Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине Б.1.1.16 «Криптографические методы защиты информации»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 2
семестр – 4
зачетных единиц – 4
часов в неделю – 4
всего часов – 144 ,
в том числе:
лекции – 32
практические занятия – 32
самостоятельная работа – 80
экзамен – 4 семестр

1. Цели и задачи дисциплины

Целью курса «Криптографические методы защиты информации» является обучение студентов основам криптографического сокрытия информации.

Задачи изучения дисциплины:

Знакомство и практическое освоение криптографическими средствами защиты информации.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Криптографические методы защиты информации» является дисциплиной базовой части цикла дисциплин ФГОС ВО по направлению 10.03.01 "Информационная безопасность" по профилю "Безопасность автоматизированных систем".

Дисциплина «Криптографические методы защиты информации» базируется на знаниях, полученных в рамках изучения следующих дисциплин: «Информатика», «Дискретная математика», «Математика».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-2 Способностью применять соответствующий математический аппарат для решения профессиональных задач;

ПК-1 Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Студент должен знать:

основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;

модели шифров и математические методы их исследования;

принципы построения криптографических алгоритмов;

криптографические стандарты и их использование в информационных системах;

основные нормативные правовые документы в области криптографической защиты информации;

аппаратные средства вычислительной техники;

технические средства защиты информации;

принципы организации информационных систем в соответствии с требованиями по защите информации;

основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах.

Студент должен уметь:

эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;

применять математические методы исследования моделей шифров;

использовать программные и аппаратные средства персонального компьютера;

осуществлять поиск информации по профилю деятельности в различных источниках, в том числе в глобальных компьютерных системах;

применять нормативные правовые документы в области криптографической защиты информации на практике;

анализировать и оценивать угрозы информационной безопасности объекта;

осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты;

пользоваться сетевыми средствами для осуществления поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в области криптографической защиты информации.

Студент должен владеть:

криптографической терминологией;

навыками использования типовых криптографических алгоритмов;

навыками использования ЭВМ в анализе простейших шифров;

навыками математического моделирования в криптографии;

навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.);

навыками разработки документации в области криптографической защиты информации;

методами и средствами выявления угроз безопасности автоматизированным системам;

методами технической защиты информации.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**		**8**	**9**
4 семестр									
1	1	1	История криптографии.	14	2			4	8
1	2	2	Характер криптографической деятельности.	2	2				
1	3	3	Простейшие шифры и их свойства. Композиции шифров.	6	2			4	
1	4	4	Системы шифрования с открытым и секретным ключами.	6	2			4	
1	5	5	Виды информации, подлежащие закрытию, их модели и свойства.	6	2			4	
1	6	6	Модели шифров. Основные	2	2				

			требования к шифрам. Совершенные шифры.						
1	7	7	Криптографическая стойкость шифров. Теоретико-информационный подход к оценке криптостойкости шифров. Имитостойкость и помехоустойчивость шифров.	18	2			4	12
1	8	8	Блочные и поточные шифры.	2	2				
2	9, 10	9	Принципы построения криптографических алгоритмов.	26	4			4	18
2	11	10	Российский стандарт шифрования ГОСТ 28147-89. Стандарт шифрования США AES.	2	2				
2	12, 13	11	Криптографические хэш-функции.	20	4			4	12
2	14	12	Электронная подпись.	20	2			4	14
2	15-16	13	Криптографические протоколы.	20	4				16
Всего				144	32			32	80

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	2	3	4	5
1	2	1	**История криптографии.** Предпосылки возникновения криптографии. Шифр Цезаря, афинская криптосистема, сцитала, табличка Энея, квадрат Полибия, шифровальный диск.	1,4-8,11
2	2	2	**Характер криптографической деятельности.** Основные определения криптографии. Базовые методы преобразования информации. Основные направления использования критографических методов.	1,4-8,11
3	2	3	Классификация методов шифрования. Методы подстановки (одноалфавитная, полиалфавитные), методы перестановки (простая, усложненная), методы гаммирования, шифрование с помощью аналитических преобразований. Современные комбинированные шифры. Стойкость	1,4-8,11

			комбинированного шифрования.	
4	**2**	**4**	**Системы шифрования с открытым и секретным ключами.** Симметричные и ассиметричные системы шифрования, их модели. Инфраструктура открытого ключа.	1,4-8,11
5	**2**	**5**	**Виды информации, подлежащие закрытию, их модели и свойства.** Классификация информации по назначению использования, особенностям представления, возможностям трансформации.	1,4-8,11
6	**2**	**6**	**Модели шифров. Основные требования к шифрам.** Конечные и бесконечные ключевые потоки. Опорный шифр, его степень. Формирование модели. Степень надежности и трудоемкости шифров. Оценка ключевой последовательности. Шифры совершенные по Шеннону. Необходимое и достаточное условия совершенности.	1,4-11
7	**2**	**7**	**Криптографическая стойкость шифров. Теоретико-информационный подход к оценке криптостойкости шифров. Имитостойкость и помехоустойчивость шифров.** Методы криптоанализа. Причины уменьшения криптосойкости. Оценка надежности криптоалгоритмов. Вероятность имитации и вероятность подмены. Стойкость к воздействию преднамеренных и непреднамеренных помех в канале связи.	1-3,11
8	**2**	**8**	**Блочные и поточные шифры.** Режимы работы блочных шифров. Синхронные поточные шифры. Самосинхронизирующиеся поточные шифры.	1-7,11
9	**4**	**9,10**	**Принципы построения криптографических алгоритмов.** Симметричные (DES, Twofish) и асимметричные криптоалгоритмы (RSA).	1-7,11
10	**2**	**11**	**Российский стандарт шифрования ГОСТ 28147-89. Стандарт шифрования США AES.** Структурный и сравнительный анализ алгоритмов.	1-9,11
11	**4**	**12,13**	**Криптографические хэш-функции.** Принципы построение и свойства хэш-функций. Российский стандарт хэширования ГОСТ Р 34.11-2012. Стандарт хэширования США. Хэш-функция Keccak	1-4,11
12	**2**	**14**	**Электронная подпись.** Принципы построения Электронной подписи. Классификация, свойства, атаки. Алгоритмы Эль-Гамаля, Рабина, Шнорра, Шамира. Российский стандарт построения ЭП ГОСТ Р 34.10-2012. Алгоритмы построения ЭП ECDSA и DSA. «Слепая» подпись.	1-7,11
13	**4**	**15-16**	**Криптографические протоколы.** Введение в	1-3,11

			криптографические протоколы. Структуризация криптографических протоколов. Современные криптографические протоколы. Криптографические протоколы Интернета (SSL, PPTP, SET). Распределение ролей в криптографическом протоколе. Программные и аппаратные реализации ключей. Соглашение об аутентификации. Вычислительная сложность протокола. Согласование ключей с помощью пароля. часов в криптографии. Серверы ключей. Система Kerberos. Сравнительный анализ версий протокола Kerberos 4 и Kerberos5.	

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	2	3	4	5

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4	5
3	4	1-2	**Простейшие шифры и их свойства.** Шифрование и дешифрование с помощью шифра Цезаря, квадрата Полибия, таблицы Вижинера, шифров перестановки для заданного ключа.	1,4-6,11
3	4	3-4	**Композиции шифров.** Создание различных комбинаций изученных шифров.	1,4-6,11
4	4	5-6	**Системы шифрования с открытыми ключами.** Работа в системе PGP.	1,4-7,11
5	4	7-8	**Программная реализация изученных шифров.** Программная реализация монофонической замены и шифра Вижинера.	1,4-7,11
7	4	9-10	**Вопросы практической стойкости.** Оценка надежности криптоалгоритмов в зависимости от длины ключа.	1,4-7,11
9	2	11	**Принципы построения криптографических алгоритмов.** Программная реализация одного из изученных криптоалгоритмов.	1,4-7,11
9	2	12	**Особенности использования вычислительной техники в криптографии.** Программная реализация защищенного канала общения.	1,4-7,11
11	4	13-14	**Криптографические хэш-функции**. Создание модели безопасной хэш – функции.	1,4-7,11
12	4	15-16	**Электронная цифровая подпись.**	1,4-7,11

			Программная реализация ЭЦП по заданным параметрам.	

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	4	3

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
1	8	Древние шифры, их использование.	1,4-7,11
7	12	Проблемы создания надежных криптосистем.	1,4-7,8-9,11
9	10	Арифметика по модулю простого числа. Алгоритм поиска НОД. Расширенный алгоритм Евклида. Китайская теорема об остатках. Алгоритм быстрого возведения в степень по модулю.	1,4-7,11
9	8	Симметричные и асимметричные алгоритмы шифрования.	1,4-7,8-9,11
11	12	Сравнительный анализ алгоритмов хэш – функций MD4 и MD5.	1,4-7,11
12	14	Новые стандарты ЭЦП. Стандарт ЭЦП основанный на построении эллиптических кривых.	1,4-7,11
13	16	Проблема генерации ключей.	1,4-7,11

Виды, график контроля СРС, (по решению кафедры УМКС/УМКН).

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
5 семестр			
1-8	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация)
9-13	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	экзамен

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [11].

10. Расчетно-графическая работа

Учебным планом не предусмотрена

11. Курсовая работа

Учебным планом не предусмотрена

12. Курсовой проект

Учебным планом не предусмотрена

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-2 Способностью применять соответствующий математический аппарат для решения профессиональных задач;

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях; модели шифров и математические методы их исследования; принципы построения криптографических алгоритмов; криптографические стандарты и их использование в информационных системах; основные нормативные правовые документы в области криптографической защиты информации.	Лекции Самостоятельная работа Семинары Семинары в диалоговом режиме, в виде групповых дискуссий	Тестирование
Умеет: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять математические методы исследования моделей шифров; использовать программные и аппаратные средства персонального компьютера; осуществлять поиск информации по профилю деятельности в различных источниках, в том числе в	Лабораторные работы с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты

глобальных компьютерных системах; применять нормативные правовые документы в области криптографической защиты информации на практике.		
Владеет: криптографической терминологией; навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии.	Лекции Семинарские занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

ПК-1 Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Части компонентов	Технологии формирования	Средства и технологии оценки
Знает: аппаратные средства вычислительной техники; технические средства защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах.	Лекции Самостоятельная работа Семинары Семинары в диалоговом режиме, в виде групповых дискуссий	Тестирование

Умеет: анализировать и оценивать угрозы информационной безопасности объекта; осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты; пользоваться сетевыми средствами для осуществления поиска, изучения, обобщения и систематизации научно-технической информации, нормативных и методических материалов в области криптографической защиты информации.	Лабораторные работы с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
Владеет: навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.); навыками разработки документации в области криптографической защиты информации; методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации.	Лекции Семинарские занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Экзамен

При выставлении экзаменационных оценок предлагается руководствоваться следующим:
оценки «отлично» заслуживает студент, показавший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой.
оценки «хорошо» заслуживает студент, показавший полное знание учебно-программного материала, успешно выполняющий предусмотренные в программе задания.
оценки «удовлетворительно» заслуживает студент, показавший знание учебно-программного материала в объеме, необходимом для дальнейшей учебы и профессиональной деятельности.

оценки «неудовлетворительно» заслуживает студент, показавший пробелы в знаниях основного учебно-программного материала, допустивший принципиальные ошибки в выполнении предусмотренных программой заданий.

Вопросы для экзамена

1. История криптографии.
2. Шифры. Простейшие шифры. Композиции шифров.
3. Хэш – функция. Особенности построения. Виды хэш – функций. MD5, SHA-1, SHA-256.
4. Системы шифрования с секретным и открытым ключами.
5. Блочные шифры (DES, 3DES, AES, SERPENT, TOWFISH, RS-6, MARS, ГОСТ 28147-89).
6. Режимы работы блочных шифров.
7. Виды атак.
8. Идеальные шифры по Шеннону.
9. Коды аутентичности.(Алгоритмы CBC-MAC, HMAC (HMAC-SHA-256), принцип Хортона).
10. Электронная цифровая подпись. Принципы построения. Алгоритмы Эль – Гамаля, Шамира, схемы с использованием эллиптических кривых).
11. Безопасный канал общения.
12. Проблемы реализации (создание правильного ПО, создание безопасного ПО, атаки с использованием побочных каналов).
13. Генерация случайных чисел. (Истинно случайные числа, псевдослучайные числа).
14. ГПСЧ FORTUNA (генератор, аккумулятор, управление файлом начального числа).
15. Алгоритм Диффи – Хелмана. Базовый алгоритм. Атака посредника. Надежные простые числа. Практические правила.
16. Алгоритм RSA. Китайская теорема об остатках. Шифрование. Цифровая подпись. Генерация ключей.
17. Система PGP.
18. Введение в криптографические протоколы.(Роли, доверие, стимул, сообщения и действия)
19. Протокол согласования ключей.(1-5 попытки, анализ протокола с различных точек зрения, взлом ключа).
20. Проблемы реализации протокола согласования ключей.(Вупинг, метод Монтгомери, выполнение протоколов).
21. Часы. Виды угроз.
22. Серверы ключей. Система управления ключами Kerberos.

Тестовые задания по дисциплине

Для проведения тестирования используются тестовые материалы, разработанные в среде АСТ-Тест.

1. Шифры замены бывают:

А) простые одноалфавитные
Б) одноконтурные полиалфавитные.
В) многоконтурные полиалфавитные.
Г) монофонические полиалфавитные.
Д) усложненные по маршрутам

2. Криптосистемы с секретным ключом называют:

А) Симметричными криптосистемами.

Б) Асимметричными криптосистемами.
В) Одноключевыми криптосистемами.
Г) Двуключевыми криптосистемами.

3. Хэш-функция должна обладать следующими функциями:
А) Устойчивость к коллизиям.
Б) Симметричность.
В) Однонаправленность.
Г) Линейность

4. Алгоритм RSA основан на использовании
А) односторонней функции
Б) односторонней функции с лазейкой
В) надежного простого числа
Г) составного числа, образованного двумя простыми числами

5. Коды аутентичности сообщений позволяют
А) шифровать сообщения
Б) дешифровывать сообщения
В) подтверждать целостность сообщения
Г) подтверждать подлинность отправителя

6. К симметричным криптосистемам относятся алгоритмы
А) DES
Б) 3DES
В) AES
Г) RSA
Д) TWOFISH

7. Устройство «Сцитало» является примером шифрования:
А) Методом подстановки
Б) Методом перестановки
В) Методом гаммирования

8. Шифры делятся на
А) Блоковые и последовательные
Б) Блочные и поточные
В) Потоковые и дискретные

9. К достоинствам блочных шифров относят
А) высокую скорость шифрования
Б) дешевизну реализации
В) похожесть процедур шифрования и расшифрования

10. Стандарт шифрования ГОСТ 28147-89 предусматривает шифрование и расшифровку данных в следующих режимах работа:
А)простая замена;
Б)маршрутная перестановка
В)гаммирование;
Г)гаммирование с обратной связью;
Д)выработка имитовставки.

11. Режим выработка имитовставки в стандарте шифрования ГОСТ 28147-89 гарантирует:
А) конфиденциальность сообщения
Б) целостность сообщения
В) аутентификацию сообщения

12. В чем состоит задача криптографа?
1) взломать систему защиты
2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

13. Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи называется
А) криптография
Б) стеганография

14. К методам защиты от НСД относятся:
А) разделение доступа;
Б) разграничение доступа;
В) увеличение доступа;
Г) ограничение доступа.
Д) аутентификация и идентификация

15. Выделите группы, на которые делятся средства защиты информации:
А) физические, аппаратные, программные, криптографические, комбинированные;
Б) химические, аппаратные, программные, криптографические, комбинированные;
В) физические, аппаратные, программные, этнографические, комбинированные;

16. Что такое целостность информации?
А) Свойство информации, заключающееся в возможности ее изменения любым субъектом
Б) Свойство информации, заключающееся в возможности изменения только единственным пользователем
В) Свойство информации, заключающееся в ее существовании в виде единого набора файлов
Г) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

17. К аспектам ИБ относятся
А) дискретность
Б) целостность
В) конфиденциальность
Г) актуальность
Д) доступность

18. Что такое криптология?
А) защищенная информация
Б) область доступной информации
В) тайная область связи

19. Что такое несанкционированный доступ (нсд)?
А) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

Б) Создание резервных копий в организации
В) Правила и положения, выработанные в организации для обхода парольной защиты
Г) Вход в систему без согласования с руководителем организации
Д) Удаление не нужной информации

20. Какой режим применяется для шифрования небольших объемов информации, размером не более одного блока или для шифрования ключей
А) Обратная связь по шифротексту
Б) Электронная кодовая книга
В) Сцепление блоков шифротекста

14. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Рябко Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс]/ Рябко Б.Я., Фионов А.Н.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 232 с.— Режим доступа: http://www.iprbookshop.ru/12018.— ЭБС «IPRbooks», по паролю
2. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/16713.— ЭБС «IPRbooks», по паролю
3. Штарьков Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс]/ Штарьков Ю.М.— Электрон. текстовые данные.— М.: ФИЗМАТЛИТ, 2013.— 280 с.— Режим доступа: http://www.iprbookshop.ru/24451.— ЭБС «IPRbooks», по паролю

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Мао, В. Современная криптография. Теория и практика. / В. Мао. - М.; СПб.; Киев : Изд. дом "Вильямс", 2005. - 768 с. ил. ; 24 см. - Библиогр.: с. 731-754 (312 назв.). - ISBN 5-8459-0847-7
(1 экз)
5. Смарт Н. Криптография / Н. Смарт ; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - М. : Техносфера, 2005. - 528 с. : ил. ; 24 см. - (Мир программирования). - ISBN 5-94836-043-1
(4 экз.)

6. Алферов А. П. Основы криптографии : учеб. пособие / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 480 с. : ил. ; 20 см. - Гриф: допущено М-вом образования РФ в качестве учеб. пособия для студ. вузов, обучающихся по группе спец. в обл. информационной безопасности. - ISBN 5-85438-137-0
(20 экз)
7. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры : учеб. пособие / А. Ю. Зубов. - М. : Гелиос АРВ, 2005. - 192 с. ; 20 см. - Гриф: допущено УМО вузов по образованию в обл. информационной безопасности в качестве учеб. пособия для студ. вузов, обучающихся по спец. группы "Информационная безопасность". - ISBN 5-85438-135-4 (5 экз.)

ПЕРИОДИЧЕСКИЕ ИЗДАНИЯ

8. Информационная безопасность регионов [Текст] : науч.-техн. журнал. - Саратов : Изд-во СГСЭУ, 2007 - . - Выходит раз в три месяца. - ISSN 1995-5731 http://elibrary.ru/title_about.asp?id=28126

ИНТЕРНЕТ-РЕСУРСЫ

9. Аграновский А.В. Практическая криптография: алгоритмы и их программирование [Электронный ресурс] / Аграновский А.В. - Москва : СОЛОН-Пресс, 2009. - . - ISBN 5-98003-002-6 : http://www.studentlibrary.ru/book/ISBN5980030026.html
10. Мировые информационные ресурсы [Электронный ресурс] / А.В. Коротков. -Москва: МГИМО,2012.-.- ISBN 978-5-9228-0806-4 http://www.studentlibrary.ru/book/ISBN9785922808064.html

ИСТОЧНИКИ ИОС

11. https://portal.sstu.ru/Fakult/FETIP/IBS/b314/default.aspx (ИОС СГТУ)

16. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Для реализации образовательной программы подготовки бакалавра по направлению «Информационная безопасность», имеется материально-техническая база, обеспечивающая проведение всех видов занятий по дисциплине «Криптографические методы защиты информации», включая лекционные, лабораторные и практические занятия, которая соответствует действующим санитарным и противопожарным правилам и нормам.

Для преподавания дисциплины предоставляется оснащенная современным проекционным оборудованием лекционная аудитория и компьютерные классы.

В компьютерном классе установлено по 15 персональных компьютеров, объединенных в локальную сеть с автоматическим выходом в корпоративную сеть СГТУ и глобальную сеть Интернет. Все персональные компьютеры оснащены лицензионным ПО Microsoft Windows, Microsoft Office.

Для пользования электронными изданиями и информационно-обучающей средой (ИОС) СГТУ во время самостоятельной подготовки студентам предоставляются рабочие места в библиотеке СГТУ.