МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	Заведующий кафедрой _ТиИГиП
А.Н.Харитонова	А.Н.Харитонова
«02» _июня_ 2022 г.	«02» _июня_ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Составитель(-и)	**Коканова Р.А.; канд.пед.наук, доцент;**
Направление подготовки	**46.03.02 ДОКУМЕНТОВЕДЕНИЕ И АРХИВОВЕДЕНИЕ**
Направленность (профиль) ОПОП	
Квалификация (степень)	**бакалавр**
Форма обучения	**заочная**
Год приема	**2020 г.,**
Курс	**3 курс**
Семестр	**5**

Астрахань - 2022 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Целями освоения дисциплины (модуля) «Информационная безопасность и защита информации» являются: получение студентами знаний и навыков, необходимых для безопасного использования информационных технологий.

1.2. Задачи освоения дисциплины (модуля): «Информационная безопасность и защита информации»**:**

- ознакомление с понятием информационных ресурсов, изучение классификации информационных ресурсов, характеристики их основных свойств;
- изучение понятий надежности информации и защиты от несанкционированного доступа;
- изучение основ информационной безопасности человека и общества, ознакомление с задачами, методами и средствами информационной безопасности;
- изучение понятия защиты информации, классификации и характеристики основных методов и средств, практика применения защиты информации по областям.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Дисциплина «Информационная безопасность и защита информации» относится к обязательной части изучения дисциплин Б1.Б16

Дисциплина встраивается в структуру ОПОП ВО как с точки зрения преемственности содержания, так и с точки зрения непрерывности процесса формирования компетенций выпускника. При освоении данной дисциплины необходимы следующие знания, умения, навыки, приобретённые в результате освоения предшествующих дисциплин обучающимися:

- анализ информационных потоков и информационного взаимодействия в организации;
- технологическая деятельность:
- работа по обеспечению сохранности документов на разных носителях.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения и навыки, формируемые предшествующими учебными дисциплинами*:*

- Информатика;
- Гражданское право;
- Трудовое право;
- Информационное право;
- Документоведение;
- Организация и технология документационного обеспечения управления;

Знания: основных понятий информатики, структуры систем документационного обеспечения, НПА.

Умения: использовать программные и аппаратные средства персонального компьютера, использовать НПА.

Навыки: навыки поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.), использования НПА.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

- Трудовые конфликты
- Конфиденциальное делопроизводство
- Организационно-информационное обеспечение деятельности руководителя

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки

(специальности):

а) общепрофессиональных (ОПК): ОПК-6 «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»;

в) профессиональных (ПК): ПК – 17 «владеть методами защиты информации».

Таблица 1. Декомпозиция результатов обучения

код компетенции	Планируемые результаты освоения дисциплины		
	Знать	Уметь	Владеть
ОПК-6	Знать сущность и значение информационной безопасности	Самостоятельно использовать знания по информационной безопасности при решении стандартных задач профессиональной деятельности	Навыками решения задач профессиональной деятельности с учетом основных требований информационной безопасности
ПК – 17	Знать методы защиты информации	Работать с информацией, используя методы защиты	Методами защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) составляет 3 зачетные единицы, в том числе 10 часов, выделенных на контактную работу обучающихся с преподавателем (из них *2* часов – лекции, 8 часов – практические, семинарские занятия), и 98 часа – на самостоятельную работу обучающихся.

Таблица 2. Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоя т. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	Тема 1. Проблемная сфера информационной безопасности и защиты информации	5						16	Устное собеседование
2	Тема 2. Основы информационной безопасности в информационной сфере	5		2				16	Устное собеседование Контрольная работа 1
3	Тема 3. Интересы личности, общества и государства в	5			2			16	Устное собеседование Контрольная -

	информационной сфере								блиц Практическая работа
4	Тема 4. Законодательство в области информационной безопасности и защиты информации	5			2			16	Устное собеседование Практическая работа Контрольная работа 2
5	Тема 5. Понятие и виды информации, защищаемой законодательством Российской Федерации	5			2			16	Устное собеседование Деловая игра
6	Тема 6. Методы обеспечения информационной безопасности	5			2			18	Устное собеседование Итоговое тестирование IT-метод
ИТОГО 108				**2**	**8**			**98**	**ЗАЧЕТ**

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3 – Матрица соотнесения разделов, тем учебной дисциплины (модуля) и формируемых компетенций

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции (указываются компетенции перечисленные в п.3)*			*Σ общее количество компетенций*
		ОПК 6	*ПК 17*		
Тема 1. Проблемная сфера информационной безопасности и защиты информации	16	+			1
Тема 2. Основы информационной безопасности в информационной сфере	16	+			1
Тема 3. Интересы личности, общества и государства в информационной сфере	18	+	+		2
Тема 4. Законодательство в области	18	+	+		2

информационной безопасности и защиты информации					
Тема 5. Понятие и виды информации, защищаемой законодательством Российской Федерации	18	+	+		2
Тема 6. Методы обеспечения информационной безопасности	20	+	+		2
ИТОГО	108				

Краткое содержание каждой темы дисциплины (модуля)

Тема 1. Проблемная сфера информационной безопасности и защиты информации

Информационная общество, информационная сфера. Определение и эволюция термина «информационная безопасность». Соперничество в информационной сфере. Понятие информационных ресурсов. Документирование информации как обязательное условие документированных информационных ресурсов.

Тема 2. Основы информационной безопасности в информационной сфере

Понятие и виды информации; классификация информационных продуктов и услуг. Критерии ценности информационных ресурсов.

Тема 3. Интересы личности, общества и государства в информационной сфере.

Виды и источники угроз информационной безопасности. Реализации конституционных прав человека и гражданина на доступ к информации и на использование информации. Информационное обеспечение государственной политики.

Тема 4. Законодательство в области информационной безопасности и защиты информации

Правовая охрана информационных ресурсов. Правовой режим защиты государственной тайны. Электронная цифровая подпись. Лицензирование и сертификация в области обеспечения информационной безопасности. Защита авторских и смежных прав в законодательстве Российской Федерации.

Тема 5. Понятие и виды информации, защищаемой законодательством Российской Федерации.

Классификация информации ограниченного доступа. Государственная тайна. Персональные данные. Личная и семейная тайна. Служебная тайна. Коммерческая тайна. Профессиональная тайна. Тайна связи. Тайна страхования. Налоговая тайна. Банковская тайна. Тайна нотариальных действий. Адвокатская тайна. Врачебная тайна. Тайна усыновления. Тайна предварительного следствия и судопроизводства.

Тема 6. Методы обеспечения информационной безопасности.

Доктрина информационной безопасности. Правовые, экономические, организационно-технические методы. Разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности. Использование средств защиты информации. Контроль за действием персонала в защищаемых информационных системах.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекции, семинарским занятиям, выполнение самостоятельных работ необходимо воспользоваться системой «Цифровое обучение»:

https://moodle.asu.edu.ru/course/view.php?id=832

Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться. Подготовка к практическому (семинарскому) занятию начинается с тщательного ознакомления с условиями предстоящей работы, т. е. с обращения к вопросам семинарских занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. При подготовке к практическому (семинарскому) занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации.

Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее докладами и презентациями, принимать участие в выполнении практических заданий.

С целью обеспечения успешного обучения студент должен готовиться к лекции, поскольку она является важной формой организации учебного процесса: знакомит с новым учебным материалом; разъясняет учебные элементы, трудные для понимания; систематизирует учебный материал; ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем: - внимательно прочитайте материал предыдущей лекции; - узнайте тему предстоящей лекции (по тематическому плану); - ознакомьтесь с учебным материалом по учебным пособиям; - постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке; - запишите возможные вопросы, которые вы зададите преподавателю на лекции. Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме. К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по дисциплине.

В самом начале учебного курса студенту следует познакомиться со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен овладеть;
- тематическими планами лекций, семинарских занятий;
- контрольными мероприятиями;
- учебными пособиями по дисциплине;
- перечнем вопросов к зачету.

После этого у студента должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях, семинарских занятиях и в процессе самостоятельной работы позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Методические указания предназначены для рационального распределения времени студентами по видам самостоятельной работы и разделам дисциплины (модуля).

Таблица 4. Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
Тема 1	Выполнение самостоятельной работы 2	16	Опрос

Тема 2	Выполнение самостоятельной работы 2 Подготовка к контрольной работе 1	16	КОНТРОЛЬНАЯ РАБОТА 1
Тема 3	Выполнение самостоятельной работы 2 Доктрина информационной безопасности	16	Контрольная - блиц Практическая работа
Тема 4	Подготовка к контрольной работе 2 Подготовка к промежуточному тестированию	16	Практическая работа Контрольная работа 2
Тема 5	Выполнение самостоятельной работы 2 Деловая игра	16	Деловая игра
Тема 6	IT-метод	18	IT-метод

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно.

Методические рекомендации по выполнению контрольных работ, проведению зачета

Контрольные работы

Контрольная работа состоит из 2-х заданий. Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Проведение зачета

Оценивание студентов на зачете осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных и тематических контрольных работ. Он предусматривает проверку готовности студентов к плановым занятиям, оценку качества и самостоятельности выполнения заданий на практических занятиях, проверку правильности решения задач, выданных на самостоятельную проработку.

На зачете осуществляется комплексная проверка знаний, навыков и умений студентов по всему теоретическому материалу дисциплины и с проверкой практических навыков и умений. Теоретические знания оцениваются путем компьютерного тестирования или на основании письменных ответов студентов по нескольким теоретическим вопросам.

Критерии оценки:

– оценка «отлично» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу верно, представлен отчет, информация в отчете сформулирована обоснованно, логично и последовательно, применен творческий подход, учтены основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет, информация в отчете сформулирована обоснованно, формулировки конкретные, приведены ссылки на нормативно-правовые документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент выполнил ситуационную (профессиональную) задачу преимущественно верно, представлен отчет,

информация в отчете сформулирована с нарушением логики, не полная, формулировка общая или неполная, имеются одна или две негрубые ошибки, приведены неверные ссылки на нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не выполнил ситуационную (профессиональную) задачу или выполнил ее неверно, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют ссылки на нормативно-правовые документы по информационной безопасности.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов, диспутов, дебатов, портфолио, круглых столов и пр.) в сочетании с внеаудиторной работой с целью формирования и развития требуемых компетенций обучающихся.

6.1. Образовательные технологии

В соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров в рамках изучения дисциплины «ИБ и ЗИ» предусмотрено использование в учебном процессе следующих активных и интерактивных форм проведения занятий:

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Тема 1. Проблемная сфера информационной безопасности и защиты информации	*Обзорная лекция*	*Фронтальный опрос,*	*Не предусмотрено*
Тема 2. Основы информационной безопасности в информационной сфере	*Лекция-диалог*	*Фронтальный опрос,* контрольная работа 1	*Не предусмотрено*
Тема 3. Интересы личности, общества и государства в информационной сфере	*Обзорная лекция*	*Фронтальный опрос* Контрольная - блиц *Анализ конкретных ситуаций*	*Не предусмотрено*
Тема 4. Законодательство в области информационной безопасности и защиты информации	*Лекция презентация*	*Фронтальный опрос* *Анализ конкретных ситуаций*	*Не предусмотрено*
Тема 5. Понятие и виды информации, защищаемой законодательством Российской	*Лекция презентация*	*Фронтальный опрос* Деловая игра	*Не предусмотрено*

Федерации			
Тема 6. Методы обеспечения информационной безопасности	*Лекция-диалог*	*Фронтальный опрос* *Анализ конкретных ситуаций*	*Не предусмотрено*

6.2. Информационные технологии

- использование возможностей Интернета в учебном процессе (использование информационного сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление учащихся с оценками и т.д.));
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источников информации;
- использование возможностей электронной почты преподавателя;
- использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т.д.);
- использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т.е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);
- использование виртуальной обучающей среды (LMS Moodle *«Электронное образование»*) или иных информационных систем, сервисов и мессенджеров.

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Kaspersky Endpoint Security	Средство антивирусной защиты
Google Chrome	Браузер
OpenOffice	Пакет офисных программ

6.3.2. Современные профессиональные базы данных и информационные справочные системы

Наименование современных профессиональных баз данных, информационных справочных систем
Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем». https://library.asu.edu.ru
Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/

Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО "ИВИС". http://dlib.eastview.com Имя пользователя: AstrGU Пароль: AstrGU
Справочная правовая система КонсультантПлюс. Содержится огромный массив справочной правовой информации, российское и региональное законодательство, судебную практику, финансовые и кадровые консультации, консультации для бюджетных организаций, комментарии законодательства, формы документов, проекты нормативных правовых актов, международные правовые акты, правовые акты, технические нормы и правила. http://www.consultant.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Паспорт фонда оценочных средств.

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие разделов, тем дисциплины (модуля), результатов обучения по дисциплине (модулю) и оценочных средств

Контролируемый раздел, тема дисциплины (модуля)	Код контролируемой компетенции	Наименование оценочного средства
Тема 1. Проблемная сфера информационной безопасности и защиты информации	ОПК6	Устное собеседование
Тема 2. Основы информационной безопасности в информационной сфере	ОПК6	Устное собеседование Контрольная работа 1
Тема 3. Интересы личности, общества и государства в информационной сфере	ОПК6 ПК17	Устное собеседование Контрольная - блиц Практическая работа
Тема 4. Законодательство в области информационной безопасности и защиты информации	ОПК6 ПК17	Устное собеседование Практическая работа Контрольная работа 2
Тема 5. Понятие и виды информации, защищаемой законодательством Российской Федерации	ОПК6 ПК17	Устное собеседование Деловая игра

Тема 6. Методы обеспечения информационной безопасности	ОПК6 ПК17	Устное собеседование IT-метод

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7

Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8

Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетвори тельно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетво рительно»	не способен правильно выполнить задание

7.3. Контрольные задания и иные материалы, необходимые для оценки результатов обучения по дисциплине (модулю)

Тема 1. Проблемная сфера информационной безопасности и защиты информации

1.Вопросы для обсуждения

1. Информационная общество, информационная сфера.
2. Определение и эволюция термина «информационная безопасность». Соперничество в информационной сфере.
3. Понятие информационных ресурсов. Документирование информации как обязательное условие документированных информационных ресурсов.

Тема 2. Основы информационной безопасности в информационной сфере

1.Вопросы для обсуждения

1. Понятие и виды информации.
2. Классификация информационных продуктов и услуг.
3. Критерии ценности информационных ресурсов.

2.Контрольная работа1

1. Информационное общество, информационная сфера.
2. Понятие национальной безопасности, виды безопасности, информационная безопасность (ИБ) в системе национальной безопасности.
3. Понятие информационных ресурсов.
4. Определение и эволюция термина «информационная безопасность».
5. Понятие и виды информации;
6. Классификация информационных продуктов и услуг.

4. Практическая работа

1. Исследовать состав информационного рынка и описать его структуру в виде схемы (товары и услуги). Привести примеры по каждому виду товаров и услуг.(Пояснение: взять один из секторов информационного рынка и исследовать его)

2. Проанализировать цены на различные виды информационных продуктов и услуг.

Содержание отчета по практичесой работе работе

1. Схема структуры рынка информационных товаров и услуг.
2. Выводы о месте информационных продуктов и услуг в современной экономике

Тема 3. Интересы личности, общества и государства в информационной сфере.

1.Вопросы для обсуждения

1. Виды и источники угроз информационной безопасности.
2. Реализации конституционных прав человека и гражданина на доступ к информации и на использование информации.
3. Информационное обеспечение государственной политики.

2.Блиц - контрольная работа

Термины:

1. Информационная безопасность
2. Защита информации
3. Угроза
4. Атака
5. Злоумышленник
6. Окно безопасности
7. Доступность
8. Конфиденциальность
9. Целостность

3.Практическая работа

1. В СПС Консультант+ или Гарант найти «Доктрину информационной безопасности
2. Выписать определение ИБ
3. В чем заключаются интересы личности, общества, государства
4. Выписать 4 составляющие национальных интересов
5. Выписать основные функции системы обеспечения ИБ РФ

Тема 4. Законодательство в области информационной безопасности и защиты информации

1.Вопросы для обсуждения

1. Правовая охрана информационных ресурсов.
2. Правовой режим защиты государственной тайны.
3. Электронная цифровая подпись.
4. Лицензирование и сертификация в области обеспечения информационной безопасности.
5. Защита авторских и смежных прав в законодательстве Российской Федерации.

2.Практическая работа

Найти в СПС Гарант или Консультант Плюс подзаконные акты и выписать:

1. Что относят к информации конфиденциального характера, государственной тайны?
2. Основные положения инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне.
3. Перечень должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне.
4. В чем заключается стратегия национальной безопасности Российской федерации?
5. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

3.Контрольная работа 2

Вариант 1

1. Виды и источники угроз информационной безопасности.
2. Реализации конституционных прав человека и гражданина на доступ к информации и на использование информации.

Вариант 2

3. Информационное обеспечение государственной политики.
4. Правовая охрана информационных ресурсов.

Вариант 3

5. Правовой режим защиты государственной тайны.
6. Электронная подпись.

Вариант 4

7. Лицензирование и сертификация в области обеспечения информационной безопасности.
1. Защита авторских и смежных прав в законодательстве Российской Федерации.

Тема 5. Понятие и виды информации, защищаемой законодательством Российской Федерации.

1.Вопросы для обсуждения

1. Классификация информации ограниченного доступа.
2. Государственная тайна.
3. Персональные данные.
4. Личная и семейная тайна.
5. Служебная тайна.
6. Коммерческая тайна.
7. Профессиональная тайна.
8. Тайна связи.
9. Тайна страхования.
10. Налоговая тайна.
11. Банковская тайна.
12. Тайна нотариальных действий.
13. Адвокатская тайна.

14. Врачебная тайна.
15. Тайна усыновления.
16. Тайна предварительного следствия и судопроизводства.

2.Деловая игра

Тема (проблема) Составление распорядительных документов по обеспечению информационной безопасности на предприятиях различных форм собственности

Задание:

1. Разработать организационную структуру предприятия, номенклатуру должностей работников.
2. Разработать основной круг вопросов, решаемых руководством и сотрудниками предприятия по обеспечению информационной безопасности предприятия.
3. Разработать приказ по обеспечению информационной безопасности предприятия (распорядительная часть должна содержать не менее 5 пунктов мероприятий).
4. Составить указание сотрудникам предприятия по развитию и внедрению новых информационных технологий в своей отрасли.
5. Составить распоряжение о внедрении новых разработок по защите информации.
6. Составить решение о подготовке к проведению конференции по информационной безопасности.
7. Составить краткий протокол совещания по вопросам информационной безопасности.
8. Быть в готовности в роли руководителя, начальника службы безопасности решать управленческие задачи, связанные с обеспечением комплексной безопасности предприятия (принимать решения, отдавать распоряжения, осуществлять контроль за выполнением отданных распоряжений).
9. Студентам письменно выполнить задание (объем 5-7 листов) и быть в готовности к его защите на практическом занятии.

Тема 6. Методы обеспечения информационной безопасности.

1.Вопросы для обсуждения

1. Правовые, экономические, организационно-технические методы.
2. Разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности.
3. Использование средств защиты информации.
4. Контроль за действием персонала в защищаемых информационных системах

2.Вопросы для IT -метода

Задание

Используя СПС «Гарант», «КонсультантПлюс», сайты - http://www.linuxsecurity.com, http://www.osp.ru/os и другие ответить аргументировано, ссылаясь на нормативные документы, на следующие вопросы:

- Вопрос: Работник организации написал заявление с просьбой выдать следующие документы, связанные с работой: приказ о приеме на работу, копию трудовой книжки, правила внутреннего трудового распорядка, положение об оплате труда и премировании, положение о персональных данных, положение о коммерческой тайне и режиме ее обеспечения, справку о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование. Обязана ли организация выдавать затребованные документы? Может ли руководитель отказать в данном требовании работнику?
- Вопрос: Организация заключила договор о ведении бухгалтерского учета со сторонним бухгалтером. При этом текст договора не содержит условия об обеспечении конфиденциальности и безопасности персональных данных работников при их обработке, перечня действий с персональными данными, которые будут совершаться бухгалтером. Является ли неуказание данных условий в договоре нарушением Федерального закона от

27.07.2006 N 152-ФЗ "О персональных данных"?

Перечень вопросов и заданий, выносимых на зачёт

Таблица 9

Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
	Код и наименование проверяемой компетенции ОПК 6			
1.	Задание открытого типа	Используя СПС «Гарант» или «КонсультантПлюс» определить статью Федерального закона от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне», которая содержит четкие указания о разработке перечня информации, составляющей коммерческую тайну, установлении порядка обращения с этой информацией и контроля за соблюдением такого порядка, а также о ведении учета лиц, получивших доступ к информации, составляющей коммерческую тайну.	Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» в ст. 10 «Охрана конфиденциальности информации»	10
2.		Используя СПС «Гарант» или «КонсультантПлюс» определить НПА, которые определяют перечни сведений, доступ к которым по действующему законодательству не может быть ограничен	Такие перечни содержатся в ч. 4 статьи 8 Закона № 149-ФЗ и ст. 5 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».	10
3.		Используя СПС «Гарант» или «КонсультантПлюс» определить, в отношении каких локальных нормативных актов работодателя не может быть установлен режим коммерческой тайны	ст. 5 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» режим коммерческой тайны не может быть установлен в отношении следующих локальных нормативных актов работодателя: • штатного расписания (как документа, содержащего сведения о численности и о составе работников); • положений о системах оплаты труда; • положений об охране труда (как сведений об условиях труда, об охране труда, о показателях производственного травматизма и профессиональной заболеваемости).	10
4.		Найти решение суда по данным вопросам: Истица обращалась с заявлениями о	Решением суда первой инстанции иск был удовлетворен частично:	17

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		предоставлении ей сведений по штатному расписанию, однако в предоставлении ей таких сведений было отказано со ссылкой на коммерческую тайну ответчика.	суд признал отказы администрации о выдаче К. копий штатного расписания незаконными и обязал предприятие их предоставить. Судебная коллегия, напротив, нашла ошибочным вывод суда о том, что штатное расписание является документом, связанным с работой истицы, поскольку не содержит сведений, касающихся только трудовой деятельности истицы.	
5.		Найти решение суда по данным вопросам: Истица обратилась к ответчику с заявлением о выдаче ей документов, связанных с ее бывшей работой: справки о ее заработной плате и копии приказов, на основании которых ответчик ей выплатил премии в 2005 г. Ответчик выдал истице справку о заработной плате, но отказался выдать копии приказов.	Суд пришел к выводу о том, что требования истицы не подлежат удовлетворению, так как у ответчика отсутствовала обязанность по предоставлению истице копий приказов о премировании всех работников, поскольку истица обосновала свою необходимость в их предоставлении для убеждения в том, что она не была ответчиком дискриминирована, то есть ей необходима информация об оплате труда других работников. Поэтому оснований для истребования и изучения в целях правовой оценки локального нормативного акта о порядке премирования работников учреждения не имеется.	17
6.	Задание закрытого типа	К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. Разработка и	3	

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		конкретизация правовых нормативных актов обеспечения безопасности		
7		Основными источниками угроз информационной безопасности являются все указанное в списке: 1. Хищение жестких дисков, подключение к сети, инсайдерство 2. Перехват данных, хищение данных, изменение архитектуры системы 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы	2	
8		Виды информационной безопасности: 1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	1	
9		Цели информационной безопасности – своевременное обнаружение, предупреждение: 1. несанкционированного доступа, воздействия в сети 2. инсайдерства в организации 3. чрезвычайных ситуаций	1	
10		Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы	1	
	Код и наименование проверяемой компетенции ПК 17			
1.	Задания открытого типа	При ведении конфиденциального делопроизводства уделяется большое внимание уничтожению конфиденциальных документов. Как происходит уничтожение документов?	уничтожение документов, в том числе черновиков, должно производится в машинках для уничтожении бумаг (шредерах) в присутствии нескольких человек и с проставлением соответствующих пометок в журналах уничтожения конфиденциальных документов. При	6-10

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			большом количестве документов, возможно, их сжигание.	
2.		Хранение конфиденциальных документов?	Хранить конфиденциальные документы только в сейфах. Кроме того, в делах или в архивах конфиденциальные документы должны храниться отдельно от открытых, по завершении оформления дел на последнем листе делается запись о количестве пронумерованных в нем листов, заверенная соответствующей подписью и печатью.	6-10
3.		Отправка конфиденциальных документов	Отправку конфиденциальных документов производить только заказными или ценными письмами, по каналам специальной связи или осуществлять доставку корреспонденции нарочным из числа сотрудников, допущенных к работе с такими документами.	6-10
4.		Этапы создания бумажного делопроизводства при ведении конфиденциального делопроизводства	1 этап - создание Секретариата (подразделения, отвечающего за делопроизводство) или введение в штат должности, в чьи функциональные обязанности будет входить обеспечение делопроизводства организации. 2 этап - закупка необходимых принадлежностей для функционирования делопроизводства (сейфы, печати, оборудование помещений и т.д.). 3 этап - создание необходимых нормативных документов (инструкций, должностных обязанностей и т.д.).	14

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			4 этап - доведение нормативных документов до сотрудников в рамках функциональных обязанностей. 5 этап - создание механизмов контроля за соблюдением делопроизводства. 6 этап - создание механизма ответственности за нарушение правил делопроизводства.	
5.		организационные мероприятия защиты информации	К организационным мероприятиям защиты информации относится комплекс мер правового и управленческого характера, направленных на формирование системы защиты информации в компании, в том числе системы конфиденциального делопроизводства.	6-10
6.	Задания закрытого типа	Основными рисками информационной безопасности являются: 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации	3	4-5
7		К основным принципам обеспечения информационной безопасности относится: 1. Экономической эффективности системы безопасности 2. Многоплатформенной реализации системы 3. Усиления защищенности всех звеньев системы	1	4-5
8		Основными субъектами информационной безопасности являются: 1. руководители, менеджеры, администраторы компаний 2. органы права, государства, бизнеса 3. сетевые базы данных, фаерволлы	2	4-5
9		К основным функциям системы безопасности можно отнести все перечисленное:	1	4-5

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей		
10		Принципом информационной безопасности является принцип недопущения: 1. Неоправданных ограничений при работе в сети (системе) 2. Рисков безопасности сети, системы 3. Презумпции секретности	1	4-5

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения

7.4 Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю)

Максимальное количество баллов за работу в течение 7 семестра: 100 баллов

	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок предоставления
Основной блок				
	Ответ на занятии	4/5	20	по расписанию
	Выполнение практического задания	3/8	24	по расписанию
	Контрольная работа	2/10	20	по расписанию
	Контрольная- блиц	1/7	7	по расписанию
	Деловая игра	1/10	10	по расписанию
	IT-метод	1/9	9	
	Всего		**90**	
Блок бонусов				
	Посещение занятий	9/0.5	4,5	по расписанию
	Своевременное выполнение всех заданий	5/1,1	5,5	по расписанию
	Всего		**Итого: 100 баллов**	

Таблица 11 – Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	0,2
Нарушение учебной дисциплины	0,2
Неготовность к занятию	0,3
Пропуск занятия без уважительной причины	0,3

Таблица 12 – Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	Зачтено
85–89	4 (хорошо)	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	Не зачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Ищейнов В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : рек. УМО по образованию в области историко-архивоведения в качестве учеб. пособия для студентов вузов, обуч. по спец. "Организация и технология защиты информации", "Комплексная защита объектов информации" - М. : ФОРУМ; ИНФРА-М, 2014. - 256 с. (10 экз)

2. Куняев Н.Н., Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев, А.С. Дёмушкин, Т.В. Кондрашова, А.Г. Фабричнов; под общ. ред. Н.Н. Куняева - М. : Логос, 2017. - 500 с. (Новая университетская библиотека) - ISBN 978-5-98704-711-8 - Текст :электронный// ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785987047118.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

3. Галатенко, В.А. Основы информационной безопасности : курс лекций. Рек. УМО в области прикладной информатики в качестве учеб. пособ. для вузов... "Прикладная информатика" / В. А. Галатенко ; под ред. В.Б. Бетелина. - 2-е изд. ; исправ. - М. : ИНТУИТ. РУ, 2004. - 264 с. (37 экз)

4. Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф.-М.:ДМК Пресс, 2014. - http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).

5. Садердинов, А.А. Информационная безопасность предприятия : учеб. пособ. / А. А. Садердинов, Трайнев, В.А., Федулов, А.А. - 2-е изд. - М. : Дашков и К, 2005. - 336 с. (37 экз.)

6. Конституция Российской Федерации // СПС КонсультантПлюс

7. Доктрина информационной безопасности РФ. Утверждена Президентом РФ 09.09.2000. № Пр-1895 // СПС КонсультантПлюс

8. Уголовный Кодекс РФ // СПС КонсультантПлюс

9. Гражданский кодекс РФ. Ч. 4 // СПС КонсультантПлюс

10. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ // СПС КонсультантПлюс

11. Закон РФ «О государственной тайне» // СПС КонсультантПлюс

12. Закон РФ «О безопасности» // СПС КонсультантПлюс

13. Закон РФ «О персональных данных» от 27.07.2006 №152-ФЗ. // СПС КонсультантПлюс

14. Закон РФ «О средствах массовой информации» // СПС КонсультантПлюс

15. Закон РФ «О связи» // СПС КонсультантПлюс

16. Закон РФ «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ.//СПС КонсультантПлюс

17. Закон РФ «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ//СПС КонсультантПлюс

18. Федеральный закон от 22.10.2004 N 125-ФЗ "Об архивном деле в Российской Федерации"//СПС КонсультантПлюс

19. Закон РФ «О техническом регулировании» от 27.12.2002 № 184-ФЗ//СПС КонсультантПлюс

20. Постановление Правительства РФ от 04.09.1995 г. № 870 «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // СПС КонсультантПлюс

21. Постановление Правительства РФ от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти // СПС КонсультантПлюс

22. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» // СПС КонсультантПлюс

23. Указ Президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне» // СПС КонсультантПлюс

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru. *Регистрация с компьютеров АГУ*

2. Единое окно доступа к образовательным ресурсам http://window.edu.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебные аудитории, библиотеки АГУ, компьютерные классы, мультимедийные аудитории.

Программное обеспечение: Microsoft Office.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).