МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Г.Ю. Нагорная
«30» 03 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства обеспечения безопасности информационных систем

Уровень образовательной программы магистратура

Направление подготовки 09.04.03 Прикладная информатика

Направленность (профиль) Прикладная информатика в экономике и управлении

Форма обучения очная (очно-заочная, заочная)

Срок освоения ОП 2 года (2 года 3 месяца, 2 года 6 месяцев)

Институт Цифровых технологий

Кафедра разработчик РПД Прикладная информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института ЦТ _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Хапаева Л.Х.

г. Черкесск, 2023 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Методы и средства обеспечения безопасности информационных систем» является формирование у обучающихся фундаментальных знаний защиты информации, связанных с созданием и изучением современных защищенных информационных систем различного применения и степени сложности, предотвращением ущерба пользователю информации, и современных методов и инструментальных средств прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов, различных научных подходов в автоматизации информационных процессов и информатизации предприятий и организаций в экономике.

При этом задачами дисциплины являются:

- изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;
- изучение современных технологий построения безопасных информационных систем;
- изучение этапов и технологий проектирования и создания безопасных информационных систем;
- изучение современных программных и аппаратных средств защиты информации;
- изучение основных угроз информации в современных информационных системах и сетях;
- изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей;
- формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации;
- формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Методы и средства обеспечения безопасности информационных систем» относится к вариативной части Блока 1 дисциплины по выбору обучающегося (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

Предшествующие дисциплины	Последующие дисциплины
Комплексная информационная безопасность	Информационное общество и проблемы прикладной информатики

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

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

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:
1	2	3	4
1.	ПК-2	способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	ПК-2.1 Анализирует применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике ПК-2.2 Разрабатывает и применяет математические модели в области проектирования и управления информационными системами ПК-2.3 Анализирует и оценивает угрозы информационной безопасности; применяет отечественные и зарубежные стандарты в области компьютерной безопасности.
2	ПК-5	Способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	ПК-5.1 Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем ПК-5.2 Выбирает и использует облачные сервисы для решения прикладных задач различных классов и создания информационных систем ПК-5.3 Выявляет и анализирует риски информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ
Очная форма обучения

Вид учебной работы		**Всего часов**	**Семестры**
			№ 3
			часов
1		2	3
Аудиторная контактная работа (всего)		**48**	**48**
В том числе:			
Лекции (Л)		16	16
Практические занятия (ПЗ)		16	16
Лабораторные работы (ЛР)		16	16
Контактная внеаудиторная работа		**1,5**	**1,5**
В том числе индивидуальные и групповые консультации		1,5	1,5
Самостоятельная работа обучающегося (СРО) (всего)		**58**	**58**
Работа с книжными источниками		14	14
Работа с электронными источниками		14	14
Подготовка к практическим занятиям		10	10
Подготовка к контрольной работе		2	2
Подготовка к тестированию		4	4
Доклад		4	4
Подготовка к текущему контролю (ПТК)		10	10
Подготовка к промежуточному контролю (ППК)			
Промежуточная аттестация	Зачет с оценкой	ЗаО	ЗаО
	Прием зач., час	0,5	0,5
ИТОГО: Общая трудоемкость	**часов**	**108**	**108**
	Зачетных единиц	**3**	**3**

Очно-заочная форма обучения

Вид учебной работы		Всего часов	Семестры
			№ 1
			часов
1		2	3
Аудиторная контактная работа (всего)		**48**	**48**
В том числе:			
Лекции (Л)		16	16
Практические занятия (ПЗ)		16	16
Лабораторные работы (ЛР)		16	16
Контактная внеаудиторная работа		**1,5**	**1,5**
В том числе: индивидуальные и групповые консультации		1,5	1,5
Самостоятельная работа студента (СРС) (всего)		**58**	**58**
Работа с книжными источниками		14	14
Работа с электронными источниками		14	14
Доклад		6	6
Подготовка к тестированию		10	10
Подготовка к контрольной работе		4	4
Подготовка к текущему контролю (ПТК)		4	4
Подготовка к промежуточному контролю (ППК)		4	4
Промежуточная аттестация	Зачет с оценкой	ЗаО	ЗаО
	Прием зач., час	0,5	0,5
ИТОГО: Общая трудоемкость	**часов**	**108**	**108**
	Зачетных единиц	**3**	**3**

Заочная форма обучения

Вид учебной работы		Всего часов	Семестры
			№ 1
			часов
1		2	3
Аудиторная контактная работа (всего)		**10**	**10**
В том числе:			
Лекции (Л)		4	4
Практические занятия (ПЗ), Семинары (С)		6	6
Лабораторные работы (ЛР)		-	-
Внеаудиторная контактная работа		**1**	**1**
В том числе: индивидуальные и групповые консультации		1	1
Самостоятельная работа студента (СРС) (всего)		**93**	**93**
Работа с книжными источниками		14	14
Работа с электронными источниками		14	14
Доклад		6	6
Подготовка к тестированию		24	24
Подготовка к контрольной работе		12	12
Подготовка к текущему контролю (ПТК)		9	9
Подготовка к промежуточному контролю (ППК)		14	14
Промежуточная аттестация	Зачет с оценкой	ЗаО	ЗаО
	Прием зач., час	0,5	0,5
	СРО	3,5	3,5
ИТОГО: Общая трудоемкость	**часов**	**108**	**108**
	Зачетных единиц	**3**	**3**

4.2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Очная форма обучения

№ п/п	№ семестра	Наименование раздела дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации)
			Л	ЛР	ПЗ	СР	Всего	
1	2	3	4	5	6	7	8	9
1.	3	Системы криптографической защиты.	2	2	2	12	18	Устный опрос, контрольная работа доклад, тестирование
2.	3	Средства стенографической защиты информации	2	2	2	12	18	
3.	3	Программно-аппаратные средства обеспечения безопасности информационных систем	2	2	2	12	18	
4.	3	Стеганографические средства в ОС Linux и ОС Windows. Файловая система StegFS	2	2	2	12	18	
5.	3	Защита файлов, контроль доступа, уязвимость паролей.	2	2	2	10	16	
6.	3	Встраиваемые водяные знаки. DRM.	2	2	2		18	
7.	3	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	4	4	4		24	
8.	3	Внеаудиторная контактная работа					1,5	Индивидуальные и групповые консультации
9.	3	Промежуточная аттестация.					0,5	Зачет с оценкой
Итого:			**16**	**16**	**16**	**58**	**108**	

Очно-заочная форма обучения

№ п/п	№ семестра	Наименование раздела дисциплины	Виды учебной деятельности, включая самостоятельную работу студентов (в часах)	Формы текущей и промежуточной аттестации)

			Л	ЛР	ПЗ	СРО	Всего	
1	1	3	4	5	6	7	8	9
1.	3	Системы криптографической защиты.	4	4	4	12	24	Устный опрос, текущий тестовый контроль
2.		Средства стенографической защиты информации	4	4	4	12	24	Контрольная работа, текущий тестовый контроль
3.		Программно-аппаратные средства обеспечения безопасности информационных систем	4	4	4	12	24	Устный опрос, текущий тестовый контроль
4.		Стеганографические средства в ОС Linux и ОС Windows. Файловая система StegFS	2	2	2	12	18	Доклад, презентации, текущий тестовый контроль
5.		Защита файлов, контроль доступа, уязвимость паролей.	2	2	2	10	16	Устный опрос, доклад текущий тестовый контроль
6.		Внеаудиторная контактная работа					1,5	Индивидуальные и групповые консультации
7.		Промежуточная аттестация.					0,5	Зачет с оценкой
Итого:			**16**	**16**	**16**	**58**	**108**	

Заочная форма обучения

№ п/п	**№ семестра**	**Наименование раздела дисциплины**	**Виды учебной деятельности, включая самостоятельную работу студентов (в часах)**					**Формы текущей и промежуточной аттестации*)***
			Л	**ЛР**	**ПЗ**	**СРО**	**Всего**	
1	1	3	4	5	6	7	8	9
1.	2	Системы криптографической защиты.	2		2	12	26	Устный опрос, текущий тестовый контроль

2.		Средства стенографической защиты информации	2		2	12	26	Контрольная работа, текущий тестовый контроль
3.		Программно-аппаратные средства обеспечения безопасности информационных систем			2	12	24	Устный опрос, текущий тестовый контроль
4.		Стеганографические средства в ОС Linux и ОС Windows. Файловая система StegFS				12	12	Доклад, презентации, текущий тестовый контроль
5.		Защита файлов, контроль доступа, уязвимость паролей.				45	10	Устный опрос, доклад текущий тестовый контроль
6.		Встраиваемые водяные знаки. DRM.					1	Индивидуальные и групповые консультации
7.		Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.					0,5	Зачет с оценкой
Итого:			**4**		**6**	**93**	**108**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы Лекции	Содержание лекции	Всего часов		
				офо	озфо	зфо
1	2	3	4	5	6	7
Семестр 3						
1.	Системы криптографической защиты.	Системы аппаратной и программной криптографической защиты.	Угрозы безопасности информации, АС и субъектов информационных отношений, источники угроз безопасности, классификация угроз безопасности, основные преднамеренные и непреднамеренные искусственные угрозы.	4	4	2
2.	Средства стенографической защиты информации	Средства стенографической и криптографической защиты информации	Уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ. Информационная инфраструктура. Причины уязвимости ИС.	4	4	2

3.	Программно-аппаратные средства обеспечения безопасности информационных систем	Классификация каналов проникновения в систему и утечки информации.	Прямые и косвенные каналы проникновения в систему и утечки информации. Физические, электромагнитные, информационные каналы.	2	2	
4.	Стеганографические средства в ОС Linux и ОС Windows. Файловая система StegFS	Основные защитные механизмы операционной системы семейства ОС Unix и ОС Windows.	Идентификация и аутентификация пользователя при входе в систему; разграничение прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа; аудит. Принципиальные недостатки защитных механизмов операционной системы семейства ОС Unix и ОС Windows.	2	2	
5.	Защита файлов, контроль доступа, уязвимость паролей.	Защита файлов, контроль доступа, уязвимость паролей.	Сервисы безопасности. Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры. Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Дополнительная информация и итоговые рекомендации по защите открытых ИС. Встраиваемые водяные знаки. DRM.	2	2	
6.	Система безопасности ОС	Windows и Unix	Параметры безопасности. Настройка операционной системы. Права пользователей и система управления доступом. Квалификация пользователей. Средства защиты.	2		
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	Обеспечение надежности и бесперебойного функционирования информационных систем	Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении. Сетевые вирусы. Виды		2	

			угроз ресурсам интранета и Интернета.			
Итого часов в семестре				**16**	**16**	**4**

4.2.3. Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Наименование темы лабораторного практикума	Содержание	Всего часов		
				офо	оз фо	зфо
1	2	3	4	5	6	7
Семестр 3						
8.	Системы криптографической защиты.	Системы аппаратной и программной криптографической защиты.	Угрозы безопасности информации, АС и субъектов информационных отношений, источники угроз безопасности, классификация угроз безопасности, основные преднамеренные и непреднамеренные искусственные угрозы.	4	4	
9.	Средства стенографической защиты информации	Средства стенографической и криптографической защиты информации	Уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ. Информационная инфраструктура. Причины уязвимости ИС.	4	4	
10.	Программно-аппаратные средства обеспечения безопасности информационных систем	Классификация каналов проникновения в систему и утечки информации.	Прямые и косвенные каналы проникновения в систему и утечки информации. Физические, электромагнитные, информационные каналы.	2	2	
11.	Стеганографические средства в ОС Linux и ОС Windows. Файловая система StegFS	Основные защитные механизмы операционной системы семейства ОС Unix и ОС Windows.	Идентификация и аутентификация пользователя при входе в систему; разграничение прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа; аудит. Принципиальные недостатки защитных механизмов операционной системы семейства ОС Unix и ОС Windows.	2	2	
12.	Защита файлов, контроль доступа, уязвимость паролей.	Защита файлов, контроль доступа, уязвимость паролей.	Сервисы безопасности. Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры. Аутентификация в сетях: обычные и одноразовые пароли; серверы	2	2	

			аутентификации. Дополнительная информация и итоговые рекомендации по защите открытых ИС. Встраиваемые водяные знаки. DRM.			
13.	Система безопасности ОС	Windows и Unix	Параметры безопасности. Настройка операционной системы. Права пользователей и система управления доступом. Квалификация пользователей. Средства защиты.	2	2	
Итого часов в семестре				**16**	**16**	

4.2.4. Практические занятия

№ п/п	Наименование раздела дисциплины	Наименование практического занятия	Содержание практического занятия	Всего часов		
				офо	озфо	зфо
1	2	3	4	5	6	7
Семестр 3						
1.	Системы криптографической защиты.	Каналы утечки информации данных. Обзор программ Страж NT, Secret Net	Страж NT, Secret Net	4	4	2
2.	Средства стенографической защиты информации	Особенности работы программ Аккорд-АМДЗ 5.5, Электронный замок «Соболь»	Аккорд-АМДЗ 5.5, Электронный замок «Соболь»	4	4	2
3.	Программно-аппаратные средства обеспечения безопасности информационных систем	Технологии аутентификации и шифрования	Защищенная среда информационного обмена VipNet	4	4	2
4.	Стеганографические средства в ОС Linux и ОС Windows.	Средства для защиты объектов ВТ	Средства для защиты объектов ВТ от утечки по каналам ПЭМИН на линии электропитания	4	4	
ИТОГО часов в семестре:				**16**	**16**	**6**

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Очная форма обучения

№ п/п	**Наименование раздела (темы) дисциплины**	**№ п/п**	**Виды СРО**	**Всего часов**
1	3	4	5	6
Семестр 3				

1.	Системы криптографической защиты.	1.1.	Работа с книжными источниками Работа с электронными источниками	12
2.	Средства стенографической защиты информации	2.1.	Подготовка к практическим занятиям Подготовка к текущему контролю	12
3.	Программно-аппаратные средства обеспечения безопасности информационных систем	3.1.	Подготовка доклада	12
4.	Стеганографические средства в ОС Linux и ОС Windows.	4.1	Подготовка к контрольной работе	12
5.	Защита файлов, контроль доступа, уязвимость паролей.	5.1	Итоговый тестовый контроль	10
6.	Встраиваемые водяные знаки. DRM.	6.1		
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	7.1		
ИТОГО часов за год:				**58**

Очно-заочная форма обучения

№ п/п	**Наименование раздела (темы) дисциплины**	**№ п/п**	**Виды СРО**	**Всего часов**
1	3	4	5	6
Семестр 3				
3.	Системы криптографической защиты.	1.1.	Работа с книжными источниками Работа с электронными источниками	12
4.	Средства стенографической защиты информации	2.1.	Подготовка к практическим занятиям Подготовка к текущему контролю	12
3.	Программно-аппаратные средства обеспечения безопасности информационных систем	3.1.	Подготовка доклада	12

4.	Стеганографические средства в ОС Linux и ОС Windows.	4.1	Подготовка к контрольной работе	12
5.	Защита файлов, контроль доступа, уязвимость паролей.	5.1	Итоговый тестовый контроль	10
6.	Встраиваемые водяные знаки. DRM.	6.1		
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	7.1		
ИТОГО часов за год:				**58**

Заочная форма обучения

№ п/п	**Наименование раздела (темы) дисциплины**	**№ п/п**	**Виды СРО**	**Всего часов**
1	3	4	5	6
Семестр 3				
5.	Системы криптографической защиты.	1.1.	Работа с книжными источниками Работа с электронными источниками	12
6.	Средства стенографической защиты информации	2.1.	Подготовка к практическим занятиям Подготовка к текущему контролю	12
3.	Программно-аппаратные средства обеспечения безопасности информационных систем	3.1.	Подготовка доклада	12
4.	Стеганографические средства в ОС Linux и ОС Windows.	4.1	Подготовка к контрольной работе	12
5.	Защита файлов, контроль доступа, уязвимость паролей.	5.1	Итоговый тестовый контроль	45
6.	Встраиваемые водяные знаки. DRM.	6.1		

7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	7.1		
ИТОГО часов за год:				**93**

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

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

Обучающимся на лекции необходимо:

- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;
- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;
- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

На лекциях рекомендуется деятельность обучающегося в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания темы и рекомендуется конспектирование основных положений лекции.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

В начале семестра обучающиеся получают сводную информацию о формах проведения занятий и формах контроля знаний.

Подготовка к лабораторным занятиям предполагает предварительную самостоятельную работу обучающихся в соответствии с методическими разработками по каждой запланированной теме.

Лабораторные занятия позволяют интегрировать теоретические знания и формировать практические умения и навыки обучающихся в процессе учебной деятельности. Структура и последовательность занятий: на первом, вводном, занятии проводится инструктаж обучающихся по охране труда, технике безопасности и правилам работы в лаборатории по инструкциям утвержденного образца с фиксацией результатов в журнале инструктажа. Обучающиеся также знакомятся с основными требованиями преподавателя по выполнению учебного плана, с графиком прохождения лабораторных занятий, с графиком прохождения контрольных заданий, с основными формам отчетности по выполненным работам.

5.3. Методические указания для подготовки обучающихся к практическим занятиям

Подготовка к практическим занятиям

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. На основе индивидуальных предпочтений

обучающемуся необходимо самостоятельно выбрать тему доклада по проблеме семинара и по возможности подготовить по нему презентацию.

Если программой дисциплины предусмотрено выполнение практического задания, то его необходимо выполнить с учетом предложенной инструкции (устно или письменно). 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 семинара, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

5.4. Методические указания по самостоятельной работе обучающихся

Работа с литературными источниками и интернет ресурсами

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

Подготовка доклада

Презентация, согласно толковому словарю русского языка Д.Н. Ушакова: «… способ подачи информации, в котором присутствуют рисунки, фотографии, анимация и звук». Для подготовки презентации рекомендуется использовать: PowerPoint, MS Word, Acrobat Reader. Самая простая программа для создания презентаций – Microsoft PowerPoint. Для подготовки презентации необходимо собрать и обработать начальную информацию.

Последовательность подготовки презентации:

1. Четко сформулировать цель презентации: вы хотите свою аудиторию мотивировать, убедить, заразить какой-то идеей или просто формально отчитаться.
2. Определить каков будет формат презентации: живое выступление (тогда, сколько будет его продолжительность) или электронная рассылка (каков будет контекст презентации).
3. Отобрать всю содержательную часть для презентации и выстроить логическую цепочку представления.
4. Определить ключевые моменты в содержании текста и выделить их.
5. Определить виды визуализации (картинки) для отображения их на слайдах в соответствии с логикой, целью и спецификой материала.
6. Подобрать дизайн и форматировать слайды (количество картинок и текста, их расположение, цвет и размер).
7. Проверить визуальное восприятие презентации.

К видам визуализации относятся иллюстрации, образы, диаграммы, таблицы. Иллюстрация - представление реально существующего зрительного ряда. Образы – в

отличие от иллюстраций - метафора. Их назначение - вызвать эмоцию и создать отношение к ней, воздействовать на аудиторию. С помощью хорошо продуманных и представляемых образов, информация может надолго остаться в памяти человека. Диаграмма - визуализация количественных и качественных связей. Их используют для убедительной демонстрации данных, для пространственного мышления в дополнение к логическому. Таблица - конкретный, наглядный и точный показ данных. Ее основное назначение - структурировать информацию, что порой облегчает восприятие данных аудиторией.

Практические советы по подготовке презентации готовьте отдельно:

- печатный текст + слайды + раздаточный материал;
- слайды - визуальная подача информации, которая должна содержать минимум текста, максимум изображений, несущих смысловую нагрузку, выглядеть наглядно и просто;
- текстовое содержание презентации – устная речь или чтение, которая должна включать аргументы, факты, доказательства и эмоции;
- рекомендуемое число слайдов 17-22;
- обязательная информация для презентации: тема, фамилия и инициалы выступающего; план сообщения; краткие выводы из всего сказанного; список использованных источников;
- раздаточный материал – должен обеспечивать ту же глубину и охват, что и живое выступление: люди больше доверяют тому, что они могут унести с собой, чем исчезающим изображениям, слова и слайды забываются, а раздаточный материал остается постоянным осязаемым напоминанием; раздаточный материал важно раздавать в конце презентации; раздаточный материалы должны отличаться от слайдов, должны быть более информативными.

Тема доклада должна быть согласованна с преподавателем и соответствовать теме учебного занятия. Материалы при его подготовке, должны соответствовать научно-методическим требованиям вуза и быть указаны в докладе. Необходимо соблюдать регламент, оговоренный при получении задания. Иллюстрации должны быть достаточными, но не чрезмерными.

Работа обучающегося над докладом-презентацией включает отработку умения самостоятельно обобщать материал и делать выводы в заключении, умения ориентироваться в материале и отвечать на дополнительные вопросы слушателей, отработку навыков ораторства, умения проводить диспут.

Докладчики должны знать и уметь: сообщать новую информацию; использовать технические средства; хорошо ориентироваться в теме всего семинарского занятия; дискутировать и быстро отвечать на заданные вопросы; четко выполнять установленный регламент (не более 10 минут); иметь представление о композиционной структуре доклада и др.

Структура выступления

Вступление помогает обеспечить успех выступления по любой тематике. Вступление должно содержать: название, сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов, живую интересную форму изложения, акцентирование внимания на важных моментах, оригинальность подхода.

Основная часть, в которой выступающий должен глубоко раскрыть суть затронутой темы, обычно строится по принципу отчета. Задача основной части – представить достаточно данных для того, чтобы слушатели заинтересовались темой и захотели ознакомиться с материалами. При этом логическая структура теоретического блока не должны даваться без наглядных пособий, аудио-визуальных и визуальных материалов.

Заключение – ясное, четкое обобщение и краткие выводы

Подготовка к тестированию

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов. При самостоятельной подготовке к тестированию обучающемуся необходимо:

1) готовясь к тестированию, проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

2) четко выяснить все условия тестирования заранее, знать, сколько тестов будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

3) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

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

5) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

6) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

Тестирование - позволяет оценить знание фактического материала, умение логически мыслить, способность к рефлексии и творчески подходить к решению поставленной задачи.

Промежуточная аттестация

По итогам 1 семестра проводится Зачет с оценкой. При подготовке к сдаче Зачет с оценкойа рекомендуется пользоваться материалами, изученными в ходе текущей самостоятельной работы. Зачет с оценкой проводится в устной или письменной форме, включает подготовку и ответы студента на теоретические вопросы. По итогам Зачет с оценкойа выставляется оценка. По итогам обучения проводится Зачет с оценкой, к которому допускаются студенты, имеющие положительные результаты по защите контрольных и самостоятельных работ.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	№ семестра	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4	5
1	3	Лекция: «Системы аппаратной и программной криптографической защиты».	Лекция – презентация	2
2	3	Лекция: «Средства стеганографической и криптографической защиты информации».	Лекция – презентация	2
3	3	Практическое занятие. «Каналы утечки информации данных. Обзор программ Страж NT, Secret Net»	Тематический семинар, использование компьютерных технологий для выполнения практических работ	2
4	3	Практическое занятие. «Особенности работы программ Аккорд-АМДЗ 5.5, Электронный замок «Соболь»».	Тематический семинар, использование компьютерных технологий для выполнения практических работ	4
5	3	Практическое занятие. «Технологии аутентификации и шифрования»	Тематический семинар, использование компьютерных технологий для выполнения практических работ	2
6	3	Практическое занятие. «Средства для защиты объектов ВТ»	Тематический семинар, использование компьютерных технологий для выполнения практических работ	2

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

Список основной литературы

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33430.html
2. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций : учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2021. — 116 с. — ISBN 978-5-7262-2807-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/125496.html
3. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/33857.html

Список дополнительной литературы

1. Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.- 324 с.
2. Корнеев, И.К. Защита информации в офисе [Текст]: учебник/ И.К. Корнеев, Е.А. Степанов.- М.: ТК Велби, Проспект, 2010.- 336 с.
3. Куприянов, А.И. Основы защиты информации [Текст]: учеб. пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов.- М.: Академия, 2008.- 256 с.
4. Петренко, С. А. Политики безопасности компании при работе в Интернет / С. А. Петренко, В. А. Курбатов. — 3-е изд. — Москва : ДМК Пресс, 2018. — 396 с. — ISBN 978-5-93700-057-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89596.html
5. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87998.html
6. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст]: учеб. пособие для студ. высш. учеб. заведений/ П.Б. Хорев - М.: Академия, 2008.- 256 с.

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http:// www. rsl. ru / - сайт Российской государственной библиотеки
2. http://www.gpntb.ru/ - сайт Государственной публичной научно-технической библиотеки России
3. http:// elibrary. ru / - сайт Научной электронной библиотеки

7.3. Информационные технологии

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Microsoft Azure Dev Tools for Teaching 1. Windows 7, 8, 8.1, 10 2. Visual Studio 2008, 2010, 2013, 2019 5. Visio 2007, 2010, 2013 6. Project 2008, 2010, 2013 7. Access 2007, 2010, 2013 и т. д.	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022 (продление подписки)
MS Office 2003, 2007, 2010, 2013	Сведения об Open Office: 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
Цифровой образовательный ресурс IPRsmart	Лицензионный договор № 10423/23П от 30.06.2023 г. Срок действия: с 01.07.2023 г. до 01.07.2024г.

Свободное программное обеспечение:
WinDjView, Sumatra PDF, 7-Zip

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:
Доска меловая - 1шт., стол преподавательский - 1шт., парты - 8шт., стулья - 26шт., компьютерные столы - 10шт., стул мягкий – 1шт. Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой

2. Лаборатория новых компьютерных технологий
Специализированная мебель: Доска меловая - 1шт., стол преподавательский - 1шт., парты - 8шт., стулья - 26шт., компьютерные столы - 10шт., стул мягкий – 1шт. Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории: ПК-10 шт.

3. Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Специализированная мебель: Доска меловая - 1шт., стол преподавательский - 1шт., парты - 8шт., стулья - 26шт., компьютерные столы - 10шт., стул мягкий – 1шт. Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории: ПК-10 шт.
4.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 тема-тические иллюстрации:
Экран настенный -1шт.
Проектор -1 шт.
Ноутбук -1 шт.

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 до-ступа в электронную информационно-образовательную среду ФГБОУ ВО «СевКавГА»:
Персональный компьютер – 1шт.
Сканер -1 шт.
МФУ – 1шт.

Отдел обслуживания электронными изданиями
Специализированная мебель:
Рабочие столы на 1 место – 24 шт.
Стулья – 24 шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тема-тические иллюстрации:
Интерактивная система - 1 шт.
Монитор– 20 шт.
Монитор - 1 шт.
Сетевой терминал -18 шт.
Персональный компьютер -3 шт.
МФУ– 2 шт.
Принтер–1шт.

4. Помещение для хранения и профилактического обслуживания учебного оборудования.
Специализированная мебель:
Шкаф – 1 шт., стул -2 шт., кресло компьютерное – 2 шт., стол угловой компьютерный – 2 шт.,
тумбочки с ключом – 2 шт.
Учебное пособие (персональный компьютер в комплекте) – 2 шт.

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 Методы и средства обеспечения безопасности информационных систем

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Методы и средства обеспечения безопасности информационных систем»

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-2	способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике
ПК-5	способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем

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 обучающимися.

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

Разделы (темы) дисциплины	Формируемые компетенции (коды)	
	ПК-2	ПК-5
Раздел 1. Системы криптографической защиты Тема 1.1. Системы аппаратной и программной криптографической защиты.	+	
Раздел 2. Средства стеганографической защиты информации. Тема 2.1. Средства стеганографической и криптографической защиты информации	+	
Раздел 3. Программно-аппаратные средства обеспечения безопасности информационных систем. Тема 3.1. Классификация каналов проникновения в систему и утечки информации		+
Раздел 4. Стеганографические средства в ОС Linux и ОС Windows. Файловая система StegFS. Тема 4.1. Основные защитные механизмы операционной системы семейства ОС Unix и ОС Windows.		+
Раздел 5. Защита файлов, контроль доступа, уязвимость паролей. Тема 5.1. Средства защиты открытых информационных систем.		+
Тема 5.2. Технологии аутентификации и шифрования	+	
Раздел 6. Встраиваемые водяные знаки. DRM. Тема 6.1. Система безопасности ОС Windows и Unix.		+
Раздел 7. Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак. Тема 7.1. Обеспечение надежности и бесперебойного функционирования информационных систем среды.	+	
Тема 7.2. Безопасность web-ориенти-рованного контента		+

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

ПК-2- способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике
ПК-5 способен применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем

Индикаторы достижения компетенций	Критерии оценивания результатов обучения	Средства оценивания результатов обучения			Средства оценивания результатов обучения	
	Минимальный уровень не достигнут (неудовл.)	Минимальный уровень (удовл.)	Хороший уровень (хорошо)	Отличный уровень (отлично)	текущий контроль	промежут. аттестация
1	2	3	4	5	6	7
ПК-2.1 Анализирует применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Не умеет анализировать различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Частично умеет анализировать различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Умеет анализировать различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Готов и умеет анализировать различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций в экономике	Доклад	Зачет с оценкой
ПК-2.2 Разрабатывает и применяет математические модели в области проектирования и управления информационными системами	Не готов применять математические модели в области проектирования и управления ин-формационными системами	Не разрабатывает, частично применяет математические модели в области проектирования и управления ин-формационными системами	Умеет разрабатывать и применять математические модели в области проектирования и управления информационными системами	Готов и умеет разрабатывать и применять математические модели в области проекти-рования и управления информационными системами	Тестирование	Зачет с оценкой
ПК-2.3 Анализирует и оценивает угрозы информационной безопасности; применяет отечественные и	Не знает как оценивать угрозы информационной безопасности; не применяет	Частично анализирует и оценивает угрозы информационной безопасности; применяет отечественные и	Умеет анализировать и оценивать угрозы информационной безопасности; применяет отечественные и	Выполняет полный анализ и оценивает угрозы информационной безопасности;	Тестирование	Зачет с оценкой

зарубежные стандарты в области компьютерной безопасности.	отечественные и зарубежные стандарты в области компьютерной безопасности.	зарубежные стандарты в области компьютерной безопасности.	зарубежные стандарты в области компьютерной безопасности.	применяет отечественные и зарубежные стандарты в области компьютерной безопасности.		
ПК-5.1 Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Не владеет методами оценки угроз информационной безопасности; непримeняет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информаци-онных систем	Анализирует и владеет отдельными методами оценки угроз информационной безопасности; применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Владеет основными методами анализа и оценивания угроз информационной безопасности; применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Анализирует и оценивает угрозы информационной безопасности; Применяет современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания информационных систем	Доклад	Зачет с оценкой
ПК-5.2 Выбирает и использует облачные сервисы для решения прикладных задач различных классов и создания информационных систем	Допускает существенные ошибки при использовании облачных сервисов для решения прикладных задач различных классов и создания информационных систем	Демонстрирует частичные знания в осуществлении облачных сервисов для решения прикладных задач различных классов и создания информационных систем	Демонстрирует знания при использовании облачных сервисов для решения прикладных задач различных классов и создания информационных систем	Демонстрирует исчерпывающие знания при выборе и использовании облачных сервисов для решения прикладных задач различных классов и создания информационных систем	Тестирование	Зачет с оценкой

ПК-5.3 Выявляет и анализирует риски информационной безопасности	Не выявляет и не анализирует риски информационной безопасности	Частично выявляет и анализирует риски информационной безопасности	Демонстрирует знания при выявлении и анализе рисков информационной безопасности	Выявляет в полном объеме и анализирует риски информационной безопасности	Устный опрос, тестирование	Зачет с оценкой

4. Комплект контрольно-оценочных средств по дисциплине.

Вопросы к зачету с оценкой по дисциплине «Методы и средства обеспечения безопасности информационных систем»

1. Предмет и задачи дисциплины «Методы и средства обеспечения безопасности информационных систем».
2. Основные задачи защиты информации.
3. Основные этапы защищенной инфраструктуры.
4. Классификация стеганографии
5. Классическая стеганография
6. Симпатические чернила
7. Другие стеганографические методы
8. Стеганографические модели
9. Основные понятия
10. Компьютерная стеганография
11. Цифровая стеганография
12. Сетевая стеганография. Алгоритмы
13. Фазовое кодирование
14. Атаки на стегосистемы
15. Стеганография и цифровые водяные знаки
16. Применение стеганографии в современных принтерах
17. Применение цифровой стеганографии
18. Классификация стеганографии
19. Симпатические чернила
20. Другие стеганографические методы
21. Стеганографические модели
22. Компьютерная стеганография
23. Цифровая стеганография
24. Сетевая стеганография.
25. Фазовое кодирование
26. Метод расширенного спектра

Вопросы для устного опроса
по дисциплине «Методы и средства обеспечения безопасности информационных систем»

Вопросы к разделу 1.

- Угрозы безопасности информации.
- Архитектуры системы защиты: особенности современных АС как объекта защиты
- Источники угроз безопасности
- Классификация угроз безопасности
- Основные преднамеренные и непреднамеренные искусственные угрозы

Вопросы к разделу 2.

- Уязвимость, угроза ИБ
- Источник угрозы ИБ
- Модель угроз ИБ
- Модель нарушителя ИБ
- Информационная инфраструктура
- Причины уязвимости ИС

Вопросы к разделу 3.

- Прямые и косвенные каналы проникновения в систему и утечки информации.
- Физические, электромагнитные, информационные каналы

Вопросы к разделу 4.

- Идентификация и аутентификация пользователя при входе в систему.
- Разграничение прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа
- Аудит
- Принципиальные недостатки защитных механизмов операционной системы семейства Unix

Вопросы к разделу 5.

- Сервисы безопасности.
- Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры.
- Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации.
  Дополнительная информация и итоговые рекомендации по защите открытых ИС.

Вопросы к разделу 6.

- Параметры безопасности.
- Настройка операционной системы Windows.
- Права пользователей и система управления доступом.
- Квалификация пользователей.
- Средства защиты

Вопросы к разделу 7.

- Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web.

- команды удаленного выполнения, Sendmail и электронная почта, другие утилиты.
- Средства замены уязвимых сервисов TCP/IP.
- Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении.
- Сетевые вирусы. Виды угроз ресурсам интранета и Интернета

Темы для докладов
по дисциплине: «Методы и средства обеспечения безопасности информационных систем»

1. Обзор современных методов криптографической защиты информации.
2. Классическая стеганография
3. Симпатические чернила
4. Стеганографические модели. Основные понятия
5. Компьютерная стеганография
6. Виды умышленных угроз безопасности информации
7. Методы и средства защиты информации
8. Криптографические методы защиты информации
9. Secret Disc
10. Электронный ключ eToken
11. Secret Net 5.0.
12. Аккорд-АМДЗ 5.5
13. Электронный замок «Соболь»
14. Страж NT 2.5
15. Общая характеристика объектов защиты информационной деятельности и обеспечения ИБ
16. Механизм выработки детальных предложений по формированию политики и построению системы информационной безопасности.
17. Обобщенная модель способов несанкционированного доступа к источникам конфиденциальной информации.
18. Криптографический интерфейс приложений операционной системы Windows (Cryptoapi).
19. Методы защиты инсталляционных дисков от копирования.
20. Методы противодействия исследованию алгоритма работы системы защиты

Задания для контрольной работы
по дисциплине «Методы и средства обеспечения безопасности информационных систем»

1 вариант
1.Выбор мер защиты информации для реализации в информационной системе в рамках системы защиты информации.
2.Классификация информационной системы по требованиям защиты информации.

2 вариант
1.Определение угроз безопасности информации в информационной системе.
2.Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации

3 вариант
1. Идентификация и аутентификация субъектов доступа и объектов доступа
2.Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных

4 вариант
1. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
2. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

5 вариант
1. Защита обратной связи при вводе аутентификационной информации
2. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

6 вариант
1. Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа
2.Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

7 вариант
1.Реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
2.Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

8 вариант
1.Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

2.Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

9 вариант

1.Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

2.Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных оператором правил обработки информации

10 вариант

1.Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему

2.Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

ТЕСТОВЫЕ ВОПРОСЫ
по дисциплине «Методы и средства обеспечения безопасности информационных систем»

1. Что из перечисленного не относится к возможным угрозам информационной безопасности? (ПК-2)

Выберите один ответ:

1. компьютерные преступления на основе ложной идентификации клиента
2. подделка электронных документов
3. получение злоумышленником конфиденциальной информации
4. кажущаяся анонимность при работе в Internet

2. Как можно определить систему защиты информации? (ПК-2)

Выберите один ответ:

1. как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз
2. как совокупность информационной инфраструктуры, субъектов, осуществляющих сбор,
3. формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений
4. как одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.

3. Что может быть представлено как совокупность набора передаваемых сведений и порядка (алгоритмов) их кодирования в набор знаков сообщения и декодирования в сведения? (ПК-2)

4. Какой вид собственного обеспечения системы защиты информации включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы? (ПК-2)

1. аппаратное обеспечение
2. организационное обеспечение
3. информационное обеспечение
4. правовое обеспечение

5. Какое свойство информации в форме сообщения предполагает возможность количественной оценки параметров сообщения (количество знаков, составляющих сообщение)? (ПК-2)

1. проблемная ориентированность
2. сложность
3. материальность
4. измеримость

6. Какой вид собственного обеспечения системы защиты информации предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты? (ПК-2)

1. нормативно-методическое обеспечение

2. лингвистическое обеспечение
3. математическое обеспечение

7. Какая причина уязвимости Интернет сформулирована неверно? (ПК-5)
1. простота конфигурирования средств защиты
2. кажущаяся анонимность при работе в Internet
3. человеческий фактор

8. Кем защищаются пути доступа, малый бизнес и образовательные учреждения (при этом используются средства защиты информации среднего уровня, как коммерческие, так и свободно распространяемые в исследовательских центрах)? (ПК-2)
1. правительством
2. частными лицами
3. общественными организациями
4. корпорациями

9. Какой тип взломщиков интрасетей, согласно одной из классификаций компьютерных злоумышленников, отличается от других типов тем, что после входа в систему он должен найти и перенести определенную информацию на свой компьютер, что делает его задачу более сложной, чем простое проникновение? (ПК-5)

10. Что является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз? (ПК-2)
1. концепция современных информационных технологий
2. концепция безопасности информации
3. концепция информационных ресурсов

11. Какая причина уязвимости Интернет сформулирована неверно? (ПК-6)
1. работа в Internet обслуживается большим числом сервисов, информационных служб и сетевых протоколов, знание правильности и тонкостей использования всех или хотя бы большинства сервисов, служб и протоколов одному человеку в лице администратора сети нереально;
2. «утечка» технологий высокого уровня из секретных источников при вскрытии представленных в сети Web-узлов и сетей организаций, занимающихся разработкой этих технологий, и доступность информации о средствах защиты;
3. зашифрованность большей части передаваемой через Internet информации

12. Целью какого организационного мероприятия является исключение возможности тайного проникновения на территорию и в помещения посторонних лиц и обеспечение удобства контроля прохода и перемещения сотрудников и посетителей? (ПК-5)
1. организации работы по анализу внутренних и внешних угроз
2. организации работы с документами
3. организации работы с сотрудниками
4. организации использования технических средств
5. организации режима и охраны

13. Содержание какой функции системы защиты информации направлено на непрерывный контроль средств, комплексов, систем обработки, защиты информации и различных компонентов защищаемой информации с целью своевременного обнаружения фактов воздействия на них угроз? (ПК-2)

14. Что из перечисленного не включает в себя организационная защита? (ПК-5)
Выберите один ответ:
1. организацию работы с сотрудниками
2. организацию использования технических средств
3. организацию режима и охраны
4. организацию разработки инструкции о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию
5. организацию работы с документами

15. Как называется документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации? (ПК-2)

16. Согласно каким методам шифрования информации, шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите? (ПК-2)
Выберите один ответ:
1. аддитивным методам
2. методам перестановки
3. методам замены (подстановки)

17. Дайте определение организационной защиты? (ПК-2)

18. Как называется разрешение, выдаваемое государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставление права использовать защищенные патентами изобретения, технологии, методики? (ПК-5)

19. Как называется форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями? (ПК-2)
1. обязательство
2. договор
3. конфиденциальность

20. Как называется поиск вирусов по запросу пользователя? (ПК-6)
1. ложное срабатывание (Falsepositive)
2. обратный термин (Falsenegative)
3. сканирование по запросу (on-demand)
4. сканирование на лету (real-time, on-the-fly)

21. Как регулируется правовая защита на государственном уровне? (ПК-2)
Выберите один ответ:
1. конвенциями
2. государственными и ведомственными актами
3. межгосударственными договорами
4. декларациями

22. Что из перечисленного не относится к особенностям алгоритма работы вирусов? (ПК-2)

Выберите один ответ:

1. самошифрование и полиморфичность
2. использование нестандартных приемов
3. резидентность
4. использование «стелс»-алгоритмов
5. опасность

23. Как называется детектирование вируса в незараженном объекте (файле, секторе или системной памяти)? (ПК-2)

1. сканирование по запросу (on-demand)
2. обратный термин (Falsenegative)
3. сканирование на лету (real-time, on-the-fly)
4. ложное срабатывание (Falsepositive)

24. Какой Закон РФ определяет основы защиты информации в системах обработки и при ее использовании с учетом категорий доступа к открытой информации и к информации с ограниченным доступом? (ПК-2)

1. Закон «Об информации, информатизации и защите информации»
2. Закон «Об органах государственной безопасности»
3. Закон «О государственной тайне»

25. Какое организационное мероприятие предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.? (ПК-2)

Выберите один ответ:

1. организация режима и охраны
2. организация работы с документами
3. организация использования технических средств
4. организация работы с сотрудниками
5. организация работы по анализу внутренних и внешних угроз

26. К каким задачам защиты информации относится класс 1.2. «Дезинформация противника»? (ПК-6)

Выберите один ответ:

1. к задачам уменьшения степени распознавания объектов
2. к задачам защиты информации от информационного воздействия
3. к задачам защиты содержания обрабатываемой, хранимой и передаваемой информации

27. Что на сегодняшний день является основным источником вирусов? (ПК-2)

28. В алгоритм каких вирусов заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти и др. (по классификации компьютерных вирусов по деструктивным возможностям)? (ПК-2)

29. Какие компьютерные вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты? (ПК-6)

Выберите один ответ:

1. файловые вирусы
2. загрузочные вирусы
3. сетевые вирусы
4. макровирусы

30. Дайте определение коммерческая тайна? (ПК-2)

31. В чем заключается основная задача систем контроля вскрытия аппаратуры? (ПК-5)

32. Суть каких методов шифрования информации состоит в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов? (ПК-2)

Выберите один ответ:

1. аддитивных методов
2. методов перестановки
3. методов замены (подстановки)

33. Как называется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей? (ПК-2)

Выберите один ответ:

1. защита информации от утечки по акустическому каналу
2. защита информации от утечки по электромагнитным каналам
3. защита информации от утечки по визуально-оптическому каналу

34. В чем заключается ограничение доступа? (ПК-2)

35. В чем заключается основная задача разделения привилегий на доступ к информации? (ПК-2)
36. В чем заключается защита информации методом криптографического преобразования? (ПК-2)

5. Методические материалы, определяющие процедуры оценивания компетенции

*Для оценивания **доклада** используются следующие критерии оценивания:*

Не зачтено	Зачтено
- Содержание не соответствует теме. - Литературные источники выбраны не по теме, не актуальны. - Нет ссылок на использованные источники информации - Тема не раскрыта - В изложении встречается большое количество орфографических и стилистических ошибок. Требования к оформлению и объему материала не соблюдены - Структура доклада не соответствует требованиям - Не проведен анализ материалов реферата - Нет выводов. - В тексте присутствует плагиат	- Тема соответствует содержанию доклада - Широкий круг и адекватность использования литературных источников по проблеме - Правильное оформление ссылок на используемую литературу; - Основные понятия проблемы изложены полно и глубоко - Отмечена грамотность и культура изложения; - Соблюдены требования к оформлению и объему доклада - Материал систематизирован и структурирован; - Сделаны обобщения и сопоставления различных точек зрения по рассматриваемому вопросу, - Сделаны и аргументированы основные выводы - Отчетливо видна самостоятельность суждений

*Описание шкалы и критериев оценивания для проведения **промежуточной аттестации** обучающихся по дисциплине в форме зачета с оценкой*

Критерии оценивания:
- полнота усвоения материала,
- качество изложения материала,
- правильность выполнения заданий,
- аргументированность решений.

Оценка			
«2» (неудовлетворительно)	Пороговый уровень освоения «3» (удовлетворительно)	Углубленный уровень освоения «4» (хорошо)	Продвинутый уровень освоения «5» (отлично)
Обучающийся не знает значительной части программного материала, плохо ориентируется в экономической	Обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает	Обучающийся твердо знает материал, не допускает существенных неточностей в	Обучающийся знает научную терминологию, методы и приемы анализа проблем в экономике и управлении, глубоко и прочно усвоил

терминологии, допускает существенные ошибки.	неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.	ответе на вопрос.	программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, не затрудняется с ответом при видоизменении заданий.
Не умеет использовать методы и средства обеспечения безопасности информационных систем, не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, большинство предусмотренных программой обучения учебных заданий не выполнено.	Теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос	Теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое.	Умеет использовать основные положения и методы при решении профессиональных задач. Умеет объяснять и анализировать процессы в экономике и управлении. Теоретическое содержание курса освоено полностью, без пробелов; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.
Обучающийся не имеет навыков анализировать безопасность информационных систем, допускает существенные ошибки, с большими затруднениями выполняет практические работы, большинство предусмотренных программой обучения учебных заданий не выполнено	Обучающийся допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала	Обучающийся грамотно и по существу излагает материал, не допуская существенных неточностей в ответе на вопрос.	Обучающийся имеет навыки обеспечения безопасности информационных систем, глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.

Критерии оценки устного опроса:

-*оценка «отлично» выставляется студенту, если:*

- даны исчерпывающие и обоснованные ответы на все поставленные

вопросы, правильно;

- при ответах выделялось главное, все теоретические положения умело увязывались с требованиями руководящих документов;
- ответы были четкими и краткими, а мысли излагались в логической последовательности;
- показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии;

- *оценка «хорошо»:*

- даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания;
- при ответах не всегда выделялось главное, отдельные положения недостаточно увязывались с требованиями руководящих документов;
- ответы в основном были краткими, но не всегда четкими.

- *оценка «удовлетворительно»:*

- даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования
- на уточняющие вопросы даны правильные ответы;
- при ответах не выделялось главное;
- ответы были многословными, нечеткими и без должной логической последовательности;
- на отдельные дополнительные вопросы не даны положительные ответы.

- *оценка «неудовлетворительно»:*

- не выполнены требования, предъявляемые к знаниям, оцениваемым “удовлетворительно”.

Критерии оценки контрольной работы:

- оценка «отлично» выставляется студенту, если:

- даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно;
- при ответах выделялось главное, все теоретические положения умело увязывались с требованиями руководящих документов;
- ответы были четкими и краткими, а мысли излагались в логической последовательности;
- показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии;

- оценка «хорошо»:

- даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания;
- при ответах не всегда выделялось главное, отдельные положения недостаточно увязывались с требованиями руководящих документов;
- ответы в основном были краткими, но не всегда четкими.

- оценка «удовлетворительно»:

- даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования
- на уточняющие вопросы даны правильные ответы;
- при ответах не выделялось главное;
- ответы были многословными, нечеткими и без должной логической последовательности;
- на отдельные дополнительные вопросы не даны положительные ответы.

- оценка «неудовлетворительно»:

- не выполнены требования, предъявляемые к знаниям, оцениваемым “удовлетворительно”.

Критерии оценивания тестирования

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