МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Е.Ю. Нагорная
«30» 03 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Борьба с преступлениями в IT-сфере

Уровень образовательной программы бакалавриат

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль) Прикладная информатика в юриспруденции

Форма обучения очная (заочная)

Срок освоения ОП 4 года (4 года 9 месяцев)

Институт Прикладной математики и информационных технологий

Кафедра разработчик РПД Прикладная информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Хапаева Л.Х.

г. Черкесск, 2022 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Борьба с преступлениями в IT - сфере» является формирование у обучающихся необходимых знаний, умений и навыков в области кибербезопасности в автоматизированных информационных системах, знаний основ кибербезопасности и навыков идентификации рисков и управления ими.

При этом задачами дисциплины являются:

- знакомство со структурой государственной системы обеспечения информационной безопасности и основными стандартами по управлению информационной безопасностью; изучение теоретических, методологических и практических проблем в области кибербезопасности автоматизированных информационных систем;
- приобретение практических навыков работы с нормативно-правовыми документами в области обеспечения защиты АИС;
- формирование навыков принятия стратегических решений по обеспечению информационной безопасности в ходе планирования жизненного цикла информационных систем;
- ознакомление с основными угрозами кибербезопасности, правилами их выявления, анализа и формирования требований к разным уровням обеспечения кибербезопасности;
- формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Борьба с преступлениями в IT - сфере» относится к обязательной части, Блока 1. Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1.	Информационная безопасность Использование информационных технологий организации внутренних дел в раскрытии преступлений	Программное обеспечение юридической деятельности

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 09.03.03 Прикладная информатика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:
1	2	3	4
1.	УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач УК-2.3 Использует знания о правовых нормах действующего законодательства, регулирующих отношения в различных сферах жизнедеятельности УК-2.4 Вырабатывает пути решения конкретной задачи, выбирая оптимальный способ ее реализации, исходя из действующих правовых норм и имеющихся ресурсов и ограничений

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы		**Всего часов**	**Семестр**
			№ 7 часов
1		2	3
Аудиторная контактная работа (всего)		42	42
В том числе:			
Лекции (Л)		14	14
Практические занятия (ПЗ)		14	14
Лабораторные работы (ЛР)		14	14
Контактная внеаудиторная работа, в том числе:		2	2
Групповые и индивидуальные консультации		2	2
Самостоятельная работа обучающихся (СРО) (всего)		28	28
Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса		8	8
Выполнение и подготовка к защите лабораторной и практической работы		8	8
Работа с электронным портфолио		6	6
Подготовка к тестированию		6	6
Промежуточная аттестация	Экзамен(Э)	Э	Э
	экзамен (Э) **в том числе:**	36	36
	Прием экз., час.	0,5	0,5
	Консультация, час.	2	2
	СРО, час.	33,5	33,5
ИТОГО: Общая трудоемкость	**часов**	**108**	**108**
	зач. ед.	**3**	**3**

Заочная форма обучения

Вид учебной работы		**Всего часов**	**Семестр**
			№ 7 часов
1		2	3
Аудиторная контактная работа (всего)		12	12
В том числе:			
Лекции (Л)		4	4
Практические занятия (ПЗ), Семинары (С)		4	4
Лабораторные работы (ЛР)		4	4
Контактная внеаудиторная работа, в том числе:		1	1
Групповые и индивидуальные консультации		1	1
Самостоятельная работа обучающихся (СРО) (всего)		86	86
Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса		20	20
Просмотр и конспектирование видеолекций		16	16
Работа с электронным портфолио		16	16
Выполнение и подготовка к защите лабораторной, практической и контрольной работ		18	18
Подготовка к тестированию		16	16
Промежуточная аттестация	Экзамен(Э)	Э	Э
	экзамен (Э) **в том числе:**	9	9
	Прием экз., час.	0,5	0,5
	СРО, час.	8,5	8,5
ИТОГО: Общая трудоемкость	**часов**	**108**	**108**
	зач. ед.	**3**	**3**

4.2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля

Очная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР	ПЗ	СРО	Всего	
1	2	3	4	5	6	7	8
Семестр 7							
1.	Раздел 1. Основные понятия кибербезопасности и информационной безопасности	2			4	6	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе
2.	Раздел 2. Правовые основы кибербезопасности	2	2	2	4	10	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе
3.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	2	2	2	4	10	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе
4.	Раздел 4. Аппаратные и программные средства защиты данных	2	2	2	6	12	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе
5.	Раздел 5. Практические аспекты обеспечения защиты данных	2	4	4	6	16	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе
6.	Раздел 6. Биометрические системы идентификации	4	4	4	4	16	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе
7.	Контактная внеаудиторная работа					2	групповые и индивидуальные консультации
8.	Промежуточная аттестация					36	Экзамен
Итого часов в семестре:		**14**	**14**	**14**	**28**	**108**	
Всего:		**14**	**14**	**14**	**28**	**108**	

Заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР	ПЗ	СРО	Всего	
1	2	3	4	5	6	7	8
Семестр 7							
1.	Раздел 1. Основные понятия кибербезопасности и информационной безопасности	2			14	16	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе, защита контрольной работы
2.	Раздел 2. Правовые основы кибербезопасности		2	2	14	18	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе, защита контрольной работы
3.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации				14	14	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе, защита контрольной работы
4.	Раздел 4. Аппаратные и программные средства защиты данных	2	2	2	14	20	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе, защита контрольной работы
5.	Раздел 5. Практические аспекты обеспечения защиты данных				14	14	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе, защита контрольной работы
6.	Раздел 6. Биометрические системы идентификации				16	16	устный опрос, компьютерное тестирование, отчет по лабораторной и практической работе, защита контрольной работы
7.	Контактная внеаудиторная работа					1	групповые и индивидуальные консультации
8.	Промежуточная аттестация					9	Экзамен
Итого часов в 6 семестре:		**4**	**4**	**4**	**86**	**108**	
Всего:		**4**	**4**	**4**	**86**	**108**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
Семестр 7					
1.	Раздел 1. Основные понятия кибербезопасности и информационной безопасности	Тема 1.1 Основные понятия кибербезопасности и информационной безопасности	Информатизация общества: социальные условия, предпосылки и последствия. Основные понятия информационной безопасности и защиты данных. Целостность, доступность и конфиденциальность информации.	2	2
2.	Раздел 2. Правовые основы кибербезопасности	Тема 2.1 Нормативно-правовые акты в области обеспечения информационной безопасности и кибербезопасности. Виды защищаемой информации.	Нормативно-правовые акты в области обеспечения информационной безопасности и кибербезопасности. Виды защищаемой информации.Виды программного обеспечения. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo). Лицензионное ПО. Правовая охрана программ для ЭВМ и БД. Авторское право. Понятие и виды интеллектуальной собственности. Правовая охрана программ для ЭВМ и БД.	2	

3.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	Тема 3.1 Понятие и классификация угроз безопасности защищаемой информации	Понятие угроз кибербезопасности. Понятие угрозы безопасности защищаемой информации. Источники угроз информационной безопасности и меры по их предотвращению. Риски и угрозы персональным данным. Примеры атак на информационные системы. Нарушители информационной безопасности. Классификация угроз безопасности информации. Общий анализ рисков. Внешние и внутренние угрозы кибербезопасности. Источники угроз информационной безопасности личности. Определение целей защиты данных на предприятии. Случайные угрозы. Угрозы доступности информации. Угрозы нарушения целостности информации. Угрозы конфиденциальности информации. Особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения. Определения угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в компьютерной системе и сети. Источники угроз безопасности информации (по	2	

			рекомендациям ФСТЭК). Модель угроз информационной безопасности и политика информационной безопасности предприятия Политика информационной безопасности предприятия (организации). Уязвимости компьютерных систем и сетей.		
4.	Раздел 4. Аппаратные и программные средства защиты данных	Тема 4.1 Аппаратные и программные средства защиты данных	Понятие и сущность защиты данных. Цели защиты данных	2	2
5.	Раздел 5. Практические аспекты обеспечения защиты данных	Тема 5.1 Практические аспекты обеспечения защиты данных	Восстановление и защита данных. Резервное копирование.	2	
6.	Раздел 6. Биометрические системы идентификации	Тема 6.1 Биометрические системы идентификации	Механизмы идентификации и аутентификации. Способы аутентификации. Понятие биометрической системы. Формирование теоретических знаний и практических навыков анализа возможностей использования средств биометрической идентификации для защиты данных и идентификации пользователей систем при выполнении комплекса практических заданий.	4	
Итого часов в семестре:				**14**	**4**
Всего:				**14**	**4**

4.2.3. Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Наименование лабораторного занятия	Содержание лабораторного занятия	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
Семестр 7					
1.	Раздел 2. Правовые основы кибербезопасности	Правовые основы кибербезопасности	Нормативно-правовые акты в области обеспечения информационной безопасности и кибербезопасности	2	2
2.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	Задание требований к защите информации компьютерной системы. Модель угроз информационной безопасности. Разработка/корректировка политики информационной безопасности в соответствии с базовой моделью угроз ФСТЭК.	2	
3.	Раздел 4. Аппаратные и программные средства защиты данных	Аппаратные и программные средства защиты данных	Создание USB ключа для ограничения доступа к компьютеру средствами ОС WINDOWS. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Аппаратные средства. USB ключ защиты. Формальные средства защиты информации. Физические средства защиты информации. Аппаратные средства защиты информации. Принципы работы и правила эксплуатации программноаппаратных средств защиты данных. Правила и принципы безопасного использования технических и программных средств защиты информации	2	2

4.	Раздел 5. Практические аспекты обеспечения защиты данных	Практические аспекты обеспечения защиты данных	Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных устройств.	4	
5.	Раздел 6. Биометрические системы идентификации	Биометрические системы идентификации	Биометрическая идентификация. Виды биометрических систем. Группы биометрических параметров. Физиологические (статические) группы методов идентификации. Способы построения систем биометрической идентификации личности. Обзор готовых решений. Динамические (поведенческие) методы биометрической идентификации. Перспективы использования биометрических систем	4	
Итого часов в 6 семестре:				**14**	**4**
Всего:				**14**	**4**

4.2.4. Практические занятия

№ п/п	Наименование раздела дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов	
				ОФО	ЗФО
1	2	3	4	5	6
Семестр 7					
1.	Раздел 2. Правовые основы кибербезопасности	Правовые основы кибербезопасности	Нормативно-правовые акты в области обеспечения информационной безопасности и кибербезопасности	2	2
2.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	Разработка/корректировка модели угроз информационной безопасности в соответствии с базовой моделью угроз ФСТЭК.Принципы построения моделей угроз и нарушителей по методике ФСТЭК. Методика определения угроз безопасности информации в информационных системах (согласно методическим рекомендациям ФСТЭК).	2	
3.	Раздел 4. Аппаратные и программные средства защиты данных	Аппаратные и программные средства защиты данных	Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и 2 10 асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны.	2	2
4.	Раздел 5. Практические аспекты обеспечения защиты данных	Практические аспекты обеспечения защиты данных	Защита объектов критической информационной инфраструктуры	4	
5.	Раздел 6. Биометрические системы идентификации	Биометрические системы идентификации	Биометрическая идентификация. Виды биометрических систем. Группы биометрических параметров.	4	

			Физиологические (статические) группы методов идентификации. Способы построения систем биометрической идентификации личности. Обзор готовых решений. Динамические (поведенческие) методы биометрической идентификации. Перспективы использования биометрических систем		
Итого часов в семестре:				**14**	**4**
Всего:				**14**	**4**

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Очная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов ОФО
1	**2**	**3**	**4**	**5**
Семестр 7				
1.	Раздел 1. Основные понятия кибербезопасности и информационной безопасности	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	4
		1.2	Подготовка к текущему контролю (Тестовый контроль)	
		1.3	Составление тематического портфолио	
2.	Раздел 2. Правовые основы кибербезопасности	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	4
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контрольта)	
		1.4	Составление тематического портфолио	
3.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	4
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
4.	Раздел 4. Аппаратные и программные средства защиты данных	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	6
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
5.	Раздел 5. Практические аспекты обеспечения защиты данных	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	6
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
6.	Раздел 6. Биометрические системы идентификации	1.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	4
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль)	
		1.4	Составление тематического портфолио	
Итого часов в семестре:				**28**
Всего:				**28**

Заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов ЗФО
1	**2**	**3**	**4**	**5**
Семестр 7				
1.	Раздел 1. Основные понятия кибербезопасности и информационной безопасности	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	14
		1.2	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.3	Составление тематического портфолио	
2.	Раздел 2. Правовые основы кибербезопасности	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	14
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
3.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	14
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
4.	Раздел 4. Аппаратные и программные средства защиты данных	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	14
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
5.	Раздел 5. Практические аспекты обеспечения защиты данных	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	14
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
6.	Раздел 6. Биометрические системы идентификации	1.1	Работа с лекционным видео материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса	16
		1.2	Выполнение и подготовка к защите лабораторной и практической работы	
		1.3	Подготовка к текущему контролю (Тестовый контроль, Контрольная работа)	
		1.4	Составление тематического портфолио	
Итого часов в семестре:				**86**
Всего:				**86**

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обучение по учебной дисциплине «Борьба с преступлениями в IT - сфере» предполагает изучение дисциплины на аудиторных занятиях и самостоятельную работу обучающихся. Основными видами выполнения аудиторной работы обучающихся по дисциплине являются лекции, лабораторные и практические занятия.

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

С целью обеспечения успешного обучения, обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, знакомит с новым материалом, разъясняет учебные элементы, трудные для понимания, систематизирует учебный материал и ориентирует в учебном процессе. Подготовка к лекционному занятию включает выполнение всех видов заданий размещенных к каждой лекции, т.е. задания выполняются еще до лекционного занятия по соответствующей теме.

В ходе лекционных занятий рекомендуется вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой - в ходе подготовки к лабораторный занятиям изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы. Подготовить тезисы для выступлений по всем учебным вопросам, выносимым на семинар. Готовясь к докладу или реферативному сообщению, обращаться за методической помощью к преподавателю. Составить план-конспект своего выступления. Продумать примеры с целью обеспечения тесной связи изучаемой теории с реальной жизнью. Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих указаний и изучении рекомендованной литературы.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

Ведущей дидактической целью лабораторных занятий является систематизация и обобщение знаний по изучаемой теме, приобретение практических навыков по тому или другому разделу курса, закрепление полученных теоретических знаний. Лабораторные работы сопровождают и поддерживают лекционный курс. Подготовка к лабораторным занятиям и практикумам носит различный характер, как по содержанию, так и по сложности исполнения.

Многие лабораторные занятия требуют большой исследовательской работы, изучения дополнительной научной литературы. Прежде чем приступить к выполнению такой работы, обучающемуся необходимо ознакомиться обстоятельно с содержанием задания, уяснить его, оценить с точки зрения восприятия и запоминания все составляющие его компоненты. Это очень важно, так как при проработке соответствующего материала по конспекту лекции или по рекомендованной литературе могут встретиться определения, факты, пояснения, которые не относятся непосредственно к заданию. Обучающийся должен хорошо знать и понимать содержание задания, чтобы

быстро оценить и отобрать нужное из читаемого. Далее, в соответствии со списком рекомендованной литературы, необходимо отыскать материал к данному заданию по всем пособиям.

Весь подобранный материал нужно хотя бы один раз прочитать или внимательно просмотреть полностью. По ходу чтения помечаются те места, в которых содержится ответ на вопрос, сформулированный в задании. Читая литературу по теме, обучающийся должен мысленно спрашивать себя, на какой вопрос задания отвечает тот или иной абзац прорабатываемого пособия. После того, как материал для ответов подобран, желательно хотя бы мысленно, а лучше всего устно или же письменно, ответить на все вопросы. В случае если обнаружится пробел в знаниях, необходимо вновь обратиться к литературным источникам и проработать соответствующий раздел. Только после того, как преподаватель убедится, что обучающийся хорошо знает необходимый теоретический материал, что его ответы достаточно аргументированы и доказательны, можно считать обучающегося подготовленным к выполнению лабораторных работ.

5.3. Методические указания для подготовки обучающихся к практическим занятиям

В процессе подготовки и проведения практических занятий обучающиеся закрепляют полученные ранее теоретические знания, приобретают навыки их практического применения, опыт рациональной организации учебной работы.

Поскольку активность на практических занятиях является предметом внутри семестрового контроля его продвижения в освоении курса, подготовка к таким занятиям требует ответственного отношения.

При подготовке к занятию в первую очередь должны использовать материал лекций и соответствующих литературных источников. Самоконтроль качества подготовки к каждому занятию осуществляют, проверяя свои знания и отвечая на вопросы для самопроверки по соответствующей теме.

Входной контроль осуществляется преподавателем в виде проверки и актуализации знаний, обучающихся по соответствующей теме.

Выходной контроль осуществляется преподавателем проверкой качества и полноты выполнения задания.

Подготовку к практическому занятию каждый обучающийся должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала, а затем изучение обязательной и дополнительной литературы, рекомендованной к данной теме.

Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса. Результат такой работы должен проявиться в способности обучающегося свободно ответить на теоретические вопросы, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий. Предлагается следующая опорная схема подготовки к практическим занятиям.

Обучающийся при подготовке к практическому занятию может консультироваться с преподавателем и получать от него наводящие разъяснения, задания для самостоятельной работы.

1. Ознакомление с темой практического занятия. Выделение главного (основной темы) и второстепенного (подразделы, частные вопросы темы).

2. Освоение теоретического материала по теме с опорой на лекционный материал, учебник и другие учебные ресурсы. Самопроверка: постановка вопросов, затрагивающих основные термины, определения и положения по теме, и ответы на них.

3. Выполнение практического задания. Обнаружение основных трудностей, их решение с помощью дополнительных интеллектуальных усилий и/или подключения дополнительных источников информации.

5.4. Методические указания по самостоятельной работе обучающихся
Работа с литературными источниками и интернет ресурсами

Самостоятельная работа обучающегося является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Самостоятельная работа обучающегося над усвоением учебного материала может выполняться в библиотеке, учебных кабинетах, компьютерных классах, а также в домашних условиях. Учебный материал учебной дисциплины, предусмотренный рабочим учебным планом для усвоения обучающимся в процессе самостоятельной работы, выносится на итоговый контроль наряду с учебным материалом, который разрабатывался при проведении учебных занятий. Содержание самостоятельной работы обучающихся определяется учебной программой дисциплины, методическими материалами, заданиями и указаниями преподавателя.

Самостоятельная работа обучающихся осуществляется в аудиторной и внеаудиторной формах.

Самостоятельная работа обучающихся в аудиторное время может включать: конспектирование (составление тезисов) лекций; выполнение контрольных работ; решение задач; работу со справочной и методической литературой; работу с нормативными правовыми актами; выступления с докладами, сообщениями на семинарских занятиях; защиту выполненных работ; участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины; участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях; участие в тестировании и др.

Самостоятельная работа обучающихся во внеаудиторное время может состоять из: повторение лекционного материала; изучения электронной, учебной и научной литературы; изучения нормативных правовых актов (в т.ч. в электронных базах данных); решения задач, выданных на лабораторных занятиях; подготовки к контрольным работам, тестированию и т.д.; подготовки к семинарам устных докладов (сообщений); подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя; выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями на их консультациях; проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах рабочей программы дисциплины задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы.

Формой поиска необходимого и дополнительного материала по дисциплине с целью доработки знаний, полученных во время лекций, есть индивидуальные задания для обучающихся. Выполняются отдельно каждым обучающимся самостоятельно под руководством преподавателей. Именно овладение и выяснения обучающимся рекомендованной литературы создает широкие возможности детального усвоения данной дисциплины.

Индивидуальные задания обучающихся по дисциплине осуществляются путем выполнения одного или нескольких видов индивидуальных или научно-исследовательских задач, избираемых обучающимся с учетом его творческих возможностей, учебных достижений и интересов по согласованию с преподавателем, который ведет лекции или семинарские занятия, или по его рекомендации. Он предоставляет консультации, обеспечивает контроль за качеством выполнения задания и оценивает работу.

Индивидуальные задания должны быть представлены преподавателю и (при необходимости) защищены до окончания учебного курса. Виды, тематика, методические

рекомендации и критерии оценки индивидуальных работ определяется отдельными методическими рекомендациями. Результаты выполнения и обсуждения индивидуального задания влияют на выставление итоговой оценки по учебной дисциплине.

5.5 Методические рекомендации по подготовке, написанию и оформлению курсовой работы *(не предусмотрены учебным планом)*

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов	
			ОФО	ЗФО
1	2	3	4	5
Семестр 7				
1.	Раздел 2. Правовые основы кибербезопасности	Мультимедийные технологии	2	2
2.	Раздел 3. Анализ и оценивание угроз кибербезопасности в условиях цифровой трансформации	Технология исследовательского обучения	2	
3.	Раздел 4. Аппаратные и программные средства защиты данных	Командная и групповая работа по индивидуальным заданиям лабораторного практикума с применением компьютерных технологий	2	2
4.	Раздел 5. Практические аспекты обеспечения защиты данных	Устный контроль по вопросам раздела. Практическое закрепление тем раздела на примерах задач практикума.	2	
Итого часов в семестре:			**8**	**4**
Всего:			**8**	**4**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

Список основной литературы

1. Корабельников, С. М. Преступления в сфере информационных отношений : учебное пособие / С. М. Корабельников. — Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2015. — 120 с. — ISBN 978-5-00094-144-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/43237.html
2. Пушкарев, В. П. Защита информационных процессов в компьютерных системах : учебное пособие / В. П. Пушкарев, В. В. Пушкарев. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 131 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/13929.html
3. Чуянов, А. Г. Обеспечение информационной безопасности в компьютерных системах : учебное пособие / А. Г. Чуянов, А. А. Симаков. — Омск : Омская академия МВД России, 2012. — 204 с. — ISBN 978-5-88651-535-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/36015.html
4. Шелухин, О. И. Системы обнаружения вторжений в компьютерные сети : учебное пособие / О. И. Шелухин, А. Н. Руднев, А. В. Савелов. — Москва : Московский технический университет связи и информатики, 2013. — 88 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/63360.html

Список дополнительной литературы

1. Будаковский, Д. С. Выявление и расследование преступлений в сфере компьютерной информации, совершаемых в таможенных органах : монография / Д. С. Будаковский. — Москва : Российская таможенная академия, 2012. — 100 с. — ISBN 978-5-9590-0352-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/69703.html
2. Будаковский, Д. С. Выявление и расследование преступлений в сфере компьютерной информации, совершаемых в таможенных органах : монография / Д. С. Будаковский. — Москва : Российская таможенная академия, 2012. — 100 с. — ISBN 978-5-9590-0352-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/69703.htmlи
3. Учебно-методическое пособие по написанию курсовой работы по дисциплине Защита информационных процессов в компьютерных системах / составители В. А. Мочалов. — Москва : Московский технический университет связи и информатики, 2014. — 20 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/61475.html
4. Горев, А. И. Обработка и защита информации в компьютерных системах: учебно-практическое пособие / А. И. Горев, А. А. Симаков. — Омск: Омская академия МВД России, 2016. — 88 с. — ISBN 978-5-88651-642-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/72856.htmlи
5. Качановский, Ю. П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами : методические указания к проведению лабораторной работы по курсу «Информатика» / Ю. П. Качановский, А. С. Широков. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2014. — 24 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/55120.html

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

http://elibrary.ru - Научная электронная библиотека.

7.3. Информационные технологии, лицензионное программное обеспечение

В компьютерном классе должны быть установлены средства:

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Microsoft Azure Dev Tools for Teaching 1. Windows 7, 8, 8.1, 10	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022 (продление подписки)
Office 2003, 2007, 2010, 2013	Сведения об OpenOffice: 63143487, 63321452, 64026734, 6416302, 64344172, 64394739, 64468661, 64489816, 64537893, 64563149, 64990070, 65615073 Лицензия бессрочная
Антивирус Dr.Web Desktop Security Suite	Лицензионный сертификат Серийный № 8DVG-V96F-H8S7-NRBC Срок действия: с 20.10.2022 до 22.10.2023
Консультант Плюс	Договор № 272-186/С-23-01 от 20.12.2022 г.
ЭБС IPRbooks	Лицензионный договор № 9368/22П от 11.06.2021 г. Срок действия: с 01.07.2022 до 01.07.2023
SumatraPDF	Бесплатное ПО
7-Zip	Бесплатное ПО
1С: Предприятие 8.3 Учебная версия	Бесплатное ПО

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к аудиториям (помещениям, местам) для проведения занятий

1. Учебная аудитория для проведения занятий лекционного типа.

Специализированная мебель:
Кафедра настольная - 1шт., доска меловая - 1шт., стулья - 65шт., парты - 34шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Экран на штативе – 1 шт.
Проектор – 1 шт.
Ноутбук – 1 шт.

2. Лаборатория сетевых технологий. Лаборатория архитектуры ЭВМ.

Специализированная мебель:
Парты - 5шт., стулья - 26шт., доска - 1шт., лаб. столы - 6шт., стол преподавательский - 2шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
ПК – 10 шт.

3. Лаборатория синергетики и фракталов.

Специализированная мебель:
Стол преподавательский - 1шт., стул мягкий - 1шт., доска меловая - 1шт., парты - 10шт., компьютерные столы - 11шт., стулья - 21 шт.,
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Персональный компьютер – 11шт.
Экран рулонный настенный – 1 шт.
Проектор – 1 шт.

4. Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнение курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Специализированная мебель:
Стол преподавательский - 1шт., стул мягкий - 1шт., доска меловая - 1шт., парты - 10шт., компьютерные столы - 11шт., стулья - 21 шт.,
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Персональный компьютер – 11шт.
Экран рулонный настенный – 1 шт.
Проектор – 1 шт.

5. Помещение для самостоятельной работы.
Библиотечно-издательский центр.

Отдел обслуживания печатными изданиями
Специализированная мебель:
Рабочие столы на 1 место – 21 шт.
Стулья – 55 шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации:
Экран настенный – 1 шт.
Проектор – 1шт.
Ноутбук – 1шт.
Информационно-библиографический отдел.
Специализированная мебель:

Рабочие столы на 1 место - 6 шт.
Стулья - 6 шт.
Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ФГБОУ ВО «СевКавГА»:
Персональный компьютер – 1шт.
Сканер – 1 шт.
МФУ – 1 шт.
Отдел обслуживания электронными изданиями
Специализированная мебель:
Рабочие столы на 1 место – 24 шт.
Стулья – 24 шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации:
Интерактивная система - 1 шт.
Монитор – 21 шт.
Сетевой терминал -18 шт.
Персональный компьютер -3 шт.
МФУ – 2 шт.
Принтер –1шт.

8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся
1. Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.
2. Рабочие места обучающихся, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

8.3. Требования к специализированному оборудованию
Нет

9. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается (в случае необходимости) адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья комплектуется фонд основной учебной литературой, адаптированной к ограничению электронных образовательных ресурсов, доступ к которым организован в БИЦ Академии. В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ:
«БОРЬБА С ПРЕСТУПЛЕНИЯМИ В IT - СФЕРЕ»

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Борьба с преступлениями в IT - сфере»

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

2. Этапы формирования компетенции в процессе освоения дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающихся.

Этапность формирования компетенций прямо связана с местом дисциплины в образовательной программе.

Разделы (темы) дисциплины	**Формируемые компетенции (коды)**
	УК-2
Раздел 1. Основные понятия кибербезопасности и информационной безопасности	+
Раздел 2. Правовые основы кибербезопасности	+
Раздел 3. Анализ и оценивание угроз кибербез-опасности в условиях цифровой трансформации	+
Раздел 4. Аппаратные и программные средства защиты данных	+
Раздел 5. Практические аспекты обеспечения защиты данных	+
Раздел 6. Биометрические системы идентификации	+

3.Показатели, критерии и средства оценивания компетенций, формируемых в процессе изучения дисциплины

УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Индикаторы достижения компетенции	**Критерии оценивания результатов обучения**				**Средства оценивания результатов обучения**	
	неудовлетв	**удовлетв**	**хорошо**	**отлично**	**Текущий контроль**	**Промежуточная аттестация**
1	**2**	**3**	**4**	**5**	**6**	**7**
УК-2.2 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Не умеет выполнять задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Частично умеет выполнять задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Хорошо умеет выполнять задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	Отлично умеет выполнять задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач	ОФО: практико-ориентированные задания, защита контрольных работ, вопросы для устного собеседования, компьютерное тестирование ЗФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование, защита контрольных работ	Экзамен
УК-2.3 Использует знания о правовых нормах действующего законодательства, регулирующих отношения в различных сферах	Не умеет использовать знания о правовых нормах действующего законодательства, регулирующих	Частично умеет использовать знания о правовых нормах действующего законодательства, регулирующих	Хорошо умеет использовать знания о правовых нормах действующего законодательства, регулирующих	Отлично умеет использовать знания о правовых нормах действующего законодательств	ОФО: практико-ориентированные задания, защита контрольных работ, вопросы для устного собеседования, компьютерное	Экзамен

жизнедеятельности	отношения в различных сферах жизнедеятельности	отношения в различных сферах жизнедеятельности	отношения в различных сферах жизнедеятельности	а, регулирующих отношения в различных сферах жизнедеятельности	тестирование ЗФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование, защита контрольных работ	
УК-2.4 Вырабатывает пути решения конкретной задачи, выбирая оптимальный способ ее реализации, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	Не владеет способностью вырабатывать пути решения конкретной задачи, выбирая оптимальный способ ее реализации, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	Частично владеет способностью вырабатывать пути решения конкретной задачи, выбирая оптимальный способ ее реализации, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	Показывает хорошие способности в умении вырабатывать пути решения конкретной задачи, выбирая оптимальный способ ее реализации, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	Демонстрирует отличные способности в умении вырабатывать пути решения конкретной задачи, выбирая оптимальный способ ее реализации, исходя из действующих правовых норм и имеющихся ресурсов и ограничений учетом основных требований информационной безопасности	ОФО: практико-ориентированные задания, защита контрольных работ, вопросы для устного собеседования, компьютерное тестирование ЗФО: практико-ориентированные задания, вопросы для устного собеседования, компьютерное тестирование, защита контрольных работ	Экзамен

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к экзамену по дисциплине: «Борьба с преступлениями в IT - сфере»

1. Защита информации. Предмет и объект защиты.
2. Угроза безопасности. Уязвимость системы. Атака.
3. Несанкционированный доступ.
4. Основные методы и средства защиты информации, применяемые в ЭИС.
5. Уязвимость компьютера и сети. Виды угроз.
6. Угроза отказ в обслуживании.
7. Социальная инженерия и ИБ.
8. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
9. Шифрование. Метод подстановки.
10. Матрицы Вижинера.
11. Частотный анализ текстов. Шифрование методом перестановки.
12. Криптосистема с открытым ключом.
13. Симметричные и асимметричные криптосистемы.
14. Электронная цифровая подпись.
15. Использование электронных ключей для организации ИБ.
16. Формирование политики безопасности предприятия (организации).
17. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
18. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
19. Потенциальные угрозы безопасности в сети Интернет. Методы защиты информации в сети Интернет.
20. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
21. Аудит информационной безопасности.
22. Характеристика основных объектов и средств физической защиты, применяемых ведущими зарубежными странами в системе защиты территорий и помещений.
23. Характеристика систем контроля доступа в защищаемые помещения, распространённые за рубежом.
24. Классификация технических средств защиты информации, распространённых на Российском рынке продукции и их особенности.
25. Особенности стеганографической защиты информации.
26. Особенности машинной криптографии.
27. Электронно-цифровая подпись конфиденциальных документов.
28. Антивирусная защита конфиденциальных документов.
29. Централизованное управление жизненным циклом электронных ключей с помощью программного продукта SafeNet Authentication Manager.
30. Централизованное управление жизненным циклом электронных ключей с помощью системы Token Management System.

Задачи к экзамену по дисциплине:
«Борьба с преступлениями в IT - сфере»

1. Зашифруйте сообщение, используя функции MS Excel «НАСТОЯЩИЙ ДРУГ С ТОБОЙ, КОГДА ТЫ НЕ ПРАВ. КОГДА ТЫ ПРАВ, ВСЯКИЙ БУДЕТ С ТОБОЙ» (Марк Твен), используя систему Цезаря со значением ключа соответствующим номеру вашего варианта по журналу учебной группы (например, номер по списку – 5; вариант –5; ключ К = 5).
2. Используя систему Вижинера и функции MS Excel, зашифруйте сообщения «За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами». Ключевое слово «РАДОСТЬ», используя функций MSExcel.
3. Используя систему Вижинера, и функции MS Excel, зашифруйте сообщения «Первые криптографические системы были изобретены в глубокой древности, но не перестали развиваться в наши дни». Ключевое слово «УСПЕХ».
4. Используя систему Вижинера, и функции MS Excel, зашифруйте сообщения «Процесс преобразования открытого текста с целью сделать непонятным его смысл для посторонних называется шифрованием». Ключевое слово «РАДОСТЬ».
5. Используя систему Вижинера, и функции MS Excel, зашифруйте сообщения «За пару секунд компьютер успевает сделать ошибку таких размеров, что сотни людей трудятся над ней месяцами». Ключевое слово «УДАЧА».
6. В приложении MS Excel создать книгу, содержащую пронумерованные символы русского алфавита и зашифровать слово «ГЛАГОЛ» с помощью шифра Цезаря с выбранным ключом. К=15.
7. Зашифровать слово КРИПТОГРАФИЯ, выбрав значение ключа шифрования в соответствии с номером своего варианта по журналу учебной группы.
8. Расшифровать криптограмму «пжйжимл», полученную с помощью шифра Цезаря. К=31. Используйте функции MS Excel.
9. Расшифровать криптограмму «юхъыъхщ», полученную с помощью шифра Цезаря, при значении ключа=13. Используйте функции MS Excel.
10. Расшифровать криптограмму «яюышѐшо», полученную с помощью шифра Цезаря, при значении ключа=16. Используйте функции MS Excel.
11. Расшифровать криптограмму «еъѐъщхмх», полученную с помощью шифра Цезаря. К=22. Используйте функции MS Excel.
12. Зашифровать слово «АЛФАВИТ» с помощью шифра Виженера с ключевым словом «СЫР». Используя функции ВПР при шифровании.
13. Зашифровать вручную свои данные «фамилия имя отчество» по парольной фразе из любого известного классического произведения двумя способами: «символы на символы» и «символы на цифры». Представить матрицы-ключи.
14. Зашифровать и дешифровать открытый текст: P= «*информационная безопасность» с ключом* K= *Фамилия (студента)* методом многоалфавитной подстановки на ключе К.
15. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) принтер – ярйыдеа; 2) винчестер – оивжуююее.
16. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) клавиатура – мыеозввшья; 2) проектор – юхюкцчыл;
17. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) монитор – цьъьчак; 2) ноутбук – юудгйты;
18. Определить ключевое слово шифра Виженера, если известны пары «Открытый текст – шифртекст»: 1) лестница - ьквгхзз; 2) архитектор – мюацдуфюьы;
19. Определить ключ шифрования и дешифровать сообщение, полученное шифром Цезаря: 1) арутуьчн; 2) дьюка.
20. Определить ключ шифрования и дешифровать сообщение, полученное шифром Цезаря: 1) пюынг; 2) омпыж.

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Кафедра «Прикладная информатика»

20_- 20_ учебный год

Экзаменационный билет № 1

по дисциплине: «Борьба с преступлениями в IT - сфере»

для обучающихся направления подготовки 09.03.03 - Прикладная информатика

1. Правовое обеспечение защиты информации
2. Электронная цифровая подпись.
3. Задача: Зашифровать и дешифровать открытый текст: P= «*информационная безопасность» с ключом* K= *Фамилия (студента)* методом многоалфавитной подстановки на ключе K.

Зав. кафедрой Хапаева Л.Х.

Вопросы к устному опросу по дисциплине:
«Борьба с преступлениями в IT - сфере»

1. Методы защиты управление доступом
2. Методы защиты механизмы шифрования
3. Методы защиты противодействие атакам вредоносных программ
4. Методы защиты регламентация
5. Понятие кибербезопасности
6. Компьютерная безопасность
7. Компьютерные преступления
8. Понятие информационных угроз
9. Вредоносное программное обеспечение
10. Понятие киберпреступности. Классификация киберпреступности
11. Хакеры
12. Спам
13. Киберпреступность и Интернет
14. Кибератаки и их типы
15. Похищение паролей
16. Стадии Кибератаки
17. Защита от киберпреступности
18. Шифрование данных
19. Симметричное шифрование
20. Асимметричное шифрование или шифрование открытым ключом
21. ЭЦП
22. Защита документов MS Word. Защита документов MS Excel
23. Архивирование файлов Windows и их защита
24. Вирусы и методы борьбы с ними.
25. Антивирусные программы и пакеты.

Тестовые вопросы и задачи по дисциплине:
«Борьба с преступлениями в IT - сфере»

1._____ - это политика информационной безопасности

2._____ это гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные

3._____это предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы.

4. _____ — это присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации.

5. _____ — это проверка подлинности пользователя по предъявленному им идентификатору.

6. _____ — это проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы.

7. _____ — это свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов.

8. _____ — это степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования.

9. «Уполномоченные серверы» были созданы для решения проблемы _____

10. Битовые протоколы передачи данных реализуются _____на взаимодействия открытых систем

11. Длина исходного ключа у алгоритма шифрования DES (бит) равна _____

12. Длина исходного ключа в ГОСТ 28147-89 (бит) равна _____

13.К основным характеристикам защищаемой информации относится
a) Кодируемость, корректность, целостность
b) Государственность, служебность, доступность
c) Конфиденциальность, целостность и доступность
d) Целостность, защищенность и доступность
e) Угроза безопасности информации это

14. Событие или действие, которое может вызвать изменение функционирования компьютерных систем, связанное с нарушением защищенности обрабатываемой в ней информации
a) Действие, которое может вызвать искажение обрабатываемой информации
b) Событие, которое может послужить потере конфиденциальной информации

c) Событие или действие, которое может вызвать изменение функционирования физического канала связи в компьютерных системах, по которому передается защищаемая информация

15. Уровни правового обеспечения информационной безопасности
a) Международные договоры, подзаконные акты, государственные стандарты, локальные нормативные акты
b) Международные договоры, Федеральные законы, государственные стандарты, Указы Президента РФ
c) Подзаконные акты, государственные стандарты, Постановления Правительства РФ
d) Локальные нормативные акты, письма Арбитражного Суда РФ, международные договоры

16.Комплексная система защиты информации это _____

17. Основные недостатки парольной аутентификации
a) Сложно обеспечить реальную уникальность и сложность каждого вновь выбираемого пользователем пароля
b) Возможность перехвата пароля в открытом виде или его подбора по хеш-значению
c) Возможность получения или смены пароля в результате обмана
d) Все вышеперечисленные недостатки

18.Биометрические характеристики пользователей, которые могут применяться для их аутентификации
a) Отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза
b) Рисунок сетчатки глаза, геометрическая форма и размеры лица
c) Тембр голоса, геометрическая форма и размеры уха
d) Все выше перечисленные биометрические характеристики

19.Двухфакторная аутентификация это _____
a) Метод идентификации пользователя в каком-либо сервисе при помощи запроса всевозможных аутентификационных данных
b) Система доступа, основанная на двух «ключах»: одним владеет сам пользователь, например, это телефон, на который приходит SMS с кодом, другой – это его обычные логин и пароль
c) Процедура прохождения алгоритма аутентификации строго в два этапа
d) Один из способов защиты информации от несанкционированного доступа, требующий помимо основного пароля и биометрические данные пользователя

20.В основе работы протокола S/Key лежит _____
a) Протокол PAP для аутентификации пользователей на основе встроенной базы данных одноразовых паролей
b) Протокол PAP, который не может существовать без S/Key
c) Лежит процедура аутентификации по биометрическим характеристикам
d) Протокол, определяющий пользователя при помощи специальных аппаратных средств (смарт-карты, USB-токенов и т.д.)

4. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство _____

5. Восстановление данных является дополнительной функцией услуги защиты_____

6. Назовите виды электронной цифровой подписи, определенные в ФЗ «Об электронной подписи»_____

7. Перечислите комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей._____

8. Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается:_____

9. Вставьте пропущенное слово: Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ называется_____

10. Согласно следующим методам шифрования информации, шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите _____

11. Какой вид собственного обеспечения системы защиты информации включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы?
a. аппаратное обеспечение
b. организационное обеспечение
c. информационное обеспечение
d. правовое обеспечение

12. Безопасность информации – это
a. создание компьютерных вирусов, в качестве которых выступают специально; разработанные программы, начинающие работать только по определенному сигналу;
b. познание окружающего мира, включающее формирование представлений о структуре окружающей среды;
c. способность системы ее обработки обеспечить в заданный промежуток времени возможность выполнения заданных требований по величине вероятности наступления событий, выражающихся в утечке, модификации или утрате данных, представляющих ту или иную ценность для их владельца

13. Основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз является _____

Задания к контрольной работе по дисциплине:
«Борьба с преступлениями в IT - сфере»

1 вариант

1. Концептуальная модель защиты информации при защищенном документообороте.
2. Формирование и хранение дел, содержащих конфиденциальные документы.

2 вариант

1. Проверка наличия конфиденциальных документов.
2. Порядок комплектования ведомственного архива и классификация хранилищ документов.

3 вариант

1. Научно-справочный аппарат к архивам конфиденциальных документов
2. Машиноориентированная содержания и форм конфиденциальных документов

4 вариант

1. Локальная и комплексная автоматизация процессов обработки конфиденциальных документов в документационной службе
2. Состав конфиденциальных документов вычислительного центра, их обработка и хранение

5 вариант

1. Домашинная и послемашинная технология выполнения операций по блокам: блока подготовки и издания конфиденциальных документов, справочно-информационного блока, блока оперативного хранения и использования конфиденциальных документов.
2. Принципы аналитической работы с людьми, обладающими конфиденциальной информацией.

6 вариант

1. Характеристика основных объектов и средств физической защиты, применяемых ведущими зарубежными странами в системе защиты территорий и помещений.
2. Особенности стенографической защиты информации.

7 вариант

1. Характеристика систем контроля доступа в защищаемые помещения, распространённые за рубежом.
2. Особенности машинной криптографии.

8 вариант

1. Классификация технических средств защиты информации, распространённых на Российском рынке продукции и их особенности.
2. Электронно-цифровая подпись конфиденциальных документов.

9 вариант

1. Антивирусная защита конфиденциальных документов.
2. Долгосрочное хранение: подготовка конфиденциальных дел, архивное хранение, подготовка и порядок уничтожения конфиденциальных документов.

10 вариант

1. Виды юридической ответственности за разглашение и незаконное получение конфиденциальной информации.
2. Анализ информационных ресурсов и оптимизация информационных потоков по защите конфиденциальной информации на предприятии.

5. Методические материалы, определяющие процедуры оценивания компетенции

5.1 Критерии оценивания качества выполнения лабораторного практикума

Оценка **«зачтено»** выставляется обучающемуся, если лабораторная работа выполнена правильно и обучающийся ответил на все вопросы, поставленные преподавателем на защите.

Оценка **«не зачтено»** выставляется обучающемуся, если лабораторная работа выполнена не правильно или обучающийся не проявил глубоких теоретических знаний при защите работы

5.2 Критерии оценивания качества выполнения практического практикума

Оценка **«зачтено»** выставляется обучающемуся, если практическая работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Оценка **«не зачтено»** выставляется обучающемуся, если практическая работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов

5.3 Критерии оценивания качества устного ответа

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка **«хорошо»** – за твердое знание основного (программного) материала, за грамотные, без существенных неточностей ответы на поставленные вопросы.

Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала.

Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в материале, за незнание основных понятий дисциплины.

5.4 Критерии оценивания тестирования

При тестировании все верные ответы берутся за 100%.
90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно
менее 60% неудовлетворительно

5.5 Критерии оценивания выполнения контрольной работы

Оценка **«отлично»** выставляется при условии, что обучающийся полностью выполнил задание контрольной и проявил отличные знания учебного материала. При этом работа оформлена в соответствии с требованиями и ГОСТом, к ней можно предъявить минимум замечаний.

Оценка **«хорошо»** ставится тогда, когда обучающийся выполнил все задания, показал хорошие знания по пройденному материалу, но не сумел обосновать предложенные решения задач, когда есть недочеты в оформлении контрольной работы и общие небольшие замечания, не влияющие на ее качество.

Оценку **«удовлетворительно»** обучающийся получает за полностью выполненное задание контрольной при наличии в ней существенных неточностей и недочетов, не умении обучающимся верно применить полученные знания, в оформлении работы есть нарушения ГОСТ, не аргументированные ответы, неактуальные или ненадежные источники информации.

Оценку **«неудовлетворительно»** обучающийся получает в том случае, когда он не полностью выполнил задание проявил недостаточный уровень знаний, не смог объяснить полученные результаты. Такая контрольная работа не отвечает требованиям, содержит противоречивые сведения, задачи в ней решены неверно.

5.6 Критерии оценивания результатов освоения дисциплины на экзамене

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, содержащегося в основных и дополнительных рекомендованных литературных источниках, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы, за умение анализировать изучаемые явления в их взаимосвязи и диалектическом развитии, применять теоретические положения при решении практических задач.

Оценка **«хорошо»** – за твердое знание основного (программного) материала, включая расчеты (при необходимости), за грамотные, без существенных неточностей ответы на поставленные вопросы, за умение применять теоретические положения для решения практических задач.

Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала, за слабое применение теоретических положений при решении практических задач.

Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в расчетах, за незнание основных понятий дисциплины.