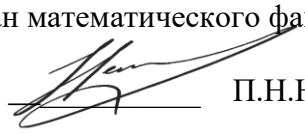
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Методы и системы защиты информации, информационная безопасность»

Направление подготовки
10.06.01 Информационная безопасность

Направленность (профиль)
«Методы и системы защиты информации,
информационная безопасность»

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Дисциплина «Методы и системы защиты информации, информационная безопасность» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является овладение базовыми понятиями и методами в области защиты информации, прежде всего криптографическими методами, овладение современным математическим аппаратом, используемым в криптографии для дальнейшего использования в приложениях.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Методы и системы защиты информации, информационная безопасность» является обязательной дисциплиной вариативной части. Данная дисциплина направлена на подготовку к сдаче кандидатского экзамена научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- **Профессиональные компетенции:**
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-1);
- способность разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулировку, восстановление работоспособности (ПК-2).

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);
«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий Уровень**
способностью выявлять	**Знать:** основные	**Знает:** основные	**Знает:** основные	**Знает:** основные

основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-1)	угрозы безопасности информации и способы построения модели нарушителя. **Уметь:** строить модели нарушителя в компьютерных системах . **Владеть:** навыками исследования модели нарушителя в компьютерных системах.	угрозы безопасности информации и способы построения модели нарушителя.	угрозы безопасности информации и способы построения модели нарушителя. **Умеет:** Строить модели нарушителя в компьютерных системах .	угрозы безопасности информации и способы построения модели нарушителя. **Умеет:** Строить модели нарушителя в компьютерных системах . **Владеет:** Навыками исследования модели нарушителя в компьютерных системах.
Способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулирование, восстановление работоспособности (ПК-2)	**Знать:** защитные механизмы и средства обеспечения информационной безопасности. **Уметь:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеть:** навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.	**Знает:** защитные механизмы и средства обеспечения информационной безопасности.	**Знает:** защитные механизмы и средства обеспечения информационной безопасности. **Умеет:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности.	**Знает:** защитные механизмы и средства обеспечения информационной безопасности. **Умеет:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеет:** навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 акад.часов

Дисциплина изучается в течение четырех семестров. Формой итоговой промежуточной аттестации по дисциплине в последнем семестре ее изучения является кандидатский экзамен.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)					Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			лекции	практические	лабораторные	консультации	самостоятельная работа	
1.	**Методы и системы защиты информации**	**2**	**8**			**2**	**62**	
1.1.	*Законодательные и правовые основы защиты компьютерной информации информационных технологий.*	2	2				20	
1.2.	*Проблемы защиты информации в информационных системах*	2	2				20	
1.3.	*Содержание системы средств защиты компьютерной информации в информационных системах.*	2	4			2	22	Зачет. 2-ой семестр
2.	**Информационная безопасность**	**3,4, 5**	**18**			**4**	**122**	
2.1.	*Изучение традиционных симметричных криптосистем.*	3	2				10	
2.2.	*Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.*	3	2				10	
2.3.	*Применение ассиметричных криптосистем для защиты компьютерной*	3	2				10	Зачет. 3-й семестр

	информации в информационных системах.							
2.4.	*Методы идентификации и проверки подлинности пользователей компьютерных систем.*	4	2			1	8	
2.5.	*Защита компьютерных систем от удаленных атак через сеть* Internet.	4	2				10	
2.6.	*Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.*	4	2			1	10	Зачет. 4-ый семестр
2.7.	*Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).*	5	2				14	
2.8.	*Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.*	5	4			1	14	
						1	36	Экзамен. 5-ый семестр
	Всего		**26**			**6**	**184**	

Содержание разделов дисциплины:

1. Методы и системы защиты информации

1.1.Законодательные и правовые основы защиты компьютерной информации информационных технологий.

Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы;
персональные данные о гражданах; права на доступ к информации;
разработка и производство информационных систем;
вычислительные сети и защита информации;
нормативно-правовая база функционирования систем защиты информации; компьютерные преступления и особенности их расследования;
российское законодательство по защите информационных технологий;
промышленный шпионаж и законодательство, правовая защита программного

обеспечения авторским правом.

1.2.Проблемы защиты информации в информационных системах.

Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах;

основные задачи обеспечения безопасности информации в информационных системах; защита локальных сетей и операционных систем;

интеграция систем защиты;

Internet в структуре информационно-аналитического обеспечения информационных систем;

рекомендации по защите информации в Internet.

1.3.Содержание системы средств защиты компьютерной информации в информационных системах.

Защищенная информационная система и система защиты информации;

принципы построения систем защиты информации и их основы;

законодательная, нормативно-методическая и научная база системы защиты информации;

требования к содержанию нормативно-методических документов по защите информации;

научно-методологический базис, стратегическая направленность и инструментальный базис защиты информации;

структура и задачи (типовой перечень) органов, выполняющих защиту информации;

организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры;

политика безопасности: организация секретного делопроизводства и мероприятий по защите информации;

программно-технические методы и средства защиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера;

типы несанкционированного доступа и условия работы средств защиты;

вариант защиты от локального несанкционированного доступа и от удаленного ИСД;

средства защиты, управляемые модемом, надежность средств защиты.

2 . Информационная безопасность

2.1.Изучение традиционных симметричных криптосистем.

Основные этапы становления криптографии.

Теоретические основы криптографии: основные понятия и определения; общее понятие шифра, алгебраическая и вероятностная модели шифра; простейшие исторические шифры и их криптоанализ; основные классы шифров и их свойства: шифры перестановки и шифры замены; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

2.2.Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.

Блочные системы шифрования: изучение американских стандартов шифрования данных DES и AES;

основные режимы работы алгоритмов DES и AES;

отечественные стандарты шифрования данных ГОСТ 28147-89 и ГОСТ Р 34.12-2015;

режимы работы блочных шифров ГОСТ Р 34.13-2015: режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки;

сравнение блочных и поточных шифров; надежность шифров.

2.3.Применение ассиметричных криптосистем для защиты компьютерной информации в информационных системах.

Концепция криптосистемы с открытым ключом;
однонаправленные функции;
системы шифрования с открытым ключом: криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA;
схема шифрования Полига-Хеллмана;
схема шифрования Эль-Гамаля, комбинированный метод шифрования.

2.4.Методы идентификации и проверки подлинности пользователей компьютерных систем.

Основные понятия и концепции;
идентификация и механизмы подтверждения подлинности пользователя;
взаимная проверка подлинности пользователей;
протоколы идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний;
проблема аутентификации данных и электронная цифровая подпись;
однонаправленные хэш-функции; алгоритм безопасного дешифрования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции ГОСТ Р 34.11-2012;
алгоритм цифровой подписи RSA;
алгоритм цифровой подписи Эль Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественные стандарты цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2012; протоколы распределения ключей.

2.5.Защита компьютерных систем от удаленных атак через сеть Internet.

Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация;
основные схемы сетевой защиты на базе межсетевых экранов;
применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

2.6.Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.

Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты данных;
контроллер смарт-карт SCAT-200;
программно-аппаратная система защиты от НСД КРИПТОН-ВЕТО;
защита от НСД со стороны сети абонентское шифрование и ЭЦП;
шифрование пакетов, аутентификация, защита компонентов ЛВС от НСД;
защита абонентского пункта, маршрутизаторов и устройств контроля;
технология работы с ключами.

2.7.Методы защита программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).

Классификация способов защиты;
защита от отладок и дизассемблирования;
способы встраивания защитных механизмов в программное обеспечение;
понятие разрушающего программного воздействия;
модели взаимодействия прикладной программы и программной закладки;
методы перехвата и навязывания информации;
методы внедрения программных закладок;
компьютерные вирусы как особый класс разрушающих программных воздействий; защита от РПВ; понятие изолированной программной среды.

2.8.Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.

Возможности СИИТ для обеспечения комплексной

защиты программ в момент их выполнения и данных при их обработке в компьютере;
метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок;
разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов;
метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации;
защита арифметических вычислений в компьютерных системах;
основные направления создания защищенных компьютерных систем нового поколения на основе СИИТ.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система MikTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992.
2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ

Гостехкомиссии России. М. ГТК РФ, 1992.
3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.-.ГТК РФ, 1992.
4. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
5. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М., Горячая линия - Телеком, 2006. 544 с.
6. ГОСТ 34.12-2015. Информационная технология, Криптографическая защита информации. Блочные шифры. Москва. Стандартинформ. 2015.
7. ГОСТ 34.13-2015. Информационная технология, Криптографическая защита информации. Режимы работы блочных шифров. Москва. Стандартинформ. 2015.
8. ГОСТ 34.11-2012. Информационная технология, Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Москва. Стандартинформ. 2012.
9. ГОСТ 34.10-2012. Информационная технология, Криптографическая защита информации. Функция хэширования. Москва. Стандартинформ. 2012.

б) дополнительная литература

1. Безопасность информационных технологий. Выпуск 1. М.: Госкомитет РФ по высшему образованию, МИФИ, 1994.
2. Безопасность информационных технологий. Выпуск 3. Московский государственный инженерно-физический институт (технический университет), 1995.
3. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
4. Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. М.: Прометей, 1999.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Радио и связь, 1999.
7. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. М.: КУДИЦ-ОБРАЗ, 2003.
8. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
9. Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
10. Введение в криптографию: новые математические дисциплины / под ред. В. В. Ященко, СПб., Питер, 2001, 287с.
11. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Издательский дом "Академия", 2009.
12. Чмора А. Современная прикладная криптография / А.Л. Чмора. М.: Гелиос АРВ, 2002. 256 с.
13. Хенк К.А. ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2005. 465 с.
14. Зензин О.С. Стандарт криптографической защиты AES. Конечные поля / О.С. Зензин, М.А. Иванов. КУДИЦ-ОБРАЗ, 2003.
15. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.

16. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
17. Бабаш А.В., Шанкин Г.П. История криптографии. Учебное пособие. М.: “Гелиос АРВ”, 2002
18. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
19. Ноден П., Китте К. Алгебраическая алгоритмика /под ред. Л.С. Казарина. М: Мир, 1999.
20. Ростовцев А.Г. Алгебраические основы криптографии / А.Г. Ростовцев. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2000. 354 с.
21. Ростовцев А.Г. Введение в криптографию с открытым ключом / А.Г. Ростовцев, Е.Б. Маховенко. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2001. 336 с.
22. Маховенко Е.Б. Теоретическая криптография / Е.Б. Маховенко, А.Г. Ростовцев. Санкт-Петербург. АНО НПО "Профессионал". ООО "Интерлайн", 2004.
23. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. М.: Научное издательство "ТВП", 2001. 254 с.
24. Мао В. Современная криптография. Теория и практика / В. Мао. М.: Издательский дом "Вильямс", 2005. 768 с.
25. Харин Ю.С. Математические и компьютерные основы криптологии / Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Минск: ООО "Новое знание", 2003. 382 с.
26. Шнайер Б. Прикладная криптография / Б. Шнайер. М.: Триумф, 2002. 816 с.
27. Под ред. Погорелова Б.А., Сачкова В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list) представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php**)**

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

Зав. кафедрой компьютерной
безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г.

Приложение к №1 рабочей программе дисциплины
«Методы и системы защиты информации,
информационная безопасность»

Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Задания для самостоятельной работы по теме **"Изучение традиционных симметричных криптосистем"** подраздел "Теоретические основы криптографии". Задания для самостоятельного решения № 1 - 12 из главы I учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельной работы по теме **"Изучение традиционных симметричных криптосистем"** подраздел "Простейшие исторические шифры и их криптоанализ."

Задания для самостоятельного решения № 22 - 30 из параграфа 3 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Для самостоятельной работы по теме **"Изучение традиционных симметричных криптосистем"** подразделы "Основные этапы становления криптографии" и "Общее понятие шифра, алгебраическая и вероятностная модели шифра" и по теме **"Применение симметричных криптосистем для защиты компьютерной информации в информационных система"** подраздел "Надежность шифров" предлагаются вопросы для подготовки дома развернутого ответа с последующим обсуждением на консультациях

1. Схемы противоборства сторон. Модели угроз при передачи и хранении информации.
2. Примеры исторических шифров
3. Идея шифрования с открытым ключом на основе одно направленной функции с секретом.
4. Математическая модель открытых текстов.
5. Критерии на открытый текст.
6. Алгебраическая модель шифра.
7. Вероятностная модель шифра.
8. Шифры замены, классификация и анализ.

9. Шифры перестановки, классификация и анализ.
10. Шифры гаммирования. Криптоанализ шифра Виженера.
11. Шифры гаммирования. Неравновероятная гамма.
12. Шифры гаммирования. Повторное использование гаммы.
13. Дисковые шифраторы многоалфавитной замены.
14. Дисковые шифраторы гаммирования.
15. Теоретическая стойкость шифров по Шеннону
16. Понятие о расстоянии единственности.
17. Метод тотального опробования ключей шифра
18. Практическая стойкость шифров.
19. Вопросы имитостойкости шифров.
20. Коды аутентификации
21. Помехоустойчивость шифров. Теорема Маркова.

Задания для самостоятельного решения № 1 - 15 из главы II учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельной работы по теме **"Изучение традиционных симметричных криптосистем"** подраздел "Основные классы шифров и их свойства. "

Задания для самостоятельного решения № 31 - 38 из параграфа 4 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Задания для самостоятельного решения № 1 - 8 из главы III учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельного решения № 1 - 5 из главы IV учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельного решения № 1 - 5 из главы V учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельной работы по теме **"Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. подраздел"** подраздел "Блочные системы шифрования**. "**

Задания для самостоятельного решения № 185 - 191 из параграфа 22 и № 195 - 200 из параграфа 24 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Задания для самостоятельного решения № 1 - 6 из главы VIII учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельной работы по теме **"Методы идентификации и проверки подлинности пользователей компьютерных систем"** подраздел **"Хеш-функции."**

Задания для самостоятельного решения № 192 - 194 из параграфа 23 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Задания для самостоятельного решения № 1 - 6 из главы XIII учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельной работы по теме **"Применение ассиметричных криптосистем для защиты компьютерной информации в информационных системах"** подраздел "Системы шифрования с открытым ключом."

Задания для самостоятельного решения № 86 - 99 из параграфа 9 и № 100 - 123 из параграфа 10 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Задания для самостоятельного решения № 1 - 6 из главы IX учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельного решения № 1 - 5 из главы XIV учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельной работы по теме **"Методы идентификации и проверки подлинности пользователей компьютерных систем"** подраздел "Протоколы распределения ключей."

Задания для самостоятельного решения № 171 - 173 из параграфа 18 сборника задач

Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Задания для самостоятельного решения № 1 - 10 из главы XV учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

Задания для самостоятельного решения № 1 - 5 из главы XVI учебника Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.

По ряду тем предлагаются вопросы для самостоятельного углубленного изучения с последующим обсуждением на консультациях

1. Поточные шифры и принципы их построения.
2. Генераторы псевдослучайных последовательностей и их характеристики.
3. Методы усложнения линейных рекуррентных последовательностей.
4. Криптографические параметры булевых функций.
5. Блочные шифры и принципы их построения.
6. Режимы использования блочных шифров. Стандарт ГОСТ Р 34.13-2015.
7. Стандарт шифрования DES.
8. Стандарт шифрования ГОСТ-28147-89.
9. Стандарт шифрования ГОСТ Р 34.12-2015.
10. Стандарт шифрования AES.
11. Криптосистемы на основе открытого ключа. Сложные проблемы математики.
12. Криптосистема RSA и выбор параметров.
13. Понятие цифровой подписи. ГОСТ Р 34.10-2012.
14. Методы анализа протокола RSA.
15. Основные методы дискретного логарифмирования.
16. Криптосистема Эль-Гамаля.
17. Понятие хэш-функции, способы их построения.

18. Ключевые хэш-функции и связь с кодами аутентификации.
19. Бесключевые хэш-функции, парадокс дней рождений.
20. Российский стандарт хэш-функции ГОСТ Р 34.11-2012.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету (2 семестр)

1. Основные задачи в области обеспечения информационной безопасности, решаемые криптографическими методами.
2. Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр Плейфейра, шифр Хилла. Решетка Кардано, книжный шифр, шифр Виженера, гаммирование, дисковый шифратор Т.Джефферсона, шифр Вернама и др.
3. Криптология и криптоанализ. Принцип Керкгоффса.
4. Математическая модели открытых текстов. Критерии на открытый текст.
5. Классификация шифров.
6. Простейшие шифры замены и их криптоанализ. Индекс совпадения Фридмана.
7. Простейшие шифры перестановки и их анализ.
8. Шифры гаммирования и их анализ. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой. Табличное и модульное гаммирование.
9. Дисковые шифраторы многоалфавитной замены.
10. Основные этапы становления криптографии. Роль К.Шеннона и отечественные достижения в области защиты информации.
11. Способы представления информации, подлежащей шифрованию (оцифровка).
12. Общее понятие шифра, алгебраическая и вероятностная модели шифра
13. Определение шифра и его математические модели. Ручные и машинные шифры.
14. Ключевая система шифра. Основные требования к шифрам.
15. Общее понятие криптосистемы. Симметричные и асимметричные системы шифрования.
16. Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки.
17. Одноалфавитные и многоалфавитные шифры замены. Шифрвеличины и шифробозначения. Распределители.

Вопросы к зачету (3 семестр)

1. Поточные системы шифрования и принципы их построения.
2. Типовые генераторы псевдослучайных последовательностей и их свойства.
3. Линейные рекуррентные последовательности, их периодичность. Методы усложнения линейных рекуррентных последовательностей.
4. Шифрование в европейской системе мобильной телефонии - шифрсистема А5.
5. Блочные шифры и принципы их построения. S-P-сеть. Выбор линейных и нелинейных блоков.
6. Современные стандарты блочных шифров DES, ГОСТ 28147-89, AES, ГОСТ Р 34.12-2015. XSL-структура алгоритмов шифрования.
7. Режимы использования блочных шифров ГОСТ Р 34.13-2015.
8. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций.
9. Использование хеш-функций и блочных шифров в системах аутентификации сообщений. Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC.
10. Современные стандарты хеш-функций ГОСТ Р 34.11-2012.
11. Системы шифрования с открытым ключом ключом - асимметричные системы шифрования.

12. Понятие односторонней функции и односторонней функции с «лазейкой».
13. Использование в ассиметричной криптографии вычислительно сложных задач математики.
14. Криптосистема RSA и ее анализ.
15. Криптосистемы Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана.

Вопросы к зачету (4 семестр)

16. Электронная подпись документов. Цифровая подпись Фиата-Шамира и подпись Эль-Гамаля. ГОСТ Р 34.10-2012.
17. Протоколы распределения ключей.
18. Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.
19. Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.
20. Открытое распределение ключей.
21. Предварительное распределение ключевых материалов.
22. Возможные атаки на протоколы распределения ключей. Управление ключами.
23. Схемы разделения секрета. Доказательства с нулевым разглашением.
24. Некоторые практические аспекты использования шифрсистем.
25. Проблемы реализации криптографической подсистемы и системы управления ключами .

Список вопросов к экзамену (5 семестр).

1.1. Список вопросов для кандидатского экзамена

1.1.1.Методы и системы защиты информации

1. Определение, особенности и общее содержание теории защиты информации. Научно-методический базис теории защиты.
2. Система моделей защиты информации.
3. Факторы, влияющие на формирование стратегий защиты. Общая характеристика основных стратегий.
4. Определение и назначение инструментально методологического базиса защиты информации. Требования к инструментально-методологическому базису.
5. Структура и общее содержание унифицированной концепции защиты информации.
6. Система концептуальных решений по защите информации.
7. Технические средства защиты, их сущность, возможности, достоинства и недостатки.
8. Критерии классификации и классификационная структура технических средств. Автономные, сопряженные и встроенные технические средства.
9. Программы аутентификации пользователей. Парольные системы аутентификации, их сущность, содержание, достоинства и недостатки.
10. Программы защиты ЭВМ от электронных вирусов.
11. Криптографические средства защиты, их сущность, достоинства и недостатки. Основные понятия криптографического преобразования данных.
12. Криптографические системы с открытым ключом, их сущность и необходимость. Методы построения.
13. Система RSA: шифрование и цифровая подпись.
14. Другие алгоритмы шифрования с открытым ключом.

15. Электронная подпись, ее назначение и сущность, принципы и методы формирования.
16. Стандарты электронной подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2012.
17. Шифры перестановки. Поточные шифры замены. Блочные шифры простой замены и особенности их анализа.
18. Американский стандарт шифрования данных DES.
19. Российский стандарт шифрования данных ГОСТ-28147-89.
20. Российский стандарт шифрования данных ГОСТ Р 34.12-2015.
21. Криптоалгоритм RIJNDAEL и американский стандарт шифрования данных AES.
22. Основные режимы работы блочных шифров.
23. Режимы работы алгоритмов DES и AES.
24. Режимы работы блочных шифров ГОСТ Р 34.13-2015.
25. Общеметодологические принципы построения систем защиты информации (СЗИ), их сущность и содержание.
26. Основы архитектурного построения СЗИ. Функциональная, организационная и структурная модели СЗИ.
27. Ядро СЗИ, его функции и состав. Типизация и стандартизация архитектурного построения СЗИ.
28. Основы методологии проектирования СЗИ. Классификация и анализ постановок задач проектирования СЗИ.
29. Методика выбора требований к защите информации. Методика создания СЗИ на основе типовых проектных решений.
30. Методика оптимального выбора задач, необходимых для осуществления функций защиты.
31. Методика выбора средств защиты, необходимых и достаточных для эффективного решения выбранных средств защиты. Методика объединения выбранных средств в СЗИ.
32. Теоретико-вероятностные методы определения значений показателей уязвимости, подходы к построению моделей.
33. Теоретико-эмпирические методы определения значений показателей. Подходы к построению теоретико-эмпирических моделей.
34. Понятие базового показателя уязвимости, аналитическая и статистическая модели его определения. Зависимости для определения значений обобщенных показателей уязвимости.
35. Основные понятия и определения теории информационно-телекоммуникационных систем (ИТКС): сети передачи данных, мультиплексирование, сети с коммутацией каналов и пакетов, протоколы и архитектура сетей.
36. Использование радиосредств в ИТКС: организация стационарного радиодоступа к телефонным сетям и к подвижным абонентам, стандарты сотовых систем подвижной радиосвязи. 30. Основные принципы построения систем сотовой связи. Информационная безопасность систем мобильной связи.
37. Методика построения защищенных компьютерных систем.
38. Анализ рисков и выбор направлений защиты компьютерных систем. Разработка системы организационных и физических мер защиты компьютерных систем.
39. Разработка системы программно-технических мер защиты компьютерных систем.
40. Нейтрализация угроз и уязвимых мест компьютерных систем. Защита компьютерных систем от персонала.
41. Особенности защиты информации в базах данных. Защищенные файловые системы.
42. Защита в СУБД. Защита баз данных в сетях ЭВМ. Протоколы и процедуры передачи файлов.
43. Динамическая защита баз данных.
44. Контекстно-ориентированная защита.

45. Доступ к электронным документам и порядок эффективного закрытия его для обеспечения безопасности информации на рабочих местах в организации.
46. Порядок заключения договоров об обмене электронными документами.
47. Электронная цифровая подпись. Получение сертификата электронной цифровой подписи.
48. Условия применения электронной цифровой подписи при подписании документов. Реализация схемы цифровой метки.
49. Принципы и средства защитных преобразований сигналов при передаче аналоговых и дискретных сигналов. Спектральные, временные и комбинированные преобразования.
50. Проблема защиты служебных сигналов при передаче.
51. Симметричное и асимметричное шифрование в задачах защиты информации электронного документооборота.
52. Модели шифров. Простейшие криптографические протоколы.
53. Характеристики имитостойкости шифров и их оценки. Параметры имитостойких и неимитостойких шифров.
54. Шифры, не размножающие искажений типа замены знаков.
55. Шифры, не размножающие искажений типа пропуск-вставка знаков для систем документооборота.
56. Системы шифрования с открытым ключом. Алгоритмы цифровых подписей.
57. Цифровые подписи на основе шифросистем с открытым ключом.
58. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля.
59. Алгоритмы распределения ключей. Алгоритмы передачи ключей (с использованием и без использования цифровой подписи).
60. Шифросистема Эль-Гамаля.
61. Шифросистема на основе задачи об «укладке рюкзака».
62. Анализ шифросистемы RSA.
63. Практические аспекты использования шифросистем с открытым ключом в системах электронного документооборота.

1.1.2 Информационная безопасность

1. Централизация управления информационными ресурсами.
2. Двух- и трехуровневые клиент-серверные системы.
3. Многоуровневые клиент-серверные системы.
4. Принципы разделения и изоляции этапов информационного взаимодействия с позиции безопасности
5. Структура информационной системы с Web-доступом.
6. Распределенные серверы приложений и бизнез-логика.
7. Технология вызова удаленных процедур.
8. Современные технологии разработки клиент-серверных приложений. Технология NET Remoting.
9. Современные технологии разработки клиент-серверных приложений. Технологии ASP, ASP .NET.WEB-сервисы.
10. Современные технологии разработки клиент-серверных приложений. XML – технологии. Протокол SOAP.
11. Проблемы безопасного использования клиентских и серверных сценариев, ActiveX-объектов и апплетов.
12. Принципы и приемы разработки компонентов безопасных приложений.
13. Высокоуровневые программные интерфейсы доступа к серверам баз данных – (ODBC, ADO, ADO.NET).

14. Методы защиты серверов баз данных.
15. Методы обеспечения безопасности информационного взаимодействия между программными компонентами информационных систем.
16. Протоколы взаимной аутентификации шифрования данных.
17. Основные проблемы обеспечения безопасности доступа при использовании беспроводных каналов передачи данных.
18. Протоколы аутентификации и шифрования данных в беспроводных сетях.

1.2. Рекомендуемая литература

а) основная литература

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992.
2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. М. ГТК РФ, 1992.
3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.-.ГТК РФ, 1992.
4. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
5. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М., Горячая линия - Телеком, 2006. 544 с.
6. ГОСТ 34.12-2015. Информационная технология, Криптографическая защита информации. Блочные шифры. Москва. Стандартинформ. 2015.
7. ГОСТ 34.13-2015. Информационная технология, Криптографическая защита информации. Режимы работы блочных шифров. Москва. Стандартинформ. 2015.
8. ГОСТ 34.11-2012. Информационная технология, Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Москва. Стандартинформ. 2012.
9. ГОСТ 34.10-2012. Информационная технология, Криптографическая защита информации. Функция хэширования. Москва. Стандартинформ. 2012.

б) дополнительная литература

1. Безопасность информационных технологий. Выпуск 1. М.: Госкомитет РФ по высшему образованию, МИФИ, 1994.
2. Безопасность информационных технологий. Выпуск 3. Московский государственный инженерно-физический институт (технический университет), 1995.
3. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
4. Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. М.: Прометей, 1999.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М.: Радио и связь, 1999.

7. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. М.: КУДИЦ-ОБРАЗ, 2003.
8. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
9. Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
10. Введение в криптографию: новые математические дисциплины / под ред. В. В. Ященко, СПб., Питер, 2001, 287с.
11. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Издательский дом "Академия", 2009.
12. Чмора А. Современная прикладная криптография / А.Л. Чмора. М.: Гелиос АРВ, 2002. 256 с.
13. Хенк К.А. ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2005. 465 с.
14. Зензин О.С. Стандарт криптографической защиты AES. Конечные поля / О.С. Зензин, М.А. Иванов. КУДИЦ-ОБРАЗ, 2003.
15. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.
16. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
17. Бабаш А.В., Шанкин Г.П. История криптографии. Учебное пособие. М.: “Гелиос АРВ”, 2002
18. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
19. Ноден П., Китте К. Алгебраическая алгоритмика /под ред. Л.С. Казарина. М: Мир, 1999.
20. Ростовцев А.Г. Алгебраические основы криптографии / А.Г. Ростовцев. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2000. 354 с.
21. Ростовцев А.Г. Введение в криптографию с открытым ключом / А.Г. Ростовцев, Е.Б. Маховенко. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2001. 336 с.
22. Маховенко Е.Б. Теоретическая криптография / Е.Б. Маховенко, А.Г. Ростовцев. Санкт-Петербург. АНО НПО "Профессионал". ООО "Интерлайн", 2004.
23. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. М.: Научное издательство "ТВП", 2001. 254 с.
24. Мао В. Современная криптография. Теория и практика / В. Мао. М.: Издательский дом "Вильямс", 2005. 768 с.
25. Харин Ю.С. Математические и компьютерные основы криптологии / Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Минск: ООО "Новое знание", 2003. 382 с.
26. Шнайер Б. Прикладная криптография / Б. Шнайер. М.: Триумф, 2002. 816 с.
27. Под ред. Погорелова Б.А., Сачкова В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.
28. Зайцев А.П. Технические средства и методы защиты информации. – М.: Горячая линия- Телеком, 2009.
29. Грибунин В.Г. Комплексная система защиты информации на предприятии. – М.: Академия, 2009.
30. Харин Ю.С. Математические и компьютерные основы криптологии. – М.: Новое знание, 2008.
31. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2007.
32. Партыка Т.Л. Информационная безопасность. – М.: Инфра-М, 2007.
33. Торокин А.А. Инженерно-техническая защита информации. М.: Аспект Пресс, 2006.

34. Коханович Г.Ф. и др. Защита информации в телекоммуникационных системах. – М.: Пресс, 2005.
35. Рябко Б.Я. Криптографические методы защиты информации. М.: Горячая линия - Телеком, 2005.
36. Смарт Н. Криптография. – М.: Техносфера, 2006.
37. Игнатов В.Г. Безопасность глобальных сетевых технологий. – СПб.: Питер, 2007.
38. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2006.
39. Чекалин А.А. Защита информации в системах мобильной связи. – М.: Горячая линия- Телеком, 2005.
40. Фомичев В.М. Дискретная математика и криптология. 2-е изд. –М,: ДИАЛОГ-МИФИ, 2009.
41. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: ИД Форум: НИЦ Инфра-М, 2012.
42. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение
43. информационной безопасности. – М.: ИЦ Академия, 2008.
44. Петраков А.В. Основы практической защиты информации. – М.: Солон-Пресс, 2005.
45. Семкин К.Н. и др. Основы организационного обеспечения информационной
46. безопасности объектов информатизации. – М.: Гелиос АРВ, 2007.

Приложение № 2 к рабочей программе дисциплины
«Методы и системы защиты информации,
информационная безопасность»

Методические указания для аспирантов по освоению дисциплины

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и криптографические методы обеспечения информационной безопасности. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома аспирантам предлагаются задачи, аналогичные разобранным на лекциях или более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на лекциях и консультациях по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

Аспиранты сдают зачет во втором, третьем и четвертом семестрах. Зачет проводится на основании выполнения домашних заданий, контрольной работы и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины. В пятом семестре сдается экзамен - кандидатский экзамен по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Учебно-методическое обеспечение самостоятельной работы аспирантов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу? , указанную в разделе № 7 данной рабочей программы.