МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Проректор по научной работе
(наименование должности полностью)
_____ О.Г. Добросердов
(подпись, инициалы, фамилия)
«28» 06 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и системы защиты информации, информационная безопасность
(наименование дисциплины)

направление подготовки 10.06.01
шифр согласно ФГОС ВО

Информационная безопасность
наименование направления подготовки

Методы и системы защиты информации, информационная безопасность
наименование профиля (специализация подготовки)

квалификация (степень) выпускника: Исследователь. Преподаватель-исследователь

форма обучения очная
(очная, заочная)

Курск – 2016

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (уровень подготовки кадров высшего образования) направления подготовки 10.06.01 «Информационная безопасность», на основании учебного плана профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 11 «27» 06 2016 г.

Рабочая программа обсуждена и рекомендована к применению в образовательном процессе для обучения аспирантов по направлению подготовки 10.06.01 «Информационная безопасность», профиля (специализации) «Методы и системы защиты информации, информационная безопасность» на заседании кафедры информационной безопасности, протокол № 1 от «30» 08 2016 г.

Зав. кафедрой _____ М.О. Таныгин

Разработчик программы _____ Ю.А. Халин

Согласовано:

Директор научной библиотеки _____ В.Г. Макаровская

Начальник отдела аспирантуры и докторантуры _____ О.Ю. Прусова

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 1 от 28.08.2017

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 8 «26» 03 2018 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 12 от 29.06.2018.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол № 9 «24» 06 2019 г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол 11 от 27.06.2019

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №11 «29» 06 2020г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол N 1 от 31.08.2020

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №8 «31» 05 2021г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____ / протокол N 11 от 28.06.2021

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №8 «31» 05 2021г. на заседании кафедры информационной безопасности. протокол №11 от 30.06.2022

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №8 «31» 05 2021г. на заседании кафедры информационной безопасности. протокол №1 от 30.08.2023

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.06.01 «Информационная безопасность» профиля (специализации) «Методы и системы защиты информации, информационная безопасность», одобренного Ученым советом университета протокол №__ «__»_____20__г. на заседании кафедры информационной безопасности.

Зав. кафедрой _____

1 Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения ОП

1.1 Цель преподавания дисциплины

Целью преподавания дисциплины «Методы и системы защиты информации, информационная безопасность» является получение аспирантами знаний о принципах построения, идеологии и архитектуре современных систем защиты информации.

1.2 Задачи изучения дисциплины

В результате изучения дисциплины аспиранты должны:

- получить знания о назначении, принципах функционирования и структуре систем защиты информации;
- получить знания о функционировании подсистемы управления процессами защиты информации;
- получить знания о функционировании систем управления распределением доступа к ресурсам
- получить знания о функционировании подсистем управления и защиты памяти в различных системах;
- получить знания о назначении, организации и функционировании подсистем защиты файловых систем;
- получить знания о функционировании подсистемы защиты устройств ввода – вывода;
- получить знания о принципах организации защиты информации в операционных системах семейств Windows и UNIX;
- получить знания о методах и средствах оценки производительности и эффективности систем защиты информации.
- получить знания о механизмах защиты объектов.

1.3 Компетенции, формируемые в результате освоения дисциплины

У обучающихся формируются следующие **компетенции**:

ОПК-1 – способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность;

ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности;

ОПК-3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности;

ПК-1 - способностью к решению научных и технических проблем разработки новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности объектов;

ПК-2 - способностью исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки;

ПК-3 – способность анализировать степень защищенности и совершенствовать системы документооборота и средства защиты циркулирующей в них информации;

ПК-4 – способность разрабатывать новые и совершенствовать имеющиеся методы, аппаратно-программные и организационные средства защиты информационных систем и ресурсов.

ПК-5 – способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа;

УК-1 - способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Методы и системы защиты информации, информационная безопасность» Б1.В.ОД.6 является дисциплиной вариативной части Блока 1«Дисциплины (модули)» раздела «Обязательные дисциплины» УП по направлению подготовки 10.06.01 «Информационная безопасность», изучается на 4 курсе в 8 семестре.

3 Содержание и объем дисциплины»

3.1 Содержание дисциплины и лекционных занятий

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единицы (з.е.), 144 часа.

Таблица 3.1 –Объём дисциплины по видам учебных занятий

Объём дисциплины	Всего, часов
Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	
в том числе:	54,15
лекции	36
лабораторные занятия	не предусмотрено
практические занятия	18
экзамен	0,15
зачет	не предусмотрено
Аудиторная работа (всего):	54
в том числе:	
лекции	36
лабораторные занятия	не предусмотрено
практические занятия	18
Самостоятельная работа обучающихся (всего)	54
Контроль/экз (подготовка к экзамену)	не предусмотрено

Таблица 3.2 – Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ лаб.	№ пр.			
1	2	3	4	5	6	7	8
1	Основные угрозы информации, обрабатываемой в компьютерных системах. Особенности построения систем защиты информации в зависимости от источника угроз	1, 2 часа	0	1	У-1 У-2	КО 1 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
2	Использование средств разграничения доступа для повышения защищённости компьютерных систем. Использование мониторов безопасности повышения защищённости компьютерной системы.	2, 2 часа	0	2	У-1 У-2	КО 2 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1

3	Особенности реализации политик безопасности в компьютерных системах	3, 2 часа	0	3	У-1 У-2	К 3 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
4	Изменение конфигурации оборудования для повышения защищённости компьютерных систем	4, 2 часа	0	4	У-1 У-2	КО 4 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
5	Использования шифрования для повышения защищённости компьютерных систем. Использование криптографического хэширования для контроля целостности программ и данных	5, 2 часа	0	5	У-1 У-2	КО 5 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
6	Механизмы защиты баз данных. Разграничение доступа. Механизмы защиты баз данных. Механизм ролей	6, 2 часа	0	6	У-1 У-2 У-3	КО 6 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
7	Обеспечение надёжности баз данных. Особенности резервного копирования. Журналирование изменений	7, 2 часа	0	7	У-1 У-2	К 7 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
8	Механизмы повышения защищённости, реализуемые в центральном процессоре	8, 2 часа	0	8	У-1 У-2	КО 8 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4

							ПК-5 УК-1
9	Механизмы повышения защищённости, реализуемые во внешних устройствах	9, 2 часа	0	9	У-1 У-2	КО 9 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
10	Механизмы защиты файловых систем	10, 2 часа	0	10	У-1 У-2	КО 10 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
11	Скрытые каналы по памяти и по данным. Борьба со скрытыми каналами.	11, 2 часа	0	11	У-1 У-2	КО 11 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
12	Межсетевые экраны. Назначение, основные виды, особенности использования.	12, 2 часа	0	12	У-1 У-2	КО 12 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
13	Виртуальные частные сети. Назначение, основные виды, особенности использования.	13, 2 часа	0	13	У-1 У-2	КО 13 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
14	Системы обнаружения атак. Назначение, основные виды, особенности использования.	14, 2 часа	0	14	У-1 У-2	КО 14 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2

							ПК-3 ПК-4 ПК-5 УК-1
15	Кольцевая система защиты памяти процессов. Особенности совместного использования процессами общих объектов в памяти.	15, 4 часа	0	15	У-1 У-2	КО 15-16 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
16	Уязвимости платформы Windows NT. Переполнение буфера	16, 4 часа	0	16	У-1 У-2	КО 17-18 неделя	ОПК1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1
	ИТОГО	36				Э	

Таблица 3.3 – Краткое содержание лекционного курса

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Тема 1. Основные угрозы информации, обрабатываемой в компьютерных системах.	Особенности построения систем защиты информации в зависимости от источника угроз
2	Тема 2. Использование средств разграничения доступа для повышения защищённости компьютерных систем.	Использование мониторов безопасности повышения защищённости компьютерной системы.
3	Тема 3. Особенности реализации политик безопасности в компьютерных системах	Назначение, основные виды, особенности использования.
4	Тема 4. Изменение конфигурации оборудования для повышения защищённости компьютерных систем	Назначение, основные виды, особенности использования.
5	Тема 5. Использования шифрования для повышения защищённости компьютерных систем.	Использование криптографического хэширования для контроля целостности программ и данных

6	Тема 6. Механизмы защиты баз данных.	Разграничение доступа. Механизмы защиты баз данных. Механизм ролей
7	Тема 7. Обеспечение надёжности баз данных.	Особенности резервного копирования. Журналирование изменений
8	Тема 8. Механизмы повышения защищённости, реализуемые в центральном процессоре	Назначение, основные виды, особенности использования.
9	Тема 9. Механизмы повышения защищённости, реализуемые во внешних устройствах	Назначение, основные виды, особенности использования.
10	Тема 10. Механизмы защиты файловых систем	Назначение, основные виды, особенности использования.
11	Тема 11. Скрытые каналы по памяти и по данным.	Борьба со скрытыми каналами.
12	Тема 12. Межсетевые экраны.	Назначение, основные виды, особенности использования.
13	Тема 13. Виртуальные частные сети.	Назначение, основные виды, особенности использования.
14	Тема 14. Системы обнаружения атак.	Назначение, основные виды, особенности использования.
15	Тема 15. Кольцевая система защиты памяти процессов.	Особенности совместного использования процессами общих объектов в памяти.
16	Тема 16. Уязвимости платформы Windows NT.	Переполнение буфера платформы Windows NT.

3.2 Лабораторные работы и (или) практические занятия

3.2.2 Практические занятия

Таблица 3.4 –Практические занятия

№	Наименование практического занятия	Объем, час.
1	2	3
1	Изучение организации защиты визуальной памяти	3
2	Реализация политики безопасности	3
3	Изучение организации защиты визуальной памяти	3
4	Изучение принципов организации ввода-вывода	3
5	Реализация скрытого канала передачи информации	3
6	Моделирование системы защиты информации	3
Итого		18

3.3 Самостоятельная работа аспирантов (СРС) (пунк 4-5 не знаю)

Таблица 3.5 – Самостоятельная работа студентов

№ раздела (темы)	Наименование раздела (темы) дисциплины	Срок выполнения	Время, затрачиваемое на выпол-нение СРС, час.
1	2	3	4
1	Изучение организации защиты визуальной памяти Подготовка *доклада с презентацией* и выступление с ним на круглом столе	2 - 3 неделя	6
2	Изучение модели «рабочий набор» при страничной организации визуальной памяти Подготовка *доклада с презентацией* и выступление с ним на круглом столе	4 - 5 неделя	6
3	Изучение принципов организации ввода-вывода Подготовка *доклада с презентацией* и выступление с ним на круглом столе	6 - 7 неделя	6
4	Реализация политики безопасности Подготовка *доклада с презентацией* и выступление с ним на круглом столе	8 - 9 неделя	6
5	Реализация скрытого канала передачи информации Подготовка *доклада с презентацией* и выступление с ним на круглом столе	10 - 11 неделя	6
6	Моделирование системы защиты информации Подготовка *доклада с презентацией* и выступление с ним на круглом столе	12-14 неделя	8
7	Изучение функций диспетчера памяти Подготовка *доклада с презентацией* и выступление с ним на круглом столе	15-16 неделя	8
8	Методы построения математических моделей для определения характеристик систем защиты информации Подготовка *доклада с презентацией* и выступление с ним на круглом столе	17-18 неделя	8
Итого			54

Общие рекомендации аспирантам изложены в Методических указаниях к выполнению самостоятельной работы.

4 Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

Аспиранты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки:

– методических рекомендаций, пособий по организации самостоятельной

– работы студентов;

– тем рефератов;

– вопросов к зачету;

– методических указаний к выполнению лабораторных работ и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

5 Образовательные технологии

В соответствии с требованиями Федеральным государственным образовательным стандартом высшего образования направления подготовки *10.06.01 – «Информационная безопасность»,* утвержденного Министерством образования и науки Российской Федерации приказом № 301 от 05.04.2017г., реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков аспирантов. В рамках дисциплины предусмотрены встречи с экспертами и специалистами по информационной системам.

Таблица 5.1 – Образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Образовательные технологии	Объем, час.
1	2	3	4
1	Механизмы защиты баз данных.	лекция с элементами проблемного изложения	4
2	Механизмы повышения защищённости, реализуемые в центральном процессоре	технологии эвристического обучения	2
3	Механизмы повышения защищённости, реализуемые во внешних устройствах	технологии эвристического обучения	2
4	Реализация скрытого канала передачи информации	технологии коллективной мыслительной деятельности	4
5	Моделирование системы защиты информации	технологии развития критического мышления	4
Итого:			16

6 Фонд оценочных средств для проведения промежуточной аттестации

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 6.1 Этапы формирования компетенции

Код компетенции, содержание компетенции	Дисциплины (модули) при изучении которых формируется данная компетенция
1	2
ОПК-1 – способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной

	работы (диссертации)
ОПК-2 – способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ОПК-3 – способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Б1.В.ОД.4 Методология научных исследований при подготовке диссертации Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-1 - способность к решению научных и технических проблем разработки новых и совершенствования имеющихся методов и средств защиты информации и обеспечения информационной безопасности объектов	Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных

	результатах подготовленной научно-квалификационной работы (диссертации)
ПК-2 - способность исследовать угрозы нарушения информационной безопасности и совершенствовать методы, способы и средства защиты информации в процессе ее сбора, хранения и обработки	Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-3 – способность анализировать степень защищенности и совершенствовать системы документооборота и средства защиты циркулирующей в них информации	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-4 – способность разрабатывать новые и совершенствовать имеющиеся методы, аппаратно-программные и организационные средства защиты информационных систем и ресурсов	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.1 Системы документооборота и средства защиты циркулирующей в них информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
ПК-5 - способность разрабатывать новые и совершенствовать имеющиеся технологии идентификации и аутентификации пользователей и субъектов информационных процессов, систем разграничения доступа	Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.2 Технологии идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.1 Нейросетевые технологии в защите информации Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка

	научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)
УК-1 - анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Б1.Б.1 История и философия науки Б1.В.ОД.1 Методология науки и образовательной деятельности Б1.В.ОД.4 Методология научных исследований Б1.В.ОД.5 Методы анализа рисков нарушения информационной безопасности Б1.В.ОД.6 Методы и системы защиты информации, информационная безопасность Б1.В.ДВ.1.2 Технология идентификации и аутентификации пользователей и субъектов информационных процессов Б1.В.ДВ.2.2 Алгоритмы факторизации натуральных чисел как средство реализации асимметричного шифрования Б4.Г.1 Подготовка к сдаче и сдача государственного экзамена Б2.1 Педагогическая практика Б2.2 Научно-исследовательская практика Б3.1 Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук Б4.Д.1 Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)

Средствами промежуточного контроля успеваемости студентов являются защита практических заданий, опросы на практических занятиях по темам лекций. В конце семестра – экзамен. Перечень вопросов к зачеты представлен в приложении А.

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

- раскрыть различные аспекты усиления неопределенности и полезности риска;
- выделить критерии классификации рисков и охарактеризовать виды рисков в соответствии с выделенными критериями;
- ознакомить с теоретическими основами исследования рисков;
- охарактеризовать традиционные и современные методы исследования рисков, методы количественной оценки рисков;
- ознакомить с основными аксиомами и элементами современной теорией рисков и существующими концепциями риска;
- представить порядок проведения исследования рисков;
- охарактеризовать ценность информации в рисковых ситуациях;
- охарактеризовать критерии выбора в рисковых ситуациях;

– изучить методы моделирования рисковых ситуаций и обоснования решений;

– получение практических навыков идентификации рисков, сопровождающих те или иные виды деятельности в сфере информационной безопасности, связанных с той или иной ситуацией, формализации рисковых ситуаций, выбора методов оценки рисков и принятия решений.

Таблица 6.2 Показатели и критерии определения уровня сформированности компетенций (частей компетенций)

№ п/п	Код компетенции (или её части)	Уровни сформированности компетенции		
		Пороговый (удовлетворительный)	Продвинутый (хорошо)	Высокий (отлично)
1	2	3	4	5
1	ОПК-1	Знать:методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать:методы защиты информации,алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь:применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты

				информации, методологией научных исследований в области защиты информации
2	ОПК-2	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
3	ОПК-3	Знать: методы защиты информации. Уметь: применять	Знать: методы защиты информации, алгоритмы защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации,

		средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
4	ПК-1	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения

		на среднем удовлетворительном уровне.	Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
5	ПК-2	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов инфор-

				матизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
6	ПК-3	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных

				достижений в области защиты информации, методологией научных исследований в области защиты информации
7	ПК-4	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации

8	ПК-5	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности. Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации
9	УК-1	Знать: методы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности.	Знать: методы защиты информации, алгоритмы защиты информации. Уметь: применять средства защиты информации для решения практических задач в области ин-	Знать: методы защиты информации, алгоритмы защиты информации, методы анализа угроз и оценки рисков информационной безопасности.

	Владеть: основами теории и практики защиты информации на среднем удовлетворительном уровне.	формационной безопасности, проводить настройку средств защиты информации. Владеть: основами теории и практики защиты информации на хорошем уровне, методикой анализа научных достижений в области защиты информации.	Уметь: применять средства защиты информации для решения практических задач в области информационной безопасности, проводить настройку средств защиты информации, оценивать защищенность объектов информатизации. Владеть: основами теории и практики защиты информации на высоком профессиональном уровне, методикой анализа научных достижений в области защиты информации, методологией научных исследований в области защиты информации

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 6.3 Паспорт комплекта оценочных средств

№ п/п	Раздел (тема) дисциплины	Код компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Основные угрозы информации,	ОПК-1 ОПК-2 ОПК-3	Лекция	См. МУ	1	Оценка *отлично* – исчерпывающее владение программным материалом, понимание сущности

	обрабатываемой в компьютерных системах. Особенности построения систем защиты информации в зависимости от источника угроз	ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1				рассматриваемых процессов и явлений, твердое знание основных положений дисциплины, умение применять концептуальный аппарат при анализе актуальных проблем. Логически последовательные, содержательные, конкретные ответы на все вопросы экзаменационного билета и на дополнительные вопросы членов комиссии, свободное владение источниками. Статья или Реферат приняты без замечаний. Оценка *хорошо* – достаточно полные знания программного материала, правильное понимание сути вопросов, знание определений, умение формулировать тезисы и аргументы. Ответы последовательные и в целом правильные, хотя допускаются неточности, поверхностное знакомство с отдельными теориями и фактами, достаточно формальное отношение к рекомендованным для подготовки материалам. Статья или Реферат приняты без существенных замечаний. Оценка *удовлетворительно* – фрагментарные знания, расплывчатые представления о предмете. Ответ содержит как правильные утверждения, так и ошибки, возможно, грубые. Испытуемый плохо ориентируется в учебном материале, не может устранить неточности в своем ответе даже после наводящих вопросов членов комиссии. Статья или Реферат приняты с небольшими замечаниями. Оценка *неудовлетворительно* – отсутствие ответа хотя бы на один из основных вопросов, либо грубые ошибки в ответах, полное непонимание смысла проблем, не достаточно полное владение
2	Использование средств разграничения доступа для повышения защищённости компьютерных систем. Использование мониторов безопасности повышения защищённости компьютерной системы.	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция Практическое занятие	См. МУ	2	
3	Особенности реализации политик безопасности в компьютерных системах	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 УК-1	Лекция	См. МУ	3	
4	Изменение конфигурации оборудования для повышения защищённости компьютерных систем	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 УК-1	Лекция	См. МУ	4	
5	Использования шифрования для повышения защищённости компьютерных систем. Использование криптографического хэширования для контроля	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция	См. МУ	5	

	целостности программ и данных					терминологией. Статья или Реферат не приняты или не предоставлены.
6	Механизмы защиты баз данных. Разграничение доступа. Механизмы защиты баз данных. Механизм ролей	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция Практическое занятие	См. МУ	6	
7	Обеспечение надёжности баз данных. Особенности резервного копирования. Журналирование изменений	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция	См. МУ	7	
8	Механизмы повышения защищённости, реализуемые в центральном процессоре	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция	См. МУ	8	
9	Механизмы повышения защищённости, реализуемые во внешних устройствах	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция	См. МУ	9	
10	Механизмы защиты файловых систем	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция Практическое занятие	См. МУ	10	
11	Скрытые каналы по памяти и по	ОПК-1 ОПК-2 ОПК-3	Лекция	См. МУ	11	

	данным. Борьба со скрытыми каналами.	ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1				
12	Межсетевые экраны. Назначение, основные виды, особенности использования.	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция Практическое занятие	См. МУ	12	
13	Виртуальные частные сети. Назначение, основные виды, особенности использования.	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция	См. МУ	13	
14	Системы обнаружения атак. Назначение, основные виды, особенности использования.	ОПК-1 ОПК-2 ОПК-3 ПК-3 ПК-4 ПК-5 УК-1	Лекция Практическое занятие	См. МУ	14	
15	Кольцевая система защиты памяти процессов. Особенности совместного использования процессами общих объектов в памяти.	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция	См. МУ	15	
16	Уязвимости платформы Windows NT. Переполнение буфера	ОПК-1 ОПК-2 ОПК-3 ПК-1 ПК-2 ПК-3 ПК-4 ПК-5 УК-1	Лекция Практическое занятие	См. МУ	16	

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Список методических указаний, используемых в образовательном процессе, представлен в п. 7.2;
- Оценочные средства представлены в учебно-методическом комплексе дисциплины.

Текущий контроль знаний аспирантов осуществляется путём устного опроса при защите практических работ по лекционному материалу, связанному с тематикой защищаемой практической работы. По количеству защищённых аспирантом практических работ, уровню показанных им на защите знаний делается вывод о текущей успеваемости аспиранта.

На защите практических работ аспирант должен продемонстрировать знание методики выполнения практической работы, дать оценку полученным в ходе выполнения работы результатам, обосновать их теоретически, ответить на ряд вопросов, рассмотренных на лекциях и практических занятиях, связанных с тематикой выполненной работы.

Рейтинговый контроль не предусмотрен.

Описание оценочных средств и шкал оценивания ответов см. в Таблице 6.3.

Формой итогового контроля уровня знаний аспиранта является кандидатский экзамен.

На экзамене аспирант должен продемонстрировать знание лекционного материала, материалов, изученных на практических занятиях, в ходе индивидуальных занятий с аспирантами и при самостоятельной работе аспиранта.

Примерный перечень экзаменационных вопросов:

1. Понятия группы, "кольца, поля, их основные свойства.
2. Кольца вычетов. Кольцо многочленов над конечным полем. Поля Галуа.
3. Основные понятия теории вероятностей и математической статистики. Условная вероятность и независимость.
4. Цепи Маркова. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
5. Сходимость последовательностей случайных величин и сходимость распределений. Закон больших чисел.
6. Центральная предельная теорема. Основные задачи математической статистики.
7. Конечные автоматы. Граф перехода автомата. Графы и орграфы.
8. Перечисление графов и отображений. Алгоритмические задачи на графах.
9. Архитектура современной ЭВМ.
10. .Программный интерфейс вычислительной системы.
11. .Технология объектно-ориентированного программирования.

12. Функции ядра операционной системы и защита информации. Однопользовательская и многопользовательские многозадачные операционные системы.

13.Типовые конфигурации сети. Протоколы обмена данными. Маршрутизация сообщений в сети.

14. Системы управления базами данных. Реляционная, иерархическая и сетевая модели.

15.Основные принципы современной концепции обеспечения защиты информации. Требования к защите с позиции пользователя.

16. Основные методы защиты информации. Методология организации и проведении .работ по разработке и анализу средств защиты информации.

17. Основные положения государственной политики обеспечения информационной безопасности. Современная нормативно-правовая база в области защиты информации.

18. Понятие информации с ограниченным доступом. Цели защиты информации и степени секретности. Лицензирование в области защиты информации.

19. Сертификации средств защиты информации. Аттестации объектов информатики. Правовая основа сертификации.

20. Понятие угрозы информационной безопасности системы. Классификация угроз информационной безопасности.

21.Понятия непосредственных и опосредованных угроз. Основные уровни защиты информации в автоматизированных системах. Основные направления и методы реализации информационных угроз.

22. Понятие политики информационной безопасности. Каноническая модель управления доступом. Классификация каналов взаимодействия субъектов доступа.

23. Основные модели управления доступом с взаимодействием субъектов доступа.
24. Понятия дискреционного и мандатного механизмов управления доступом.

25. Метки безопасности, их назначение в разграничении прав доступа при реализации мандатной модели доступа.

26. Правила разграничения доступа для полномочной модели управления доступом. Особенности использования мандатного механизма управления доступом при разграничении прав доступа субъектов.

27. Правила назначения меток безопасности иерархическим объектам доступа.

28. Анализ возможностей корректной реализации канонических моделей управления доступом в ОС с использованием дискреционного механизма.

29. Анализ возможностей корректной реализации" моделей управления доступом с каналом взаимодействия субъектов доступа для ОС UNIX.

30. Принципы организации мандатного управления доступом к устройствам.

31 Возможности разграничения доступа к системному диску для ОС Windows NT/2000/XPи Unix.

32. Механизм обеспечения замкнутости программной среды и его роль в системе защиты.

33. Реализация механизмов парольной защиты.- Процедуры идентификации пользователя на рабочей станции и взаимной идентификации удаленных рабочих станций.

34.Контроль целостности информации, основные схемы контроля. Аутентификация информации.

.35. Угрозы преодоления парольной защиты. Усиление парольной защиты.

36. Стандарты в области защиты информации в вычислительной системе, "Оранжевая книга" США, российские стандарты.

37. Понятие симметричной и ассиметричной криптосистем. Основные типы криптоаналитических атак.

38. Шифрование методом простой замены. Алгоритм простой замены.

39. Шифрование методом полиалфавитной замены. Алгоритм полиалфавитной замены с использованием таблицы Вижинера.

40.Аддитивные методы шифрования. Шифрование методом перестановки. Карты Гамильтона.

41. Система открытого распространения ключей. Использование схемы открытого шифрования для создания цифровых подписей.

42.Применение хэш-функции для создания цифровых подписей. Алгоритм цифровой подписи с использованием хэш-функции.

43.Основные физические каналы утечки информации о функционировании информационной системы.

44. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки.

45.Технические параметры современных средств перехвата побочных сигналов. Методы и средства зашиты от инженерно-технической разведки.

46. Методика оценки качества инженерно-технической защиты.

47.Разрушающие программные воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействий.

48. Классификация вирусов. Методы выявления и защиты от вирусов.

49. Методика анализа алгоритмов защиты программных реализаций информационных систем.

50. Методы восстановления алгоритмов защиты в программных продуктах Оценка уровня криптографической защиты типовых программных продуктов.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная и дополнительная литература

а) основная литература:

1. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М. А. Иванов, И. Чугунков. – Москва : МИФИ, 2012. - 400 с. – Режим доступа : Biblioclub.ru

2. Таныгин, М. О. Программно-аппаратные системы защиты информации [Текст]: учебное пособие / Юго-Западный гос. ун-т ; Министерство образования и науки Российской Федерации, Юго-Западный государственный университет. - Курск : ЮЗГУ, 2012. - 147 с.

3. Таныгин, М. О. Программно-аппаратные системы защиты информации [Электронный ресурс] : учебное пособие / М. О. Таныгин ; Министерство

образования и науки Российской Федерации, Юго-Западный государственный университет. - Курск : ЮЗГУ, 2012. - 147 с.

4. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=276557

5. Методологические основы построения защищенных автоматизированных систем [Электронный ресурс] : учебное пособие / А. В. Душкин [и др.]. – Воронеж : ВГУИТ, 2013. - 258 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=255851

б) дополнительная литература:

1. Жуков И. Ю. Стохастические методы и средства защиты информации в компьютерных системах и сетях [Текст] / под ред. И. Ю. Жукова. - М. : КУДИЦ-ПРЕСС, 2009. - 512 с.

2. Торокин, А. А. Инженерно-техническая защита информации [Текст] : учебное пособие / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 960 с.

3. Пескова, С. А. Сети и телекоммуникации [Текст] : учебное пособие / С. А. Пескова, А. В. Кузин, А. Н. Волков. - 2-е изд., стер. - М. : Академия, 2007. - 352 с.

4. Илюшечкин, Владимир Михайлович. Основы использования и проектирования баз данных [Текст] : учебное пособие / В. М. Илюшечкин. - М. : Юрайт, 2010. - 213 с.

5. Бройдо, В. Л. Архитектура ЭВМ и систем [Текст] : учебник для вузов / В. Л. Бройдо, О. П. Ильина. - 2-е изд. - СПб. : Питер, 2009. - 720 с.

6. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

7. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты [текст] : учебное пособие / В. А. Тихонов, В. В. Райх. – М. : Гелиос АРВ, 2006. - 528 с.

8. Малюк А. А. Информационные безопасность: концептуальные и методологические основы защиты информации [Текст] / А. А. Малюк – М. : Горячая линия, 2004.-280 с.

9. Баричев, С. Г. Основы современной криптографии [Текст] : учебный курс / В. В. Гончаров, Р. Е. Серов. - 2-е изд., перераб. и доп. - М. : Горячая линия - Телеком, 2002. - 175 с.

10. Методы и средства защиты компьютерной информации [Электронный ресурс] : учебное пособие / А. А. Безбогов, А. В. Яковлев, В. Н. Шамкин. – Тамбов : Издательство ТГТУ, 2006.- 196 с. – Режим доступа : http://window.edu.ru

7.2 Перечень методических указаний

1. Организация работы групповых политик безопасности Windows XP Professional [Электронный ресурс] : методические указания по выполнению лабораторной работы для студентов специальности 090104 / ЮЗГУ ; сост.: И. В.

Калуцкий, А. А. Липунов. - Курск : ЮЗГУ, 2011. - 40 с.

2. Настройка межсетевого взаимодействия [Электронный ресурс] : методические указания по выполнению лабораторной работы по дисциплинам «Администрирование вычислительных сетей», «Администрирование вычислительных систем», «Программно-аппаратная защита информации», «Методы и средства защиты информации в системах электронного документооборота» / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, С.В. Пономарев. Курск, 2014. - 20 с.

7.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. http://school-collection.edu.ru/ - федеральное хранилище Единая коллекция цифровых образовательных ресурсов
2. http://www.edu.ru/ - федеральный портал Российское образование
3. www.edu.ru– сайт Министерства образования РФ
4. http://www.iqlib.ru – электронная библиотека образовательных и просветительных изданий
5. http://www.lib.msu.su/index.html - Научная библиотека Московского государственного университета им. М.В.Ломоносова
6. http://elibrary.ru/defaultx.asp - научная электронная библиотека «Elibrary»

7.4 Перечень информационных технологий

Чтение лекций с использованием слайд-презентаций.
Консультирование посредством электронной почты.
Использование слайд-презентаций при проведении научно-практических занятий.

8 Материально-техническое обеспечение дисциплины

Для обеспечения учебного процесса используются: лекционная аудитория, оснащенная мультимедийными средствами, аудитория для практических занятий, компьютерная аудитория, обеспечивающая выход в ИНТЕРНЕТ.

8 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

№ изменения	Номера страниц				Всего	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1		5			1	01.09.17	Приказ ФГБОУ «Юго-Западный государственный университет» № 576 от 31.08.2017 г. « О внесении изменений в приказ №263 от 29.03.2017 г. « Об утверждении норм времени для расчета учебной и других видов работы»
2		11			1	01.09.17	Приказ № 301 от 05.04.2017 г.
3		30-31			2	13.12.17	Протокол заседания кафедры ИСиТ №10 от 13.12.17

Приложение А

Перечень экзаменационных вопросов по дисциплине «Методы и системы защиты информации, информационная безопасность»

1. Понятия группы, "кольца, поля, их основные свойства.
2. Кольца вычетов. Кольцо многочленов над конечным полем. Поля Галуа.
3. Основные понятия теории вероятностей и математической статистики. Условная вероятность и независимость.
4. Цепи Маркова. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
5. Сходимость последовательностей случайных величин и сходимость распределений. Закон больших чисел.
6. Центральная предельная теорема. Основные задачи математической статистики.
7. Конечные автоматы. Граф перехода автомата. Графы и орграфы.
8. Перечисление графов и отображений. Алгоритмические задачи на графах.
9. Архитектура современной ЭВМ.
10. Программный интерфейс вычислительной системы.
11. Технология объектно-ориентированного программирования.
12. Функции ядра операционной системы и защита информации. Однопользовательская и многопользовательские многозадачные операционные системы.
13. Типовые конфигурации сети. Протоколы обмена данными. Маршрутизация сообщений в сети.
14. Системы управления базами данных. Реляционная, иерархическая и сетевая модели.
15. Основные принципы современной концепции обеспечения защиты информации. Требования к защите с позиции пользователя.
16. Основные методы защиты информации. Методология организации и проведении .работ по разработке и анализу средств защиты информации.
17. Основные положения государственной политики обеспечения информационной безопасности. Современная нормативно-правовая база в области защиты информации.
18. Понятие информации с ограниченным доступом. Цели защиты информации и степени секретности. Лицензирование в области защиты информации.
19. Сертификации средств защиты информации. Аттестации объектов информатики. Правовая основа сертификации.
20. Понятие угрозы информационной безопасности системы. Классификация угроз информационной безопасности.
21. Понятия непосредственных и опосредованных угроз. Основные уровни защиты информации в автоматизированных системах. Основные направления и методы реализации информационных угроз.
22. Понятие политики информационной безопасности. Каноническая модель управления доступом. Классификация каналов взаимодействия субъектов доступа.
23. Основные модели управления доступом с взаимодействием субъектов доступа.
24. Понятия дискреционного и мандатного механизмов управления доступом.

25. Метки безопасности, их назначение в разграничении прав доступа при реализации мандатной модели доступа.

26. Правила разграничения доступа для полномочной модели управления доступом. Особенности использования мандатного механизма управления доступом при разграничении прав доступа субъектов.

27. Правила назначения меток безопасности иерархическим объектам доступа.

28. Анализ возможностей корректной реализации канонических моделей управления доступом в ОС с использованием дискреционного механизма.

29. Анализ возможностей корректной реализации" моделей управления доступом с каналом взаимодействия субъектов доступа для ОС UNIX.

30. Принципы организации мандатного управления доступом к устройствам.

31 Возможности разграничения доступа к системному диску для ОС Windows NT/2000/XPи Unix.

32. Механизм обеспечения замкнутости программной среды и его роль в системе защиты.

33. Реализация механизмов парольной защиты.- Процедуры идентификации пользователя на рабочей станции и взаимной идентификации удаленных рабочих станций.

34.Контроль целостности информации, основные схемы контроля. Аутентификация информации.

.35. Угрозы преодоления парольной защиты. Усиление парольной защиты.

36. Стандарты в области защиты информации в вычислительной системе, "Оранжевая книга" США, российские стандарты.

37. Понятие симметричной и ассиметричной криптосистем. Основные типы криптоаналитических атак.

38. Шифрование методом простой замены. Алгоритм простой замены.

39. Шифрование методом полиалфавитной замены. Алгоритм полиалфавитной замены с использованием таблицы Вижинера.

40.Аддитивные методы шифрования. Шифрование методом перестановки. Карты Гамильтона.

41. Система открытого распространения ключей. Использование схемы открытого шифрования для создания цифровых подписей.

42.Применение хэш-функции для создания цифровых подписей. Алгоритм цифровой подписи с использованием хэш-функции.

43.Основные физические каналы утечки информации о функционировании информационной системы.

44. Узлы и блоки оборудования информационной системы, уязвимые для технической разведки.

45.Технические параметры современных средств перехвата побочных сигналов. Методы и средства зашиты от инженерно-технической разведки.

46. Методика оценки качества инженерно-технической защиты.

47.Разрушающие программные воздействия. Компьютерные вирусы как особый класс разрушающих программных воздействий.

48. Классификация вирусов. Методы выявления и защиты от вирусов.

49. Методика анализа алгоритмов защиты программных реализаций информационных систем.

50. Методы восстановления алгоритмов защиты в программных продуктах Оценка уровня криптографической защиты типовых программных продуктов.

ПРИЛОЖЕНИЕ Б
ФОРМА ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Юго– Западный государственный университет

Факультет _____
Направление подготовки _____
Направленность (профиль, специализация)
_____
Курс_____
Дисциплина _____
_____

Утверждено на заседании кафедры
_____
«___»_____ 20__г.(протокол №__)

Зав. кафедрой _____

Экзаменационный билет № _____

1. Текст вопроса .
1.1. Текст подвопроса .
1.2. Текст подвопроса.
….

2. Текст вопроса.
2.1. Текст подвопроса.
2.2. Текст подвопроса.
….

Экзаменатор _____ И.О. Фамилия