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
«29» сентября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защищенные информационные системы и среды

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 Прикладной математики и информационных технологий

Кафедра разработчик РПД Прикладная информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л.У.

Директор института ПМ и ИТ _____ Тебуев Д.Б.

Заведующий выпускающей кафедрой _____ Хапаева Л.Х.

г. Черкесск, 2021 г.

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Защищенные информационные системы и среды» является:

1. овладение знаниями защиты информации, связанных с созданием и изучением современных защищенных информационных систем различного применения и степени сложности, предотвращением ущерба пользователю информации;
2. овладение навыками применения новых научных принципов и методов исследований.

При этом задачами дисциплины являются:

- изучение современной классификации средств защиты информации в корпоратив ных вычислительных сетях и системах;
- изучение современных технологий построения безопасных информационных сис тем
- 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 защитыинформации: файрволлов, интерактивных детекторов атак, защищенных доменныхсервисов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Защищенные информационные системы и среды» относится к части, формируемой участниками образовательных отношений Блока 1 Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. В таблице приведены предшествующие 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	Опирается на знания, умения и навыки, сформированные дисциплинами предыдущего уровня образования	Комплексная информационная безопасность Правовое обеспечение ИТ деятельности Производственная практика (научно-исследовательская практика)

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта направлению подготовки 09.04.03 Прикладная информатика 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-7	Способность на практике применять новые научные принципы и методы исследований	ПК-7.1 Оценивает экономическую эффективность информационных процессов, ИС, а также проектных рисков ПК-7.2 Выявляет и анализирует риски информационной безопасности ПК-7.3 Ставит и решает прикладные задачи в условиях неопределенности и определяет методы и средства их эффективного решения

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы	Всего часов	Семестры
		№ 1
		часов
1	2	3
Аудиторная контактная работа (всего)	**42**	**42**
В том числе:		
Лекции (Л)	14	14
Практические занятия (ПЗ), Семинары (С)	28	28
Лабораторные работы (ЛР)	-	-
Контактная внеаудиторная работа, в том числе	**1,5**	**1,5**
Групповые и индивидуальные консультации	1,5	1,5
Самостоятельная работа обучающегося (СРО) (всего)	**64**	**64**
Работа с книжными источниками	14	14
Работа с электронными источниками	6	6
Выполнение индивидуальных практических заданий	12	12
Подготовка к контрольной работе	6	6
Доклад	4	4
Подготовка к тестированию	6	6
Подготовка к коллоквиуму	6	6

Подготовка к промежуточному контролю (ППК)		10	10
Промежуточная аттестация	зачет (ЗаО)	Зачет с оценкой	Зачет с оценкой
	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**
			№ 3
			часов
1		2	3
Аудиторная контактная работа (всего)		32	32
В том числе:			
Лекции (Л)		16	16
Практические занятия (ПЗ), Семинары (С)		16	16
Лабораторные работы (ЛР)		-	-
Контактная внеаудиторная работа, в том числе		**1,5**	**1,5**
Групповые и индивидуальные консультации		1,5	1,5
Самостоятельная работа обучающегося (СРО) (всего)		74	74
Работа с книжными источниками		20	20
Работа с электронными источниками		7	7
Выполнение индивидуальных практических заданий		12	12
Подготовка к контрольной работе		6	6
Доклад		2	2
Подготовка к тестированию		8	8
Подготовка к коллоквиуму		2	2
Подготовка к промежуточному контролю (ППК)		17	17
Промежуточная аттестация	зачет (ЗаО)	Зачет с оценкой	Зачет с оценкой
	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**
		№ 3
		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)	-	-

Контактная внеаудиторная работа, в том числе		**1**	**1**
Групповые и индивидуальные консультации			
Самостоятельная работа обучающегося (СРО) (всего)		93	93
Работа с книжными источниками		19	19
Работа с электронными источниками		20	20
Выполнение индивидуальных практических заданий		12	12
Подготовка к контрольной работе		6	6
Просмотр и конспектирование видеолекций		6	6
Доклад		6	6
Подготовка к тестированию		12	12
Подготовка к коллоквиуму		2	2
Подготовка к промежуточному контролю (ППК)		10	10
Промежуточная аттестация	зачет (ЗаО)	Зачет с оценкой(4)	Зачет с оценкой(4)
	Прием зач., час	0,5	0,5
	СРО, час.	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	Наименование раздела 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 1							
1.	Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	2			10	12	Контрольная работа, доклад, коллоквиум тестирование, выполнение индивидуальных практических заданий
2.	Уязвимость основных структурно-функциональных элементов распределенных АС.	2		8	14	24	
3.	Классификация каналов проникновения в систему и утечки информации.	2		4	12	18	
4.	Основные функции подсистемы защиты: основные защитные механизмы операционной системы семейства Unix, недостатки ее защитных механизмов.	2		-	10	12	
5.	Защита файлов, контроль доступа, уязвимость паролей.	2		4	9	15	
6.	Система безопасности Windows, система управления доступом, политика ограничений.	2		4	4	10	
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	2		8	5	15	
8.	Контактная внеаудиторная работа					1,5	Индивидуальные и групповые консультации
9.	Промежуточная аттестация.					0,5	Зачет с оценкой
Итого:		**14**		**28**	**64**	**108**	

Очно-заочная форма обучения

№ п/п	Наименование раздела 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 3							
1.	Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	4			10	14	Контрольная работа, доклад, коллоквиум тестирование, выполнение индивидуальных практических заданий
2.	Уязвимость основных структурно-функциональных элементов распределенных АС.	2		6	10	18	
3.	Классификация каналов проникновения в систему и утечки информации.	2		2	10	14	
4.	Основные функции подсистемы защиты: основные защитные механизмы операционной системы семейства Unix, недостатки ее защитных механизмов.	2			10	12	
5.	Защита файлов, контроль доступа, уязвимость паролей.	2		4	10	16	
6.	Система безопасности Windows, система управления доступом, политика ограничений.	2			14	16	
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	2		4	10	16	
8.	Контактная внеаудиторная работа					1,5	Индивидуальные и групповые консультации
9.	Промежуточная аттестация.					0,5	Зачет с оценкой
Итого:		**16**		**16**	**74**	**108**	

Заочная форма обучения

№ п/п	Наименование раздела 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 3							
1.	Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	2		-	14	16	Контрольная работа, доклад, коллоквиум тестирование, выполнение индивидуальных практических заданий
2.	Уязвимость основных структурно-функциональных элементов распределенных АС.			2	14	16	
3.	Классификация каналов проникновения в систему и утечки информации.			-	14	14	
4.	Основные функции подсистемы защиты: основные защитные механизмы операционной системы семейства Unix, недостатки ее защитных механизмов.	2			14	16	
5.	Защита файлов, контроль доступа, уязвимость паролей.			2	14	16	
6.	Система безопасности Windows, система управления доступом, политика ограничений.				14	14	
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.			2	9	11	
8.	Контактная внеаудиторная работа					1	Индивидуальные и групповые консультации
9.	Промежуточная аттестация.					4	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 1 ОЗФО , ЗФО 3 семестр						
1.	Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	Угрозы безопасности информации.	Угрозы безопасности информации, АС и субъектов информационных отношений, источники угроз безопасности, классификация угроз безопасности, основные преднамеренные и непреднамеренные угрозы.	2	4	2
2.	Уязвимость основных структурно-функциональных элементов распределенных АС.	Модели угроз и нарушителей информационной безопасности	Уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ. Информационная инфраструктура. Причины уязвимости ИС.	2	2	
3.	Классификация каналов проникновения в систему иутечки информации.	Классификация каналов проникновения в систему утечки информации.	Прямые и косвенные каналы проникновения в систему и утечки информации. Физические, электромагнитные, информационные каналы.	2	2	
4.	Основные функции подсистемы защиты: основные защитные механизмы операционной системы, недостатки защитных механизмов.	Основные защитные механизмы операционной системы.	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, используемых в операционных системах.	2	2	2
5.	Защита файлов, контроль доступа,	Средства защиты открытых информацион	Сервисы безопасности. Средства обеспечения ИБ в сетях. Их назначение, особенности применения	2	2	

	уязвимость паролей.	ных систем.	и примеры. Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Дополнительная информация и итоговые рекомендации по защите открытых ИС.			
6.	Система безопасности Windows, система управления доступом, политика ограничений.	Система безопасности Windows	Параметры безопасности. Настройка операционной системы Windows. Права пользователей и система управления доступом. Квалификация пользователей. Средства защиты.	2	2	
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	Обеспечение надежности и бесперебойного функционирования информационных систем среды.	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.	2	2	
Итого часов в семестре				**14**	**16**	**4**

4.2.3. **Лабораторный практикум** *(не предусмотрен)*

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 1 ОФО, ОЗФО и ЗФО семестр 3						
1.	Уязвимость основных структурно-функциональных элементов распределенных АС.	Каналы утечки информации в современных автоматизированных системах электронной обработки данных.	Сканирование уязвимостей. Тестирование проникновения. Удаленное администрирование web-сервера.	8	6	2
2.	Классификация каналов проникновения в систему и утечки информации.	Классификация внутренних и внешних нарушителей	Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне	4	2	-
3.	Защита файлов, контроль доступа, уязвимость паролей	Технологии аутентификации и шифрования	Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS. Требования к реализации SSL/TLS. Список действий для технологий аутентификации и шифрования. Firewall прикладного уровня для web — ModSecurity.	4	4	2

			Взаимодействие ModSecurity с пакетным фильтром			
4.	Система безопасности Windows, система управления доступом, политика ограничений	Средства защиты открытых информационных систем.	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.	4	-	-
5.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	Безопасность web-ориентированного контента	Опубликование информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Список действий для обеспечения безопасности web-содержимого	4	2	-
6.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и	Обеспечение надежности и бесперебойного функционирования информационных систем среды.	Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World	4	2	2

	внешних атак.		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.			
ИТОГО часов в семестре:				**28**	**16**	**6**

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов	
				ОФО	ОЗФО
1	3	4	5	6	7
Семестр 1 ОФО 3 семестр ОЗФО					
1.	Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	1.1.	Работа с книжными источниками	2	2
		1.2.	Работа с электронными источниками	1	1
		1.3.	Выполнение индивидуальных практических заданий	2	2
		1.4.	Подготовка к тестированию	2	2
		1.5.	Подготовка к промежуточному контролю (ППК)	3	3
2.	Уязвимость основных структурно-функциональных элементов распределенных АС.	2.1.	Работа с книжными источниками	4	2
		2.2.	Выполнение индивидуальных практических заданий	2	2
		2.3	Подготовка к коллоквиуму	6	2
		2.4	Подготовка к промежуточному контролю (ППК)	2	4
3.	Классификация каналов проникновения в систему и утечки информации.	3.1.	Работа с книжными источниками	2	2
		3.2.	Работа с электронными источниками	2	2
		3.3.	Выполнение индивидуальных практических заданий	2	2
		3.4.	Подготовка доклада	4	2
		3.5.	Подготовка к тестированию	2	2
4.	Основные функции подсистемы защиты: основные защитные механизмы операционной системы семейства Unix, недостатки ее защитных механизмов	4.1	Работа с книжными источниками	2	2
		4.2	Работа с электронными источниками	2	2
		4.3	Выполнение индивидуальных практических заданий	6	6
5.	Защита файлов, контроль доступа, уязвимость паролей	5.1	Работа с книжными источниками	2	2
		5.2	Работа с электронными источниками	1	2
		5.3	Подготовка к контрольной работе	6	6
6.	Система безопасности Windows, система управления доступом, политика ограничений.	6.1	Работа с книжными источниками	2	10
		6.2	Подготовка к тестированию	2	4

7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	7.1	Подготовка к промежуточному контролю (ППК)	5	10
ИТОГО часов за год:				**64**	**74**

Заочная форма обучения

№ п/п	**Наименование раздела (темы) дисциплины**	**№ п/п**	**Виды СРО**	**Всего часов**
				ЗФО
1	3	4	5	6
Семестр 3				
1.	Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	1.1.	Работа с книжными источниками	2
		1.2.	Работа с электронными источниками	2
		1.3.	Выполнение индивидуальных практических заданий	2
		1.4.	Подготовка доклада	2
		1.5.	Подготовка к тестированию	2
		16.	Подготовка к промежуточному контролю (ППК)	2
		1.7	Просмотр и конспектирование видеолекций	2
2.	Уязвимость основных структурно-функциональных элементов распределенных АС.	2.1.	Работа с книжными источниками	2
		2.2.	Работа с электронными источниками	2
		2.3.	Выполнение индивидуальных практических заданий	2
		2.4	Подготовка к коллоквиуму	2
		2.6	Подготовка к промежуточному контролю (ППК)	2
		2.7	Просмотр и конспектирование видеолекций	4
3.	Классификация каналов проникновения в систему и утечки информации.	3.1.	Работа с книжными источниками	2
		3.2.	Работа с электронными источниками	2
		3.3.	Выполнение индивидуальных практических заданий	2
		3.4.	Подготовка доклада	4
		3.5.	Подготовка к тестированию	4
4.	Основные функции	4.1	Работа с книжными источниками	4

	подсистемы защиты: основные защитные механизмы операционной системы семейства Unix, недостатки ее защитных механизмов	4.2	Работа с электронными источниками	4
		4.3	Выполнение индивидуальных практических заданий	6
5.	Защита файлов, контроль доступа, уязвимость паролей	5.1	Работа с книжными источниками	4
		5.2	Работа с электронными источниками	4
		5.3	Подготовка к контрольной работе	6
6.	Система безопасности Windows, система управления доступом, политика ограничений.	6.1	Работа с книжными источниками	4
		6.2	Работа с электронными источниками	4
		6.3	Подготовка к тестированию	6
7.	Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	7.1	Работа с книжными источниками	1
		7.2	Работа с электронными источниками	2
		7.3	Подготовка к промежуточному контролю (ППК)	6
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

Основными формами обучения дисциплины являются лекции и практические занятия, а также самостоятельная работа.

Лекция является основной формой обучения в высшем учебном заведении. Записи лекций в конспектах должны быть избирательными, полностью следует записывать только определения. В конспекте рекомендуется применять сокращение слов, что ускоряет запись. Вопросы, возникающие в ходе лекции, рекомендуется записывать на полях и после окончания лекции обратиться за разъяснением к преподавателю. Необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях.

Работа над конспектом лекции осуществляется по этапам:

- повторить изученный материал по конспекту;
- непонятные положения отметить на полях и уточнить;
- неоконченные фразы, пропущенные слова и другие недочеты в записях устранить, пользуясь материалами из учебника и других источников;
- завершить техническое оформление конспекта (подчеркивания, выделение главного, выделение разделов, подразделов и т.п.).

Самостоятельную работу следует начинать с доработки конспекта, желательно в тот же день, пока время не стерло содержание лекции из памяти. Работа над конспектом не должна заканчиваться с прослушивания лекции. После лекции, в процессе самостоятельной работы, перед тем, как открыть тетрадь с конспектом, полезно мысленновосстановить в памяти содержание лекции, вспомнив ее структуру, основные положения ивыводы.

С целью доработки необходимо прочитать записи, восстановить текст в памяти, а

также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Далее прочитать материал по рекомендуемой литературе, разрешая в ходе чтения, возникшие ранее затруднения, вопросы, а также дополнения и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. В ходе доработки конспекта углубляются, расширяются и закрепляются знания, а также дополняется, исправляется и совершенствуется конспект. Еще лучше, если вы переработаете конспект, дадите его в новой систематизации записей. Это, несомненно, займет некоторое время, но материал вами будет хорошо проработан, а конспективная запись его приведена в удобный для запоминания вид. Введение заголовков, скобок, обобщающих знаков может значительно повысить качество записи. Этому может служить также подчеркивание отдельных мест конспекта красным карандашом, приведение на полях или на обратной стороне листа краткой схемы конспекта и др.

Подготовленный конспект и рекомендуемая литература используется при подготовке к практическому занятию. Подготовка сводится к внимательному прочтению учебного материала, к выводу с карандашом в руках всех утверждений и формул, к решению примеров, задач, к ответам на вопросы, предложенные в конце лекции преподавателем или помещенные в рекомендуемой литературе. Примеры, задачи, вопросы по теме являются средством самоконтроля.

Непременным условием глубокого усвоения учебного материала является знание основ, на которых строится изложение материала. Обычно преподаватель напоминает, какой ранее изученный материал и в какой степени требуется подготовить к очередному занятию. Эта рекомендация, как и требование систематической и серьезной работы над всем лекционным курсом, подлежит безусловному выполнению. Потери логической связи как внутри темы, так и между ними приводит к негативным последствиям: материал учебной дисциплины перестает основательно восприниматься, а творческий труд подменяется утомленным переписыванием. Обращение к ранее изученному материалу не только помогает восстановить в памяти известные положения, выводы, но и приводит разрозненные знания в систему, углубляет и расширяет их. Каждый возврат к старому материалу позволяет найти в нем что-то новое, переосмыслить его с иных позиций, определить для него наиболее подходящее место в уже имеющейся системе знаний. Неоднократное обращение к пройденному материалу является наиболее рациональной формой приобретения и закрепления знаний. Очень полезным, но, к сожалению, еще мало используемым в практике самостоятельной работы, является предварительное ознакомление с учебным материалом. Даже краткое, беглое знакомство с материалом очередной лекции дает многое. Обучающиеся получают общее представление о ее содержании и структуре, о главных и второстепенных вопросах, о терминах и определениях. Все это облегчает работу на лекции и делает ее целеустремленной.

Методические указания магистрантам по освоению дисциплины представлены также в пособии:

Бостанова Л.К., Рядченко В.П. Защищенные информационные системы и среды. Учебно-методическое пособие для магистрантов 1 курса направления подготовки 09.04.03 Прикладная информатика/ Л.К. Бостанова– Черкесск: БИЦ СевКавГГТА, 2015. – 2 п.л

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

- не предусмотрены

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 семинараи 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.

Методические рекомендации по проведению устного опроса.

Устный опрос является одним из основных способов учета знаний обучающихся. Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на определенную тему, показывать его умение применять определения, правила в конкретных случаях.

Основные качества устного ответа подлежащего оценке.

1. Правильность ответа по содержанию (учитывается количество и характер ошибок при ответе).

2. Полнота и глубина ответа (учитывается количество усвоенных лексических единиц, грамматических правил и т. п.).

3. Сознательность ответа (учитывается понимание излагаемого материала).

4. Логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией).

5. Рациональность использованных приемов и способов решения поставленной учебной задачи (учитывается умение использовать наиболее прогрессивные и эффективные способы достижения цели).

6. Своевременность и эффективность использования наглядных пособий и технических средств при ответе (учитывается грамотно и с пользой применять наглядность и демонстрационный опыт при устном ответе).

7. Использование дополнительного материала (приветствуется, но не обязательно для всех обучающихся).

8. Рациональность использования времени, отведенного на задание (не одобряется затянутость выполнения задания, устного ответа во времени, с учетом индивидуальных особенностей обучающихся).

Методические рекомендации по проведению коллоквиума.

Коллоквиум -групповое обсуждение под руководством преподавателя достаточно широкого круга проблем, например, относительно самостоятельного большого раздела лекционного или практического курса.

На коллоквиум может быть вынесен раздел лекционного курса, знание которого должен продемонстрировать обучающийся. Коллоквиум проводится в форме собеседования преподавателя с обучающимися и содержит в себе элементы проверки знаний и консультации.

На современном этапе утвердились два вида проведения коллоквиумов - устного и письменного. В первом случае предполагается организация контроля в виде открытого диалога или группового обсуждения темы, во втором - проверка знаний обучающихся в виде письменного изложения ответов (развёрнутые ответы на вопросы, рефераты, эссе и т.д.)

Если коллоквиум проводится в письменной форме, то результаты деятельности обучающихся представляют собой:

- развёрнутые ответы на контрольные вопросы;
- решения контрольных заданий.

Объем одного блока вопросов содержит 20-30 вопросов.

1.Коллоквиум проводится, как правило, во внеаудиторное время. В порядке исключения с учетом наличия ресурсов обеспечения учебного процесса коллоквиум может быть проведён в аудиторное время, выделенное на изучение данной дисциплины.

2. В случае неудовлетворительного результата сдачи коллоквиума обучающемуся разрешается его пересдать в оставшийся до экзаменационной сессии период. При не сданном коллоквиуме обучающийся не допускается до зачета по этой дисциплине

Особенности проведение устного коллоквиума по теме или разделу дисциплины: Собеседование ведется с каждым обучающимся индивидуально в присутствии малой группы (5-6 человек).

В случае затруднения обучающегося при ответе на поставленный вопрос, последний может быть переадресован другим. При этом обучающиеся могут дополнять друг друга, дискутировать, задавать вопросы, всесторонне обсуждая проблему. Таким образом, коллоквиум представляет собой групповую форму беседы преподавателя с обучающимися с целью выяснения их знаний.

При этом каждому выставляется дифференцированная оценка. На коллоквиуме обучающиеся могут пользоваться своими записями изученных материалов. Не следует сводить коллоквиум к семинару. Если семинар сегодня не рекомендуется проводить лишь вопросно-ответным методом, то на коллоквиуме такой метод является основным.

На коллоквиуме обучающийся должен продемонстрировать, что он:

- знает содержание и структуру лекционного или практического курса, отдельных её глав и параграфов (если на коллоквиум выносится отдельный труд);
- уяснил логику изложения материала;
- умеет выделить узловые идеи и положения;
- умеет обобщать материал с помощью схем, таблиц, вопросов и делать записи прочитанного (сделать выписки, составить план, тезисы, аннотацию, резюме, конспект);
- видит связь изучаемой теории с практикой;
- имеет собственное мнение о прочитанном.

Методические рекомендации по подготовке обучающихся к тестированию.

В современном образовательном процессе тестирование как новая форма оценки знаний занимает важное место и требует серьезного к себе отношения.

Цель тестирований в ходе учебного процесса обучающихся состоит не только в систематическом контроле за знанием точных дат, имен, событий, явлений, но и в развитии умения обучающихся выделять, анализировать и обобщать наиболеесущественные связи, признаки и принципы разных исторических явлений и процессов. Одновременно тесты способствуют развитию творческого мышления, умению самостоятельно локализовать и соотносить исторические явления и процессы во времении пространстве.

Как и любая другая форма подготовки к контролю знаний, тестирование имеет ряд особенностей, знание которых помогает успешно выполнить тест.

Можно дать следующие методические рекомендации:

- Прежде всего, следует внимательно изучить обучающемуся структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, какого типа задания в нем содержатся. Это поможет настроиться на работу.
- Лучше начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока не останавливаясь на тех, которые могут вызвать долгие раздумья. Это позволит успокоиться и сосредоточиться на выполнении более трудных вопросов.
- Очень важно всегда внимательно читать задания до конца, не пытаясь понять условия «по первым словам» или выполнив подобные задания в предыдущих тестированиях. Такая спешка нередко приводит к досадным ошибкам в самых легких вопросах.
- Если Вы не знаете ответа на вопрос или не уверены в правильности, следует пропустить его и отметить, чтобы потом к нему вернуться.
- Психологи также советуют думать только о текущем задании. Как правило, задания в тестах не связаны друг с другом непосредственно, поэтому необходимо концентрироваться на данном вопросе и находить решения, подходящие именно к нему. Кроме того, выполнение этой рекомендации даст еще один психологический эффект – позволит забыть о неудаче в ответе на предыдущий вопрос, если таковая имела место.
- Многие задания можно быстрее решить, если не искать сразу правильный вариант ответа, а последовательно исключать те, которые явно не подходят. Метод исключения позволяет в итоге сконцентрировать внимание на одном-двух вероятных вариантах.
- Рассчитывать выполнение заданий нужно всегда так, чтобы осталось время на проверку и доработку (примерно 1/3-1/4 запланированного времени). Тогда вероятность описок сводится к нулю и имеется время, чтобы набрать максимум баллов на легких заданиях и сосредоточиться на решении более трудных, которые вначале пришлось пропустить.
- Процесс угадывания правильных ответов желательно свести к минимуму, так как это чревато тем, что обучающийся забудет о главном: умении использовать имеющиеся накопленные в учебном процессе знания, и будет надеяться на удачу. Если уверенности в правильности ответа нет, но интуитивно появляется предпочтение, то психологи рекомендуют доверять интуиции, которая считается проявлением глубинных знаний и опыта, находящихся на уровне подсознания.

При подготовке к тесту не следует просто заучивать, необходимо понять логику изложенного материала. Этому немало способствует составление развернутого плана, таблиц, схем, внимательное изучение разделов курса. Большую помощь оказывают опубликованные сборники тестов, Интернет-тренажеры, позволяющие, во-первых, закрепить знания, во-вторых, приобрести соответствующие психологические навыки

саморегуляции и самоконтроля. Именно такие навыки не только повышают эффективность подготовки, позволяют более успешно вести себя во время зачета, но и вообще способствуют развитию навыков мыслительной работы.

Методические рекомендации для выполнения индивидуальных практических заданий.

Методические указания для выполнения индивидуальных практических заданий (мультимедийных проектов). Индивидуальные задания – разнообразные работы научного, методического или учебно-практического характера. Индивидуальные задания носят заведомо нестандартный характер и оцениваются в каждом случае индивидуально. Содержание индивидуального задания должно быть согласовано с преподавателем, ведущим практические занятия.

Презентация.

Содержание презентации соответствует содержанию контрольной работы.

Объем – не менее 10 слайдов.

1-й – тема, ФИО обучающегося, год издания.

2-й – СОДЕРЖАНИЕ.

3-4-й – введение: кратко - актуальность, цели, задачи, объект и предмет исследования, теоретическая, нормативная и эмпирическая основа, методологическая основа, структура работы.

С 5-го - основная часть (текст) со схемами, таблицами, диаграммами, картинками, фото, статистическими данными и т.д. 13

Заключение: краткие выводы по работе. (1-2 слайда).

Список использованной литературы – весь. (1-2 слайда).

Сноски не нужны.

Последний слайд указывает на логическое завершение работы: Спасибо за внимание! или Благодарим за внимание!

Текст выравнивается на слайдах по ширине и приблизительно одинакового размера.

Цвет фона слайда не должен сливаться с цветом шрифта текста.

Рекомендуется применять эффекты анимации. Смену слайдов можно выставлять по времени или «по щелчку». Допускается прикрепление музыкального файла.

Методические рекомендации для выполнения контрольной работы.

Контрольная работа – это форма текущего контроля знаний обучающихся. Контрольная работа выполняется письменно.

Она может проводиться в разных формах:

- тестирование,
- решение практической задачи,
- ответ на проблемный теоретический вопрос и др.

Предпочтительной формой контрольной работы является тестирование.

Порядок проведения контрольных работ

Выполняя контрольную работу, необходимо внимательно ознакомиться с условиями заданий и четко их выполнить.

Как правило, контрольные работы проводятся на практическом занятии. Обучающимся, обучающимся по заочной форме обучения, контрольные работы могут быть заданы на дом. Контрольная работа проводится в течение всего практического занятия.

Работа выполняется самостоятельно. Пользоваться литературой на контрольной работе запрещается, если только это непосредственно не предусмотрено Программой соответствующей учебной дисциплины (возможно использование словаря). Использование на контрольной работе материалов, не разрешенных преподавателем

является основанием для удаления, обучающегося из аудитории и последующего проставления в ведомость оценки «неудовлетворительно».

Контрольная работа выполняется на отдельных листах синими чернилами разборчивым почерком (если почерк мелкий или неразборчивый, то работа выполняется печатными буквами). Запрещается использовать цветные чернила (красные, зеленые и т.д.), а также карандаш. Такие контрольные работы преподаватель вправе не проверять. В этом случае за работу выставляется низшая оценка. Если работа выполнена неаккуратно, неразборчивым почерком, то преподаватель также вправе не проверять такую работу. В этом случае обучающемуся надлежит переписать работу в консультационные часы преподавателя, при этом за вторую контрольную работу не может быть выставлена оценка «отлично».

Если выполнение контрольной работы предусмотрено дома, то работа выполняется в печатном виде (шрифт – 14, интервал – 1,5, черными чернилами) на отдельных листах формата А4, листы должны быть в обязательном порядке надежно скреплены или прошиты. Домашняя работа выполняется самостоятельно.

В случае текстуального совпадения ответов на задания домашней контрольной работы, такие контрольные работы оцениваются минимальным баллом – 0 баллов. Так же оценивается работа, написанная не по своему варианту (как домашняя, так и аудиторная). Требования к оформлению и содержанию факультативных работ устанавливаются преподавателем, проводящим такие контрольные работы, самостоятельно.

Однако предпочтительнее проводить работы, рассчитанные на 20-30 минут. В этом случае остается возможность обсудить вопросы занятия, предусмотренные программой учебной дисциплины.

Методические рекомендации для подготовки доклада.

Для подготовки презентации рекомендуется использовать: PowerPoint, MS Word, Acrobat Reader, LaTeX-овский пакет beamer. 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, которых всегда ждут слушатели

Промежуточная аттестация

По итогам 1 семестра(на ОФО) и 3 семестра (на ОЗФО и ЗФО) проводится зачет с оценкой. При подготовке к сдаче зачета рекомендуется пользоваться материалами практических занятий и материалами, изученными в ходе текущей самостоятельной работы.

Зачет проводится в устной форме, включает подготовку и ответы обучающегося на теоретические вопросы. По итогам зачета выставляется оценка.

По итогам обучения проводится зачет, к которому допускаются обучающиеся, имеющие положительные результаты по защите практических работ.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов		
			ОФО	ОЗФО	ЗФО
1	2	3	4	5	6
Семестр 1 ОФО, 3 семестр ЗФО					
1	Лекция: «Модели угроз и нарушителей информационной безопасности».	Технология развития критического мышления	2	2	2
2	Практическое занятие. «Каналы утечки информации в современных автоматизированных системах электронной обработки данных».	Игровые технологии	4	2	2
3	Практическое занятие. «Классификация внутренних и внешних нарушителей»	Игровые технологии	2	2	2
4	Практическое занятие. «Технологии аутентификации и шифрования»	Игровые технологии	2	2	2
5	Практическое занятие. «Безопасность web-ориентированного контента»	Игровые технологии	2	2	2
Итого часов в семестре:			**12**	**10**	**10**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной 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. 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
3. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — Самара : Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/43183.html
4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87992.html

Список дополнительной литературы

1. Аверченков, В. И. Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. — Брянск : Брянский государственный технический университет, 2012. — 184 с. — ISBN 978-89838-489-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/7002.html
2. Инструментальный контроль и защита информации : учебное пособие / Н. А. Свинарев, О. В. Ланкин, А. П. Данилкин [и др.]. — Воронеж : Воронежский государственный университет инженерных технологий, 2013. — 192 с. — ISBN 978-5-00032-018-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/47422.html

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

7.3. Информационные технологии, лицензионное программное обеспечение:

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 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)
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 IPR SMART	Лицензионный договор № 9368/22П от 01.07.2022 г. Срок действия: с 01.07.2022 до 01.07.2023
Бесплатное ПО: Lazarus, Firebird, IBE Expert, Python, VBA, 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:

Кафедра напольная - 1шт., стул преподавательский мягкий - 1шт., парты - 18шт., стулья мягкие -32шт., стулья – 11шт., доска меловая - 1шт.

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

Специализированная мебель:

Парты - 6шт., доска меловая - 1шт., компьютерные столы - 7шт., стол преподавательский - 3шт., стулья - 28 шт.

Технические средства обучения, служащие для предоставления учебной информации большой аудитории:

Компьютер в сборе(Системный блок)-7 шт.

3. 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 -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 доступа 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 тематические иллюстрации:
Интерактивная система - 1 шт.
Монитор– 20 шт.
Монитор - 1 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 Защищенные информационные системы и среды

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Защищенные информационные системы и среды

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-7	Способность на практике применять новые научные принципы и методы исследований

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-7
1	2
Раздел 1. Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты	+
Раздел 2. Уязвимость основных структурно-функциональных элементов распределенных АС.	+
Тема 2.2. Классификация внутренних и внешних нарушителей	+
Раздел 3. Классификация каналов проникновения в систему и утечки информации.	+
Раздел 4. Основные функции подсистемы защиты: основные защитные механизмы операционной системы семейства Unix, недостатки ее защитных механизмов.	+
Раздел 5. Защита файлов, контроль доступа, уязвимость паролей.	+
Раздел 6. Система безопасности Windows, система управления доступом, политика ограничений.	+
Раздел 7. Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.	+

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

Планируемы результаты обучения(показатели заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовл.	удовл.	хорошо	отлично	текущий контроль	промежут. аттестация
1	2	3	4	5	6	7
ПК-7 - способность на практике применять новые научные принципы и методы исследований						
ПК-7.1 Оценивает экономическую эффективность информационных процессов, ИС, а также проектных рисков	Допускает существенные ошибки при раскрытии экономической эффективности информационных процессов, ИС, а также проектных рисков	Неполные знания при раскрытии экономической эффективности информационных процессов, ИС, а также проектных рисков.	Сформированные, но содержащие отдельные пробелы в знаниях экономической эффективности информационных процессов, ИС, а также проектных рисков.	Сформированные и систематические знания экономической эффективности информационных процессов, ИС, а также проектных рисков.	ОФО, ОЗФО: Контрольная работа, доклад, коллоквиум тестирование, выполнение индивидуальных практических заданий ЗФО: Контрольная работа, доклад, коллоквиум тестирование, выполнение индивидуальных практических заданий	Зачет с оценкой
ПК-7.2 Выявляет и анализирует риски информационной безопасности	Не умеет и не готов выявлять и анализировать риски информационной безопасности.	При формулировке не использует методы для выявления и анализа рисков информационной безопасности	Выявляет и анализирует риски информационной безопасности.	Готов и умеет выявлять и анализировать риски информационной безопасности		Зачет с оценкой
ПК-7.3 Ставит и решает прикладные задачи в условиях неопределенности и определяет методы и средства их эффективного решения	Не владеет навыками решения прикладных задач в условиях неопределенности и определения методов и средств их эффективного решения.	Владеет отдельными навыками решения прикладных задач в условиях неопределенности и определения методов и средств их эффективного решения.	Владеет отдельными навыками решения прикладных задач в условиях неопределенности и определения методов и средств их эффективного решения.	Демонстрирует владение навыками решения прикладных задач в условиях неопределенности и определения методов и средств их эффективного решения.		Зачет с оценкой

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к зачету по дисциплине «Защищенные информационные системы и среды»

1. Предмет и задачи дисциплины «Защищенные информационные системы и среды».
2. Основные задачи защиты информации.
3. Классификация информации по уровню конфиденциальности. Реквизиты документов. Хранение информации.
4. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии
5. Основные направления защиты. Защита документов. Защита каналов утечки.
6. Мониторинг (аудит) действий пользователей.
7. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне. Другие типы нарушителей.
8. Нетехнические меры защиты от внутренних угроз. Психологические меры. Организационные меры.
9. Права локальных пользователей. Стандартизация ПО. Специфические решения.
10. Классификация firewall'oB.
11. Пакетные фильтры. Пограничные роутеры.
12. Персональные firewall'bi и персональные устройства firewall'a.
13. Прокси-сервер прикладного уровня. Выделенные прокси-серверы.
14. Гибридные технологии firewall'a. Трансляция сетевых адресов (NAT). Статическая трансляция сетевых адресов. Скрытая трансляция сетевых адресов.
15. Принципы построения окружения firewaH'a. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-сетями.
16. Виртуальные частные сети.
17. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях.
18. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы.
19. SMTP-серверы. Политика безопасности firewall'a. Политика firewall'a. Реализация набора правил firewall'a. Тестирование политики firewall'a. Возможные подходы к эксплуатации firewaH'a.
20. Сопровождение firewall'a и управление firewall'oM. Физическая безопасность окружения firewaH'a. Администрирование firewaH'a.
21. Встраивание firewall'oB в ОС.Стратегии восстановления после сбоев firewall'a.
22. Инциденты безопасности.
23. Основные характеристики пакетных фильтров в ОС FreeBSD.
24. ПО пакетным фильтрам. OpenBSD Packet Filter (PF) и ALTQ.
25. Трансляция сетевых адресов для очень больших LAN. Использование пула публичных адресов. Port Redirection
26. Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS.
27. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target.
28. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление.
29. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based

IDS. Application-Based IDS.

30. Анализ, выполняемый IDS. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS. Активные действия. Сбор дополнительной информации.
31. Изменение окружения. Выполнение действия против атакующего. Пассивные действия. Тревоги и оповещения. Использование SNMP Traps. Возможности отчетов и архивирования.
32. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей.
33. Host-Based анализ уязвимостей.
34. Network-Based анализ уязвимостей.
35. Преимущества и недостатки систем анализа уязвимостей.
36. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS.
37. Цели и задачи использования IDS.
38. Ограничения на ресурсы, существующие в организации. Возможности IDS.
39. Развертывание IDS. Стратегия развертывания IDS.
40. Типичные выходные данные IDS.
41. Типы компьютерных атак, обычно определяемые IDS.
42. Безопасность DNS. Сервисы DNS. Инфраструктура DNS.
43. Компоненты DNS и понятие безопасности для них.
44. Основные механизмы безопасности для сервисов DNS.
45. Данные DNS и ПО DNS. Зонный файл. Name-серверы. Авторитетные name- серверы. Кэширующие name-серверы. Resolver'bi. Транзакции DNS. Запрос / ответ DNS.
46. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.
47. Причины уязвимости web-сервера. Планирование развертывания web-сервера. Безопасность лежащей в основе ОС.
48. Безопасное инсталлирование и конфигурирование ОС. Применение Patch иUpgrade ОС. Удаление или запрещение ненужных сервисов и приложений. Конфигурирование аутентификации пользователя в ОС.
49. Управление ресурсами на уровне ОС. Альтернативные платформы для web- сервера. Trusted ОС.
50. Использование Appliances для web-сервера. Специально усиленные (pre-hardened) ОС и web-серверы.
51. Тестирование безопасности операционной системы. Список действий для обеспечения безопасности ОС, на которой выполняется web-сервер.
52. Безопасное инсталлирование и конфигурирование web-сервера. Безопасное инсталлирование web-сервера. Конфигурирование управления доступом.
53. Разграничение доступа для ПО web-сервера. Управление доступом к директории содержимого web-сервера.
54. Управление влиянием web Bots. Использование программ проверки целостности файлов. Список действий для безопасного инсталлирования и конфигурирования web-сервера.
55. Опубликование информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
56. Уязвимости технологий активного содержимого на стороне клиента.
57. Уязвимости технологий создания содержимого на стороне сервера. Списокдействий для обеспечения безопасности web-содержимого.
58. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-

адресе. Basic-аутентификация. Digest-аутентификация.

59. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS.Требования к реализации SSL/TLS.
60. Список действий для технологий аутентификации и шифрования. Firewall прикладного уровня для web — ModSecurity. Взаимодействие ModSecurity с пакетным фильтром.
61. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы.
62. Роутер и firewall.
63. Автоматизированные инструментальные средства анализа лог-файлов. Процедуры создания backup web-сервера.
64. Политики и стратегии выполнения backup'a web-сервера. Поддержка тестового web-сервера.
65. Поддержка аутентичной копии web-содержимого. Восстановление при компрометации безопасности.
66. Тестирование безопасности web-серверов. Сканирование уязвимостей. Тестирование проникновения.
67. Удаленное администрирование web-сервера. Список действий для безопасного администрирования web-сервера

Вопросы для устного опроса

по дисциплине «Защищенные информационные системы и среды»

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.

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

Вопросы для коллоквиума

по дисциплине «Защищенные информационные системы и среды»

1. Основные понятия, категории и инструменты проектирования, разработки, внедрения и управления информационными системами предприятия и информационной защиты.
2. Классификация информационных систем по способу распределения вычислительных ресурсов.
3. Средств обеспечения безопасности информационных систем.
4. Правовое обеспечение информационных систем.
5. Классификация информационных систем по типу вычислительной среды.
6. Понятие системы кодирования информации. Виды систем кодирования.
7. Классификация информационных систем по количеству ЭВМ. Факторы перехода к многомашинным информационным системам.
8. Угрозы безопасности информационных систем.
9. Основные международные и российские стандарты в области информационной безопасности.
10. Внешняя и внутренняя среда предприятия с точки защищенности информационной системы, ее ключевые элементы.
11. Комплекс мер по обеспечению защиты информационных систем и сред.
12. Современные программно-аппаратные системы информационной защиты применительно к конкретному предприятию.

Темы для докладов

по дисциплине: «Защищенные информационные системы и среды»

1. Применение защищенных информационных систем среды.
2. Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
3. Методы и средства защиты информационных систем.
4. Проблема оценки защищенности информационных систем среды.
5. Виртуальная консолидация данных.
6. Способы хранения информации.
7. Интеллектуальные дисковые массивы.
8. Криптографическая защита информации.
9. Требования к аутентификации и шифрованию.
10. Классификация информации по уровню конфиденциальности. Реквизиты документов.
11. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей
12. Нетехнические меры защиты от внутренних угроз.
13. Психологические меры. Организационные меры
14. Персональные firewall'bi и персональные устройства firewall'a
15. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы.
16. Основные характеристики пакетных фильтров в ОС FreeBSD.
17. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS.
18. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS.
19. Авторитетные name-серверы. Кэширующие name-серверы. Resolver'bi.
20. Безопасное инсталлирование и конфигурирование ОС
21. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
22. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе.
23. Автоматизированные инструментальные средства анализа лог-файлов

Вопросы для контрольной работы

по дисциплине «Защищенные информационные системы и среды»

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

.

Индивидуальные задания к практическим занятиям

по дисциплине Защищенные информационные системы и среды

1. Создать группу gBuh и выполнить регистрацию двух пользователей uBuh1 и uBuh2, включив их в созданную группу.
2. Создать рабочую папку FBuh. Предоставить полный доступ к папке только членам группы gBuh.
3. Создать папку Share с вложенными папками In и Out. Предоставить сетевой доступ к папкам по принципу: ..Share\In – только на запись, Share\Out – только на чтение.
4. Выполнить настройки парольной защиты: длина пароля, срок действия, сложность.
5. Выполнить регистрацию пользователя и предоставить ему административные права.
6. Выполнить регистрацию пользователя, включить пользователя в группу "Опытные пользователи". Создать рабочую папку для зарегистрированного пользователя в папке c:\work и предоставить только этому пользователю полный доступ к созданной папке.
7. Провести настройку входа в систему: в окне регистрации отображаются поля для ввода логина и пароля пользователя.
8. Настроить политику блокировки учетных записей: пороговое значение блокировки, продолжительность блокировки учетной записи.
9. Настроить политику аудита: Аудит входа в систему, Аудит системных событий.
10. Написать командный файл, выполняющий регистрацию пользователя. Имя пользователя (логин) и пароль должны вводиться по запросу.
11. Написать командный файл, который добавляет новую группу и регистрирует в этой группе пользователя. Имя группы и пользователя вводятся по запросу.
12. Написать командный файл, выводящий список зарегистрированных пользователей и формирующий запрос на удаление пользователя: имя удаляемого запрашивается.
13. Выполнить отключение служб:

- Удаленный реестр.
- Удаленные рабочие столы.
- Вспомогательный IP.
- Удаленный реестр (его лучше отключать даже в том случае, если вы работаете в сети).
- Модуль NetBios.
- Браузер персональных компьютеров.
- Сервер.
- Поставщик домашних групп.

ТЕСТОВЫЕ ВОПРОСЫ

по дисциплине «Защищенные информационные системы и среды»

Раздел 1.Угрозы безопасности, архитектуры системы защиты: особенности современных АС как объекта защиты

1.Укажите что из перечисленного не относится к числу основных аспектов информационной безопасности:

1) Доступность;
2) Целостность;
3) Защита от копирования;
4) Конфиденциальность.

2.Укажите какие слова пропущены в следующей фразе

«Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё - это _____ _____.»

3.Укажите какая из приведенных техник является самой важной при выборе конкретных защитных мер

а) Анализ рисков
б) Анализ затрат / выгоды
в) Результаты ALE
г) Выявление уязвимостей и угроз, являющихся причиной риска

4.Эффективная программа безопасности требует сбалансированного применения:

а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования

Раздел 2. Уязвимость основных структурно- функциональных элементов распределенных АС.

1.Укажите какое слово пропущено в следующей фразе

«Субъект (лицо или группа лиц), реализующий угрозы информационной безопасности организации (по ошибке, незнанию или осознанно), путем нарушения предоставленных ему полномочий по доступу к активам организации или по распоряжению ими – это _____ информационной безопасности.»

2. Системы, которые используют два математически связанных друг с другом ключа, называют:

1) асимметричными;
2) симметричным;
3) квадратурными;
4) циклическими.

3.Искусственные угрозы безопасности информации вызваны:

1) Деятельностью человека;
2) Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4) Корыстными устремлениями злоумышленников;
5) Ошибками при действиях персонала.

4. Укажите пропущенное слово в следующем предложении

«Наиболее рискованной для организации с точки зрения вероятного мошенничества и нарушения безопасности является категория людей -_____ организации.»

Раздел 3. Классификация каналов проникновения в систему и утечки информации.

1. Укажите какое слово пропущено в следующем предложении

« Каналы _____ информации -методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой.»

2. Укажите какое слово пропущено в предложении

«_____ каналы не требуют непосредственного доступа к техническим средствам информационной системы.

3. Укажите что относится к акустическим каналам утечки информации

1. запись звука, подслушивание и прослушивание;
2. получение информации через звуковые волны с дальнейшей передачей её через сети электропитания;
3. сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
4. визуальные методы, фотографирование, видеосъемка, наблюдение.

4.Укажите пропущенное слово в следующем предложении

«_____информации от утечки по техническим каналам осуществляется на основе конституций и законов, а также защита обеспечивается наличием авторских свидетельств, патентов, товарных знаков»

Раздел 4. Основные функции подсистемы защиты: основные защитные механизмы операционной системы, недостатки защитных механизмов.

1. Укажите какое слово пропущено в следующем предложении

«В ОС семейства _____, вследствие реализуемой ею концепции администрирования (не централизованная),невозможно обеспечить замкнутость (или целостность)программной среды.»

2. Укажите какое слово пропущено в следующем предложении

«_____доступа называют любой элемент ОС, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен».

3. Укажите правильную последовательность формулирования правил разграничения доступа в модели безопасности

Варианты ответов

1. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
2. Для каждой четверки субъект—объект—метод—процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться.
3. Для любого объекта ОС существует владелец.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.

4. Укажите виды информационной безопасности:

1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

Раздел 5. Защита файлов, контроль доступа, уязвимость паролей.

1.Укажите пропущенное слово в предложении

«Широкие, высокоуровневые заявления руководства - _____ безопасности.»

2.Информация по способу доступа к ней бывает:

1. открытая (общедоступная) и закрытая (конфиденциальная);
2. избыточная, достаточная и недостаточная;
3. исходная, промежуточная и результирующая;
4. постоянная, переменная и смешанная

3.Укажите название группы к которой относятся угрозы,которые основываются на переполнении буфера для входных данных (переполнение стека)и последующей передачи управления на исполняемый код,занесенный при этом в стек.

1. Угрозы, позволяющие несанкционированно запустить исполняемый код
2. Угрозы,позволяющие осуществить несанкционированные операции чтения/записи
3. Угрозы,позволяющие обойти установленные разграничения прав доступа
4. Угрозы,приводящие к отказу в обслуживании (Denial of Service — системный сбой)

4. Укажите какое слово пропущено в предложении

«_____ защищенности -попытку "взлома" информационной системы, осуществляемого силами самой организации или уполномоченными лицами».

Раздел 6. Система безопасностиWindows, система управления доступом, политика ограничений.

1.Основными субъектами информационной безопасности являются:

1. руководители, менеджеры, администраторы компаний
2. органы права, государства, бизнеса
3. сетевые базы данных, фаерволлы

2.К основным функциям системы безопасности можно отнести все перечисленное:

1. Установление регламента, аудит системы, выявление рисков
2. Установка новых офисных приложений, смена хостинг-компании
3. Внедрение аутентификации, проверки контактных данных пользователей

3.К основным типам средств воздействия на компьютерную сеть относится:

1. Компьютерный сбой
2. Логические закладки («мины»)
3. Аварийное отключение питания

4.Наиболее распространены средства воздействия на сеть офиса:

1. Слабый трафик, информационный обман, вирусы в интернет
2. Вирусы в сети, логические мины (закладки), информационный перехват
3. Компьютерные сбои, изменение администрирования, топологии

5. Укажите какое слово пропущено следующем предложении

«Политики паролей используются для учетных записей _____.»

Раздел 7. Обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.

1. Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

2.Окончательно, ответственность за защищенность данных в компьютерной сети несет:

1. Владелец сети
2. Администратор сети
3. Пользователь сети

3.Наиболее важным при реализации защитных мер политики безопасности является:

1. Аудит, анализ затрат на проведение защитных мер
2. Аудит, анализ безопасности

3. Аудит, анализ уязвимостей, риск-ситуаций

4.Укажите под какие системы распространение вирусов происходит наиболее динамично:

1. Windows
2. Mac OS
3. Android

5. Укажите какие слова пропущены в предложении

«Преднамеренной угрозой безопасности информации является _____.»

5. Методические материалы, определяющие процедуры оценивания компетенции

5.1. Критерии оценивания доклада

Критерии оценки:

- *оценка «зачтено» выставляется обучающемуся, если*:

- тема соответствует содержанию доклада;
- широкий круг и адекватность использования литературных источников по проблеме;
- правильное оформление ссылок на используемую литературу;
- основные понятия проблемы изложены достаточно 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;

- *оценка «не 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 методических указаний;
- не проведен анализ материалов реферата;
- нет выводов.

5.2. Критерии оценивания коллоквиума

- *«зачтено» выставляется обучающемуся, 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;

-*«не зачтено»:*

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

5.3. Критерии оценки устного опроса

- **Оценка «отлично»** выставляется обучающемуся, если он свободно владеет терминологией, демонстрирует прекрасное знание предмета, соединяя при ответе

знания из разных разделов дисциплины, добавляя комментарии, пояснения, может быстро и безошибочно проиллюстрировать ответ собственными примерами.Владеет аргументацией, грамотной, доступной и понятной речью.

- **Оценка «хорошо»**, владеет терминологией, делая ошибки, при неверном употреблении сам может их исправить, хорошо владеет содержанием изучаемой темы, видит взаимосвязи, может провести анализ, но не всегда делает это самостоятельно без помощи преподавателя, может подобрать соответствующие примеры, чаще из имеющихся в учебных материалах. Хорошая аргументация, четкость, лаконичность ответов.
- **Оценка «удовлетворительно»**, редко использует при ответе термины, подменяет одни понятия другими, не всегда понимая разницы, отвечает на конкретный вопрос соединяя знания только при наводящих вопросах преподавателя, с трудом может соотнести теорию и практические примеры из учебных материалов; примеры не всегда правильные. Слабая аргументация, нарушена логика при ответе, однообразные формы изложения мыслей.
- **Оценка «неудовлетворительно»**, при ответе не владеет профессиональной терминологией. Неуверенное и логически непоследовательно излагает материал, обнаруживает пробелы в знаниях основного учебного материала, не может привести примеры из учебной литературы, затрудняется с ответом на поставленные преподавателем вопросы.

5.4. Критерии оценивания дифференциального зачета:

Описание шкалы и критериев оценивания для проведения промежуточной аттестации обучающихся по дисциплине в форме дифференцированного зачета

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

Оценка			
«2» (неудовлетворительно)	Пороговый уровень освоения	Углубленный уровень освоения	Продвинутый уровень освоения
	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Обучающийся не знает значительной части программного материала, плохо ориентируется в экономической терминологии, допускает существенные ошибки.	Обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательност	Обучающийся твердо знает материал, не допускает существенных неточностей в ответе на вопрос.	Обучающийся знает научную терминологию, методы и приемы анализа проблем в экономике и управлении, глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, не затрудняется с ответом при видоизменении заданий.

	и в изложении программного материала.		
Не умеет анализировать и оценивать угрозы информационной безопасности, 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 анализировать и оценивать угрозы информационной безопасности в защищенных информационных системах и средах. 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 организации и обеспечения режима секретности 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 организации и обеспечения режима секретности информационных систем, глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний.

5.5. Критерии оценивания тестирования

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

5.6. Критерии оценивания контрольной работы

Критерии оценки:
- «отлично» выставляется обучающемуся, если полностью раскрыт вопрос задания, приведены формулы и решения;
- оценка «хорошо» вопрос задания раскрыт на ¾, допускаются неточности в формулах;
- оценка «удовлетворительно» вопрос задания раскрыт на 2/4, допускаются ошибки в формулах и решениях;
- оценка «неудовлетворительно» вопрос задания нераскрыт или приведен ответ на другой вопрос.

5.7 Критерии оценки индивидуальных практических заданий:

Оценка «отлично» выставляется обучающемуся, если он свободно владеет терминологией, демонстрирует прекрасное знание предмета, соединяя при ответе знания из разных разделов дисциплины, добавляя комментарии, пояснения, может быстро и безошибочно проиллюстрировать ответ собственными примерами. Владеет аргументацией, грамотной, доступной и понятной речью.

Оценка «хорошо», владеет терминологией, делая ошибки, при неверном употреблении сам может их исправить, хорошо владеет содержанием изучаемой темы, видит взаимосвязи, может провести анализ, но не всегда делает это самостоятельно без помощи преподавателя, может подобрать соответствующие примеры, чаще из имеющихся в учебных материалах. Хорошая аргументация, четкость, лаконичность ответов.

Оценка «удовлетворительно», редко использует при ответе термины, подменяет одни понятия другими, не всегда понимая разницы, отвечает на конкретный вопрос соединяя знания только при наводящих вопросах преподавателя, с трудом может соотнести теорию и практические примеры из учебных материалов; примеры не всегда правильные. Слабая аргументация, нарушена логика при ответе, однообразные формы изложения мыслей.

Оценка «неудовлетворительно», при ответе не владеет профессиональной терминологией. Неуверенное и логически непоследовательно излагает материал, обнаруживает пробелы в знаниях основного учебного материала, не может привести примеры из учебной литературы, затрудняется с ответом на поставленные преподавателем вопросы.