МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.В	**Организационно-правовое обеспечение информационной безопасности образовательной организации**

Код направления подготовки	44.04.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Управление информационной безопасностью в профессиональном образовании
Уровень образования	магистр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Старший преподаватель	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	10	13.06.2019	
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	1	13.09.2020	

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Организационно-правовое обеспечение информационной безопасности образовательной организации» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.04.04 «Профессиональное обучение (по отраслям)» (уровень образования магистр). Дисциплина является дисциплиной по выбору.

1.2 Общая трудоемкость дисциплины составляет 4 з.е., 144 час.

1.3 Изучение дисциплины «Организационно-правовое обеспечение информационной безопасности образовательной организации» основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин образовательной программы бакалавриата или специалитета.

1.4 Дисциплина «Организационно-правовое обеспечение информационной безопасности образовательной организации» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «выполнение и защита выпускной квалификационной работы», «Охрана труда в организациях профессионального образования», «Методология научного исследования», «Программно-аппаратное обеспечение информационной безопасности», для проведения следующих практик: «производственная практика (научно-исследовательская работа)».

1.5 Цель изучения дисциплины:

сформировать компетенции, необходимые для профессиональной деятельности, предусмотренной стандартами магистратуры и направлением обучения.

1.6 Задачи дисциплины:

1) формировать представления о содержании основных нормативных правовых актов в области обеспечения информационной безопасности и нормативных методических документов ФСБ России и ФСТЭК России в области защиты информации;

2) формировать знания, умения и навыки организации работы и нормативных правовых актов и стандартов по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

3) формировать представления об основах организационного и правового обеспечения информационной безопасности;

1.7 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы:

№ п/п	Код и наименование компетенции по ФГОС
	Код и наименование индикатора достижения компетенции
1	ПК-16 способен применять инженерно-технические и программно-аппаратные средства обеспечения информационной безопасности
	ПК.16.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП
	ПК.16.2 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП
	ПК.16.3 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, сов-ременного профессионального образования, ДПО и ДПП
2	УК-5 способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
	УК.5.1 Знает особенности непосредственной и опосредованной коммуникации с представителями различных культур и социальных групп (субкультур); основы обеспечения различных типов коммуникации с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации; правила межкультурной коммуникации
	УК.5.2 Умеет грамотно, доступно излагать профессиональную информацию в процессе межкультурного взаимодействия; соблюдать этические нормы и права человека; анализировать особенности социального взаимодействия с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации; выявлять барьеры в межкультурном взаимодействии, находить способы их преодоления или устранения

	УК.5.3 Владеет навыками подготовки и преобразования информации, выбора форм и средств ее представления для обеспечения взаимопонимания в процессе межкультурного взаимодействия; навыками активного слушания, наблюдения и интерпретации поведения представителей разных культур и социальных групп; навыками выбора адекватной коммуникативной стратегии в зависимости от культурного контекста коммуникации и поставленных целей

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.16.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП	З.1 основные принципы и подходы при организации защиты ифнормации
2	ПК.16.2 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, современного профессионального образования, ДПО и ДПП	У.1 ппримен‍ять основыне нормативно-правоые акты в области ИБ
3	ПК.16.3 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности в практике ВО, сов-ременного профессионального образования, ДПО и ДПП	В.1 владеет опытом применения нормативно-правовых актов в области ИБ
1	УК.5.1 Знает особенности непосредственной и опосредованной коммуникации с представителями различных культур и социальных групп (субкультур); основы обеспечения различных типов коммуникации с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации; правила межкультурной коммуникации	З.2 инженерно-технические и программно-аппаратные средства обеспечение ИБ
2	УК.5.2 Умеет грамотно, доступно излагать профессиональную информацию в процессе межкультурного взаимодействия; соблюдать этические нормы и права человека; анализировать особенности социального взаимодействия с учетом личностных, национально-этнических, конфессиональных и иных особенностей участников коммуникации; выявлять барьеры в межкультурном взаимодействии, находить способы их преодоления или устранения	У.2 умение аргуменртировать свою позицию по организации защиты информации

3	УК.5.3 Владеет навыками подготовки и преобразования информации, выбора форм и средств ее представления для обеспечения взаимопонимания в процессе межкультурного взаимодействия; навыками активного слушания, наблюдения и интерпретации поведения представителей разных культур и социальных групп; навыками выбора адекватной коммуникативной стратегии в зависимости от культурного контекста коммуникации и поставленных целей	В.2 опыт подготовки обзора и анализа нормативно-правоых документво в области ИБ

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Итого часов
	Л	ПЗ	СРС	
Итого по дисциплине	**6**	**18**	**84**	**108**
Первый период контроля				
Информационная безопасность и ее обеспечение	***4***	***6***	***24***	***34***
Информационная безопасность и ее обеспечение	2	2	8	12
Система обеспечения информационной безопасности РФ	2	2	8	12
Основные законодательные акты РФ в области обеспечения информационной безопасности		2	8	10
Правовое обеспечение информационной безопасности		***4***	***16***	***20***
Законодательство об информации, информационных технологиях и о защите информации».		2	8	10
Правовой режим информационных технологий.		2	8	10
Организационное обеспечение информационной безопасности.		***2***	***16***	***18***
СПС Консультант		2	8	10
СПС Гарант			8	8
Итого по видам учебной работы	4	12	56	72
Форма промежуточной аттестации				
Зачет				
Итого за Первый период контроля				**72**
Второй период контроля				
Концепция информационной безопасности организации профессионального образования		***4***	***12***	***16***
«Концепция информационной безопасности организации профессионального образования. Описание текущего состояния информационной защиты»		2	4	6
«Концепция информационной безопасности организации профессионального образования. Необходимые текущие меры для усиления информационной защиты, направления для перспективного усиления состояния защищенности»		2	8	10
Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе	***2***	***2***	***16***	***20***
«Разработка политики безопасности организации профессионального образования»	2		8	10
Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе		2	8	10
Итого по видам учебной работы	2	6	28	36
Форма промежуточной аттестации				
Экзамен				36
Итого за Второй период контроля				**72**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Информационная безопасность и ее обеспечение	***4***
Формируемые компетенции, образовательные результаты: ПК-16: З.1 (ПК.16.1), У.1 (ПК.16.2)	
1.1. Информационная безопасность и ее обеспечение 1. Информационное общество и его безопасность. 2. Информационное общество — новый этап развития человечества. 3. Безопасность в информационном обществе. 4. Информация — фактор существования и развития общества. 5. Информация как явление жизни. 6.Информационная инфраструктура. 7. Обеспечение информационной безопасности: содержание и структура понятия. Учебно-методическая литература: 1, 2, 3	2
1.2. Система обеспечения информационной безопасности РФ 1. Обеспечение информационной безопасности организации. 2. Обеспечение информационной безопасности Российской Федерации. Учебно-методическая литература: 1, 2, 4	2
2. Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе	***2***
Формируемые компетенции, образовательные результаты: УК-5: В.2 (УК.5.3)	
2.1. «Разработка политики безопасности организации профессионального образования» 1. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти. 2. Организационные структуры системы обеспечения информационной безопасности предприятия (организации). 3. Физическая защита. Учебно-методическая литература: 2, 3 Профессиональные базы данных и информационные справочные системы: 1	2

3.2 Практические

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Информационная безопасность и ее обеспечение	***6***
Формируемые компетенции, образовательные результаты: ПК-16: З.1 (ПК.16.1), У.1 (ПК.16.2)	
1.1. Информационная безопасность и ее обеспечение 1. Информационное общество и его безопасность. 2. Информационное общество — новый этап развития человечества. 3. Безопасность в информационном обществе. 4. Информация — фактор существования и развития общества. 5. Информация как явление жизни. 6.Информационная инфраструктура. 7. Обеспечение информационной безопасности: содержание и структура понятия. Учебно-методическая литература: 3, 4 Профессиональные базы данных и информационные справочные системы: 2	2

1.2.	Система обеспечения информационной безопасности РФ «Система обеспечения информационной безопасности РФ». 1. Обеспечение информационной безопасности организации. 2. Обеспечение информационной безопасности Российской Федерации. Учебно-методическая литература: 2, 3, 4 Профессиональные базы данных и информационные справочные системы: 2	2

1.3.	Основные законодательные акты РФ в области обеспечения информационной безопасности	2

К актам информационного законодательства федерального уровня относится и ФЗ от 29.11.1994 № 77-ФЗ «Об обязательном экземпляре документов». Данный нормативный акт определяет политику государства в области формирования обязательного экземпляра документов как ресурсной базы комплектования библиотечно-информационного фонда РФ и развития системы государственной библиографии, предусматривает обеспечение сохранности обязательного экземпляра документов, его общественное использование. Этим законом установлены виды обязательного экземпляра документов в категории их производителей и получателей, сроки и порядок доставки обязательного экземпляра документов, ответственность за их нарушение.

Видное место среди законов, регулирующих отношения в информационной среде, занимает закон РФ от 27.12.1991 № 2124 – 1 «О средствах массовой информации», представляющий собой комплексный нормативный акт, регламентирующий отношения, возникающие в процессе организации и функционирования средств массовой информации (СМИ). В основных разделах закона нашли правовое опосредование вопросы организации деятельности СМИ, распространения массовой информации, отношений СМИ с гражданами и организациями, прав и обязанностей журналиста, межгосударственного сотрудничества в области массовой информации, ответственности за нарушение законодательства о СМИ.

Особое место среди нормативных актов, регулирующих отношения по поводу информации, принадлежит закону РФ от 21.07.1993 № 5485 – 1 «О государственной тайне».

Один из законов, регулирующих отношения в информационной сфере, – ФЗ от 07.07.2003 № 126-ФЗ «О связи». Он устанавливает правовую основу деятельности в области связи, осуществляемой под юрисдикцией РФ, определяет полномочия органов государственной власти по регулированию этой деятельности, а также права и обязанности физических лиц, осуществляющих деятельность в области связи.

К законам, регулирующим информационные отношения, также относится и ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи». Его цель – обеспечение правовых условий использование электронной подписи в электронных документах.

Отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников отношений, в том числе государства, на рынке товаров, работ и услуг, регулируются ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

К нормативным актам данной проблематики относятся федеральные законы:

– от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»;

– от 12.05.2009 № 95-ФЗ «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами»;

– от 27.07.2006 № 152-ФЗ «О персональных данных»;

– от 28.12.2010 № 390-ФЗ «О безопасности»;

– от 28.07.2012 № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты».

Помимо названных выше существует множество законов, непосредственно не направленных на регулирование информационных отношений, но содержащих отдельные статьи, посвященные информации или связанные с ней. К числу следует отнести следующие федеральные законы: от 13.03.2006 № 38 -ФЗ «О рекламе»; от 29.12.1994 № 78-ФЗ «О библиотечном деле»; от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»; от 17.07.1999 № 176-ФЗ «О почтовой связи»; от 17.08.1995 № 147-ФЗ «О естественных монополиях»; от 21.02.1992 № 2395-1 «О недрах».

Часть норм, касающихся информационных отношений, содержатся в Гражданском кодексе РФ (ГК РФ). Так, ст. 150 относит личную и семейную тайну к нематериальным благам, ст. 726 устанавливает обязанность подрядчика передать информацию

2. Правовое обеспечение информационной безопасности	***4***
Формируемые компетенции, образовательные результаты: ПК-16: В.1 (ПК.16.3)	
2.1. Законодательство об информации, информационных технологиях и о защите информации». «Законодательство об информации, информационных технологиях и о защите информации». 1.Правовой режим информации. 2.Правовой статус обладателя информации. 3.Правовой режим информационных технологий. 4.Защита информации. 5.Законодательство о персональных данных. 6.Защита прав и законных интересов субъектов информационной сферы Учебно-методическая литература: 3, 4 Профессиональные базы данных и информационные справочные системы: 1	2
2.2. Правовой режим информационных технологий. 1. Понятие информационных технологий 2. Понятие правового режима 3. Правовые режим ИТ Учебно-методическая литература: 2, 3 Профессиональные базы данных и информационные справочные системы: 1	2
3. Организационное обеспечение информационной безопасности.	***2***
Формируемые компетенции, образовательные результаты: УК-5: З.2 (УК.5.1)	

Практическая работа №1. Работа со справочно-информационной правовой системой "КонсультантПлюс"Цель работы: ознакомиться с функционалом справочно-поисковой системой, приобрести практические навыки работы с информационной правовой системой "КонсультантПлюс
Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, выполнение упражнений, частично-поисковый метод, самостоятельная работа.
Ключевые слова: справочно-поисковая система, реквизиты нормативных актов, карточка поиска, правовой навигатор, обзор законодательства.

Краткие теоретические сведения

Справочная правовая система (СПС) «КонсультантПлюс» включает все законодательство РФ: от основополагающих документов до узкоотраслевых актов. Стартовое окно некоммерческой интернет-версии СПС представлено на рисунке 1.

Рисунок 1. Стартовое окно СПС «КонсультантПлюс» некоммерческой интернет-версии
Некоммерческие интернет–версии СПС «КонсультантПлюс» содержат федеральное и региональное законодательство, судебную практику, финансовые консультации, комментарии законодательства, тематические обзоры.
Документы, тексты которых недоступны, можно найти в коммерческой версии системы, заказать из интернет–версии; за текстом можно обратиться в региональный информационный центр.
Для поиска необходимых документов, необходимо заполнить карточку поиска (рис.2).

Рисунок 2. Карточка поиска некоммерческой интернет-версии КонсультантПлюс

Карточка поиска – основное средство поиска документов в базе данных системы. Система ищет документы, одновременно удовлетворяющие всем заполненным полям карточки поиска. Заполнять все поисковые поля не обязательно, достаточно заполнить лишь несколько полей.
В системе «КонсультантПлюс» предусмотрена возможность уточнять полученные списки несколько раз по разным полям.
Работа со справочно-правовой системой «КонсультантПлюс» сводится к следующему алгоритму:
• составление запроса на поиск документа или группы документов и их поиск;
• применение процедур обработки: сортировки, фильтрации и др.;
• использование механизма гиперссылок, поиска и создания папок и закладок при работе с текстом документа;
• чтение, редактирование, печать, сохранение текста документа в файл или экспорт данных в текстовый редактор MSWord или табличный редактор MSExcel.
На рисунке 3 представлен пример диалогового окна для тематического поиска документов.

Рисунок 3. Окно поиска документа по правовому вопросу в системе «КонсультантПлюс»

Порядок выполнения работы.

1. Открыть сайт: http://www.consultant.ru, выбрать вкладку работа с некоммерческими интернет-версиями
2. Ознакомиться с краткими теоретическими сведениями
3. Ознакомиться со структурой и возможностями некоммерческой интернет-версией СПС «КонсультантПлюс»
4. Открыть в новой вкладке MSWord, начать оформление отчета по лабораторной работе: записать тему, цель.
5. Войти из стартового окна в режим «Обзоры законодательства», просмотреть информацию в разделе: Правовые новости/ Специальный выпуск, вернуться в Стартовое окно.
6. Открыть по ссылке «Новые документы» списки документов, включенных в систему за последний месяц. Сохранить скриншот списка в отчет по лабораторной работе
7. Перейти в раздел «Законодательство», знакомиться с общим построением справочно-информационной правовой системы «КонсультантПлюс»
8. Изучить поочередно все подпункты основного меню системы, зайти в карточку поиска, рассмотреть все её элементы.
9. Зайти в режим Правового навигатора, изучить особенности поиска информации по конкретному правовому вопросу; двухуровневую структуру словаря; ключевые понятия

4. Концепция информационной безопасности организации профессионального образования	***4***
Формируемые компетенции, образовательные результаты: УК-5: У.2 (УК.5.2)	

4.1.	«Концепция информационной безопасности организации профессионального образования. Описание текущего состояния информационной защиты» Учебный проект: разработка концепции безопасности конкретного учреждения по приведенному развернутому плану-шаблону. Концепция обеспечения информационной безопасности предприятия Содержание • Общие положения • Описание объекта защиты o Назначение и основные функции информационной системы o Группы задач, решаемых в информационной системе o Классификация пользователей системы o Организационная структура обслуживающего персонала o Структура и состав комплекса программно-технических средств o Корпоративная сеть предприятия ▯ Серверы ▯ Рабочие станции ▯ Линии связи и активное сетевое оборудование ▯ Виды информационных ресурсов, хранимых и обрабатываемых в системе ▯ Структура информационных потоков ▯ Внутренние информационные потоки ▯ Внешние информационные потоки ▯ Характеристика каналов взаимодействия с другими системами и точек входа • Основные факторы, влияющие на информационную безопасность предприятия • Основные принципы обеспечения информационной безопасности • Организация работ по защите информации • Меры обеспечения информационной безопасности o Меры обеспечения информационной безопасности организационного уровня o Меры обеспечения информационной безопасности процедурного уровня • Распределение ответственности и порядок взаимодействия • Порядок категорирования защищаемой информации • Модель нарушителя информационной безопасности o Внутренние нарушители o Внешние нарушители • Модель угроз информационной безопасности o Защита информационных компонентов и группы угроз o Угрозы, реализуемые с использованием технических средств o Угрозы, реализуемые с использованием программных средств o Угрозы утечки информации по техническим каналам связи • Требования по обеспечению информационной безопасности o Требования к составу основных подсистем СОИБ o Требования к подсистеме управления политикой безопасности o Требования к подсистеме анализа и управления рисками o Требования к подсистеме идентификации и аутентификации o Требования к подсистеме разграничения доступа o Требования к подсистеме протоколирования и пассивного аудита o Требования к подсистеме активного аудита безопасности o Требования к подсистеме контроля целостности o Требования к подсистеме контроля защищенности o Требования к подсистеме «удостоверяющий центр» o Требования к подсистеме сегментирования и межсетевого экранирования o Требования к подсистеме VPN o Требования к подсистеме антивирусной защиты o Требования к подсистеме фильтрации контента o Требования к подсистеме управления безопасностью o Требования к подсистеме предотвращения утечки информации по техническим каналам • Технические требования к смежным подсистемам o Требования к структурированной кабельной системе o Требования по физической защите • Ответственность сотрудников за нарушение безопасности • Механизм реализации концепции Учебно-методическая литература: 3 Профессиональные базы данных и информационные справочные системы: 1	2

4.2. «Концепция информационной безопасности организации профессионального образования. Необходимые текущие меры для усиления информационной защиты, направления для перспективного усиления состояния защищенности»	2
Учебный проект по проверке: разработка концепции безопасности конкретного учреждения по приведенному развернутому плану-шаблону. Концепция обеспечения информационной безопасности предприятия Содержание • Общие положения • Описание объекта защиты o Назначение и основные функции информационной системы o Группы задач, решаемых в информационной системе o Классификация пользователей системы o Организационная структура обслуживающего персонала o Структура и состав комплекса программно-технических средств o Корпоративная сеть предприятия ▯ Серверы ▯ Рабочие станции ▯ Линии связи и активное сетевое оборудование ▯ Виды информационных ресурсов, хранимых и обрабатываемых в системе ▯ Структура информационных потоков ▯ Внутренние информационные потоки ▯ Внешние информационные потоки ▯ Характеристика каналов взаимодействия с другими системами и точек входа • Основные факторы, влияющие на информационную безопасность предприятия • Основные принципы обеспечения информационной безопасности • Организация работ по защите информации • Меры обеспечения информационной безопасности o Меры обеспечения информационной безопасности организационного уровня o Меры обеспечения информационной безопасности процедурного уровня • Распределение ответственности и порядок взаимодействия • Порядок категорирования защищаемой информации • Модель нарушителя информационной безопасности o Внутренние нарушители o Внешние нарушители • Модель угроз информационной безопасности o Защита информационных компонентов и группы угроз o Угрозы, реализуемые с использованием технических средств o Угрозы, реализуемые с использованием программных средств o Угрозы утечки информации по техническим каналам связи • Требования по обеспечению информационной безопасности o Требования к составу основных подсистем СОИБ o Требования к подсистеме управления политикой безопасности o Требования к подсистеме анализа и управления рисками o Требования к подсистеме идентификации и аутентификации o Требования к подсистеме разграничения доступа o Требования к подсистеме протоколирования и пассивного аудита o Требования к подсистеме активного аудита безопасности o Требования к подсистеме контроля целостности o Требования к подсистеме контроля защищенности o Требования к подсистеме «удостоверяющий центр» o Требования к подсистеме сегментирования и межсетевого экранирования o Требования к подсистеме VPN o Требования к подсистеме антивирусной защиты o Требования к подсистеме фильтрации контента o Требования к подсистеме управления безопасностью o Требования к подсистеме предотвращения утечки информации по техническим каналам • Технические требования к смежным подсистемам o Требования к структурированной кабельной системе o Требования по физической защите • Ответственность сотрудников за нарушение безопасности • Механизм реализации концепции Учебно-методическая литература: 3 Профессиональные базы данных и информационные справочные системы: 1	

5. Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе	***2***
Формируемые компетенции, образовательные результаты: УК-5: В.2 (УК.5.3)	

5.1.	Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе	2

ПРАКТИЧЕСКАЯ РАБОТА №8: ПОСТРОЕНИЕ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.

Цель: ознакомиться с содержанием и структурой частной модели угроз безопасности в информационной системе персональных данных (ИСПДн), получить опыт создания частной модели угроз безопасности для учреждения, имеющего информационную систему обработки персональных данных.
Методы и приемы: изучение теоретических источников, анализ, работа по шаблону, проектный кейс-метод, частично-поисковая работа, самостоятельная работа.
Ключевые слова: частная модель угроз, персональные данные, информационная система, модель нарушителя, угрозы утечки информации, технические каналы утечки информации, защищенность информационной системы, вероятность реализации угроз, корпоративная сеть, несанкционированный доступ.

Порядок выполнения работы
1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

Исходные условия ИСПДн «Кадры»
Организация: ЗАО «Солнышко».
Директор: Иванов Иван Иванович.
Заместитель директора: Петрова Тамара Васильевна.
Начальник отдела кадров: Южина Мария Ивановна.
Сотрудники отдела кадров: Сидорова Александра Павловна,
Копылова Юлия Фёдоровна.
Состав ИСПДн:
1. Персональные данные сотрудников организации:
- фамилия, имя, отчество
- дата и место рождения
- пол
- сведения об образовании
- сведения о предыдущем месте работы
- семейное положение
- адреса регистрации и фактического проживания
- номера контактных телефонов
- индивидуальный номер налогоплательщика
- номер страхового свидетельства пенсионного страхования
- номер полиса обязательного медицинского страхования
- данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.
2. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.
Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему – рис. 7).
Корпоративная сеть: Организации не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.
В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором - информация, составляющая персональные данные сотрудников Организации.
Комплект АРМ №1-3: Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03,
В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.
Комплект сервера: Системный блок № XXXXXXX04, Монитор Samsung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.
Сервер и коммуникационное оборудование установлены в типовой стойке.
Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.

3.3 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	**Трудоемкость (кол-во часов)**
1. Информационная безопасность и ее обеспечение	***24***
Формируемые компетенции, образовательные результаты: ПК-16: З.1 (ПК.16.1), У.1 (ПК.16.2)	

1.1. Информационная безопасность и ее обеспечение ***Задание для самостоятельного выполнения студентом:***	8

ПРАКТИЧЕСКАЯ РАБОТА №3: НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

Цель: ознакомиться с нормативными правовыми актами в области информационной безопасности, проанализировать систему действующих правовых актов РФ в области информационной безопасности, формировать устойчивые навыки самостоятельной работы.
Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, поисковая работа, анализ источников.
Ключевые слова: информационная безопасность, правовые акты, система нормативно-правовых актов.
Порядок выполнения работы
1. Используя любой интернет-браузер, найти правовые документы из представленного перечня.
2. Вставить недостающие реквизиты в перечень нормативных актов.
3. Составить аналитическую записку - обзор по предложенному перечню правовых актов.
4. Оформить отчет по лабораторной работе.

Нормативно-правовые акты в области информационной безопасности РФ
1. Конституция Российской Федерации, принята 12 декабря ___ г.
2. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О ___ отдельных видов деятельности».
3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об ___ подписи».
4. Федеральный закон от 28 декабря 2010 г. № ___ -ФЗ «О безопасности».
5. Федеральный закон от 27 июля ___ г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 июля ___ г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 19 декабря ___ г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
8. Федеральный закон от 7 июля ___ г. № 126-ФЗ «О связи».
9. Федеральный закон от 27 декабря ___ г. № 184-ФЗ «О техническом регулировании».
10. Закон РФ № 195-ФЗ от 30 декабря ___ г. «Кодекс Российской Федерации об административных правонарушениях».
11. Закон РФ № 63-ФЗ от 13 июня ___ г. «Уголовный кодекс Российской Федерации».
12. Закон РФ № 5485-1 от 21 июля ___ г. «О государственной тайне».
13. ___ национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации 31 декабря 2015 г. № 683.
14. ___ информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 5 декабря 2016 г. № 646.
15. Указ Президента Российской Федерации от 12 мая 2008 г. № ___ «Вопросы системы и структуры федеральных органов исполнительной власти».
16. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и ___ контролю».
17. Указ Президента Российской Федерации от 1 ноября 2008 г. № 1576 «О совете при Президенте Российской Федерации по развитию ___ общества в Российской Федерации».
18. Указ Президента Российской Федерации от 30 мая 2005 г. № ___ «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
19. Указ Президента Российской Федерации от 17 марта 2008 г. № ___ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
20. Указ Президента Российской Федерации от 6 марта ___ г. № ___ «Об утверждении перечня сведений конфиденциального характера».
21. Концепция долгосрочного социально-экономического развития Российской Федерации на период до ___ года. Утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.
22. Постановление Правительства Российской Федерации от 16 марта ___ г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
23. Постановление Правительства Российской Федерации № ___ от 1 ноября 2012 г. «Об утверждении требований к защите ___ данных при их обработке в информационных системах персональных данных».
24. Постановление Правительства Российской Федерации от 6 июля 2008 г. № ___

1.2. Система обеспечения информационной безопасности РФ ***Задание для самостоятельного выполнения студентом:***	8

Изучить материал, составить схему.
Глава IV. Организационная основа системы обеспечения информационной безопасности Российской Федерации
10. Основные функции системы обеспечения информационной безопасности Российской Федерации
Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.
Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;

создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;

контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;

организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;

проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;

организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;

защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих

1.3.	Основные законодательные акты РФ в области обеспечения информационной безопасности ***Задание для самостоятельного выполнения студентом:***	8

НОРМАТИВНЫЕ МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ.

Цель: ознакомиться с нормативными методическими документами в области защиты информации, систематизировать сведения о нормативно-методических документах, приобрести опыт самостоятельного поиска и анализа.
Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, поисковая работа, анализ источников.
Ключевые слова: информационная безопасность, правовые акты, система нормативно-методических документов.
Порядок выполнения работы.
5. Используя любой интернет-браузер, найти нормативно-методические документы из представленного перечня.
6. Вставить недостающие реквизиты в перечень нормативных методических документов
7. Составить аналитическую записку - обзор по предложенному перечню.
8. Оформить отчет по лабораторной работе.

Нормативно методические документы в области информационной безопасности РФ
1. «Ответ требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по Ответ каналам». Гостехкомиссия России. - М., 2002.
3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические ___ . Госстандарт России. - М., 1995.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие ___ . Госстандарт России. - М., 2006.
5. ГОСТ Р 50922-2006. Защита информации. Основные термины и ___ - М., 2006.
6. ГОСТ Р ИСО/МЭК 15408-1-___ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
7. ГОСТ Р ИСО/МЭК 15408-2-___ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт России. - М., 2013.
8. ГОСТ Р ИСО/МЭК 15408-3-___ . Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.
9. ГОСТ Р ИСО/МЭК ___ -2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
10. ГОСТ Р ИСО/МЭК 27001-___ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
11. ГОСТ Р ИСО/МЭК 27002-___ «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введен в действие с 01.01.2014
12. ГОСТ Р ИСО/МЭК 27003-___ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
13. ГОСТ Р ИСО/МЭК 27004-___ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
14. ГОСТ Р ИСО/МЭК 27005-___ «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
15. ГОСТ Р ИСО/МЭК 27006-___ «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
16. ГОСТ Р ИСО/МЭК 27011-___ «Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002».
17. ГОСТ Р ИСО/МЭК 27031-___ «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».
18. ГОСТ Р ИСО/МЭК 27033-1-___ «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

2. Правовое обеспечение информационной безопасности	***16***
Формируемые компетенции, образовательные результаты: ПК-16: В.1 (ПК.16.3)	
2.1. Законодательство об информации, информационных технологиях и о защите информации». ***Задание для самостоятельного выполнения студентом:*** Контрольные вопросы 1. В составленном перечне отметьте правовые документы, регламентирующие технические условия? 2. В составленном перечне отметьте правовые документы, регламентирующие организационные условия? 3. Какие документы из представленного перечня являются следствием ассоциирования правовых актов РФ с международным законодательством? 4. Составьте классификацию исследованных документов по органу, принявшему тот или иной документ. Признак принадлежности к классу отметьте в перечне специальным значком. 5. Какова доля документов, регламентирующих организацию работ по защите персональных данных? 6. Какова доля документов, регламентирующих организацию работ по обороту средств технической защиты? Аналитическая записка должна содержать иерархическую структуру исследованных правовых актов, сферу действия отдельных групп документов, соотношение и согласование групп правовых документов, принадлежность к государственному органу. Учебно-методическая литература: 2, 3, 4 Профессиональные базы данных и информационные справочные системы: 1	8

2.2. Правовой режим информационных технологий. ***Задание для самостоятельного выполнения студентом:***	8

Оцените ситуацию или дайте обоснование правомерности действий, описанных в задаче, приведите ссылки на правовые акты, которые использовались для обоснования. Используйте ресурсы СПС «Консультант», «Гарант».

- Задача № 1

Программист Голанов, поступая на работу в фирму «Сокол», формально отнесся к заполнению документов по типовым формам, предложенным руководством фирмы. В течение двух лет Голанов создал ряд программных продуктов, реализация которых принесла фирме «Сокол» значительную прибыль и известность в республике. Видя это, Голанов обратился к руководству фирмы с просьбой выплатить ему денежное вознаграждение как автору программ, обеспечивших заметный успех коллективу. Однако генеральный директор фирмы Валентинов, ссылаясь на регулярную выплату заявителю высокого должностного оклада, отказался удовлетворить его просьбу. При этом он заявил, что свои программы Голанов создал в служебное время.
Прав Голанов или Валентинов? Обоснуйте свой ответ со ссылкой на действующую нормативно-правовую базу.

- Задача № 2

Администрация г. Л. в целях недопущения публикации непроверенной информации о положении дел в городе и, желая усилить контроль над функционированием подведомственных служб, приняла решение о дополнительном уточнении и проверке всех материалов по этой тематике, подлежащих публикации в местных средствах массовой информации.
Оцените законность решения, принятого администрацией г. Л.

- Задача №3

В результате совместной коммерческой деятельности между фирмами «Юг» и «Звезда» был заключен договор о кредите, согласно которому фирма «Звезда» предоставила фирме «Юг» финансовую помощь на развитие производства, а фирма «Юг», в свою очередь, должна была вернуть к определенной дате сумму основного долга и проценты за пользование денежными средствами. По устной договоренности между сторонами, для ускорения и упрощения процедуры информационных отношений договор был заключен на основе способа электронного документооборота и средств защиты информации с применением электронной цифровой подписи.
Спустя месяц фирма «Юг» заявила, что считает заключенный с партнером договор недействительным и что она готова вернуть лишь основной долг и проценты за пользование денежными средствами, а пени за просрочку, предусмотренную договором, вернуть отказывается в силу несостоятельности соглашений.
Генеральный директор фирмы «Звезда» в установленном порядке обратился в арбитражный суд с иском о взыскании с фирмы «Юг» суммы основного долга, процентов и пени за просрочку возвращения долга согласно заключенному договору с применением электронного документооборота и электронной цифровой подписи.
Оцените правомерность действий названных фирм. Какая из сторон выиграет суд и почему?

- Задача №4

Администрация фирмы «Свет» поручила своему программисту Алексину, работавшему по трудовому договору, создать базу данных для учета финансовых и нематериальных активов предприятия. В целях быстрейшего выполнения поставленной задачи программист использовал некоторые типовые разработки своих знакомых коллег, работавших в других организациях. В результате установки данных программ ПЭВМ на рабочем месте Алексина была поражена вирусом. Помимо этого, по истечении некоторого времени на ПЭВМ был установлен факт уничтожения необходимой базы в результате действия вируса. В итоге фирме «Свет» пришлось закупать новую базу данных, в результате чего она понесла немалые убытки.
Администрация предприятия, рассмотрев сложившуюся ситуацию, наложила на Алексина штраф в размере 12000 грн. и лишила его премии. Программист написал жалобу в прокуратуру, требуя отмены решения руководства фирмы и снятия с него всех обвинений.
Имеются ли здесь нарушения законодательства об информации, информатизации и защите информации?

- Задача № 5

Оператор ЭВМ Горячев, работавший в локальной сети редакции газеты, в соответствии с должностной инструкцией обязан был перед вводом в ЭВМ информации, поступающей от корреспондентов на дискетах, проводить антивирусный контроль машинных носителей. Стремясь завершить работу досрочно, Горячев однажды пренебрег требованиями инструкции и в результате допущенных им нарушений информация подготовленного к печати 8-полосного номера газеты была разрушена; выпуск номера был задержан и в результате редакции причинен материальный ущерб.
Квалифицируйте действия оператора Горячева в соответствии с действующим законодательством о компьютерной информации.

- Задача №6

3. Организационное обеспечение информационной безопасности.	*16*
Формируемые компетенции, образовательные результаты: УК-5: З.2 (УК.5.1)	

3.1. СПС Консультант ***Задание для самостоятельного выполнения студентом:***	8

Порядок выполнения работы.

1. Открыть сайт: http://www.consultant.ru, выбрать вкладку работа с некоммерческими интернет-версиями
2. Ознакомиться с краткими теоретическими сведениями
3. Ознакомиться со структурой и возможностями некоммерческой интернет-версией СПС «КонсультантПлюс»
4. Открыть в новой вкладке MSWord, начать оформление отчета по лабораторной работе: записать тему, цель.
5. Войти из стартового окна в режим «Обзоры законодательства», просмотреть информацию в разделе: Правовые новости/ Специальный выпуск, вернуться в Стартовое окно.
6. Открыть по ссылке «Новые документы» списки документов, включенных в систему за последний месяц. Сохранить скриншот списка в отчет по лабораторной работе
7. Перейти в раздел «Законодательство», знакомиться с общим построением справочно-информационной правовой системы «КонсультантПлюс»
8. Изучить поочередно все подпункты основного меню системы, зайти в карточку поиска, рассмотреть все её элементы.
9. Зайти в режим Правового навигатора, изучить особенности поиска информации по конкретному правовому вопросу; двухуровневую структуру словаря; ключевые понятия и группы ключевых понятий; различные виды сортировки списка. Выйти из Правового навигатора.
10. Выполнить упражнения, указанные в таблице 1 - найти нормативно-правовые документы, используя различные виды поиска
11. Ответить на контрольные вопросы.
12. Оформить отчет к лабораторной работе.

Найдите Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Скопируйте реквизиты и преамбулу закона, вставьте эти данные в отчет по лабораторной работе.
Найдите статью, посвященную ограниченному доступу к информации, скопируйте ее сохраните её в отчет.
Поиск по ви¬ду докумен¬та и его наз¬ва¬нию Найдите основные документы по защите прав детей. Выделите три наиболее значимые, скопируйте реквизиты трех из них в отчет.
Поиск по пра¬-вовому нави-гатору Необходимо определить, чему равен минимальный размер оплаты труда (МРОТ). Найдите последний документ, которым внесены изменения в МРОТ. Вставьте его в отчет.
Поиск по при¬-нявшему ор-гану

Найдите Приказ Генпрокуратуры РФ № 39 «О применении бланков процессуальных документов». Если документ отсутствует в некоммерческой интернет-версии, сделайте скриншот сервисного сообщения системы и вставьте его в отчет
Работа со списком доку-ментов
Сформируйте список документов о защите персональных данных. Поиск информации проводите по всем разделам справочной правовой системы. Список документов по данному вопросу сохраните в отчет.

Контрольные вопросы

1. Каковы основные разделы правовых документов в СПС «КонсультантПлюс»?
2. Что включается в иную официальную правовую информацию?
3. Перечислите основные инструменты поиска данной системы.
4. Как найти списки документов, регламентирующих конкретный правовой вопрос?
5. Из каких подразделов состоят разделы «Законодательство», «Судебная практика»?
6. В каком из разделов можно посмотреть тематические обзоры по проблемным правовым вопросам?
7. Как организована обратная связь с пользователями в данной системе?
8. Для чего применяется функция закладок в СПС «КонсультантПлюс»

Содержание отчета: тема, цель, скриншоты основных этапов работы, результаты выполненных заданий, ответы на контрольные вопросы.

Учебно-методическая литература: 3, 4
Профессиональные базы данных и информационные справочные системы: 1

3.2. СПС Гарант ***Задание для самостоятельного выполнения студентом:***	8

РАБОТА СО СПРАВОЧНО-ИНФОРМАЦИОННОЙ ПРАВОВОЙ СИСТЕМОЙ «ГАРАНТ»

Цель работы: ознакомиться с функционалом и приобрести практические навыки работы со справочной правовой системой «Гарант», формировать устойчивые навыки самостоятельной работы.
Методы и приемы: лабораторная работа с использованием информационно-коммуникационных технологий, изучение алгоритмов, выполнение упражнений, частично-поисковый метод, самостоятельная работа.
Ключевые слова: справочно-поисковая система, реквизиты нормативных актов, сервисы справочно-правовой системы, обзор законодательства.

Краткие теоретические сведения
Система производится в виде информационных блоков — баз данных, сформированных по тематическому принципу. Из информационных блоков формируется комплект, который и является конечным продуктом, предлагаемым заказчику. Еженедельное пополнение максимального комплекта составляет несколько десятков тысяч документов (включая документы судебной практики в виде онлайн-архива). Система включает все существующие виды правовой информации: акты органов власти федерального, регионального и муниципального уровня, судебную практику, международные договоры, проекты актов органов власти, формы (бухгалтерской, налоговой, статистической отчётности, бланки, типовые договоры), комментарии, словари и справочники. [википедия].
Работа со справочно-правовой системой «Гарант» начинается с организации поиска документа или списка документов.
Существуют следующие виды поиска в правовой системе «Гарант»: поиск по реквизитам, поиск по классификатору, поиск по ситуации, поиск по источнику опубликования, поиск по словарю терминов. Вид поиска выбирается в зависимости от того, какую информацию необходимо получить и какие имеются известные реквизиты.
Искомые слова можно вводить в любой из этих форм. Система самостоятельно переведет каждое введенное слово в нормальную форму. Однако, следует учесть, что слова необходимо вводить полностью, поскольку при сокращении система не может точно определить, для какого именно слова русского языка требуется подобрать грамматические формы.
Результатом поиска нескольких слов, словосочетаний или целых фраз будет список документов, включающих словоформы всех слов запроса. Документы, полученные таким образом, по умолчанию будут отсортированы особым образом – по степени соответствия.
При открытии документа, найденного с использованием поиска по тексту, искомые слова будут отмечены цветом, а сам документ откроется в месте, которое больше всего соответствует введенному контексту.
Сортировка по степени соответствия возможна только для списков, полученных при работе с быстрым контекстным поиском. Чем точнее конкретный документ соответствует содержанию запроса, тем выше его место в полученном списке.
Для получения изменений законодательства в определенной области в системе существует индивидуальная новостная лента. Она позволяет оперативно получить краткие тематические обзоры наиболее важных новых документов и судебных решений по интересующим вопросам[Фомичева].
Порядок выполнения работы
1. Откройте сайт http://www.garant.ru, выберите интернет-версию ГАРАНТ.
2. Изучите краткие теоретические сведения.
3. Перейдите по ссылке «Помощь в работе, возможности системы.
4. Откройте страницу Информационно-обучающий видеокурс по работе с интернет-версией системы ГАРАНТ
5. Изучить возможности СПС «Гарант» с помощью видеокурсов занятий с 1 по 7
6. Пройти итоговый тест (рис.5). Продемонстрировать результат выполненного теста преподавателю
7. Найти нормативно-правовые документы из задания для самостоятельной работы, используя возможности СПС «Гарант». Составить краткий электронный конспект
8. Ответить на контрольные ответы
9. Оформить отчет по лабораторной работе.

Рисунок 5.Тест для диагностики знаний по функциональным возможностям СПС «ГАРАНТ»

Задания для самостоятельной работы
Составить электронный конспект по основным правовым актам в области

4. Концепция информационной безопасности организации профессионального образования	***12***
Формируемые компетенции, образовательные результаты: УК-5: У.2 (УК.5.2)	

4.1.	«Концепция информационной безопасности организации профессионального образования. Описание текущего состояния информационной защиты» ***Задание для самостоятельного выполнения студентом:*** СОДЕРЖАНИЕ КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ • Общие положения • Описание объекта защиты o Назначение и основные функции информационной системы o Группы задач, решаемых в информационной системе o Классификация пользователей системы o Организационная структура обслуживающего персонала o Структура и состав комплекса программно-технических средств o Корпоративная сеть предприятия ▯ Серверы ▯ Рабочие станции ▯ Линии связи и активное сетевое оборудование ▯ Виды информационных ресурсов, хранимых и обрабатываемых в системе ▯ Структура информационных потоков ▯ Внутренние информационные потоки ▯ Внешние информационные потоки ▯ Характеристика каналов взаимодействия с другими системами и точек входа • Основные факторы, влияющие на информационную безопасность предприятия • Основные принципы обеспечения информационной безопасности • Организация работ по защите информации • Меры обеспечения информационной безопасности o Меры обеспечения информационной безопасности организационного уровня o Меры обеспечения информационной безопасности процедурного уровня • Распределение ответственности и порядок взаимодействия • Порядок категорирования защищаемой информации • Модель нарушителя информационной безопасности o Внутренние нарушители o Внешние нарушители • Модель угроз информационной безопасности o Защита информационных компонентов и группы угроз o Угрозы, реализуемые с использованием технических средств o Угрозы, реализуемые с использованием программных средств o Угрозы утечки информации по техническим каналам связи • Требования по обеспечению информационной безопасности o Требования к составу основных подсистем СОИБ o Требования к подсистеме управления политикой безопасности o Требования к подсистеме анализа и управления рисками o Требования к подсистеме идентификации и аутентификации o Требования к подсистеме разграничения доступа o Требования к подсистеме протоколирования и пассивного аудита o Требования к подсистеме активного аудита безопасности o Требования к подсистеме контроля целостности o Требования к подсистеме контроля защищенности o Требования к подсистеме «удостоверяющий центр» o Требования к подсистеме сегментирования и межсетевого экранирования o Требования к подсистеме VPN o Требования к подсистеме антивирусной защиты o Требования к подсистеме фильтрации контента o Требования к подсистеме управления безопасностью o Требования к подсистеме предотвращения утечки информации по техническим каналам • Технические требования к смежным подсистемам o Требования к структурированной кабельной системе o Требования по физической защите • Ответственность сотрудников за нарушение безопасности • Механизм реализации концепции Учебно-методическая литература: 2	4

4.2.	«Концепция информационной безопасности организации профессионального образования. Необходимые текущие меры для усиления информационной защиты, направления для перспективного усиления состояния защищенности» ***Задание для самостоятельного выполнения студентом:***	8

Общие положения

СОИБ предприятия представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов предприятия от угроз информационной безопасности. Меры защиты организационного уровня реализуются путем проведения соответствующих мероприятий, предусмотренных документированной политикой информационной безопасности. Меры защиты программно-технического уровня реализуются при помощи соответствующих программно-технических средств и методов защиты информации.

Экономический эффект от внедрения СОИБ должен проявляться в виде снижения величины возможного материального, репутационного и иных видов ущерба, наносимого предприятию, за счет использования мер, направленных на формирование и поддержание режима ИБ. Эти меры призваны обеспечить:

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность информации (защита от несанкционированного ознакомления);
- неотказуемость (невозможность отрицания совершенных действий);
- аутентичность (подтверждение подлинности и достоверности электронных документов).

Концепция ИБ предприятия определяет состав критичных информационных ресурсов и основные принципы их защиты. Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты информации (СЗИ) и системы организационных мероприятий является предметом конкретных проектов и политик информационной безопасности, разрабатываемых на основе данной Концепции.

Настоящая концепция должна пересматриваться по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также должен производиться по мере развития информационных систем (ИС) предприятия. Рекомендуемый срок пересмотра концепции составляет три года (при условии отсутствия коренных изменений в структуре системы, в технологиях управления и передачи информации).

Подготовка настоящего документа, внесение в него изменений и общий контроль выполнения требований по обеспечению ИБ предприятия осуществляется сотрудниками отдела ИБ предприятия.

Ответственность за выполнение требований ИБ, определяемых настоящей Концепцией и другими организационно-распорядительными документами предприятия, возлагается на пользователей и администраторов корпоративной сети передачи данных предприятия, а также их руководителей.

Перечень необходимых мер защиты информации определяется по результатам аудита информационной безопасности ИС предприятия и анализа рисков с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения доступности информации и работоспособности программно-технических средств, обрабатывающих эту информацию.

Стратегия обеспечения ИБ должна строиться в соответствии с Российским законодательством в области защиты информации, требованиями международных, отраслевых и технологических стандартов.

Настоящая концепция разработана на основе нормативных и распорядительных документов в области информационной безопасности Российской Федерации.

Описание объекта защиты

Объектом защиты являются автоматизированные системы (как собственной, так и сторонней разработки), входящие в состав информационной системы предприятия.

Информационная система предприятия представляет собой совокупность территориально разнесенных объектов, информационный обмен между которыми осуществляется посредством использования открытых каналов связи, предоставленных сторонними операторами электросвязи. Передача информации осуществляется в кодированном виде на основе протокола кодирования, проверки целостности и конфиденциальности информационных потоков HASH64. Кодирование входящих и исходящих информационных потоков осуществляется на магистральных маршрутизаторах.

Назначение и основные функции информационной системы

ИС предназначена для обеспечения работоспособности информационной инфраструктуры предприятия, предоставления сотрудникам структурных подразделений различных видов информационных сервисов, автоматизации финансовой и производственной деятельности, а также бизнес-процессов

5. Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе	***16***
Формируемые компетенции, образовательные результаты: УК-5: В.2 (УК.5.3)	

5.1.	«Разработка политики безопасности организации профессионального образования» ***Задание для самостоятельного выполнения студентом:***	8

Виды информационных ресурсов, хранимых и обрабатываемых в системе
В ИС предприятия хранятся и обрабатываются различные виды открытой и служебной конфиденциальной информации.
К конфиденциальной и служебной информации, циркулирующей в КСПД, относятся:
- персональные данные сотрудников предприятия и партнеров, хранимые в БД и передаваемые по сети;
- сообщения электронной почты и информация БД, содержащие служебные сведения, информацию о деятельности предприятия и т.п.;
- конструкторская и технологическая документация, перспективные планы развития, модернизации производства, реализации продукции и другие сведения, составляющие научно-техническую и технологическую информацию, связанную с деятельностью предприятия;
- финансовая документация, бухгалтерская отчетность, аналитические материалы исследований о конкурентах и эффективности работы на финансовых рынках;
- другие сведения, составляющие деловую информацию о внутренней деятельности предприятия.

К строго конфиденциальной информации, которая потенциально может циркулировать в ИС, относятся сведения стратегического характера, разглашение которых может привести к срыву выполнения функций предприятия, прямо влияющих на его жизнедеятельность и развитие, нанести невосполнимый ущерб деятельности и престижу предприятия, сорвать решение стратегических задач, проводимой ей политики и, в конечном счете, привести к ее краху.
К категории открытой относится вся прочая информация, не относящаяся к конфиденциальной.
Структура информационных потоков
Внутренние информационные потоки
Внутри ИС выделяются следующие информационные потоки:
- Передача файлов между файловыми серверами и пользовательскими рабочими станциями по протоколу SMB (протокол открытого обмена информацией между АРМ пользователей и серверами на основе стека TCP/IP).
- Передача сообщений электронной почты, посредством использования хешированного соединения программного обеспечения Lotus Notes.
- Передача юридической и справочной информации между серверами БД и пользовательскими рабочими станциями.
- Деловая переписка.
- Передача отчетной информации.
- Передача бухгалтерской информации между пользовательскими рабочими станциями и сервером БД в рамках автоматизированных систем «1С Бухгалтерия», «1С Зарплата и Кадры», «Оперативный учет».

Внешние информационные потоки
В качестве внешних информационных потоков используются:
- Передача отчетных документов (производственные данные) от филиалов предприятия, по каналам корпоративной сети, а также с использованием магнитных носителей.
- Передача платежных документов в Банки.
- Передача финансовых и статистических отчетных документов от филиалов предприятия;
- Внутриведомственный и межведомственный обмен электронной почтой.
- Передача информации по коммутируемым каналам удаленным пользователям.
- Различные виды информационных обменов между ИС и сетью Интернет.

Характеристика каналов взаимодействия с другими системами и точек входа
В ИС предприятия используются следующие каналы взаимодействия с внешними сетями:
- Выделенный магистральный канал взаимодействия с корпоративной сетью, посредством использования технологии VPN.
- Резервная линия связи с сетью Интернет.
- Коммутируемый канал связи, посредством использования технологии GPRS.

Защита подключений к внешним сетям осуществляется при помощи МЭ и встроенных средств защиты магистрального роутера.
Доступ к информационным ресурсам сети Интернет открыт для всех пользователей ИС, посредством использования кеширующего прокси сервера на основе программного обеспечения Squid.
Основные факторы, влияющие на информационную безопасность предприятия
Основными факторами, влияющими на информационную безопасность предприятия, являются:
- расширение сотрудничества предприятия с партнерами;
- автоматизация бизнес-процессов на предприятии;
- расширение кооперации исполнителей при построении и развитии информационной инфраструктуры предприятия;

5.2.	Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе ***Задание для самостоятельного выполнения студентом:***	8

Организация работ по защите информации

Организация и проведение работ по обеспечению ИБ предприятия определяются настоящей концепцией, действующими государственными и международными стандартами и другими нормативными и методическими документами.

Организация работ по обеспечению ИБ возлагается на руководителя департамента информационных технологий, осуществляющего эксплуатацию и сопровождение ИС, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации - на руководителя отдела ИБ предприятия.

Эксплуатация ИС предприятия осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, с учетом требований и положений, изложенных в соответствующих разделах настоящего документа.

Комплекс мер по защите информации на предприятии включает в себя следующие мероприятия:

- Назначение ролей и распределение ответственности за использование информационных ресурсов корпоративной сети.
- Разработка, реализация, внедрение и контроль исполнения планов мероприятий, политик безопасности и других документов по обеспечению ИБ.
- Подготовка пользователей и технических специалистов к решению проблем, связанных с обеспечением ИБ.
- Проектирование, развертывание и совершенствование технической инфраструктуры СОИБ.
- Аудит состояния ИБ предприятия.

Техническая инфраструктура СОИБ предназначена для решения следующих задач:

- Защиты внешнего периметра корпоративной сети предприятия от угроз со стороны внешних сетей за счет использования межсетевого экранирования, контроля удаленного доступа и мониторинга информационных взаимодействий.
- Защиты корпоративных серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, регистрации и учета событий, связанных с осуществлением доступа к ресурсам корпоративных серверов, механизмов мониторинга и аудита безопасности.
- Комплексной антивирусной защиты систем, входящих в состав корпоративной сети за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по следующим уровням:
- Защиты внешнего шлюза в сеть Интернет.
- Защиты корпоративных серверов.
- Защиты рабочих мест пользователей.
- Мониторинга сетевого трафика в реальном масштабе времени с целью выявления злоумышленных действий пользователей корпоративной сети и попыток осуществления НСД к ресурсам корпоративной сети со стороны внешних злоумышленников.
- Защиты прикладных подсистем, функционирующих в составе корпоративной сети, обеспечение доступности предоставляемых ими прикладных сервисов.
- Защиты межсетевых взаимодействий между сегментами ИС предприятия.

Меры обеспечения информационной безопасности

Меры обеспечения информационной безопасности организационного уровня

СОИБ реализуется путем сочетания мер организационного и программно-технического уровней. Организационные меры состоят из мер административного уровня и процедурных мер защиты информации. Основой мер административного уровня, то есть мер, предпринимаемых руководством предприятия, является политика информационной безопасности. Под политикой информационной безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию предприятия в области ИБ, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности предприятия определяется настоящим документом, а также другими нормативными и организационно-распорядительными документами предприятия, разрабатываемыми на основе настоящей концепции. К числу таких документов относятся следующие:

- Политика защиты от НСД к информации;
- Политика предоставления доступа пользователей в ИС;
- Политика управления паролями;
- Политика восстановления работоспособности АС в случае аварии;
- Политика резервного копирования и восстановления данных;
- Политика предоставления доступа к ресурсам сети Интернет;
- Политика управления доступом к информационным ресурсам ИС предприятия;
- Политика внесений изменений в программное обеспечение;

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
	Основная литература	
1	Ажмухамедов И.М. Основы организационно-правового обеспечения информационной безопасности [Электронный ресурс]: учебное пособие/ Ажмухамедов И.М., Князева О.М.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 264 c.	Режим доступа: http://www.iprbookshop.ru/73643.html.— ЭБС «IPRbooks»
2	Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Жигулин Г.П.— Электрон. текстовые данные.— Санкт-Петербург: Университет ИТМО, 2014.— 174 c.	Режим доступа: http://www.iprbookshop.ru/67451.html.— ЭБС «IPRbooks»
3	Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н.— Электрон. текстовые данные.— Санкт-Петербург: Университет ИТМО, 2016.— 169 c.	Режим доступа: http://www.iprbookshop.ru/67452.html.— ЭБС «IPRbooks»
	Дополнительная литература	
4	Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— Москва: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 c.	Режим доступа: http://www.iprbookshop.ru/47262.html.— ЭБС «IPRbooks»

4.2. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование базы данных	Ссылка на ресурс
1	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru
2	Единое окно доступа к образовательным ресурсам	http://window.edu.ru

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС					
Код образовательного результата дисциплины	Текущий контроль				Промежуточная аттестация
	Кейс-задачи	Опрос	Проект	Тест	Зачет/Экзамен
ПК-16					
З.1 (ПК.16.1)				+	+
У.1 (ПК.16.2)		+			+
В.1 (ПК.16.3)			+		+
УК-5					
З.2 (УК.5.1)				+	+
У.2 (УК.5.2)	+				+
В.2 (УК.5.3)			+		+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Информационная безопасность и ее обеспечение":

1. Опрос

1. Каковы основные разделы правовых документов в СПС «КонсультантПлюс»?
2. Что включается в иную официальную правовую информацию?
3. Перечислите основные инструменты поиска данной системы.
4. Как найти списки документов, регламентирующих конкретный правовой вопрос?
5. Из каких подразделов состоят разделы «Законодательство», «Судебная практика»?
6. В каком из разделов можно посмотреть тематические обзоры по проблемным правовым вопросам?
7. Как организована обратная связь с пользователями в данной системе?
8. Для чего применяется функция закладок в СПС «КонсультантПлюс»

Количество баллов: 5

2. Тест

1. К каким мерам защиты относится политика безопасности?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

2. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
а) CL;
б) списки полномочий субъектов;
в) атрибутные схемы.

3. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

4. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;

5. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа;
в) ... выступает посредником при всех обращениях субъектов к объектам;
г) ... фиксирует информацию о попытках доступа в системном журнале;

6. Какие предположения включает неформальная модель нарушителя?
а) о возможностях нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о привычках нарушителя;
г) о предыдущих атаках, осуществленных нарушителем;
д) об уровне знаний нарушителя.
Количество баллов: 5

Типовые задания к разделу "Правовое обеспечение информационной безопасности":

1. Проект

Учебный проект: разработка концепции безопасности конкретного учреждения по приведенному развернутому плану-шаблону.

Концепция обеспечения информационной безопасности предприятия

Содержание

- Общие положения
- Описание объекта защиты
  - Назначение и основные функции информационной системы
  - Группы задач, решаемых в информационной системе
  - Классификация пользователей системы
  - Организационная структура обслуживающего персонала
  - Структура и состав комплекса программно-технических средств
  - Корпоративная сеть предприятия
    - Серверы
    - Рабочие станции
    - Линии связи и активное сетевое оборудование
    - Виды информационных ресурсов, хранимых и обрабатываемых в системе
    - Структура информационных потоков
    - Внутренние информационные потоки
    - Внешние информационные потоки
    - Характеристика каналов взаимодействия с другими системами и точек входа
- Основные факторы, влияющие на информационную безопасность предприятия
- Основные принципы обеспечения информационной безопасности
- Организация работ по защите информации
- Меры обеспечения информационной безопасности
  - Меры обеспечения информационной безопасности организационного уровня
  - Меры обеспечения информационной безопасности процедурного уровня
- Распределение ответственности и порядок взаимодействия
- Порядок категорирования защищаемой информации
- Модель нарушителя информационной безопасности
  - Внутренние нарушители
  - Внешние нарушители
- Модель угроз информационной безопасности
  - Защита информационных компонентов и группы угроз
  - Угрозы, реализуемые с использованием технических средств
  - Угрозы, реализуемые с использованием программных средств
  - Угрозы утечки информации по техническим каналам связи
- Требования по обеспечению информационной безопасности
  - Требования к составу основных подсистем СОИБ
  - Требования к подсистеме управления политикой безопасности
  - Требования к подсистеме анализа и управления рисками
  - Требования к подсистеме идентификации и аутентификации
  - Требования к подсистеме разграничения доступа
  - Требования к подсистеме протоколирования и пассивного аудита
  - Требования к подсистеме активного аудита безопасности
  - Требования к подсистеме контроля целостности
  - Требования к подсистеме контроля защищенности
  - Требования к подсистеме «удостоверяющий центр»
  - Требования к подсистеме сегментирования и межсетевого экранирования
  - Требования к подсистеме VPN
  - Требования к подсистеме антивирусной защиты
  - Требования к подсистеме фильтрации контента
  - Требования к подсистеме управления безопасностью
  - Требования к подсистеме предотвращения утечки информации по техническим каналам
- Технические требования к смежным подсистемам
  - Требования к структурированной кабельной системе
  - Требования по физической защите
- Ответственность сотрудников за нарушение безопасности
- Механизм реализации концепции

Количество баллов: 10

Типовые задания к разделу "Организационное обеспечение информационной безопасности.":

1. Тест

1. К каким мерам защиты относится политика безопасности?
а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

2. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?
а) ACL;
б) списки полномочий субъектов;
в) атрибутные схемы.

3. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?
а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

4. К основным принципам построения системы защиты АИС относятся:
а) открытость;
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;
д) простота.

5. Диспетчер доступа...
а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа;
б) ... использует атрибутные схемы для представления матрицы доступа;
в) ... выступает посредником при всех обращениях субъектов к объектам;
г) ... фиксирует информацию о попытках доступа в системном журнале;
Количество баллов: 5

Типовые задания к разделу "Концепция информационной безопасности организации профессионального образования":

1. Кейс-задачи

• Задача №7

Юрист Бурков , работая в адвокатской фирме «Норма» помощником генерального директора, в свободное от работы время несанкционированно получал доступ к чужим программам, базам данных и постоянно пользовался ими.

Информацию, полученную из них, Бурков часто использовал не по назначению, продавал ее своим клиентам. При этом из-за несанкционированного проникновения помощника генерального директора в названные программы и базы данных в них стали появляться сбои. Впоследствии собственники информационных ресурсов установили причины сбоев и потребовали строгого наказания Буркова .

Дайте правовую оценку действиям Буркова.

• Задача №8

Химический завод г.Д. осуществил выброс ядовитых веществ в реку N. Городские власти, получив от санэпидемслужбы города соответствующую информацию, не оповестили граждан об опасности. В результате купания в реке дети — пять мальчиков и одна девочка — получили серьезные кожные заболевания.

Оцените ситуацию. Кто должен нести ответственность за сокрытие данной информации?

• Задача №9

Желая помочь своим коллегам, программист Сальников и адвокат Сабуров — работники нотариальной конторы «ОКС» — внесли изменения в программу «Акты и документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации объектов недвижимости за последний год и нарушена работа ПЭВМ.

Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова.

Есть ли в действиях Сальникова и Сабурова состав преступления?

• Задача №10

Инженер Смыслов был приглашен на работу в акционерное общество «Оптрон» для организации выпуска нового вида продукции. В процессе работы Смыслов обратил внимание на то, что сведения о переходе предприятия на выпуск новых изделий и их характеристики известны многим работникам и никаких мер по защите этой информации руководство общества не принимает. Смыслов поделился своими сомнениями с бывшим работником «Оптрона» Недремовым.

Вскоре акционерное общество «Кулон», где работал Недремов, освоило производство указанных выше новых изделий, тем самым опередив по всем параметрам предприятие «Оптрон». Руководство «Оптрона» обвинило Смыслова в разглашении коммерческой тайны и пожаловалось на него в прокуратуру города.

Можно ли вменить Смыслову разглашение коммерческой тайны?

• Задача №11

По заявлению истца компании «Запад» о выдаче исполнительного листа на принудительное исполнение решения к ответчику акционерному обществу «Восток» арбитражным судом было вынесено решение о принудительном взыскании суммы основного долга и процентов за пользование денежными средствами с ответчика.

Однако в процессе совместной работы ответчик заключил договор на обслуживание своего расчетного счета с другим банком, реквизиты которого не сообщил партнеру по коммерческим соображениям, а отношения с банком, указанным в договоре с компанией «Запад», прекратил. Кредитор истца обратился с заявлением в арбитражный суд, в котором просил направить в адрес налоговой инспекции по месту нахождения ответчика информацию о расчетных счетах партнера по коммерческим отношениям.

В ответ на запрос арбитражного суда налоговая инспекция сообщила, что, исходя из учредительных документов акционерного общества «Восток», информация о нахождении и состоянии расчетных счетов ответчика является коммерческой тайной и поэтому она не может быть передана истцу.

Дайте информационно-правовую оценку действиям налоговой инспекции на запрос арбитражного суда.

Количество баллов: 5

Типовые задания к разделу "Построение частной модели угроз безопасности персональных данных при их обработке в информационной системе":

1. Проект

Порядок выполнения работы

1. Изучить исходные условия существующей ИСПДн
2. Копировать шаблон частной модели угроз
3. Заполнить шаблон частной модели угроз по исходным условиям информационной систем обработки персональным данным.
4. Защитить свой проект частной модели угроз ИСПДн.

Количество баллов: 5

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Зачет

Вопросы к зачету:

1. • Информация как объект правоотношений. Структура информационной сферы и характеристика ее элементов. В иды защищаемой информации по законодательству РФ.
2. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.
3. • Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
4. • Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.
5. • Уровни ИБ: законодательный, административный, процедурный
6. • Правовые режимы конфиденциальной информации: особенности и содержание.
7. • Законодательный уровень ИБ в РФ: обзор основных правовых документов.
8. • Управление доступом. Объектно-ориентированный подход к управлению доступом. Матрица доступа. Программно-аппаратная реализация матрицы доступа.
9. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.
10. • Основные понятия и критерии в классификации угроз.
11. • Стандарты и спецификации в области ИБ.
12. • Правовой режим защиты государственной тайны. Государственная тайна как особый вид защищаемой информации, и ее характерные признаки.
13. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.
14. • Понятие конфиденциальной информации, основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
15. • Юридическая ответственность за нарушения правовых режимов конфиденциальной информации - дисциплинарная, гражданско-правовая, административная, уголовная.
16. • Понятие лицензирования по законодательству РФ. Виды деятельности, подлежащие лицензированию.
17. • Правовые режимы конфиденциальной информации: особенности и содержание.
18. • Правовая регламентация лицензионной деятельности в области обеспечения ИБ.
19. • Правовая регламентация сертификационной деятельности в области обеспечения ИБ. Объекты сертификации. Органы сертификации и их полномочия.
20. • Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав.
21. • Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.
22. • Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.
23. • Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.
24. • Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения.
25. • Идентификация и аутентификация. Парольная аутентификация, меры по усилению парольной аутентификации. Биометрическая идентификация и аутентификация, достоинства и недостатки.
26. • Протоколирование и аудит ИС. Активный аудит.
27. • Порядок доступа и допуска к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.
28. • Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.
29. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.
30. • Справочно-поисковые системы «Консультант» и «Гарант»: сфера применения, основные функции
31. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.
32. • Контроль доступа, средства поиска и досмотра. Системы контроля доступа. Технологии считывания электронных ключей, электронных пропусков.

33. • Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

34. • Физическая защита неподвижных объектов. Пропускной режим.

35. • Проблема безопасности технологии. Организация работы персонала. Система инструкций и правил

36. • Правовая охрана баз данных, топологий интегральных схем и единых технологий.

37. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

38. • Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей.

39. • Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

40. • Национальная доктрина информационной безопасности РФ

Второй период контроля

1. Экзамен

Вопросы к экзамену:

1. • Информация как объект правоотношений. Структура информационной сферы и характеристика ее элементов. В иды защищаемой информации по законодательству РФ.

2. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

3. • Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.

4. • Понятие информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в РФ.

5. • Уровни ИБ: законодательный, административный, процедурный

6. • Правовые режимы конфиденциальной информации: особенности и содержание.

7. • Законодательный уровень ИБ в РФ: обзор основных правовых документов.

8. • Управление доступом. Объектно-ориентированный подход к управлению доступом. Матрица доступа. Программно-аппаратная реализация матрицы доступа.

9. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.

10. • Основные понятия и критерии в классификации угроз.

11. • Стандарты и спецификации в области ИБ.

12. • Правовой режим защиты государственной тайны. Государственная тайна как особый вид защищаемой информации, и ее характерные признаки.

13. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.

14. • Понятие конфиденциальной информации, основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.

15. • Юридическая ответственность за нарушения правовых режимов конфиденциальной информации - дисциплинарная, гражданско-правовая, административная, уголовная.

16. • Понятие лицензирования по законодательству РФ. Виды деятельности, подлежащие лицензированию.

17. • Правовые режимы конфиденциальной информации: особенности и содержание.

18. • Правовая регламентация лицензионной деятельности в области обеспечения ИБ.

19. • Правовая регламентация сертификационной деятельности в области обеспечения ИБ. Объекты сертификации. Органы сертификации и их полномочия.

20. • Законодательство РФ об интеллектуальных правах. Понятие и виды интеллектуальных прав.

21. • Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Иные преступления в информационной сфере.

22. • Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими.

23. • Понятие «режим защиты информации». Режим защиты информации как составная часть организационной защиты информации.

24. • Объекты обеспечения физической безопасности: сооружения, предметы, люди. Проектирование здания. Охрана территории. Охрана здания. Сигнализация. Противостояние взлому: двери, замки, запоры, ограждения.

25. • Идентификация и аутентификация. Парольная аутентификация, меры по усилению парольной аутентификации. Биометрическая идентификация и аутентификация, достоинства и недостатки.

26. • Протоколирование и аудит ИС. Активный аудит.

27. • Порядок доступа и допуска к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения.

28. • Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах.

29. • Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия.

30. • Справочно-поисковые системы «Консультант» и «Гарант»: сфера применения, основные функции

31. • Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну.

32. • Контроль доступа, средства поиска и досмотра. Системы контроля доступа. Технологии считывания электронных ключей, электронных пропусков.

33. • Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

34. • Физическая защита неподвижных объектов. Пропускной режим.

35. • Проблема безопасности технологии. Организация работы персонала. Система инструкций и правил

36. • Правовая охрана баз данных, топологий интегральных схем и единых технологий.

37. • Защита интеллектуальных прав. Юридическая ответственность за нарушение авторских прав.

38. • Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей.

39. • Защита документов от подделок. Обнаружение фальсификации документов. Предварительная защита документов. Приборы и методы контроля документов. Хранилища. Сейфы. Запирающие устройства.

40. • Национальная доктрина информационной безопасности РФ

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы
"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов
"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2. Практические

Практические (семинарские занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения практических занятий и семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

При подготовке к практическому занятию необходимо, ознакомиться с его планом; изучить соответствующие конспекты лекций, главы учебников и методических пособий, разобрать примеры, ознакомиться с дополнительной литературой (справочниками, энциклопедиями, словарями). К наиболее важным и сложным вопросам темы рекомендуется составлять конспекты ответов. Следует готовить все вопросы соответствующего занятия: необходимо уметь давать определения основным понятиям, знать основные положения теории, правила и формулы, предложенные для запоминания к каждой теме.

В ходе практического занятия надо давать конкретные, четкие ответы по существу вопросов, доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

3. Зачет

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

4. Экзамен

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять их для решения практических задач.

Экзамен проводится в устной или письменной форме по билетам, утвержденным заведующим кафедрой. Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся не позднее чем за один месяц до экзаменационной сессии.

В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп.

При любой форме проведения экзаменов по билетам экзаменатору предоставляется право задавать студентам дополнительные вопросы, задачи и примеры по программе данной дисциплины. Дополнительные вопросы, также как и основные вопросы билета, требуют развернутого ответа.

Результат экзамена выражается оценкой «отлично», «хорошо», «удовлетворительно».

5. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

− проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

− выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

− работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);

− в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

− решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.

− оставить время для проверки ответов, чтобы избежать механических ошибок.

6. Опрос

Опрос представляет собой совокупность развернутых ответов студентов на вопросы, которые они заранее получают от преподавателя. Опрос может проводиться в устной и письменной форме.

Подготовка к опросу включает в себя:

− изучение конспектов лекций, раскрывающих материал, знание которого проверяется опросом;

− повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения;

− изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний;

− составление в мысленной форме ответов на поставленные вопросы.

7. Проект

Проект – это самостоятельное, развёрнутое решение обучающимся, или группой обучающихся какой-либо проблемы научно-исследовательского, творческого или практического характера.

Этапы в создании проектов.

1. Выбор проблемы.
2. Постановка целей.
3. Постановка задач (подцелей).
4. Информационная подготовка.
5. Образование творческих групп (по желанию).
6. Внутригрупповая или индивидуальная работа.
7. Внутригрупповая дискуссия.
8. Общественная презентация – защита проекта.

8. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.

Рекомендации по работе с кейсом:

1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Проблемное обучение
2. Проектные технологии
3. Кейс-технологии

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. учебная аудитория для семинарских, практических занятий
3. Лицензионное программное обеспечение:
   - Операционная система Windows 10
   - Microsoft Office Professional Plus
   - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
   - Справочная правовая система Консультант плюс
   - 7-zip
   - Adobe Acrobat Reader DC