Приложение 1

Министерство образования и науки Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»
Кафедра «Информационная безопасность»

ОДОБРЕНО:
Методической комиссией по укрупненной группе специальности 10.00.00 «Информационная безопасность»

Председатель МК:
_____ В.Б.Мелехин
Подпись ИОФ

«17» 10 2018 г.

УТВЕРЖДАЮ:

Декан факультета КТ, ВТиЭ

_____ Ш.А.Юсуфов
Подпись ИОФ

«18» 10 2018 г.

Фонд оценочных средств 525

по дисциплине **«Криптографические методы защиты информации»** для контроля знаний обучающихся специальности 10.05.03 «Информационная безопасность автоматизированных систем»

Составитель, к.э.н. _____ Качаева Г.И.

Фонд оценочных средств обсужден на заседании кафедры
«15» 10 2018 г., протокол № 2

Зав.кафедрой ИБ, к.э.н. _____ Качаева Г.И.

Фонд оценочных средств является **приложением** к рабочей программе по дисциплине «Криптографические методы защиты информации».

Введение

Для проверки знаний составляющей компетенций, формируемых в рамках дисциплины «Криптографические методы защиты информации» в фонде оценочных средств предусмотрены:

- вопросы для устного собеседования(опроса).

Для проверки деятельностной составляющей компетенций, формируемых в рамках дисциплины «Криптографические методы защиты информации» в фонде оценочных средств размещены:

- профессионально-ориентированные задания.

Конкретные задания, выносимые для проведения текущего контроля и промежуточную аттестации по дисциплине, представлены в отдельном документе «Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по дисциплине», прилагаемом к рабочей программе.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Перечень компетенций, на освоение которых направлено изучение дисциплины «Криптографические методы защиты информации», с указанием этапов их формирования в процессе освоения образовательной программы:

способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14).

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

Показатели и критерии оценивания компетенций, используемые шкалы оценивания

Элементы компетенций (знания, умения, владения)	Показатели оценивания	Критерии оценивания	Средства оценивания	Шкалы оценивания
Знать (ПК-14)	**Знание**: правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в информационных системах, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; - принципы построения криптографических алгоритмов, криптографические стандарты и их использование в	Правильность и полнота ответов, глубина понимания вопроса	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: экзамен	Шкала 1

	информационных системах. - основные принципы, понятия, факты, законы естественных и математических наук;			
Уметь (ПК-14)	**Умение:** -анализировать и оценивать угрозы информационной безопасности объекта; - применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях: - применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации.	Правильность выполнения учебных заданий, аргументированность выводов	Текущий контроль: выполнение устных/ письменных заданий Промежуточная аттестация: экзамен	Шкала 1
Владеть (ПК-14)	**Владение** : - поиска наиболее эффективных путей обработки информации; -методами использования основных положений теории информационной безопасности в различных информационных системах, а также иметь представление о направлении развития и перепективах защиты информации.	Обоснованность и аргументированность выполнения учебной деятельности	Текущий контроль: выполнение практического задания, защита лабораторной работы Промежуточная аттестация: экзамен	Шкала 2

Описание шкал оценивания степени сформированности элементов компетенций

Шкала 1.Оценка сформированности отдельных элементов компетенций

Обозначения		**Формулировка требований к степени сформированности компетенции**		
Цифр.	Оценка	**Знать**	**Уметь**	**Владеть**
1	Неуд.	Отсутствие знаний	Отсутствие умений	Отсутствие навыков

2	Неуд.	Фрагментарные знания	Частично освоенное умение	Фрагментарное применение
3	Удовл.	Общие, но не структурированные знания	В целом успешное, но не систематически осуществляемое умение	В целом успешное, но не систематическое применение
4	Хор.	Сформированные, но содержащие отдельные пробелы знания	В целом успешное, но содержащие отдельные пробелы умение	В целом успешное, но содержащее отдельные пробелы применение навыков
5	Отл.	Сформированные систематические знания	Сформированное умение	Успешное и систематическое применение навыков

Шкала 2. Комплексная оценка сформированности знаний, умений и владений

Обозначения		**Формулировка требований к степени сформированности компетенции**
Цифр.	Оценка	
1	Неуд.	Не имеет необходимых представлений о проверяемом материале
2	Удовл. или неуд. (*по усмотрению преподавателя)*	Знать на уровне **ориентирования.** представлений. Субъект учения знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает их в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3	Удовл.	Знать и уметь на **репродуктивном** уровне. Субъект учения знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4	Хор.	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.

5	Отл.	Знать, уметь, владеть на **системном** уровне. Субъект учения знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания учебной дисциплины, его значимость в содержании учебной дисциплины.

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.

Типовые вопросы и задания для текущего контроля(оценка сформированности элементов (знаний, умений) компетенции в рамках текущего контроля по дисциплине) по разделам дисциплины

Примеры вопросов по разделу 1-5:

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.
13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.
17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.

30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. Опишите алгоритм RSA.
35. Опишите алгоритм цифровой подписи RSA.
36. Опишите алгоритм цифровой подписи Эль-Гамаля.

Защита лабораторных работ (оценка сформированности элементов (знаний, умений) компетенции в рамках текущего контроля по дисциплине) по разделам дисциплины:

Примеры вопросов при защите лабораторной работы №1

1. Методы криптографического преобразования данных.
2. Электронная цифровая подпись.
3. Проблемы реализации методов криптографической защиты в информационных системах.
4. Характеристики криптографических средств защиты информации. Криптография и гипотеза PNP.
5. Односторонние функции.
6. Псевдослучайные генераторы.
7. Доказательства с нулевым разглашением.

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

Процедуры и средства оценивания элементов компетенций по дисциплине «Криптографические методы защиты информации».

Процедура проведения	**Средство оценивания**				
	Текущий контроль				Промежуточный контроль
	Выполнение устных заданий	Выполнение письменных заданий	Выполнение практических заданий	Защита лабораторных работ	Экзамен
Продолжительность контроля	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	По усмотрению преподавателя	В соответствии с принятыми нормами времени
Форма проведения контроля	Устный опрос	Письменный опрос	Письменный опрос	Устная защита	В письменной форме

Вид проверочного задания	Устные вопросы	Письменные задания	Практические задания	Устные вопросы	экзаменационный билет
Форма отчета	Устные ответы	Ответы в письменной форме	Ответы в письменной форме	Ответы в устной форме	Ответы в письменной форме
Раздаточный материал	Нет	Справочная литература	Справочная литература	Справочная литература	Справочная литература

Методические указания для обучающихся по освоению дисциплины

Дисциплина «Криптографические методы защиты информации» предусматривает лекции раз в неделю, лабораторные работы раз в четыре недели и практические занятия раз в две недели. Изучение дисциплины завершается экзаменом. Успешное изучение дисциплины требует посещения лекций, активной работы на практических занятиях, выполнения учебных заданий преподавателя, ознакомления с основной и дополнительной литературой, нормативными правовыми актами и нормативными документами.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на лабораторные и практическое занятие и указания на самостоятельную работу.

При подготовке к лекционным занятиям студентам необходимо:

перед очередной лекцией необходимо просмотреть по конспект материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

При подготовке к практическому занятию студенты имеют возможность воспользоваться консультациями преподавателя.

При подготовке к практическим занятиям студентам необходимо:

приносить с собой рекомендованную преподавателем литературу к конкретному занятию;

до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно- правовые акты и материалы правоприменительной практики;

теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;

в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;

в ходе семинара давать конкретные, четкие ответы по существу вопросов;

на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному практическому занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины «Криптографические методы защиты информации»

ФОНД ВОПРОСОВ (ЗАДАЧ) ДЛЯ КОНТРОЛЬНЫХ РАБОТ

Вопросы для входной контрольной работы

1. Формальное описание структуры информационной системы.
2. Составление модели угроз информационной системе.
3. Формирование требований к системе защиты информации.
4. Формирование требований к политике информационной безопасности.
5. Формирование регламента действий при возникновении нештатных ситуаций.

Контрольные работы по проверке текущих знаний студентов

Аттестационная контрольная работа №1

1. Ретроспективный анализ развития подходов к разработке средств криптографической защиты информации.
2. Понятия «информация», ее «источники и носители».
3. Информация общедоступная и ограниченного доступа.
4. Категории ценности информации.
5. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; приводится классификация атак.
6. Модели сетевой безопасности и безопасности информационной системы. Информация как объект защиты.
7. Основные задачи обеспечения криптографической защиты информации.
8. Основные методы и средства защиты информации в информационных системах.
9. Анализ угроз информационной безопасности: классификация угроз.
10. Возникновение и развитие криптографии и криптоанализа.
11. Общие методы криптографии и криптоанализа.
12. Виды конфиденциальной информации и их защита.
13. Способы и средства криптографической защиты информации (СКЗИ).
14. Криптографические преобразования.
15. Шифрование и дешифрование информации. Взлом криптоалгоритмов.
16. Виды атак на криптографические протоколы.
17. Причины нарушения безопасности информации при ее обработке СКЗИ.
18. Математическая модель шифра.

19. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.
20. Алгебраические структуры. Группы. Циклические группы.
21. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа.
22. Эллиптические кривые.
23. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках.
24. Основные понятия, относящиеся к алгоритмам симметричного шифрования. Ключ шифрования.
25. Типы операций, используемые в алгоритмах симметричного шифрования.
26. Сеть Фейштеля. Основные понятия криптоанализа.
27. Линейный и дифференциальный криптоанализ.
28. Аалгоритмы DES и тройной DES.

Аттестационная контрольная работа №2

1. Предпосылки появления криптографии с открытым ключом.
2. Схемы шифрования с открытым ключом. Функция Эйлера.
3. Основные понятия, относящиеся к криптографии с открытым ключом, а также способы их использования. Обмен ключами.
4. Реализация алгоритма RSA.
5. Процедуры шифрования и расшифрования в шифрсистеме Эль-Гамаля. Процедура генерации ключей шифрсистемы Эль-Гамаля.
6. Работа в режиме подписи.
7. Криптостойкость алгоритма. Преимущества и недостатки систем асимметричного шифрования. Взлом криптосистем с открытым ключом.
8. Функции хэширования. Классификация.
9. Функции хэширования без ключа (MDC) и с ключом (MAC). Принципы построения.
10. Функции хэширования Ривеста: MD2, MD4, MD5.
11. Американский стандарт функции хэширования (SHS) и его изменения.
12. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).
13. Применение функции хэширования в схемах цифровой подписи и при построении криптосистем.
14. Сильные хэш- функции SHA-1, SHA-2.
15. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.
16. Контроль целостности данных.
17. Идентификация и аутентификация. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющих в шифртексте искажения открытого текста.
18. Шифрование, создание и проверка цифровой подписи. Использование открытых ключей.
19. Схемы подписи RSA и Рабина. Схема цифровой подписи Эль Гамаля и ее модификации.
20. Криптографические хеш-функции. ГОСТ Р 34.11-2012.
21. DES, AES.

Аттестационная контрольная работа №3

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.
13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.
17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.
30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. .Опишите алгоритм RSA.

Перечень экзаменационных вопросов по дисциплине «Криптографические методы защиты информации»

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Группы подстановок.
4. Кольца. Кольца классов вычетов.
5. Поля. Поля Галуа.
6. Эллиптические кривые над конечным полем.
7. Цели и задачи криптографии. Основные понятия.

8. Простейшие шифры: простой замены, перестановочный, аффинный.
9. Шифр Хилла.
10. Шифры гаммирования. Шифр Вернама.
11. ГОСТ Р 34.12-2015. Шифр «Магма».
12. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
13. ГОСТ Р 34.13- 2015. Режимы гаммирования.
14. ГОСТ Р 34.13-2015. Режимы простой замены, режим выработки имитовставки.
15. Стандарт шифрования DES.
16. Стандарт шифрования AES.
17. Криптография с открытым ключом.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамаля.
20. Протокол Диффи- Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. ГОСТ Р 34.11-2012.
24. Коды аутентичности сообщений. Электронная подпись.
25. ГОСТ Р 34.10-2012.

Практические задачи:

1. Изучить свойства данной алгебраической структуры.
2. Пусть G — циклическая группа порядка n с образующим x. Найти все образующие и все подгруппы данной группы.
3. Исследовать кольцо классов вычетов по модулю n.
4. Построить поле Галуа посредством неприводимого многочлена f(x). Найти образующий элемент мультипликативной группы поля.
5. Построить группу точек эллиптической кривой над полем Галуа GF(q) для данных значений параметров a, b.
6. Записать целочисленную линейную комбинацию чисел a и b.
7. Дано сообщение M. Зашифровать его с помощью данного шифра.
8. Дано сообщение M. Сформировать электронную подпись для данного сообщения по ГОСТ Р 34.10-2012, используя данные параметры эллиптической кривой.

Вопросы для проверки остаточных знаний студентов

1. Охарактеризуйте информацию и ее основные показатели.
2. Основные положения закона об информации, информационных технологиях и защите информации.
3. Основные положения закона о государственной тайне.
4. Основные положения закона о защите персональных данных.
5. Основные положения закона об электронной цифровой подписи.
6. Что такое «политика безопасности»?
7. Чем отличается понятие «модели безопасности» от понятия «политики безопасности»?
8. В каких случаях применяются модели безопасности?
9. Основные модели политик безопасности?
10. Принципы, используемые для повышения стойкости шифра?
11. Приведите схему и объясните принцип работы блочного шифра.
12. Дайте характеристику шифра DES.

13. Дайте характеристику шифра ГОСТ 28147-89.
14. Перечислите основные различия между DES и ГОСТ 28147-89.
15. Что такое – режим применения блочного шифра?
16. Чем отличается поточное и блочное шифрование.
17. Дайте характеристику шифра RC4.
18. Основные свойства криптографических хеш-функций.
19. Принципы работы хеш-функции.
20. Особенности построение хеш-функции на базе блочного шифра.
21. Опишите операцию приведения по модулю.
22. Какими свойствами обладает операция приведения по модулю?
23. Приведите определение простого числа.
24. Какие два числа называются взаимно простыми?
25. Определите понятие обратного значения по модулю.
26. Сформулируйте малую теорему Ферма.
27. Дайте определение функции Эйлера.
28. Сформулируйте теорему Эйлера.
29. Перечислите свойства простых чисел.
30. Чем отличается криптография с открытым ключом от симметричных шифров?
31. Опишите алгоритм Диффи-Хеллмана. Чем обусловлена его безопасность?
32. Опишите алгоритм Шамира.
33. Опишите алгоритм Эль-Гамаля.
34. .Опишите алгоритм RSA.

Учебно-методическое и информационное обеспечение дисциплины

«Криптографические методы защиты информации»

№ п/п	Виды заня-тий	Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет ресурсы	Автор(ы)	Изда-тельство и год издания	Количество изданий	
					В библио-теке	На кафед ре
1	2	3	4	5	6	7
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк., пз, срс	Основы современной криптографии и стеганографии. [Электронный ресурс]	Б.Я. Рябко. А.Н. Фионов.	2-е изд. — М.: Горячая линия – Телеком. 2013. — 232 с.	http://e.lanbook.com/view/book/63244/	
2.	Лк., пз, срс	Введение в теоретико-числовые методы криптографии: учебное пособие	М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин	СПб.: Издательство «Лань», 2011. — 400 с. [Электронный	http://e.lanbook.com/view/book/68466/	

				ресурс].	
3.	Лк., пз, срс	Методы и средства криптографической защиты данных в вычислительных системах. Часть 2 [Электронный ресурс]:	Борисова С.Н.	Пенза: ПензГТУ (Пензенский государственный технологический университет), 2013. — 107 с.	http://e.lanbook.com/books/element.php?pl1_id=62779
4.	Лк., пз, срс	Основы защиты информации и информационные технологии: Учебное пособие в 3 частях. – Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ [Электронный ресурс]: учебное пособие	Серёдкин А.Н.	Пенза: ПензГТУ (Пензенский государственный технологический университет), 2013. — 180 с.	http://e.lanbook.com/books/element.php?pl1_id=62755
5.	Лк., пз, срс	Введение в криптографию: сборник задач и упражнений [Электронный ресурс]	Е.Г. Кукина, В.А. Романьков	Омск: ОмГУ (Омский государственный университет им. Ф.М. Достоевского), 2013. — 91 с.	http://e.lanbook.com/books/element.php?pl1_id=75394
6.	Лк., пз, срс	Введение в криптографию [Электронный ресурс]:	В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин [и др.].	М.: МЦНМО (Московский центр непрерывного математического образования), 2012. — 348 с.	http://e.lanbook.com/books/element.php?pl1_id=71813
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА					
7.	Лк., пз, срс	Интеллектуальные системы защиты информации [Электронный ресурс]	Васильев В.И.	М.: Машиностроение, 2013. — 172 с.	http://e.lanbook.com/books/element.php?pl1_id=5792
8.	Лк., пз, срс	Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие.	В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин [и др.].	М.: ФЛИНТА, 2011. — 187 с.	http://e.lanbook.com/books/element.php?pl1_id=60717
9.	Лк., пз,	Методы и средства	Борисова С.Н.	Пенза: ПензГТУ	http://e.lanbook.co

	ерс	защиты компьютерной информации. Часть 1 [Электронный ресурс]		(Пензенский государственный технологический университет), 2013. — 55 с.	m/books/element.php?pl1_id=62780
ИНТЕРНЕТ-ИСТОЧНИКИ					
10.	Лк., пз, ерс	http://kmb.ufoctf.ru/index.html			
11.	Лк., пз, ерс	https://habrahabr.ru/hub/crypto/			
12.	Лк., пз, ерс	http://training.hackerdom.ru/			
13.	Лк., пз, ерс	http://fstec.ru/			
14.	Лк., пз, ерс	Виртуальная операционная система Microsoft Windows XP SP3 (VirtualBox, доступ из локальной сети каф. КИБЭВС. URL: file://cesir/vm/WinXPBasic).			