федеральное государственное бюджетное образовательное учреждение
высшего образования
"Красноярский государственный медицинский университет
имени профессора В.Ф. Войно-Ясенецкого"
Министерства здравоохранения Российской Федерации

Медико-психолого-фармацевтический факультет

Кафедра медицинской кибернетики и информатики

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

"Информационная безопасность"

уровень специалитета

очная форма обучения

срок освоения ОПОП ВО - 6 лет

2018 год

федеральное государственное бюджетное образовательное учреждение
высшего образования
"Красноярский государственный медицинский университет
имени профессора В.Ф. Войно-Ясенецкого"
Министерства здравоохранения Российской Федерации

25 июня 2018

РАБОЧАЯ ПРОГРАММА

Дисциплины «Информационная безопасность»

Для ОПОП ВО по специальности 30.05.03 Медицинская кибернетика

Уровень специалитета

Очная форма обучения

Срок освоения ОПОП ВО - 6 лет

Медико-психолого-фармацевтический факультет

Кафедра медицинской кибернетики и информатики

Курс - VI

Семестр - XI

Лекции - 20 час.

Практические занятия - 40 час.

Самостоятельная работа - 48 час.

Зачет - XI семестр

Всего часов - 108

Трудоемкость дисциплины - 3 ЗЕ

2018 год

1. Вводная часть

1.1. Планируемые результаты освоения образовательной программы по дисциплине

Цель освоения дисциплины "Информационная безопасность" состоит в обучении студентов принципам и средствам обеспечения информационной безопасности личности, учреждений, общества, государства.

1.2. Место дисциплины в структуре ОПОП ВО

1.2.1. Дисциплина «Информационная безопасность» относится к блоку «Факультативные дисциплины (модули)».

Информатика, медицинская информатика

Знания: общих сведений об информационных технологиях и их использовании в профессиональной деятельности; основ современных технологий сбора, обработки и представления информации; классификацию современного программного обеспечения; основные составляющие части архитектуры компьютера, их функции

Умения: использовать современные информационно-коммуникационные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) для сбора, обработки и анализа информации; использовать современные информационные технологии для получения доступа к источникам информации, хранения и обработки полученной информации

Навыки: применения в профессиональной деятельности базовых знаний в области естествознания, информатики и современных информационных технологий, подготовки документов различной сложности с использованием большинства возможностей текстового редактора; числовой обработки данных с использованием большинства возможностей электронных таблиц; подготовки иллюстративного графического материала с использованием возможностей программы для создания презентаций и графического редактора

1.3. Требования к результатам освоения дисциплины

1.3.1. Изучение данной дисциплины направлено на формирование у обучающихся следующих общекультурных (ОК), общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

В результате изучения дисциплины обучающиеся должны:

Общие сведения о компетенции ПК-17	
Вид деятельности	научно-исследовательская деятельность
Профессиональная задача	соблюдение основных требований информационной безопасности к разработке новых методов и технологий в области здравоохранения
Код компетенции	ПК-17
Содержание компетенции	способностью к организации и проведению научных исследований, включая выбор цели и формулировку задач, планирование, подбор адекватных методов, сбор, обработку, анализ данных и публичное их представление с учетом требований информационной безопасности
	Знать
1	соблюдение основных требований информационной безопасности к разработке новых методов и технологий в области здравоохранения
	Уметь
1	проводить антивирусную проверку компьютера.
2	выбирать средства обеспечения информационной безопасности компьютера, документа, организации.
3	ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему.
4	применять действующую законодательную базу в области информационной безопасности для обеспечения сферы профессиональной деятельности.
5	пользоваться программным обеспечением, реализующим основные криптографические функции, такие, как системы публичных ключей, электронную подпись, разделение доступа.
6	представлять результаты проделанной учебно-исследовательской работы в форме научного текста (отчета, статьи, доклада).
	Владеть
1	навыками работы с нормативными актами, регулирующими правоотношения в области информации.
2	методами и формами защиты информации.
3	навыками работы с электронной подписью.
4	базовыми технологиями преобразования информации: текстовыми, табличными, мультимедиаредакторами.
	Оценочные средства
1	Вопросы к зачету
2	Вопросы по теме занятия
3	Практические навыки
4	Ситуационные задачи
5	Тесты
6	Примерная тематика рефератов

2. ОСНОВНАЯ ЧАСТЬ
2.1. Объем дисциплины и виды учебной работы

		Семестр
Вид учебной работы	**Всего часов**	**XI**
1	**2**	**3**
Аудиторные занятия (всего), в том числе	60	60
Лекции (Л)	20	20
Практические занятия (ПЗ)	40	40
Из общего числа аудиторных часов – в интерактивной форме*	28 47%	28
Семинарские занятия (СЗ)		
Лабораторные работы (ЛР)		
Внеаудиторная (самостоятельная) работа обучающегося (СР), в том числе:	48	48
Подготовка к занятиям	11	11
Подготовка к тестированию	7	7
Конспектирование источников и другой учебной литературы	2	2
Подготовка презентаций, рефератов	7	7
Выполнение упражнений	9	9
Тестирование в системе дистанционного образования	2	2
Подготовка к викторине или конференции	3	3
Подготовка к промежуточной аттестации	4	4
Подготовка презентации научного проекта	3	3
Вид промежуточной аттестации		**Зачет**
Контактная работа	**60**	
Общая трудоемкость час. **ЗЕ**	**108.0** **3**	**108** **3**

2.2. Разделы дисциплины (модуля), компетенции и индикаторы их достижения, формируемые при изучении

№ раздела	Наименование раздела дисциплины	Темы разделов дисциплины	Код формируемой компетенции	Коды индикаторов достижения компетенций
1	2	3	4	5
1.	Основы информационной безопасности.			
		Введение в информационную безопасность.	ПК-17	ПК-17
		Нормативные акты, регулирующие правоотношения в области информации. Групповая дискуссия.	ПК-17	ПК-17
2.	Принципы обеспечения информационной безопасности.			
		Модели управления доступом. Групповая дискуссия.	ПК-17	ПК-17
		Криптография. Групповая дискуссия. Расчет симметричных и асимметричных шифров.	ПК-17	ПК-17
		Электронная подпись. Групповая дискуссия.	ПК-17	ПК-17
		Шифрованная файловая система. Групповая дискуссия.	ПК-17	ПК-17
		Защищенный документооборот.	ПК-17	ПК-17
		Антивирусы. Межсетевые экраны.	ПК-17	ПК-17
3.	Информационная безопасность человека.			
		Киберпреступность. Информационные войны. Ролевая игра.	ПК-17	ПК-17
		Защита персональных данных. Зачет. Групповая дискуссия. Проект.	ПК-17	ПК-17

2.3. Разделы дисциплины и виды учебной деятельности

			Виды учебной деятельности, включая самостоятельную работу (в часах)					
№ п/п	**№ семестра**	**Наименование раздела дисциплины**	**Л**	**ЛР**	**ПЗ**	**СЗ**	**СР**	**Всего**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1.	11	Основы информационной безопасности.	4		8		9	21
2.	11	Принципы обеспечения информационной безопасности.	6		24		27	57
3.	11	Информационная безопасность человека.	10		8		12	30
		Всего	20		40		48	108

2.4. Тематический план лекций дисциплины

6 курс

11 семестр

№ раздела	№ темы	Наименование раздела	Тема	Количество часов
1	2	3	4	5
1	1	Основы информационной безопасности. [2.00]	**Современное состояние и правовое регулирование сферы информационной безопасности.** ПК-17	2
1	2	Основы информационной безопасности. [2.00]	**Информационная безопасность информационных систем.** ПК-17	2
2	3	Принципы обеспечения информационной безопасности. [2.00]	**Криптографическая защита информации.** ПК-17	2
2	4	Принципы обеспечения информационной безопасности. [2.00]	**Электронная цифровая подпись и ее применение для контроля целостности программ и данных.** ПК-17	2
2	5	Принципы обеспечения информационной безопасности. [2.00]	**Обеспечение информационной безопасности в системах электронного документооборота.** ПК-17	2
3	6	Информационная безопасность человека. [2.00]	**Вредоносное программное обеспечение и методы защиты от него.** ПК-17	2

3	7	Информационная безопасность человека. [2.00]	**Информационная гигиена.** ПК-17	2
3	8	Информационная безопасность человека. [2.00]	**Преступления в сфере компьютерной информации. Понятие о компьютерно-технической экспертизе.** ПК-17	2
3	9	Информационная безопасность человека. [2.00]	**Информационные войны. Информационное неравенство.** ПК-17	2
3	10	Информационная безопасность человека. [2.00]	**Защита персональных данных.** ПК-17	2
			Всего за семестр	**20**
			Всего часов	**20**

2.5. Тематический план практических/семинарских занятий

2.5.1. Тематический план практических занятий

6 курс

11 семестр

№ раздела	№ темы	Наименование раздела	Тема	Количество часов
1	**2**	**3**	**4**	**5**
1	1	Основы информационной безопасности. [4.00]	**Введение в информационную безопасность.** ПК-17	4

1	2	Основы информационной безопасности. [4.00]	**Нормативные акты, регулирующие правоотношения в области информации. Групповая дискуссия.** (В интерактивной форме) ПК-17	4
2	3	Принципы обеспечения информационной безопасности. [4.00]	**Модели управления доступом. Групповая дискуссия.** (В интерактивной форме) ПК-17	4
2	4	Принципы обеспечения информационной безопасности. [4.00]	**Криптография. Групповая дискуссия.** (В интерактивной форме) Расчет симметричных и асимметричных шифров. ПК-17	4
2	5	Принципы обеспечения информационной безопасности. [4.00]	**Электронная подпись. Групповая дискуссия.** (В интерактивной форме) ПК-17	4
2	6	Принципы обеспечения информационной безопасности. [4.00]	**Шифрованная файловая система. Групповая дискуссия.** (В интерактивной форме) ПК-17	4
2	7	Принципы обеспечения информационной безопасности. [4.00]	**Защищенный документооборот.** ПК-17	4
2	8	Принципы обеспечения информационной безопасности. [4.00]	**Антивирусы. Межсетевые экраны.** ПК-17	4
3	9	Информационная безопасность человека. [4.00]	**Киберпреступность. Информационные войны. Ролевая игра.** (В интерактивной форме) ПК-17	4

3	10	Информационная безопасность человека. [4.00]	**Защита персональных данных. Зачет. Групповая дискуссия.** (В интерактивной форме) Проект. ПК-17	4
			Всего за семестр	**40**
			Всего часов	**40**

2.5.2. Тематический план семинарских занятий

Данный вид работы учебным планом не предусмотрен

2.6. Тематический план лабораторных работ

Данный вид работы учебным планом не предусмотрен

2.7. Контроль самостоятельной работы

Данный вид работы учебным планом не предусмотрен

2.8. Самостоятельная работа

2.8.1. Виды самостоятельной работы

6 курс

11 семестр

№ раздела	№ темы	Наименование раздела	Тема	Вид самост.работы	Количество часов
1	2	3	4	5	6
1	1	Основы информационной безопасности. [5.00]	**Введение в информационную безопасность.** ПК-17	Конспектирование источников и другой учебной литературы [2.00], Подготовка к занятиям [2.00], Подготовка к тестированию [1.00]	5
1	2	Основы информационной безопасности. [4.00]	**Информационно-правовые ресурсы.** ПК-17	Подготовка презентаций, рефератов [4.00]	4
2	3	Принципы обеспечения информационной безопасности. [4.00]	**Модели управления доступом.** ПК-17	Выполнение упражнений [1.00], Подготовка к занятиям [2.00], Подготовка к тестированию [1.00]	4
2	4	Принципы обеспечения информационной безопасности. [4.00]	**Криптография.** ПК-17	Выполнение упражнений [2.00], Подготовка к занятиям [1.00], Подготовка к тестированию [1.00]	4
2	5	Принципы обеспечения информационной безопасности. [5.00]	**Электронная подпись.** ПК-17	Подготовка к занятиям [1.00], Подготовка к тестированию [1.00], Подготовка презентаций, рефератов [3.00]	5

2	6	Принципы обеспечения информационной безопасности. [4.00]	**Шифрованная файловая система.** ПК-17	Подготовка к занятиям [2.00], Тестирование в системе дистанционного образования [2.00]	4
2	7	Принципы обеспечения информационной безопасности. [5.00]	**Защищенный документооборот.** ПК-17	Выполнение упражнений [3.00], Подготовка к занятиям [1.00], Подготовка к тестированию [1.00]	5
2	8	Принципы обеспечения информационной безопасности. [5.00]	**Антивирусы. Межсетевые экраны.** ПК-17	Выполнение упражнений [3.00], Подготовка к занятиям [1.00], Подготовка к тестированию [1.00]	5
3	9	Информационная безопасность человека. [5.00]	**Информационные войны.** ПК-17	Подготовка к викторине или конференции [3.00], Подготовка к занятиям [1.00], Подготовка к тестированию [1.00]	5
3	10	Информационная безопасность человека. [7.00]	**Систематизация изученного** ПК-17	Подготовка к промежуточной аттестации [4.00], Подготовка презентации научного проекта [3.00]	7
			Всего за семестр		**48**
			Всего часов		**48**

2.9. Оценочные средства, в том числе для проведения промежуточной аттестации обучающихся по дисциплине

2.9.1. Виды контроля и аттестации, формы оценочных средств

11 семестр					
			Оценочные средства		
№ п/п	Виды контроля	Наименование раздела дисциплины	Форма	Кол-во вопросов в задании	Кол-во независимых вариантов
1	2	3	4	5	6
1	Для входного контроля				
		Основы информационной безопасности.			
			Тесты	15	20
2	Для текущего контроля				
		Основы информационной безопасности.			
			Вопросы по теме занятия	3	5
			Ситуационные задачи	2	5
			Тесты	15	20
		Принципы обеспечения информационной безопасности.			
			Вопросы по теме занятия	3	5
			Ситуационные задачи	2	5
			Тесты	15	20
		Информационная безопасность человека.			
			Вопросы по теме занятия	3	5
			Ситуационные задачи	2	5
			Тесты	15	20
3	Для промежуточного контроля				
			Вопросы к зачету	3	20
			Оценка практических навыков	3	20
			Тесты	50	20

2.9.2. Примеры оценочных средств

Входной контроль

Тесты

1. **НАИБОЛЕЕ РИСКОВАННОЙ ДЛЯ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ С ТОЧКИ ЗРЕНИЯ ВЕРОЯТНОГО МОШЕННИЧЕСТВА И НАРУШЕНИЯ БЕЗОПАСНОСТИ ЯВЛЯЕТСЯ КАТЕГОРИЯ**

1) сотрудники

2) хакеры

3) атакующие

4) контрагенты (лица, работающие по договору)

5) руководство компании

Правильный ответ: 1

ПК-17

2. **ПРИ КЛАССИФИКАЦИИ ДАННЫХ РУКОВОДСТВО ДОЛЖНО**

1) продумать типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

2) продумать необходимый уровень доступности, целостности и конфиденциальности

3) оценить уровень риска и отменить контрмеры

4) продумать управление доступом, которое должно защищать данные

5) снизить уровень классификации информации, чтобы она была всем доступна

Правильный ответ: 2

ПК-17

3. **В КОНЕЧНОМ СЧЕТЕ НЕСЕТ ОТВЕТСТВЕННОСТЬ ЗА ГАРАНТИИ ТОГО, ЧТО ДАННЫЕ КЛАССИФИЦИРОВАНЫ И ЗАЩИЩЕНЫ**

1) владелец данных

2) пользователь

3) администратор

4) руководство

5) сотрудник

Правильный ответ: 4

ПК-17

Текущий контроль

Вопросы по теме занятия

1. **Что включает в себя система информационной безопасности?**

1) Систему информационного законодательства образуют различные законы и издаваемые в соответствии с ними иные нормативные правовые акты, посвященные прямому или опосредованному регулированию отношений, объектом которых является информация, производные от нее продукты и связанная с ними деятельность. Системы информационного законодательства включает в себя правовые акты федеральных органов и органов субъектов РФ. Среди правовых актов федеральных органов главное место занимают федеральные законы. Они обладают высшей юридической силой, регулируют наиболее важные, основополагающие отношения и содержат информационно-равовые нормы исходного характера, которые рассчитаны на постоянное либо длительное действие. Нормативные акты, не относящиеся к категории законов, являются подзаконными. В их число входят нормативные акты Президента РФ, Правительства РФ, ведомственные нормативные акты. Многие из них носят комплексный характер, но включают в себя и правила информационно-правового содержания. Указы Президента РФ – основные акты осуществления компетенции Президента РФ, непосредственно закрепленной в Конституции РФ и вытекающей из основополагающих принципов разделения властей. Правовые акты Правительства РФ издаются главным образом тогда, когда в законе есть на то прямые указания либо дано конкретное поручение Президента РФ. Ведомственные акты издаются на основе законов, указов президента и актов правительства. Они представляют собой управленческие акты органов специальной компетенции. Их юридическая сила зависит от функций издавшего их органа и специфики государственного управления информационной сферой. На уровне субъектов РФ применяются все те же формы выражения информационного права, что и на федеральном уровне (законы субъектов РФ, постановления органов исполнительной власти, акты отраслевых и территориальных органов управления). Наряду с актами законодательства и подзаконными нормативными актами существуют так называемые локальные нормативные акты Они, как правило, представляют собой приказы и распоряжения нормативного и индивидуального значения, принимаемые руководителями различных организаций. С помощью локальных актов регулируются самые различные информационные вопросы, например, порядок конфиденциального делопроизводства, допуска сотрудников к служебной и коммерческой тайнам, порядок организации защиты коммерческой тайны в организации и т. п. В систему информационного законодательства следует включить и международно-правовые акты, предметом регулирования которых являются информационные отношения.

ПК-17

2. **Какой федеральный закон является базовым для информационной сферы?**

1) Среди законов выделяют базовый для информационной сферы федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», пришедший на смену ФЗ от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации».

ПК-17

3. **Какими законами регулируются отношения в информационной сфере?**

1) 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.

ПК-17

Ситуационные задачи

1. **Ситуационная задача №1:** Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1) Какая статья уголовного кодекса была нарушена?

2) Какое наказание должен понести нарушитель?

Ответ 1: Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

Ответ 2: Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

ПК-17

2. **Ситуационная задача №2:** Работник охраны А. завладел ноутбуком, который принадлежал организации, где он работал. Скопировал информацию, относящуюся к коммерческой тайне, затем удалил файл.

1) Каков состав преступления?

2) Какие меры наказания грозят работнику?

Ответ 1: Неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее уничтожение

Ответ 2: Штраф в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет

ПК-17

3. **Ситуационная задача №3:** Работник охраны А. загрузил на рабочий компьютер вирус.

1) Каков состав преступления?

2) Какие меры наказания грозят работнику?

Ответ 1: Распространение вредоносных программ

Ответ 2: Лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы осужденного за период до 18 месяцев.

ПК-17

Тесты

1. **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**

3) «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами»

1) "О коммерческой тайне"

2) "О персональных данных"

3) "О безопасности"

4) "О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации"

5) "О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами"

Правильный ответ: 1

ПК-17

2. **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 ФЗ ОТ 07.07.2003 № 126-ФЗ**

1) О связи

2) О средствах массовой информации

3) О персональных данных

4) О коммерческой тайне

5) О безопасности

Правильный ответ: 1

ПК-17

3. **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 ОПРЕДЕЛЯЕТ ФЗ ОТ 29.11.1994 № 77-ФЗ**

1) О связи

2) О средствах массовой информации

3) О персональных данных

4) О коммерческой тайне

5) Об обязательном экземпляре документов

Правильный ответ: 5

ПК-17

Промежуточный контроль

Вопросы к зачету

1. **Классификация компьютерных преступлений**

1) Несмотря на многообразие компьютерных преступлений, их можно классифицировать по отдельным общим группам. В начале 90-х гг. XX века рабочая группа в рамках Интерпола разработала специальный классификатор. В соответствии с ним все компьютерные преступления классифицированы следующим образом. 1. QA — несанкционированный доступ и перехват: QAH — компьютерный абордаж (несанкционированный доступ); QAI — перехват с помощью специальных технических средств; QAT — кража времени (уклонение от платы за пользование); QAZ — иные виды несанкционированного доступа и перехвата. 2. QD — изменение компьютерных данных: QDL — логическая бомба; GDT — троянский конь; QDV — компьютерный вирус; QDW — компьютерный червь; QDZ — прочие виды данных. 3. QF — компьютерное мошенничество: QFC — мошенничество с банкоматами; QFF — компьютерная подделка; QFG — мошенничество с игровыми автоматами; QFM — манипуляции с программами ввода-вывода; QFP — мошенничество с платежными средствами; QFT — телефонное мошенничество; QFZ — прочие компьютерные мошенничества. В соответствии с УК РФ выделяют следующие преступления в сфере компьютерной информации: Неправомерный доступ к компьютерной информации; Создание, использование и распространение вредоносных компьютерных программ; Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

ПК-17

2. **Межсетевые экраны**

1) Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки. Межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу. Существуют два основных типа межсетевых экранов: межсетевые экраны прикладного уровня и межсетевые экраны с пакетной фильтрацией. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке

запрещенного трафика.

ПК-17

3. **Симметричные методы криптографии**

1) Криптография сегодня по праву считается одним из разделов математики, который занимается разработкой методов и алгоритмов шифрования данных. Преобразование текста из открытого сообщения в шифротекст называется зашифровыванием (шифрацией). Обратное преобразование шифротекста в исходное сообщение назовем расшифровыванием (дешифрацией). Зашифровывание и расшифровывание должно производиться по определенному методу, называемому алгоритмом зашифровывания. Любой конкретный алгоритм содержит некоторый набор параметров, позволяющих всякий раз использовать его для шифрации. Таким образом, для понятий метода и ключа шифрования введем следующие определения. Метод шифрования - это формальный алгоритм, описывающий порядок преобразования исходного сообщения в шифрованное. Ключ шифрования - это набор параметров (данных), необходимых для применения метода. Если при зашифровывании и расшифровывании применялся один и тот же ключ, то такой метод называется симметричным. Существует достаточно много методов симметричного шифрования. Как известно, Юлий Цезарь для связи со своими военачальниками использовал метод подстановки с ключом, равным 3. В исходном сообщении каждый символ заменялся другим символом, от-стоящим от него в алфавите на 3 позиции вправо.

ПК-17

Практические навыки

1. **Создать sfx-архив файла с помощью программы 7-zip**

1) Запустить программу «Пуск – Программы – «7-Zip»; указать путь к папке, где находится файл; выделить указателем мыши файл, подлежащий архивации и нажать кнопку Добавить; в открывшемся окне необходимо уточнить, если нужно, имя архивного файла и поставить галочку "Создать SFX-архив"; нажать кнопку "OK".

ПК-17

2. **Создать электронную подпись заданного текстового фрагмента с помощью программы PGP**

1) Выделить фрагмент текста; скопировать его в буфер обмена; щелкнуть правой кнопкой мыши на значке PGP на панели задач; выбрать пункт "ClipBoardSign"; выбрать владельца электронной подписи; вставить из буфера обмена сформированную электронную подпись после исходного текстового фрагмента.

ПК-17

3. **Определить IP-адрес компьютера**

1) Нажать сочетание клавиш "Win R"; в появившемся окне "Выполнить" написать "cmd"; нажать кнопку "OK"; в появившейся командой строке написать "ipconfig /all".

ПК-17

Тесты

1. **ИНФОРМАЦИЯ В ЭЛЕКТРОННОЙ ФОРМЕ, КОТОРАЯ ПРИСОЕДИНЕНА К ДРУГОЙ ИНФОРМАЦИИ В ЭЛЕКТРОННОЙ ФОРМЕ (ПОДПИСЫВАЕМОЙ ИНФОРМАЦИИ) И КОТОРАЯ ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ЛИЦА, ПОДПИСЫВАЮЩЕГО ИНФОРМАЦИЮ - ЭТО**

1) электронная подпись

2) ключ электронной подписи

3) открытый ключ проверки электронной подписи

4) сертификат открытого ключа электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

ПК-17

2. **НЕКАЯ УНИКАЛЬНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ СИМВОЛОВ, ЗАПИСАННАЯ НА ЭЛЕКТРОННЫЙ НОСИТЕЛЬ (ФЛЭШ-КАРТУ ИЛИ СМАРТ-КАРТУ) - ЭТО**

1) ключ электронной подписи

2) электронная подпись

3) сертификат открытого ключа электронной подписи

4) открытый ключ проверки электронной подписи

5) закрытый ключ электронной подписи

Правильный ответ: 1

ПК-17

3. **ФУНКЦИИ СОЗДАНИЯ И ВЫДАЧИ СЕРТИФИКАТОВ ВОЗЛОЖЕНЫ НА ЮРИДИЧЕСКОЕ ЛИЦО (ИЛИ НА ИНДИВИДУАЛЬНОГО ПРЕДПРИНИМАТЕЛЯ), КРОМЕ ТОГО ВЕДУЩЕЕ РЕЕСТР ВЫДАННЫХ И АННУЛИРОВАННЫХ СЕРТИФИКАТОВ, А ИМЕННО**

1) удостоверяющий центр

2) многофункциональный центр

3) министерство внутренних дел

4) центр выдачи сертификатов

5) паспортную службу

Правильный ответ: 1

ПК-17

2.10. Примерная тематика курсовых работ (проектов)
Данный вид работы учебным планом не предусмотрен

2.11. Перечень практических умений/навыков

6 курс

11 семестр

№ п/п	Практические умения
1	**2**
1	**Базовыми технологиями преобразования информации: текстовыми, табличными, мультимедиаредакторами.** Уровень: Владеть ПК-17
2	**Представлять результаты проделанной учебно-исследовательской работы в форме научного текста (отчета, статьи, доклада).** Уровень: Уметь ПК-17
3	**Методами и формами защиты информации.** Уровень: Владеть ПК-17
4	**Выбирать средства обеспечения информационной безопасности компьютера, документа, организации.** Уровень: Уметь ПК-17
5	**Проводить антивирусную проверку компьютера.** Уровень: Уметь ПК-17
6	**Ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему.** Уровень: Уметь ПК-17
7	**Навыками работы с нормативными актами, регулирующими правоотношения в области информации.** Уровень: Владеть ПК-17
8	**Навыками работы с электронной подписью.** Уровень: Владеть ПК-17
9	**Применять действующую законодательную базу в области информационной безопасности для обеспечения сферы профессиональной деятельности.** Уровень: Уметь ПК-17
10	**Пользоваться программным обеспечением, реализующим основные криптографические функции, такие, как системы публичных ключей, электронную подпись, разделение доступа.** Уровень: Уметь ПК-17

2.12. Примерная тематика рефератов (эссе)

6 курс

11 семестр

№ п/п	Темы рефератов
1	**2**
1	**Формы психологической защиты человека от информационной перегрузки.** ПК-17
2	**Информация как ценность и объект преступных посягательств.** ПК-17
3	**Проблемы информационной безопасности государства.** ПК-17
4	**Принципы адресации в сетях передачи данных. Типы адресов: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя). Понятие о стандарте TCP/IP.** ПК-17
5	**Проблемы информационной безопасности личности.** ПК-17
6	**Средства шифрования данных при передаче по открытым каналам связи. ViPNet.** ПК-17
7	**Опасности «глобализации».** ПК-17
8	**Криптография. История и современность.** ПК-17
9	**Киберпреступность и компьютерные преступления в глобальной сети Интернет. Виды преступлений. Наиболее яркие случаи компьютерных преступлений. Уголовно-правовые меры борьбы.** ПК-17
10	**Информационные войны.** ПК-17

2.13. Учебно-методическое и информационное обеспечение дисциплины

2.13.1. Перечень основной литературы, необходимой для освоения дисциплины

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Вид носителя (электронный/бумажный)
1	**2**	**3**
1	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2019. - 336 с. - Высшее образование. - Текст : электронный. - URL: https://ibooks.ru/reading.php?productid=361272	ЭБС iBooks

2.13.2. Перечень дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Вид носителя (электронный/бумажный)
1	**2**	**3**
1	Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. - 5-е изд., перераб. и доп. - Москва : Юрайт, 2023. - 355 с. - Текст : электронный. - URL: https://urait.ru/viewer/informatika-i-informacionnye-tehnologii-509820#page/1	ЭБС Юрайт
2	Советов, Б. Я. Информационные технологии : учебник для вузов / Б. Я. Советов, В. В. Цехановский. - 7-е изд., перераб. и доп. - М. : Юрайт , 2023. - 327 с. - Текст : электронный. - URL: https://urait.ru/viewer/informacionnye-tehnologii-510751#page/1	ЭБС Юрайт
3	Омельченко, В. П. Медицинская информатика : учебник / В. П. Омельченко, А. А. Демидова. - Москва : ГЭОТАР-Медиа, 2018. - 528 с. - Текст : электронный. - URL: https://www.studentlibrary.ru/ru/book/ISBN9785970443200.html?SSr=07E70614FE60	ЭБС Консультант студента (ВУЗ)
4	Медицинская информатика : учебник / ред. Т. В. Зарубина, Б. А. Кобринский. - 2-е изд., перераб. и доп. - Москва : ГЭОТАР-Медиа, 2022. - 464 с. - Текст : электронный. - URL: https://www.studentlibrary.ru/book/ISBN9785970462737.html	ЭБС Консультант студента (ВУЗ)
5	Обмачевская, С. Н. Медицинская информатика. Курс лекций : учебное пособие для вузов / С. Н. Обмачевская. - 4-е изд., стер. - Санкт-Петербург : Лань, 2022. - 184 с. - Текст : электронный. - URL: https://reader.lanbook.com/m/book/226475#1	ЭБС Лань

2.13.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Порядковый номер	1
Наименование	Лекции по информационной безопасности
Вид	Интернет-ресурс
Форма доступа	http%3A%2F%2Fcourse.secsem.ru%2Flections
Рекомендуемое использование	Для подготовки к занятиям

Порядковый номер	2
Наименование	Информатика для начинающих. Видеолекции
Вид	Интернет-ресурс
Форма доступа	https%3A%2F%2Fwww.youtube.com%2Fplaylist%3Flist%3DPLho0jPYl5RAEDNZnWd-xFfnIDvLJQ7FES
Рекомендуемое использование	Для самостоятельного изучения, подготовки к занятиям

Порядковый номер	3
Наименование	Кибер-безопасность и десять сфер ее применения. Дистанционный курс
Вид	Интернет-ресурс
Форма доступа	https%3A%2F%2Fwww.coursera.org%2Flearn%2Fcyber-security-domain
Рекомендуемое использование	Для подготовки к занятиям, самостоятельного изучения

Порядковый номер	4
Наименование	Единый портал электронной подписи
Вид	Интернет-ресурс
Форма доступа	www.iecp.ru
Рекомендуемое использование	Для самостоятельного изучения, подготовки к занятиям

2.13.4. Карта перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем по специальности 30.05.03 Медицинская кибернетика для очной формы обучения

№ п/п	Вид	Наименование	Режим доступа	Доступ	Рекомендуемое использование
1	2	3	4	5	6
1.	Видеоуроки практических навыков	-/-	-/-	-/-	-/-
2.	Видеолекции				
		Информационная безопасность и защита информации в медицинской организации	https://krasgmu.ru/index.php?page[common]=elib&cat=catalog&res_id=115946	По логину/паролю	Для самостоятельной работы при подготовке к текущему и промежуточному контролю.
3.	Учебно-методический комплекс для дистанционного обучения	-/-	-/-	-/-	-/-
4.	Программное обеспечение				
		ОС Windows, MS 2010, Mozilla Firefox, Google Chrome, PGP, WinRar	Компьютерные классы	По логину/паролю	Выполнение заданий на практических занятиях.

5.	Информационно-справочные системы и базы данных	ЭБС Консультант студента ВУЗ ЭБС Айбукс ЭБС Букап ЭБС Лань ЭБС Юрайт ЭБС MedLib.ru НЭБ eLibrary БД Web of Science БД Scopus ЭМБ Консультант врача Wiley Online Library Springer Nature ScienceDirect (Elsevier) СПС КонсультантПлюс СПС Консультант Плюс	http://www.studmedlib.ru/ https://ibooks.ru/ https://www.books-up.ru/ https://e.lanbook.com/ https://www.biblio-online.ru/ https://www.medlib.ru https://elibrary.ru/ http://webofscience.com/ https://www.scopus.com/ http://www.rosmedlib.ru/ http://search.ebscohost.com/ http://onlinelibrary.wiley.com/ http://journals.cambridge.org/ https://rd.springer.com/ https://www.sciencedirect.com/ http://www.consultant.ru/	По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю По логину/паролю, по IP-адресу По логину/паролю, по IP-адресу По IP-адресу По логину/паролю По IP-адресу По IP-адресу По IP-адресу По IP-адресу По IP-адресу По IP-адресу	Для самостоятельной работы, при подготовке к занятиям

2.13.5. Материально-техническая база дисциплины, необходимая для осуществления образовательного процесса по дисциплине "Информационная безопасность" по специальности 30.05.03 Медицинская кибернетика (очное, высшее образование, 6,00) для очной формы обучения

№ п/п	Наименование	Кол-во	Форма использования
1	2	3	4

	Аудитория №1		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	60	
9	Посадочные места	360	
10	Индукционная система Исток С1и	1	
11	Акустический усилитель и колонки	1	
	Аудитория №2		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	

8	Столы	60	
9	Посадочные места	360	
	Аудитория №3		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	32	
9	Посадочные места	256	
	Лекционный зал лабораторного корпуса		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	

8	Столы	60	
9	Посадочные места	300	
10	Индукционная система Исток С1и	1	
	Лекционный зал морфологического корпуса		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Микрофон	1	
3	Доска	1	
4	Компьютер	1	
5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	100	
9	Посадочные места	350	
10	Индукционная система Исток С1и	1	
11	Акустический усилитель и колонки	1	
	Актовый зал		аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Микрофон	2	
3	Доска	3	
4	Компьютер	1	

5	Колонки	1	
6	Проекционный экран	1	
7	Трибуна	1	
8	Столы	40	
9	Посадочные места	200	
10	Индукционная система Исток С1и	1	
11	Акустический усилитель и колонки	1	
	Компьютерный класс №1 (3-03)		учебная аудитория для проведения занятий семинарского типа, аудитория для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Видеопроектор	1	
2	Комплект учебной мебели, посадочных мест	13	
3	Сетевой сервер	1	
4	Экран	1	
5	Аудиоколонки	1	
6	Доска магнитно-маркерная	1	
7	Персональные компьютеры	12	
	Компьютерный класс №2 (2-103а)		учебная аудитория для проведения занятий семинарского типа, аудитория для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Комплект учебной мебели, посадочных мест	17	
2	Видеопроектор	1	
3	Клавиатура со шрифтом Брайля	1	
4	Локальный сетевой сервер	1	

5	Клавиатура программируемая крупная адаптивная	1	
6	Экран	1	
7	Ресивер для подключения устройств	1	
8	Аудиоколонки	2	
9	Индукционная система Исток С1и	1	
10	Доска магнитно-маркерная	1	
11	Джойстик компьютерный	1	
12	Персональные компьютеры	16	
13	Специализированное ПО: экранный доступ JAWS	1	
	Компьютерный класс №3 (3-46)		учебная аудитория для проведения занятий семинарского типа, аудитория для проведения занятий лекционного типа, для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Комплект учебной мебели, посадочных мест	21	
2	Видеопроектор	1	
3	Локальный сетевой сервер	1	
4	Экран	1	
5	Аудиоколонки	2	
6	Доска магнитно-маркерная	1	
7	Персональные компьютеры	20	
	Компьютерный класс №5 (3-90)		учебная аудитория для проведения занятий семинарского типа, аудитория для групповых и индивидуальных консультаций, для текущего контроля и промежуточной аттестации Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Комплект учебной мебели, посадочных мест	15	
2	Видеопроектор	1	

3	Локальный сетевой сервер	1	
4	Экран	1	
5	Аудиоколонки	1	
6	Персональные компьютеры	14	
	Читальный зал НБ		аудитория для самостоятельной работы Программное обеспечение: Microsoft Windows: 43344704, 60641926, 60641927, 61513487, 61513488, 65459253, 65459265, 69754734, 69754735,V9233887 Microsoft Office: 43344704, 60641927, 61513487, 65459253 Kaspersky Endpoint Security: 13C8-230601-131918-526-1100
1	Проектор	1	
2	Клавиатура со шрифтом Брайля	13	
3	Экран	1	
4	Ноутбук	1	
5	Персональный компьютер	18	
6	Сканирующая и читающая машина CARA CE	1	
7	Столы	30	
8	Посадочные места	43	
9	Индукционная система Исток С1и	1	
10	Головная компьютерная мышь	1	
11	Клавиатура программируемая крупная адаптивная	1	
12	Джойстик компьютерный	1	
13	Принтер Брайля (рельефно-точечный)	1	
14	Специализированное ПО: экранный доступ JAWS	1	
15	Ресивер для подключения устройств	1	

2.14. Образовательные технологии

Используемые образовательные технологии при изучении данной дисциплины: интерактивные технологии, информационно-коммуникационные технологии. 55 % интерактивных часов от объема аудиторных часов. В рамках изучения дисциплины «Информационная безопасность» обучение

студентов производится на лекциях, аудиторных (практических) занятиях, а также в результате самостоятельного изучения отдельных тем. Занятия проводятся с использованием следующих методов обучения: объяснительно-иллюстративный, метод проблемного изложения, эвристический. В рамках изучения дисциплины проводятся следующие разновидности лекций: академическая лекция, лекция-беседа, лекция с разбором конкретных ситуаций. Проводятся следующие разновидности аудиторных (практических) занятий: традиционный, с использованием докладов по вопросам темы занятия, конференция, работа в малых группах, защита презентаций, упражнение, просмотр и обсуждение видеофрагментов. Внеаудиторная (самостоятельная) работа обучающихся включает следующие виды учебной деятельности: конспектирование источников и другой учебной литературы, подготовку презентаций и рефератов, выполнение упражнений, подготовку к тестированию, подготовку к занятиям, подготовку презентации научного проекта.

2.15. Разделы дисциплины и междисциплинарные связи с последующими дисциплинами

		Разделы данной дисциплины, необходимые для изучения последующих дисциплин		
№ п/п	**Наименование последующих дисциплин**	**1**	**2**	**3**
1	Производственная практика (преддипломная практика)	+	+	+

2.16. Методические указания для обучающихся по освоению дисциплины (модуля)

Обучение складывается из аудиторных занятий (60 час.), включающих лекционный курс и практические занятия, и самостоятельной работы (48 час.) Основное учебное время выделяется на работу с нормативными актами, регулирующими правоотношения в области информации, обеспечению мер безопасности в интернете, обществе и учреждении. При изучении дисциплины необходимо освоить практические умения по обеспечению безопасности в интернете, обществе и учреждении. Практические занятия проводятся в виде демонстрации слайдов, решения ситуационных задач, ответов на тестовые задания, отработки практических навыков по работе на ПК. В соответствии с требованиями ФГОС ВО в учебном процессе широко используются активные и интерактивные формы проведения занятий: работа в малых группах, выполнение упражнений. Самостоятельная работа обучающихся подразумевает конспектирование источников и другой учебной литературы, подготовку презентаций и рефератов, выполнение упражнений, подготовку к тестированию, подготовку к занятиям, подготовку презентации научного проекта. Каждый обучающийся обеспечен доступом к библиотечным фондам университета и кафедры. По каждому разделу учебной дисциплины разработаны методические указания для обучающихся и методические рекомендации для преподавателей. Во время освоения учебной дисциплины обучающиеся самостоятельно проводят изучение теоретического материала и выполнение учебных заданий. Исходный уровень знаний обучающихся определяется тестированием, текущий контроль усвоения предмета определяется тестированием, решением ситуационных задач, устным опросом по вопросам к занятиям. В конце изучения учебной дисциплины проводится трехэтапный зачет, включающий тестовый контроль, собеседование и оценку практических навыков.

2.17. Особенности организации обучения по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

1. Обучение инвалидов и лиц с ограниченными возможностями здоровья

по заявлению обучающегося кафедрой разрабатывается адаптированная рабочая программа с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья обучающегося.

2. В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья кафедра обеспечивает:

1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

• размещение в доступных местах и в адаптированной форме справочной информации о расписании учебных занятий для обучающихся, являющихся слепыми или слабовидящими;

• присутствие преподавателя, оказывающего обучающемуся необходимую помощь;

• выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

• надлежащими звуковыми средствами воспроизведения информации;

3) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

• возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры. В случае невозможности беспрепятственного доступа на кафедру организовывать учебный процесс в специально оборудованном помещении (ул. Партизана Железняка, 1, Университетский библиотечно-информационный центр: электронный читальный зал (ауд. 1-20), читальный зал (ауд. 1-21).

3. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

4. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории студентов	Оборудование	Формы
С нарушением слуха	1. Индукционная система Исток с1и	- в печатной форме; - в форме электронного документа;
С нарушением зрения	1. Сканирующая и читающая машина SARA CE; 2. Специализированное ПО: экранный доступ JAWS; 3. Наклейка на клавиатуру со шрифтом Брайля; 4. Принтер Брайля (рельефно-точечный);	- в печатной форме (по договору на информационно-библиотечное обслуживание по межбиблиотечному абонементу с КГБУК «Красноярская краевая специальная библиотека – центр социокультурной реабилитации инвалидов по зрению» №2018/2 от 09.01.2018 (срок действия до 31.12.2022) - в форме электронного документа; - в форме аудиофайла;

С нарушением опорно-двигательного аппарата	1. Специализированный стол; 2. Специализированное компьютерное оборудование (клавиатура программируемая крупная адаптивная, головная компьютерная мышь, джойстик компьютерный);	- в печатной форме; - в форме электронного документа; - в форме аудиофайла;
1. Ресивер для подключения устройств.		