простой одинарной перестановки, блочной одинарной перестановки, табличной маршрутной перестановки.

Цель: освоить алгоритмы шифрования методами простой одинарной перестановки, блочной одинарной перестановки, табличной маршрутной перестановки, вертикальной перестановки, поворотной решетки, магического квадрата, двойной перестановки.

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

Задание: Составить шифрограмму, используя шифр Цезаря, шифр перестановки – проанализировать уровень сложности и устойчивости использованных шифров.

Криптографические методы защиты информации. Шифры замены, гаммирования

Цель: освоить алгоритмы шифрования методом Цезаря, лозунгового шифра, полибианского квадрата, системы Трисемуса, шифра Playfair, системы омофонов, шифра Виженера, сложение по «модулю 2».

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

Задание: Составить шифрограмму, используя шифр Цезаря, лозунгового шифра, полибианского квадрата, системы Трисемуса – проанализировать уровень сложности и устойчивости использованных шифров.

Вопросы для проведения опроса:

1. Предмет криптографии. Определения. Задачи. Исторические примеры.
2. Виды атак на криптографические алгоритмы. Понятие стойкости.
3. Классификация алгоритмов шифрования. Примеры простейших шифров.
4. Шифры замены. Математическая модель. Примеры.
5. Шифры перестановки. Математическая модель. Примеры.
6. Шифры гаммирования. Математическая модель. Примеры.
7. Принципы построения блочных шифров. Схема Фейстеля.
8. Алгоритм симметричного шифрования DES.
9. Алгоритм симметричного шифрования ГОСТ 28147-99.
10. Алгоритм симметричного шифрования Rijndael.
11. Алгоритмы симметричного шифрования IDEA и Blowfish.

Примерные темы для докладов:

1. Режимы выполнения алгоритмов симметричного шифрования.
2. Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
3. Линейные конгруэнтные генераторы. Линейные регистры сдвига.
4. Поточные шифры. Отличия от блочных. Стойкость. Методы анализа.
5. Примеры поточных шифров на основе LFSR.
6. Примеры поточных шифров, использующих аддитивные генераторы.
7. Примеры поточных шифров на основе FCSR.
8. Математические методы криптоанализа: метод опробывания, методы на основе теории статистических решений.
9. Линейный криптоанализ.
10. Разностный криптоанализ.
11. Основные принципы построения асимметричных криптосистем. Стойкость.
12. Шифросистема RSA. Стойкость.
13. Шифросистема Эль-Гамаля. Стойкость.
14. Шифросистема на основе принципа «рюкзака».
15. Шифросистема Рабина. Стойкость.
16. Алгоритм обмена ключами Диффи-Хеллмана.

17. Хэш-функции. Требования. Типы функций хэширования.
18. Атаки на функции хэширования.
19. Функция хеширования MD5.
20. Функция хеширования SHA-1.
21. Функция хеширования ГОСТ 3411-94.
22. Функция хеширования СТБ 1176.1-99.
23. Общие положения электронной цифровой подписи. Задачи. Требования.
24. Прямая и арбитражная цифровая подписи. Примеры.
25. Стандарт электронной цифровой подписи DSS.
26. Цифровая подпись на основе алгоритмов с открытыми ключами. Схема Фиата-Шамира.
27. Цифровая подпись Эль-Гамаля. Схема RSA.
28. Стандарт электронной цифровой подписи DSS.
29. Стандарт электронной цифровой подписи ГОСТ-Р 34.10-94.
30. Стандарт электронной цифровой подписи СТБ 1176.2-99.
31. Применение эллиптических кривых в криптографии. Алгоритм шифрования на основе эллиптических кривых.
32. Алгоритмы обмена ключами и электронной цифровой подписи на основе эллиптических кривых.
33. Стеганографические методы защиты информации. Основные понятия и определения. Области применения.
34. Общая модель стеганосистемы. Проблема устойчивости. Стегоанализ.
35. Методы сокрытия информации в неподвижных изображениях.
36. Методы сокрытия информации в текстовых данных.
37. Протоколы аутентификации. Двусторонняя аутентификация.
38. Протоколы аутентификации. Односторонняя аутентификация.

Тема №7 «Электронная подпись»

Цель: ознакомление с принципами защищенного электронного документооборота в вычислительных сетях и алгоритмами постановки электронной подписи.

Задание: на сайте ФНС России оформить электронную цифровую подпись, скриншот с отображённым результатом (запись на сайте о том, что ЭП сформирована и отправлена) предоставить на проверку.

Вопросы для проведения опроса:

1. С 1 марта 2022 года «заработал» новый порядок выдачи ЭЦП, МЧД и классификатор полномочий, особенности практического использования электронной подписи в современных условиях.
2. Что такое квалифицированная электронная подпись?
3. Для чего электронная подпись бизнесу и где она применяется?
4. Кто и где может получить электронную подпись?
5. Как получить электронную подпись в отделении банка?
6. Можно ли получить квалифицированную электронную подпись дистанционно?
7. Что делать, когда квалифицированная электронная подпись не работает?
8. Правила работы с электронной подписью.

Тема №8 «Нормативно-правовые основы информационной безопасности РФ, правовые основы обеспечения информационной безопасности экономической деятельности»

Цель: ознакомиться с нормативно-правовыми основами информационной безопасности в РФ, нормативными документами и ответственностью за нарушения информационной безопасности.

Задание: подготовить доклад, по теме занятия, в тексте доклада должно быть изложение современных тенденций развития информационной безопасности на основе анализа нормативно-правовых основ информационной безопасности в РФ, нормативных документов и норм закона, регулирующих ответственность за нарушения информационной безопасности.

Примерные темы для докладов:

1. Работы М. Кастельса о факторах развития информационной экономики.
2. Информационные факторы общественного развития в трудах Д.Белла.
3. Теория информационной экономики Дж. Стиглица.
4. Информационное обществе и экономика Ю.Хаяши.
5. Цифровая экономика и сопутствующие угрозы информационного характера.

Вопросы для проведения опроса:

1. Назовите основные признаки информациональной экономики. Выделите общие и особенные факторы развития мировой экономики и глобальной экономики. Как влияют информационные технологии на формирование вызовов и угроз развитию глобальной экономики?
2. Какие идеи и положения теории информационной экономики Дж. Стиглица актуальны для обеспечения информационной безопасности российской экономики?
3. Обоснуйте условия и возможности решения задач информационной экономики: - создание субъектами предпринимательства специальных алгоритмов хозяйствования, которые направлены на получение хозяйственной энергии из внешней среды и трансформацию ее в виде создания рабочих мест и работ; - выбор направления в развитии хозяйства в рамках происходящих глобальных процессов, которое определяется способностью хозяйственной энергии общества осуществлять движение к новым внешним ресурсам и более качественным трансформациям своей структуры - снятие административных, правовых, других барьеров, которые мешают бизнесу выходить как на существующие, так и на формирующиеся высокотехнологичные рынки для эффективного развития информационной экономики

Тема №9 «Стандарты информационной безопасности. Политика информационной безопасности предприятия»

Цель: ознакомиться со стандартами в области информационной безопасности (государственными стандартами Российской Федерации, международными и промышленными стандартами).

Задание: Используя современное законодательство в сфере стандартов информационной безопасности для предприятий, для условного предприятия разработать локальный стандарт информационной безопасности; выбрать нормативно-техническую базу ИБ, разработать основные положения системы управления ИБ, указать требования к комплексу мер и средств обеспечения ИБ, порядок согласования и утверждения стандарта информационной безопасности для условного предприятия (тип предприятия определить самостоятельно).

Вопросы для проведения опроса:

1) В чем заключается управление системой обеспечения информационной безопасности.
2) Дайте определение информационным рискам.
3) Перечислите принципы политики управления информационными рисками.
4) Опишите циклическую модель управления Дёминга.
5) Роль и место службы информационной безопасности в организации

Примерные темы докладов

1) Взаимосвязь свободы слова и права на свободный доступ к информации.
2) Доктрина информационной безопасности РФ.

3) Доктрина информационной безопасности РФ и проблемы совершенствования информационного законодательства Российской Федерации.

4) Политико-правовой анализ проблемных ситуаций в сфере защиты информационных ресурсов, средств массовых коммуникаций, блогосферы на основе знания основных положений Конституции РФ, Доктрины информационной безопасности Российской Федерации (2016 г.), законодательства о средствах массовой информации и правового регулирования Интернета.

Типовые темы для написания контрольной работы.

1) Цели и задачи создания «электронного государства», методы защиты информации в электронных государственных базах данных.

2) От «электронного государства» - к «электронному гражданину».

3) Состояние и перспективы формирования и развития государственных информационных ресурсов в контуре информационной защиты.

4) Противодействие угрозам развития отечественной индустрии информации.

5) Противодействие угрозам безопасности информационных и телекоммуникационных средств и систем.

6) Современные программные методы защиты информации.

7) Современные аппаратные методы защиты информации.

8) Отечественный Интернет (проект «Сфера»), как современная парадигма информационной защиты нации.

9) Государственные структуры, регулирующие безопасность информационных ресурсов в России: их цели и задачи.

10) Роль судебной системы в информационной защите населения.

11) Механизмы регулирования блогосферы в контексте информационной защиты населения.

12) Цели и задачи службы информационной безопасности в государственных организациях.

13) Цели и задачи службы информационной безопасности в коммерческих организациях.

14) Цели и задачи информационной безопасности в «Цифровой экономике».

15) «Индустрия 4.0» - тенденции защиты информации в цифровом сопровождении производства.

16) Злоупотребления в реализации права «свободы информации»: современные тенденции и пути противодействия угрозам злоупотреблений в информационном поле.

17) Правовое регулирование информациональной экономики: основные направления.

18) Аппаратные уязвимости и дефекты информационной защиты в коммерческих организациях.

19) Программные уязвимости и дефекты информационной защиты в коммерческих организациях.

20) Сертификаты и протоколы в сети Интернет: потенциальные угрозы информационной защиты при передачи данных по глобальным сетям.

Контрольная работа предусмотрена по темам 3.1. Криптографические методы защиты информации. Контрольная работа выполняется в электронном виде (письменно) в виде реферативного изложения ответов на поставленные вопросы, решения вычислительных задач и проведения компьютерного анализа по заданной теме.

Контрольная работа оценивается аналогично выполнению практических заданий – по количеству, полноте и правильности выполненных задач.

Критерии оценивания результатов успеваемости при осуществлении текущего

контроля

При проведении занятий лекционного типа:

Устный опрос - собеседование по теоретическим вопросам. Опрос производится при сдаче обучающимся отчета о практической работе и имеет целью выявление уровня теоретических знаний. При точных и уверенных ответах обучающимся выставляются дополнительные рейтинговые баллы, но не более, чем суммарно предусмотрено по блоку тем с учетом максимальной возможной рейтинговой оценки за лабораторные работы.

Устный опрос

Опрос проводится по темам 2, 3, 6 для оной формы обучения.

Опрос по теме 2, проводится по основным понятиям: тенденции валютного контроля трансграничных операций в свете глобальных изменений в финансовом регулировании и цифровизации экономики

Опрос по теме 3, проводится по основным понятиям: формирование общих технологических платформ для реализации цифровых финансовых технологий (автоматизированные системы в ритейле: ЕГАИС, ГИС Меркурий, он-лайн кассовые аппараты).

Опрос по теме 6 проводится по основным возможностям портала федеральной налоговой службы в направлении развития цифровых технологий.

Опрос оценивается по четырех-балльной шкале по следующим критериям:

- 2 балла – обучающийся полно и правильно отвечает на теоретические вопросы, грамотно применяет модель или алгоритм ее построения, верно дает интерпретацию результатов.

- 1,5 балла – обучающийся полно и правильно отвечает на теоретические вопросы, грамотно применяет модель или алгоритм ее построения, верно дает интерпретацию результатов, но допускает неточности в интерпретации результатов.

- 1 балл - обучающийся обнаруживает теоретические знания, но практическое применение вызывает затруднения

- 0 баллов - обучающийся отказывается отвечать по причине неподготовленности или при ответе обнаруживает незнание теоретического материала, неумение практического применения моделей или алгоритмов их построения и интерпретации результатов. Максимальное число баллов, которые можно набрать за ответы на вопросы устного опроса 4 балла.

При контроле результатов самостоятельной работы обучающихся:

Текущий контроль усвоения знаний предусмотрен по каждой теме, по итогам обучения проводится методом контрольных мероприятий по успеваемости.

Входной контроль. Основной целью входного контроля является проверка общего уровня знаний и умений обучающихся, необходимых для освоения программы учебного курса. Результаты входного контроля знаний обучающихся измеряются в % правильно выполненных заданий от общего объема и служат для диагностики готовности обучающихся к освоению курса. Входной контроль проводится на первом практическом занятии в виде письменной самостоятельной работы. *Входной контроль* в рейтинговой оценке не учитывается.

При проведении практических занятий:

Отчет по практическому занятию выполняется студеном в письменном виде на основе выполненных заданий практической работы. Преподаватель проводит собеседование со обучающимся и выставляет оценку по результатам письменного отчета и собеседования.

Отчет по практическому занятию

Отчеты о выполнении практических занятий– это результаты выполнения заданий семинарских (практических) занятий, оформленные в соответствии с предъявляемыми требованиями. Цель отчета – предъявление результатов выполненной работы, а также рефлексивные выводы по итогам деятельности. Отчет о выполнении практической работы выполняется студеном в письменном виде на основе выполненных заданий практической работы. Преподаватель проводит собеседование с обучающимся и выставляет оценку по результатам письменного отчета и собеседования. Отчеты по практическим работам предоставляются по всем темам курса, за исключением тем 1, 2, 8. Выполнение отчета оценивается по следующей шкале: менее 50% от выполнения заданий практической работы - 0 баллов (оценка

«неудовлетворительно»), 50% - 65% от выполнения заданий практической работы - 1 балл (оценка «удовлетворительно»), 66%-80% от выполнения заданий практической работы - 1,5 балла (оценка «хорошо»), 80% и более от выполнения заданий практической работы – 2 балла (оценка «отлично»).Суммарно по всем практическим работам можно набрать максимальные 36 баллов.

Интерактивные формы занятий

Занятия в интерактивной форме проводятся по всем темам курса, ввиду проведения, предусмотренных по темам, практическим работам. Лабораторные работы проводятся в мини-группах. Собеседование по отчетам к практическим работам, также имеют интерактивную форму в мини-группах.

Самостоятельная работа

Отчеты о выполнении самостоятельных работ – это результаты выполнения заданий по самостоятельному исследованию, оформленные в соответствии с предъявляемыми требованиями в виде эссе, научных статей или рефератов. Цель отчета о выполнении самостоятельной работы – предъявление результатов выполненной работы, а также рефлексивные выводы по итогам деятельности. Отчет о выполнении самостоятельной исследовательской работы выполняется студеном в письменном виде на основе ранее выполненных заданий практической работы. Преподаватель проводит собеседование со обучающимся и выставляет оценку по результатам письменного отчета и собеседования. Отчеты по самостоятельным исследовательским работам предоставляются по всем темам курса, за исключением тем 1, 2, 8. Выполнение отчета оценивается по следующей шкале: менее 50% от выполнения заданий практической работы - 0 баллов, 50% - 65% от выполнения заданий практической работы - 1 балл, 66%-80% от выполнения заданий практической работы - 1,5 балла, 80% и более от выполнения заданий практической работы – 2 балла. Суммарно по всем практическим работам можно набрать максимальные 36 баллов.

5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Зачет проводится с применением следующих методов (средств):

Зачет с оценкой проводится в формате: устно. С применением билетов с 2-мя теоретическими вопросами; посредством тестирования: Банк заданий – 100 тестов, выборка – 20 вопросов, время тестирования – 60 минут, 2 попытки.

5.2. Оценочные материалы промежуточной аттестации

Компонент компетенции	Ключевой индикатор оценивания	Критерий оценивания
УК ОС -8.1 Оценивает эффективность основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении	Осуществляет профилактику, пресечение, выявление, раскрытие и расследование преступлений и иных правонарушений, связанных с информационной безопасностью.	**Знает** теоретические приемы работы с правовыми системами для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов. **Умеет** осуществлять успешную работу с правовыми системами; получать юридически значимую информацию. **Владеет** навыками эффективной оценки основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

Компонент компетенции	Ключевой индикатор оценивания	Критерий оценивания
чрезвычайных ситуаций и военных конфликтов		
УК ОС -8.2 Демонстрирует знание основных алгоритмов поведения в целях предотвращения угроз безопасности жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов		**Знает** методы целенаправленного и эффективного предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов. **Умеет** решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности. **Владеет** навыками предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

Типовые оценочные материалы промежуточной аттестации

Зачет с оценкой проводится в письменной форме с применением тестовых заданий (20 тестовых заданий).

Типовые вопросы к зачёту

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

Типовые задачи к зачёту

Задание 1. С позиции руководителя кредитно-финансовой организации. Продумайте программу обеспечения информационной защиты информационных ресурсов организации по направлениям: 1) определение степени зрелости (ответственности организации), наличие и качество политики обеспечения ее информационной безопасности; 2) обнаружение слабо защищенных мест в экономической системе и квалификация их как угрозы экономической безопасности; 3) оценка рисков – неприемлемого значительного, приемлемого значительно, незначительного; 4) разработка программы защиты информационных ресурсов организации.

Задание 2. С позиции руководителя государственного (муниципального) учреждения (например, поликлиника или школа): продумайте программу обеспечения информационной защиты информационных ресурсов организации по направлениям: 1) определение степени зрелости (ответственности организации), наличие и качество политики обеспечения ее информационной безопасности; 2) обнаружение слабо защищенных мест в системе управления и защиты персональных данных участников системы; 3) оценка рисков – неприемлемого значительного, приемлемого значительно, незначительного; 4) разработка программы защиты информационных ресурсов организации.

Задание 3. С позиции руководителя коммерческой организации ан уровне малого бизнеса или предпринимательства, продумайте программу обеспечения информационной защиты информационных ресурсов организации по направлениям: 1) определение степени зрелости (ответственности организации), наличие и качество политики обеспечения ее информационной безопасности; 2) обнаружение слабо защищенных мест в структуре обмена данными организации с другими участника рынка; 3) оценка рисков – неприемлемого значительного, приемлемого значительно, незначительного; 4) разработка программы защиты информационных ресурсов организации.

Шкала оценивания.

Критерий оценивания	Оценка
Знает теоретические приемы работы с правовыми системами; методы целенаправленного и эффективного предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов; способы получения юридически значимой информации из различных источников; приказы, указания и иные организационно-распорядительные документы Генерального прокурора Российской Федерации и его заместителей, регламентирующие функциональную, а также предметную деятельность прокурорского работника. **Умеет** получать юридически значимую информацию из различных источников, включая правовые базы (банки) данных, решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; успешно применять организационно-распорядительные документы, регулирующие вопросы организации и деятельности прокуратуры в целом и по отдельным направлениям, исполнения требований законов и иных нормативных правовых актов, прохождения службы, распределения обязанностей, порядка работы, реализации мер материального и социального характера и др. **Владеет** навыками получения информации, решения задач профессиональной деятельности; применения организационно-распорядительных документов Генеральной прокуратуры Российской Федерации, регламентирующих функциональную, а также предметную деятельность прокурорского работника на высоком уровне.	Зачтено
Не знает или имеет очень слабое представление о теоретических приемах работы с правовыми системами; методах целенаправленного и эффективного предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов; не знает способы получения юридически значимой информации из различных источников; приказы, указания и иные организационно-распорядительные документы Генерального прокурора Российской Федерации и его заместителей, регламентирующие функциональную, а также предметную деятельность прокурорского работника. **Не умеет** или демонстрирует очень слабое умение применять правовые средства выявления, предупреждения, пресечения угроз безопасности личности, общества и государства, формулировать выводы о характере угроз и использовать соответствующие рекомендации с учетом основных требований информационной безопасности. Не умеет получать юридически значимую информацию из различных источников, включая правовые базы (банки) данных, решать задачи профессиональной деятельности на основе	Не зачтено

информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; успешно применять организационно-распорядительные документы, регулирующие вопросы организации и деятельности прокуратуры в целом и по отдельным направлениям, исполнения требований законов и иных нормативных правовых актов, прохождения службы, распределения обязанностей, порядка работы, реализации мер материального и социального характера и др. **Не владеет** или демонстрирует очень слабые навыки предотвращения угроз безопасности жизнедеятельности для обеспечения устойчивого развития общества, в том числе с учетом основных требований информационной безопасности при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов; навыками предупреждения, пресечения основных угрозы безопасности личности, общества и государства, с учетом основных требований информационной безопасности	

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

Наименование отметки	Сумма баллов (процентов)
«зачтено»	61-100
«не зачтено»	0 - 60

6. Методические материалы по освоению дисциплины

6.1 Методические указания для обучающихся по освоению материала занятий лекционного типа

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. Обучающиеся должны аккуратно вести конспект. В случае недопонимания какой-либо части предмета следует в установленном порядке задать вопрос преподавателю. В процессе работы на лекции необходимо также выполнять в конспектах модели изучаемого предмета (рисунки, схемы, чертежи и т.д.), которые использует преподаватель.

6.2 Методические указания для обучающихся по освоению материала занятий семинарского типа

Практические 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 консультации или на занятии.

6.3 Методические указания для обучающихся по подготовке к тестированию

При подготовке к тестированию необходимо внимательно изучить содержание тем дисциплины, которые выносятся на проверку.

Как и любая другая форма подготовки к контролю знаний, тестирование имеет ряд особенностей, знание которых помогает успешно выполнить тест. Можно дать следующие методические рекомендации:

– прежде всего, следует внимательно изучить структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, какого типа задания в нем содержатся;

– лучше начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока, не останавливаясь на тех, которые могут вызвать долгие раздумья. Это позволит успокоиться и сосредоточиться на выполнении более трудных вопросов;

– очень важно всегда внимательно читать задания до конца, не пытаясь понять условия «по первым словам» или выполнив подобные задания в предыдущих тестированиях. Такая спешка нередко приводит к досадным ошибкам в самых легких вопросах;

– если не знаете ответа на вопрос или не уверены в правильности, следует пропустить его и отметить, чтобы потом к нему вернуться.

Рассчитывать выполнение заданий нужно всегда так, чтобы осталось время на проверку и доработку (примерно 1/3-1/4 запланированного времени). Тогда вероятность описок сводится к нулю и имеется время, чтобы набрать максимум баллов на легких заданиях и сосредоточиться на решении более трудных, которые вначале пришлось пропустить.

6.4. Методические указания для обучающихся по подготовке к опросу

Опросы по темам проводятся в части проверки и уяснения основных правовых понятий и категорий. При подготовке к опросу, обучающийся должен изучить вопросы для самостоятельной подготовки к практическим занятиям, составить краткий конспект ответа на каждый из представленных вопросов.

6.5. Методические указания для обучающихся по самостоятельной работе

Самостоятельная работа обучающемуся является важным элементом изучения дисциплины Страховое право. Усвоение материала дисциплины на семинарах 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 являются глубокими и качественными, и позволяют формировать соответствующие компетенции как итог образовательного процесса.

Для систематизации знаний по дисциплине первоначальное внимание обучающемуся следует обратить на рабочую программу курса, которая включает в себя разделы и основные проблемы дисциплины, в рамках которых и формируются вопросы для контроля и аттестации. Поэтому обучающейся, 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 5 настоящей рабочей программы), в которой указаны количество академических часов в разрезе каждой темы, вида занятий (практическое) и часы на самостоятельную работу; Б) формой текущего контроля успеваемости (эссе, коллоквиум, выполнение индивидуальных занятий и др.); 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; авторефераты к диссертациям на соискание ученой степени; 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 сессионных занятий или на консультации с преподавателем).

3. Использование учебно-методических материалов и работу с литературой. Следует применять следующую последовательность источников для изучения тем дисциплины: А) нормативные правовые акты; Б) комментарии к законодательным актам; В) научная и учебная литература; Г) другие.

4. Подготовку к текущему контролю успеваемости и выполнению домашних индивидуальных заданий. При выполнении индивидуальных заданий, следует руководствоваться методическими рекомендациями, представленными по каждому виду индивидуальных заданий в указанном разделе. При подготовке к вопросам и заданиям контролируемой самостоятельной работы ответы необходимо изложить в письменной форме и представить на проверку, при этом ответы должны быть по существу вопроса, конструктивны, лаконичны и не должны иметь реферативного изложения.

6.6. Методические указания для обучающихся по подготовке к решению кейсов

При решении задачи необходимо дать правильную юридическую квалификацию рассматриваемых в условиях задачи фактов и отношений.

Решение задачи обязательно должно быть изложено в письменной форме в тетради для семинарских занятий по гражданскому праву и включать в себя:

- краткий анализ обстоятельств дела;
- выводы, обоснованные ссылками на конкретные правовые нормы с полным и грамотным указанием на все необходимые данные об использованных при решении задачи нормативно-правовых актах.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

7.1. Основная литература.

1. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www-iprbookshop-ru.ezproxy.ranepa.ru:2443/120489.html. — Режим доступа: для авторизир. Пользователей

2. Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www-iprbookshop-ru.ezproxy.ranepa.ru:2443/118876.html. — Режим доступа: для авторизир. пользователей. - DOI: https://doi-org.ezproxy.ranepa.ru:2443/10.23682/118876

3. Формализация подхода к определению актуальности угроз информационной безопасности : монография / О. М. Голембиовская, М. Ю. Рытов, М. М. Голембиовский [и др.]. — Саратов : Вузовское образование, 2022. — 147 c. — ISBN 978-5-4487-0840-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www-iprbookshop-ru.ezproxy.ranepa.ru:2443/121143.html. — 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 c. — ISBN 978-89838-489-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/7002.html. — 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 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17710.html. — Режим доступа: для авторизир. Пользователей

3. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 c. — Режим доступа: http://www.iprbookshop.ru/52182.html.— ЭБС «IPRbooks»

4. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/33430.html. — Режим доступа: для авторизир. Пользователей

5. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные. — М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

6. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Г. П. Жигулин. — СПб. : Университет ИТМО, 2014. — 174 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/67451.html. — Режим доступа: для авторизир. пользователей

7. 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), 2014. — 78 c. — ISBN 978-5-89172-850-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/47262.html. — Режим доступа: для авторизир. Пользователей

8. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 c.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks»

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

10. 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. — Режим доступа: для авторизир. Пользователей

11. 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. — Режим доступа: для авторизир. пользователей

12. 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. — Режим доступа: для авторизир. пользователей

13. 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. — Режим доступа: для авторизир. пользователей

14. Крылов Г.О. Понятийный аппарат информационной безопасности [Электронный ресурс]: словарь/ Крылов Г.О., Ларионова С.Л., Никитина В.Л.— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 343 c.— Режим доступа: http://www.iprbookshop.ru/64306.html.— ЭБС «IPRbooks»

15. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-методический комплекс/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 342 c.— Режим доступа: http://www.iprbookshop.ru/14642.html.— ЭБС «IPRbooks»

16. 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. — Режим доступа: для авторизир. Пользователей

17. 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. — Режим доступа: для авторизир. Пользователей

7.3 Нормативные правовые документы

1. ФГОС ВО 40.05.01 Правовое обеспечение национальной безопасности (https://rg.ru/documents/2020/09/16/minnauki-prikaz1138-site-dok.html)

2. "Общероссийский классификатор управленческой документации" ОК 011-93 (утв. Постановлением Госстандарта РФ от 30.12.1993 № 299) (ред. от 04.09.2007) // Справ.-правовая система «Консультант Плюс».

3. Доктрина информационной безопасности Российской Федерации, утвержденная

Указом Президента Российской Федерации от 5 декабря 2016 г. № 646;

4. Доктрина продовольственной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 21 января 2020 г. № 20;

5. Стратегия экономической безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 13 мая 2017 г. № 208;

6. Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02 июля 2021 г. № 400;

7. Постановление Правительства Российской Федерации № 608 от 26.06.95 "О сертификации средств защиты информации";

8. Указ Президента Российской Федерации № 188 от 06.03.97 "Об утверждении перечня сведений конфиденциального характера";

9. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // Справ.-правовая система «Консультант Плюс».

10. Федеральный закон от 29.12.94 № 77-ФЗ "Об обязательном экземпляре документов" // Справ.-правовая система «Консультант Плюс».

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.
6. Научная библиотека Дальневосточного института управления. - Режим доступа: http://biblio.dvags.ru/MarcWeb/ , свободный.
7. Электронная библиотека РАНХ и ГС .- Режим доступа: http://lib.ranepa.ru/ , свободный.
8. ЭБС «Лань» . – Режим доступа: http://e.lanbook.com/, свободный.
9. ЭБС «Электронная библиотека онлайн». –Режим доступа: http://biblioclub.ru/, по паролю.
10. ЭБС «Юрайт» . – Режим доступа: http://www.urait.ru/, по паролю.
11. Научная электронная библиотека eLIBRARY –Режим доступа: http://elibrary.ru/, по паролю.
12. Дальневосточная государственная научная библиотека - Режим доступа: www.fessl.ru, свободный.
13.

7.5 Иные источники

1. Карпов В.А., Оборнев Е.А. Основы проектирования баз данных для информационных систем. Практикум в упражнениях и задачах// Экон-информ, 2011. - 108с.–ISBN ISBN 978-5-9506-0787-5

2. Карпов В. А. Базы данных. Зачем, почему, как?//г.Москва, Издательство МУМ, 2003. - 25с.

3. Кригель, Алекс, Трухнов, Борис. К82 SQL. Библия пользователя, 2-е издание. : Пер. с англ. — М. : ООО “И.Д. Вильямс”, 2010. — 752 с.

4. Вьюгин, В. В. Математические основы машинного обучения и прогнозирования: Учебное пособие / Вьюгин В.В. - Москва :МЦНМО, 2014. - 304 с.: ISBN 978-5-4439-2014-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/958689

5. Рашка, С. Python и машинное обучение: крайне необходимое пособие по новейшей предсказательной аналитике, обязательное для более глубокого понимания методологии машинного обучения / С. Рашка ; пер. с англ. А.В. Логунова. - Москва : ДМК Пресс, 2017. - 418 с. - ISBN 978-5-97060-409-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1027758

6. Статистические сборники.

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 промежуточной аттестации	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.
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	Учебный зал судебных заседаний	Специализированная мебель для организации рабочих мест обучающихся и преподавателя, технические средства обучения, мультимедийное оборудование, доска маркерная, атрибуты, отражающие судебную символику (судебная мантия, герб и флаг Российской Федерации), молоток судьи, клетка для подсудимого, 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	Криминалистический полигон	Оборудован специальными средствами и другими материально-техническими средствами для осуществления специальной подготовки обучающихся, манекен человека. Укомплектован переносным мультимедийным оборудованием, 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	Помещение для студенческой правовой консультации (юридическая клиника)	Помещение укомплектовано специализированной мебелью и переносным мультимедийным оборудованием, доступ к сети «Интернет» и электронной информационно-образовательной среде.
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.
680000, Хабаровский край, г. Хабаровск, ул. Муравьева-Амурского, д. 33	Спортивный зал	Спортивный инвентарь