Учреждение образования «Полоцкий государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
«Полоцкий государственный университет»
_____ Ю.П. Голубев
«27» 06 2019
Регистрационный № УД-626/19/уч.

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
**1-98 01 01-01 «Компьютерная безопасность
(математические методы и программные системы)»**

2019

Учебная программа составлена на основе образовательного стандарта по специальности первой ступени высшего образования ОСВО 1-98 01 01-2013 и учебного плана по специальности 1-98 01 01-01 «Компьютерная безопасность (математические методы и программные системы)» (регистрационный № 13-13/уч. ФИТ от 29.08.2013)

СОСТАВИТЕЛИ:
Пастухов Дмитрий Феликсович, кандидат физико-математических наук, доцент кафедры технологий программирования учреждения образования «Полоцкий государственный университет»
Пастухов Юрий Феликсович, кандидат физико-математических наук, доцент кафедры технологий программирования учреждения образования «Полоцкий государственный университет»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования учреждения образования «Полоцкий государственный университет»
(протокол № 7 от 21.06 2019)

Методической комиссией факультета информационных технологий учреждения образования «Полоцкий государственный университет»
(протокол № 5 от 26.06. 2019)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс дисциплины «Криптографические протоколы» основывается на практических результатах, полученных при рассмотрении фундаментальных законов теории информации. Одним из основных направлений криптографических протоколов является изучение и разработка конкретных методов и средств эффективного, криптографического и помехоустойчивого кодирования сообщений на базе фундаментальных достижений в области теории информации, теории чисел и теории сложности алгоритмов и проблем. В настоящее время применение указанных видов кодирования стало необходимым инструментом для предварительного этапа проведения сеанса надежного и крипто-устойчивого связи хранения, обработки и передачи информации. Причем потребность в сжатии информации, криптографическом и помехоустойчивом кодировании сообщений со временем будет только возрастать. Это связано с непрерывным развитием аппаратных средств, которые позволяют реализовывать все более эффективные криптографические алгоритмы кодирования/декодирования, а также методы криптоанализа.

Целью преподавания дисциплины является изучение студентами основных разделов теории информации, включая элементы теории сложности проблем и алгоритмов, методов криптографического кодирования информации и методы защиты программного обеспечения от исследования.

Достижение поставленной цели предполагает решение следующих *задач*:

– изучение теоретических основ криптографических протоколов;

– приобретение навыков по предотвращению зеркальных атак, атак посредине и т.п. в криптографических протоколах;

– приобретение навыков по криптографическому шифрованию информации, использование псевдослучайных генераторов чисел, меток времени в протоколах;

– приобретение навыков по защите программного обеспечения от исследования.

В результате изучения дисциплины формируются следующие *компетенции*:

академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным порождать новые идеи (креативность).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

профессиональные компетенции:

ПК-8. Взаимодействовать со специалистами смежных профессий.

ПК-12. Пользоваться глобальными информационными ресурсами.

ПК-24. Работать с научной, технической и патентной литературой

В результате изучения дисциплины студент должен

знать:

– основы криптографических протоколов распределения ключей;
– основы аутентификационных протоколов;
– алгоритмы сжатия информации без потери данных;
– алгоритмы генерирования случайных чисел и их применение в протоколах, а также для создания меток времени;
– методы эффективной генерации простых больших чисел;
– криптографические алгоритмы и системы;

уметь:

– использовать на практике количественные меры информации;
– реализовывать алгоритмы эффективного кодирования для уменьшения объема хранимой и передаваемой информации;
– реализовывать криптографические алгоритмы для защиты информации от несанкционированного доступа;

владеть:

– навыками применения положений криптографических протоколов для криптографического преобразования информации;
– навыками использования новых методов и алгоритмов при реализации различных программных приложений;
– современными теоретическими и прикладными разделами криптографических протоколов;
– инструментарием научных исследований, проводимых в данной области.

Данная дисциплина основывается на таких дисциплинах как «Математический анализ», «Геометрия и алгебра», «Теория информации».

Согласно учебному плану, учебная программа изучения дисциплины «Криптографические протоколы» рассчитана следующим образом:

Форма получения образования	дневная
Курс	4
Семестр	7
Всего часов по учебной дисциплине	118
Аудиторных часов по учебной дисциплине	50
Лекции, часов	24
Лабораторные занятия, часов	26
Самостоятельная работа студентов, часов	68
Трудоемкость учебной дисциплины, зачет. Ед.	3
Форма текущей аттестации	экзамен

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

РАЗДЕЛ 1. ОБЩИЕ ПРИНЦИПЫ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ. ЭЛЛИПТИЧЕСКАЯ КРИПТОГРАФИЯ.

Тема 1.1. Предмет и основные разделы курса криптографические протоколы. Цели и свойства криптографических протоколов.

Лабораторное занятие 1. Линейный генератор случайных чисел.

Тема 1.2. Линейный генератор случайных чисел. Метки времени и случайные числа, используемые в криптографических протоколах.

Лабораторное занятие 2. Квадратичный генератор случайных чисел BBS.

Тема 1.3. Генератор случайных чисел BBS. Числа Блюма.

Лабораторное занятие 3. Группа точек эллиптической кривой.

Тема 1.4. Использование эллиптической криптографии в криптографических протоколах. Группа точек эллиптической кривой.

Лабораторное занятие 4. Эллиптическая криптография.

Тема 1.5. Основы эллиптической криптографии. Электронная подпись в эллиптической криптографии.

Лабораторное занятие 5. Алгоритм шифрования в эллиптической криптографии. Формулы сложения и формулы удвоения.

Тема 1.6. Групповое сложение эллиптических точек, операция сложения по группе, нейтральный элемент, симметрия точек (взаимно-обратные элементы в группе).

Лабораторное занятие 6. Алгоритм шифрования в эллиптической криптографии, образующий элемент группы, умножение точки на число. Роль открытого и закрытого ключей в эллиптическом коде.

Тема 1.7. Принцип уникальной алфавитной строки в эллиптической криптографии.

Лабораторное занятие 7. Принцип уникальной алфавитной строки в эллиптической криптографии.

РАЗДЕЛ 2. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. ОСНОВНЫЕ ТИПЫ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ

Тема 2.1. Криптографический протокол на базе общего секретного ключа. Упрощенная схема. Зеркальная атака. Способы предотвращения зеркальных атак.

Лабораторное занятие 8. Алгоритм шифрования – дешифрования Владимира Сизова над полем целочисленных остатков.

Тема 2.2. Аутентетификация на базе протокола HMAC. Атака посредине.

Лабораторное занятие 9. Использование бита четности в кодах криптографических протоколов. Протоколы обнаруживающие и протоколы исправляющие ошибку кратности к.

Тема 2.3. Протокол Диффи- Хеллмана.

Лабораторное занятие 10. Цифровая электронная подпись.

Тема 2.4. Аутентификация с помощью центра распределения ключей. Криптосистема без передачи ключей.

Лабораторное занятие 11. Протокол без передачи секретного ключа.

Тема 2.5. Аутентификационный протокол Недхема – Шредера. Криптосистема с открытым ключом.

Лабораторное занятие 12. Протокол на базе общего секретного ключа.

Тема 2.6. Протокол Отуэя-Риса. Протокол KERBEROS. Протокол на базе группового ключа из n-участников. Описание прямого и обратного алгоритмов.

Лабораторное занятие 13. Матричное кодирование.

Учебно-методическая карта дисциплины для студентов дневной формы получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	практические занятия	лабораторные занятия	управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	9
РАЗДЕЛ 1. ОБЩИЕ ПРИНЦИПЫ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ. ЭЛЛИПТИЧЕСКАЯ КРИПТОГРАФИЯ.							
Тема 1.1	*Лекция 1.* Предмет и основные разделы курса криптографические протоколы. Цели и свойства криптографических протоколов. *Лабораторное занятие 1.* Линейный генератор случайных чисел	2		2		[3,4], МУ	ЗЛ
Тема 1.2	*Лекция 2.* Линейный генератор случайных чисел. Метки времени и случайные числа, используемые в криптографических протоколах. *Лабораторное занятие 2.* Квадратичный генератор случайных чисел BBS.	2		2		[1,3,4],МУ	УО, ЗЛ
Тема 1.3	*Лекция 3.* Генератор случайных чисел BBS. Числа Блюма.	2		2		[1,3,4]	УО, ЗЛ

	Лабораторное занятие 3. Группа точек эллиптической кривой.						
Тема 1.4	*Лекция 4.* Области использования эллиптической криптографии в криптографических протоколах. Группа точек эллиптической кривой. *Лабораторное занятие 4.* Эллиптическая криптография.	2		2		[1,3,4], МУ	УО, ЗЛ
Тема 1.5	*Лекция 5.* Основы эллиптической криптографии. Электронная подпись в эллиптической криптографии. *Лабораторное занятие 5.* Алгоритм шифрования в эллиптической криптографии. Формулы сложения и формулы удвоения.	2		2		[1,3,4], МУ	УО, ЗЛ
Тема 1.6	*Лекция 6.* Групповое сложение эллиптических точек, операция сложения по группе, нейтральный элемент, симметрия точек (взаимно-обратные элементы в группе). *Лабораторное занятие 6.* Алгоритм шифрования в эллиптической криптографии, образующий элемент группы, умножение точки на число. Роль открытого и закрытого ключей в эллиптическом коде.	2		2		[1,3,4], МУ	УО, ЗЛ
Тема 1.7	*Лабораторное занятие 7.* Принцип уникальной алфавитной строки в эллиптической криптографии.			2		[1,3,4], МУ	УО, ЗЛ
РАЗДЕЛ 2. ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ. ОСНОВНЫЕ ТИПЫ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ							
Тема 2.1	*Лекция 7.* Криптографический протокол на базе общего секретного ключа. Упрощенная схема. Зеркальная атака. Способы предотвращения зеркальных атак. *Лабораторное занятие 8.* Алгоритм шифрования – дешифрования Владимира Сизова над полем целочисленных остатков.	2		2		[1,3,4], МУ	УО, ЗЛ
Тема 2.2	*Лекция 8.* Аутентетификация на базе протокола HMAC. Атака посредине. *Лабораторное занятие 9.* Использование бита четности в кодах криптографических протоколов. Протоколы обнаруживающие и протоколы исправляющие ошибку кратности к.	2		2		[1,4], МУ	УО, ЗЛ

Тема 2.3	*Лекция 9.* Протокол Диффи- Хеллмана. *Лабораторное занятие 10.* Цифровая электронная подпись.	2		2		[1,3], МУ	УО, ЗЛ
Тема 2.4	*Лекция 10.* Аутентификация с помощью центра распределения ключей. Криптосистема без передачи ключей. *Лабораторное занятие 11.* Протокол без передачи секретного ключа.	2		2		[1,5], МУ	УО, ЗЛ
Тема 2.5	*Лекция 11.* Аутентификационный протокол Недхема – Шредера. Криптосистема с открытым ключом. *Лабораторное занятие 12.* Протокол на базе общего секретного ключа.	2		2		[1,4], МУ	УО, ЗЛ
Тема 2.6	*Лекция 12.* Протокол Отуэя-Риса. Протокол KERBEROS. Протокол на базе группового ключа из n-участников. Описание прямого и обратного алгоритмов. *Лабораторное занятие 13.* Матричное кодирование.	2		2		[2,6], МУ	УО, ЗЛ
	Итого:	**24**		**26**			

МУ – методические указания для подготовки и к защите лабораторной работы;
УО- устный опрос;
ЗЛ- защита лабораторной работы.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Литература

Основная:

1. Голиков, А.М. Кодирование и шифрование информации в системах связи: курс лекций, компьютерый практикум, задание на самостоятельную работу [Электронный ресурс]: А.М. Голиков; Министерство образования и науки Российской Федерации. – Томск: ТУСУР, 2016. – Ч. 2. Шифрование. – 490 с.

2. Голиков, А.М. Основы проектирования защищенных телекоммуникационных систем; курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу [Электронный ресурс]: А.М. Голиков; Министерство образования и науки Российской Федерации. – Томск: ТУСУР, 2016. – 396 с.

3. Ищукова, Е.А. Криптографические протоколы и стандарты [Электронный ресурс]: учебное пособие / Е.А. Ищукова, Е.А. Лобова; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 80 с.

4. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с.

5. Пастухов, Д.Ф., Пастухов, Ю.Ф. Синица П.Р. Шифрование данных на базе эллиптических кривых [Электронный ресурс]: учебно-методическое пособие для студентов спец. 1-98 01 01 ПГУ, 2016, С.72. http//elib/psu.by:8080/ handle/ 123456789/16814.

Дополнительная:

6. Гультяева, Т.А. Основы защиты информации [Электронный ресурс]: учебное пособие: [16+] / Т.А. Гультяева; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2018. – 83 с.

7. Громов Ю.Ю. Программно-аппаратные средства защиты информационных систем: учебное пособие [Электронный ресурс]: Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 194 с

8. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / С.А. Нестеров; Министерство образования и науки Российской Федерации, Санкт-Петербургский

государственный политехнический университет. – Санкт-Петербург: Издательство Политехнического университета, 2014. – 322

9. Пастухов Д.Ф., Волосова Н.К., Пастухов Ю.Ф., Серый Т.А., Баталко И.И., Василевич В.В, Смоляк А.И. Алгебраические методы шифрования. [Электронный ресурс]: Учебно-методическое пособие для студентов спец. 1-98 01 01 ПГУ, Новополоцк: 2020.-17с. http//elib/psu.by:8080/handle/123456789/24430.

10. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс]: В.А. Сердюк; Национальный исследовательский университет – Высшая школа экономики. – Москва: Издательский дом Высшей школы экономики, 2015. – 574 с.

11. Спицын, В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие / В.Г. Спицын; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск: Эль Контент, 2011. – 148 с.

12. Трипкош, В.А. Электронная цифровая подпись в деятельности предприятий и организаций [Электронный ресурс]: учебное пособие / В.А. Трипкош, А.Г. Матвеев; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». – Оренбург: ОГУ, 2012. – 172 с.

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ РАБОТ

1. Линейный генератор случайных чисел.
2. Квадратичный генератор случайных чисел BBS.
3. Группа точек эллиптической кривой.
4. Эллиптическая криптография.
5. Алгоритм шифрования в эллиптической криптографии. Формулы сложения и формулы удвоения.
6. Алгоритм шифрования в эллиптической криптографии, образующий элемент группы, умножение точки на число. Роль открытого и закрытого ключей в эллиптическом коде.
7. Принцип уникальной алфавитной строки в эллиптической криптографии.
8. Алгоритм шифрования – дешифрования Владимира Сизова над полем целочисленных остатков.
9. Использование бита четности в кодах криптографических протоколов. Протоколы обнаруживающие и протоколы исправляющие ошибку кратности к.
10. Цифровая электронная подпись.
11. Протокол без передачи секретного ключа.
12. Протокол на базе общего секретного ключа.
13. Матричное кодирование.

ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Линейный генератор случайных чисел.
2. L-Z алгоритмы распаковки данных. Примеры.
3. Квадратичный генератор случайных чисел (Блюма).
4. Особенности программ – архиваторов.
5. Назначение криптографических протоколов, функции и свойства криптографического протокола
6. Сжатие информации с потерями.
7. Протокол на базе общего секретного ключа. Зеркальная атака. Способы предотвращения зеркальных атак.
8. Информационный канал.
9. Протокол HMAC.
10. Помехозащитное кодирование.
11. Протокол Диффи-Хеллмана. Атака посредине, способы защиты
12. Математическая модель системы связи.
13. Аутентификационный протокол с помощью центра распределения ключей
14. Матричное кодирование.
15. Криптографический протокол Недхема - Шредера.
16. Групповые коды.
17. Протокол Отуэя -Рисса.
18. Совершенные и квазисовершенные коды.
19. Протокол KERBEROS.

20. Совершенные и квазисовершенные коды.
21. Аутентификационный протокол с помощью открытого ключа.
22. Полиномиальные коды.
23. Эллиптические кривые, дискриминант кривой, связность кривой.
24. Понятие о кодах БЧХ.
25. Групповые свойства множества точек эллиптической кривой. Вывод формул сложения и удвоения.
26. Понятие о кодах БЧХ.
27. Криптосистема без передачи ключа. Теорема Эйлера – Ферма.
28. Циклические избыточные коды.
29. Электронная подпись. Применение электронной подписи в криптографических протоколах.
30. Основы теории защиты информации.
31. Криптосистема без передачи ключа.
32. Стандарт шифрования данных.
33. Адаптивные алгоритмы сжатия. Кодирование Хаффмана.
34. Криптосистема с открытым ключом.
35. Стандарт шифрования данных.
36. Электронная подпись.
37. Алгоритмы проверки и исправления ошибки при шифровании, метрика расстояния между словами по Хэммингу. Теоремы о минимальном расстоянии между словами для обнаружения и исправления ошибки кратности к. Бит четности, метка времени в протоколах.
38. Стандарт шифрования данных.
39. Криптосистема без передачи ключа. Теорема Эйлера – Ферма.
40. Применение последовательности Фибоначчи в информационном канале, емкость канала, скорость передачи информации.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

При изучении дисциплины студентами дневной формы получения образования используются следующие формы самостоятельной работы:

- углубленное изучение отдельных тем для подготовки к устным опросам;
- подготовка к защите отчетов по лабораторным работам;
- систематизация полученных знаний при подготовке к экзамену.

Содержание самостоятельной работы студентов дневной формы получения образования:

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
Углубленное изучение отдельных тем для подготовки к устным опросам на лекции	Тема 1.1 Литература: [1,3,4]	1
	Тема 1.2 Литература: [1,3,4]	1
	Тема 1.3 Литература: [1,3,4]	1
	Тема 1.4 Литература: [1,3,4]	1
	Тема 1.5 Литература: [1,4]	1
	Тема 1.6 Литература: [1,3]	1
	Тема 1.7 Литература: [1,5,7]	1
	Тема 2.1 Литература: [1,4]	1
	Тема 2.1 Литература: [2,4,6]	1
	Тема 2.3 Литература: [2,4,6]	1
	Тема 2.4 Литература: [2,6]	1
	Тема 2.5 Литература: [2,6]	1
	Тема 2.6 Литература: [2,4,6]	1
Подготовка к защите отчетов по лабораторным работам	Лабораторная работа № 1 [МУ]	1
	Лабораторная работа № 2 [МУ]	1
	Лабораторная работа № 3 [МУ]	1
	Лабораторная работа № 4 [МУ]	1
	Лабораторная работа № 5 [МУ]	1
	Лабораторная работа № 6 [МУ]	1
	Лабораторная работа № 7 [МУ]	1
	Лабораторная работа № 8 [МУ]	2
	Лабораторная работа № 9 [МУ]	2
	Лабораторная работа № 10 [МУ]	2
	Лабораторная работа № 11[МУ]	2
	Лабораторная работа № 12 [МУ]	2
	Лабораторная работа № 13 [МУ]	2
Систематизация полученных знаний при подготовке к экзамену		36
	Итого:	**68**

Перечень дополнительного информационного и учебно-методического обеспечения самостоятельной работы студентов, размещенного в Google ClassRoom университета:

1. Конспект лекций.
2. Методические указания к выполнению лабораторных работ.

СРЕДСТВА ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Диагностика результатов учебной деятельности осуществляется следующими средствами:

- устный опрос на занятии;
- письменный отчет по лабораторным работам с их устной защитой;
- письменный экзамен.

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в соответствии с Положением о рейтинговой системе оценки знаний и компетенций студентов (приказ ректора университета от 06.06.2014 № 294 (в редакции, утвержденной приказом ректора университета от 17.11.2014 № 605) в форме промежуточного контроля и текущей аттестации.

Результат промежуточного контроля за семестр оценивается отметкой в баллах по десятибалльной шкале и выводится, исходя из отметок, выставленных в ходе проведения мероприятий промежуточного контроля в течение семестра по следующей формуле:

$$П = \frac{YO_1 + ... + YO_{n_1} + ЗЛ_1 + ... + ЗЛ_{n_2}}{n_1 + n_2}$$

где $YO_1,...,YO_{n_1}$ – отметки, выставленные по результатам устных опросов на лекциях, - n_1 число устных опросов;

$ЗЛ_1,...,ЗЛ_{n_2}$ – отметки, выставленные по результатам устных защит отчетов по лабораторным работам, n_2 число лабораторных работ.

Итоговая экзаменационная отметка по дисциплине рассчитывается по формуле:

$$ИЭ = k \cdot П + (1 - k)O$$

где k– весовой коэффициент промежуточного контроля;

П – результат промежуточного контроля за семестр.

О – отметка, полученная студентом на экзамене за ответ по билету.

Весовой коэффициент принимается равным $k = 0.5$.

Результат итоговой экзаменационной оценки округляется до целого значения.

Информация о весовом коэффициенте доводится до студентов на первом занятии в семестре. Положительной является отметка не ниже 4 баллов.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Изучение дисциплины осуществляется на лекционных и лабораторных занятиях. На лекционных занятиях студенты овладевают системой теоретических знаний в области криптографических протоколов и современными алгоритмами теории чисел. В ходе лекционного изложения материала используются: проблемно-модульное изложение материала; использование видео-лекций и презентаций. Все математические утверждения, теоремы и свойства, указанные в учебно-методической карте дисциплины доказываются лектором на лекциях. Используются также интерактивные методы обучения.

На лабораторных занятиях развиваются и формируются необходимый практический опыт установления криптографических протоколов и протоколов аутентификации. Во время проведения лабораторных занятий особое внимание

уделяется формированию у студентов умения планировать работу, определять эффективную последовательность ее выполнения.