МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Ярославский государственный университет им. П.Г. Демидова

Математический факультет

УТВЕРЖДАЮ

Проректор по развитию образования

_____Е.В.Сапир

"_____"_____2012 г.

Рабочая программа дисциплины
послевузовского профессионального образования
(аспирантура)

Методы и системы защиты информации, информационная безопасность

по специальности научных работников

05.13.19 Методы и системы защиты информации, информационная безопасность

Ярославль 2012

1. Цели освоения дисциплины.

Целями освоения дисциплины **«Методы и системы защиты информации, информационная безопасность»** в соответствии с общими целями основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (далее - образовательная программа послевузовского профессионального образования) являются:

- усвоение аспирантами знаний об основных результатах в изучаемой области;
- формирование математической культуры аспиранта, фундаментальная подготовка в области математических методов защиты информации;
- овладение основными понятиями и методами, используемыми в криптографической защите информации для дальнейшего использования при решении теоретических и прикладных задач.

2. Место дисциплины в структуре образовательной программы послевузовского профессионального образования

Дисциплина «Методы и системы защиты информации, информационная безопасность» относится к разделу «Обязательные дисциплины» (подраздел «Специальные дисциплины отрасли науки и научной специальности») образовательной составляющей образовательной программы послевузовского профессионального образования по специальности научных работников 05.13.19 Методы и системы защиты информации, информационная безопасность.

Для ее успешного изучения необходимы «входные» знания и умения, полученные в процессе обучения по программам специалитета или бакалавриата-магистратуры по направлению математика, а также алгебраических и алгоритмических специальных курсов.

Специальность «Методы и системы защиты информации, информационная безопасность» – область науки, исследующая системы защиты информации, принципы построения систем защиты информации и их основы, законодательную, нормативно-методическую и научную базу системы защиты информации.

3. Требования к результатам освоения содержания дисциплины «Методы и системы защиты информации, информационная безопасность». В результате освоения дисциплины обучающийся должен:

Знать: законодательные и правовые основы защиты информации и компьютерных технологий, меры по обеспечению сохранности информации, основные задачи обеспечения безопасности информации в информационных системах; принципы построения систем защиты информации и их основы; основные направления создания защищенных информационных систем, определения и свойства математических объектов, используемых в этой области знания, формулировки утверждений, методы их доказательства, возможные сферы их приложений.

Уметь: решать задачи теоретического характера из различных разделов дисциплины, доказывать утверждения, строить примеры основных объектов и понятий.

Владеть: математическим аппаратом, используемым в системах защиты информации, основными алгоритмами, классификацией способов защиты информации; методами защиты информации от несанкционированного доступа и разрушающих программных воздействий процесса хранения и обработки информации; методами защиты арифметических вычислений в компьютерных системах.

4. Структура и содержание дисциплины «Методы и системы защиты информации, информационная безопасность»

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа)

№ п/п	Раздел Дисциплины	Курс	Неделя	Виды учебной работы, включая самостоятельную работу обучающихся, и трудоемкость (в часах) Форма обучения: Очная/заочная					Формы текущего контроля успеваемости (по неделям) Форма промежуточной аттестации
				Лекций	Лабораторных	Практических	Сам. работы	Контроль сам. работы	
1	**Тема 1.** Проблемы защиты информации.	1	1	1			6		реферат
2	**Тема 2.** Краткий исторический очерк развития криптографии**.**	1	2				6		реферат
3	**Тема 3.** Криптоанализ шифров замены**.**	1	3	1			6		реферат
4	**Тема 4**. Основные этапы становления криптографии.	1	4				6		реферат
5	**Тема 5.** Определение шифра и его математические модели.	1	5	1/0			6		реферат
6	**Тема 6.** Основные классы шифров и их свойства.	1	6		4		6		контрольная работа
7	**Тема 7.** Поточные и блочные шифры замены**.**	1	7	1			6		реферат
8	**Тема 8.** Надежность шифров и проблемы реализации криптосистемы.	1	8				6		реферат
9	**Тема 9.** Имитация и подмена сообщения.	1	9	1			6		реферат
10	**Тема 10.** Принципы построения и анализа алгоритмов защиты информации.	1	10				6		реферат
11	**Тема 11.** Теоретико-автоматные модели шифров.	1	10	1			6		реферат
12	**Тема 12.** Методы шифрования с открытым ключом.	1	11				6		реферат

13	**Тема 13.** Методы и концепции проверки подлинности пользователей компьютерных систем.	1	11	1			6		реферат
14	**Тема 14.** Понятие криптографического протокола.	1	12				6		контрольная работа
15	**Тема 15.** Электронная подпись документов.	1	12	1/0			6		реферат
16	**Тема 16.** Безопасность сетей связи.	1	13				6		реферат
17	**Тема 17.** Законодательные и правовые основы защиты компьютерной информации информационных технологий.		13	1			6		реферат
18	**Тема 18.** Проблемы защиты информации в информационных системах.		14				8		реферат
19	**Тема 19.** Содержание системы средств защиты компьютерной информации в информационных системах.		14	1			8		реферат
20	**Тема 20.** Требования к содержанию нормативно-методических документов по защите информации**.**		15				8		реферат
21	**Тема 21.** Организационно-правовой статус службы информационной безопасности.		15	1			8		реферат
		1		**10/8**			**134**		**Зачет**

Содержание дисциплины

Тема 1.

Проблемы защиты информации. Сведения, составляющие государственную тайну. Компьютерные преступления, законодательные и нормативные документы. Угрозы безопасности информации и их классификация. Государственная система защиты информации, обрабатываемой техническими средствами. Правовое обеспечение защиты информации в России и за рубежом. Лицензирование, стандартизация и сертификация деятельности по защите информации. Требования к защите информации, оценка возможностей противоборствующей стороны. Методология разработки и анализа средств защиты. Классические модели защиты информации. Стеганографические и криптографические методы защиты информации.

Тема 2.

Краткий исторический очерк развития криптографии. Исторические примеры: шифр Цезаря, квадрат Полибия, шифр «скитала», магические квадраты, шифр Плейфейра, двойной квадрат Уитстона, одноразовая система шифрования, шифр Вернама, шифр Хилла. Криптология и криптоанализ. Решетка Кардано, книжный шифр.

Тема 3.

Криптоанализ шифров замены. Индекс совпадения Фридмана. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой. Табличное и модульное гаммирование.

Тема 4.

Основные этапы становления криптографии. Роль Шеннона и отечественные достижения в области защиты информации. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений.

Тема 5.

Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Понятие криптосистемы. Симметричные и асимметричные системы шифрования.

Тема 6.

Основные классы шифров и их свойства. Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки. Одноалфавитные и многоалфавитные шифры замены.

Тема 7.

Поточные и блочные шифры замены. DES, ГОСТ 28147-89, AES. Режимы использования блочных шифров: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.

Тема 8.

Надежность шифров и проблемы реализации криптосистемы. Теоретико-информационный подход к оценке стойкости шифра. Ненадежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и практически стойкие шифры. Избыточность языка и расстояние единственности.

Тема 9.

Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость.

Тема 10.

Принципы построения и анализа алгоритмов защиты информации. Основные способы реализации криптографических алгоритмов и требования к ним.

Тема 11.

Теоретико-автоматные модели шифров. Блоки выработки шифрующей последовательности и их основные параметры. Блоки шифрования. Методы генерации псевдослучайных последовательностей.

Тема 12.

Методы шифрования с открытым ключом. Концепция шифрования с открытым ключом. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA. Безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига – Хеллмана; схема шифрования Эль-Гамаля; комбинированный метод шифрования.

Тема 13.

Методы и концепции проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователей; взаимная идентификация. Схема идентификации с нулевой передачей знаний.

Тема 14.

Понятие криптографического протокола. Основные примеры. Аутентификация данных и однонаправленные хэш-функции. Хэш-функции, используемые в криптографии. Алгоритмы выработки хэш-функций. Хэш-функции на основе симметричных блочных алгоритмов. Алгоритм SHA. Отечественный стандарт хэш-функции.

Тема 15.

Электронная подпись документов. Цифровая подпись Эль-Гамаля (EGSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA, отечественный стандарт цифровой подписи.

Тема 16.

Безопасность сетей связи. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера. Защита информации от несанкционированного копирования. Администрирование компьютерных сетей. Существующие аппаратно-программные средства криптографической защиты информации серии КРИПТОН. Проблемы и перспективы в области защиты информации. Нерешенные задачи. Итоги изучения курса.

Тема 17.

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 за-

конодательство по защите информационных технологий; промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

Тема 18.

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; зашита локальных сетей и операционных систем; интеграция систем зашиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.

Тема 19.

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 зашиты информации.

Тема 20.

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.

Тема 21.

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 зашиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера; типы несанкционированного доступа и условия работы средств зашиты; вариант защиты от локального несанкционированного доступа и от удаленного ИСД.

5. Образовательные технологии

В преподавании используются мультимедийные презентации, иллюстрации, таблицы, методические пособия.

В преподавании курса используются активные и интерактивные технологии проведения занятий в сочетании с внеаудиторной работой.

Часть практических занятий проводится в компьютерных классах.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы обучающихся.

В качестве средств текущего контроля используется 2 контрольных работы, а также написание в течение семестра 1 реферата на выбранную тему. Итоговая форма контроля (экзамен)

дает возможность выявить уровень профессиональной подготовки аспиранта по данной дисциплине.

Контрольная работа № 1 (один из 28 вариантов)

1. Определите наилучшее аффинное приближение функции f\in P_2(n). n=3, **f=x_1+x_2+x_3+x_1x_2x_3.**
2. Найти индекс совпадения Фридмана для текста задания
3. Описать известные Вам схемы получения псевдослучайной последовательности.
4. Зашифровать сообщение с помощью двойного шифра Хилла, использующего матрицы размеров 2 и 3.
5. Написать программу зашифрования с помощью шифра Плейфейра.
6. Прочитать сообщение, зашифрованное шифром Виженера (текст варьируется).

Контрольная работа № 2 (один из 28 вариантов)

1. Вычислить символ Лежандра (5/160465489).
2. Привести примеры использования ЭЦП Рабина.
3. Каковы основные этапы по вскрытию шифра Виженера?
4. Как определяются энтропия и избыточность языка?
5. Написать программу выработки имитовставки.
6. В чем заключаются достоинства и недостатки систем поточного шифрования по сравнению с блочными?
7. Сравнить достоинства и недостатки шифров DES, AES и ГОСТ-28147-89
8. Для каких целей применяются хеш-функции? Как строятся криптографические хеш-функции?

Темы рефератов:

1. Основные симметричные шифры дошенноновского периода.
2. Криптоанализ шифров замены.
3. Криптоанализ шифров перестановки.
4. Криптоанализ шифров гаммирования и шифра Виженера.
5. Шифры DES, ГОСТ 28147-89, AES.
6. Машинные шифры.
7. Имитостойкость и надежность шифров.
8. Принципы построения и анализа алгоритмов защиты информации.
9. Криптографические хэш-функции.
10. Теоретико-автоматные модели шифров.
11. Методы шифрования с открытым ключом..
12. Безопасность и быстродействие криптосистемы RSA.
13. Методы и концепции проверки подлинности пользователей компьютерных систем.

14. Хэш-функции на основе симметричных блочных алгоритмов.

15. Алгоритм SHA и отечественный стандарт хэш-функции.

16. Цифровая подпись Эль-Гамаля (EGSA). Стандарты цифровой подписи.
17. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
18. Защита информации от несанкционированного копирования. Администрирование компьютерных сетей.

19. Существующие аппаратно-программные средства криптографической защиты информации серии КРИПТОН.

20. Методы генерации псевдослучайных последовательностей.
21. Избыточность языка и расстояние единственности.
22. Правовые вопросы защиты информации.
23. Стеганографическая защита информации.
24. Законодательные и правовые основы защиты компьютерной информации информационных технологий.

25. Проблемы защиты информации в информационных системах.

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

27. Организационно-правовой статус службы информационной безопасности.

Вопросы к зачету

1. Требования к защите информации, оценка возможностей противоборствующей стороны. Методология разработки и анализа средств защиты. Классические модели защиты информации. Стеганографические и криптографические методы защиты информации.
2. Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр «скитала», магические квадраты, шифр Плейфейра, двойной квадрат Уитстона, одноразовая система шифрования, шифр Вернама, шифр Хилла. Криптология и криптоанализ. Решетка Кардано, книжный шифр.
3. Криптоанализ шифров замены. Индекс совпадения Фридмана. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой.
4. Основные этапы становления криптографии. Роль Шеннона и отечественные достижения в области защиты информации. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений.

5. Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Понятие криптосистемы. Симметричные и асимметричные системы шифрования

6. Основные классы шифров и их свойства.
7. Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки. Одноалфавитные и многоалфавитные шифры замены.

8. Поточные и блочные шифры замены. DES, ГОСТ 28147-89, AES. Режимы использования блочных шифров: режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.

9. Надежность шифров и проблемы реализации криптосистемы. Теоретико-информационный подход к оценке стойкости шифра. Ненадежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и практически стойкие шифры. Избыточность языка и расстояние единственности.
10. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость.

11. Принципы построения и анализа алгоритмов защиты информации. Основные способы реализации криптографических алгоритмов и требования к ним.
12. Теоретико-автоматные модели шифров. Блоки выработки шифрующей последовательности и их основные параметры. Блоки шифрования. Методы генерации псевдослучайных последовательностей.
13. Методы шифрования с открытым ключом. Концепция шифрования с открытым ключом. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA. Безопасность и быстродействие криптосистемы RSA. Схема шифрования Полига – Хеллмана; схема шифрования Эль-Гамаля; комбинированный метод шифрования.

14. Методы и концепции проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователей; взаимная идентификация. Схема идентификации с нулевой передачей знаний.

15. Понятие криптографического протокола. Основные примеры. Аутентификация данных и однонаправленные хэш-функции. Хэш-функции, используемые в криптографии. Алгоритмы выработки хэш-функций. Хэш-функции на основе симметричных блочных алгоритмов. Алгоритм SHA. Отечественный стандарт хэш-функции.

16. Электронная подпись документов. Цифровая подпись Эль-Гамаля (EGSA). Стандарты цифровой подписи. Алгоритм цифровой подписи DSA, отечественный стандарт цифровой подписи.

17. Безопасность сетей связи. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.

18. Защита информации от несанкционированного копирования. Администрирование компьютерных сетей.

19. Существующие аппаратно-программные средства криптографической защиты информации серии КРИПТОН.

20. 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.

21. 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; зашита локальных сетей и операционных систем; интеграция систем зашиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.
22. 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 зашиты информации.
23. 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.
24. 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 зашиты информации; программно-аппаратные методы и средства ограничения доступа к компонентам компьютера; типы несанкционированного доступа и условия работы средств зашиты; вариант защиты от локального несанкционированного доступа и от удаленного ИСД.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература*:*

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999 и 2001.
2. Торокин А.А. Инженерно-техническая защита информации, М: “Гелиос АРВ”, 2005.
3. Осипян В.О., Осипян К.В., Криптография в упражнениях и задачах, М.: “Гелиос АРВ”, 2004.

б) дополнительная литература:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М: “Гелиос АРВ”, 2001.
2. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.
3. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
4. Романеи Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
5. Введение в криптографию/Под редакцией Ященко В.В. М: МЦНМО, «ЧеРо» , 1998.
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2 кн. М.: Радио и связь, 1999.
7. Бабаш А.В., Шанкин Г.П. История криптографии. Учебное пособие. М.: “Гелиос АРВ”, 2001
8. Ноден П., Китте К. Алгебраическая алгоритмика /под ред. Л.С. Казарина. М: Мир, 1999.
9. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации; Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.
10. Безопасность информационных технологий / Госкомитет РФ по высшему образованию, М.: МИФИ. 1994. Вып. 1.
11. Безопасность информационных технологий / Московский государственный инженерно-физический институт (технический университет), 1995- Вып. 3.

12. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
13. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Руководящий документ Гостехкомиссии России. М.: ГТК РФ, 1992.
14. Средства вычислительной техники. Зашита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М,: ГТК РФ, 1992.
15. Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. М.: Прометей, 1999.

в) программное обеспечение и Интернет-ресурсы:
- для демонстрации презентаций используются программы *Windows* и *MS Office*.
- в качестве вспомогательных **интернет-ресурсов** по дисциплине используется:
Портал Math-Net.ru

8. Материально-техническое обеспечение дисциплины
- компьютерный класс;
- набор теоретико-групповых программ GAP..

Программа составлена в соответствии с федеральными государственными требованиями к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура) (приказ Минобрнауки от 16.03.2011 г. № 1365) с учетом рекомендаций, изложенных в письме Минобрнауки от 22.06.2011 г. № ИБ – 733/12.

Программа одобрена на заседании кафедры компьютерной безопасности и математических методов обработки информации 02.10.2012 (протокол № 2).

Заведующий кафедрой В.Г.Дурнев, доктор физ-мат.наук, профессор

Автор В.Г.Дурнев, доктор физ-мат.наук, профессор