Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе
и менеджменту качества

_____ Е.Н. Живицкая
26.10.2016 г.

Регистрационный № УД-6-592/р

«Криптографическая защита информации»

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности
1-98 01 02 Защита информации в телекоммуникациях

Кафедра защиты информации

Всего часов по дисциплине 312

Зачетных единиц 8,5

2016 г.

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-98 01 02-2013 и учебного плана специальности 1-98 01 02 Защита информации в телекоммуникациях.

Составитель:
А.М. Тимофеев, доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент.

Рецензенты:
В.К. Конопелько, заведующий кафедрой сетей и устройств телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор;
Кафедра телекоммуникационных систем учреждения образования «Белорусская государственная академия связи» (протокол № 9 от «6» апреля 2016).

Рассмотрена и рекомендована к утверждению:
Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 13 от 31.03.2016 г.);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 1 от 21.10.2016 г.)

СОГЛАСОВАНО

Эксперт-нормоконтролер

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

План учебной дисциплины в дневной форме обучения:

Код специальности	Название специальности	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом уво)				Академ. часов на курс. работу (проект)	Типовой расчет	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары			
1-98 01 02	Защита информации в телекоммуникациях	4	7	48	32	16	–	-	-	зачет
		4	8	110	62	32	16	-	-	зачет

Место учебной дисциплины.

Актуальность изучения учебной дисциплины «Криптографическая защита информации» состоит в том, что использование криптографических преобразований информации является одним из основных инструментов для обеспечения ее защиты от несанкционированного доступа, поэтому при подготовке специалистов в области информационной безопасности представляется весьма важным изучение криптографических принципов защиты информации. Дисциплина «Криптографическая защита информации» является одной из дисциплин, составляющих основу общей подготовки специалистов по защите информации.

Цель преподавания учебной дисциплины: формирование базовых знаний по криптографии и криптоподобным преобразованиям, используемых для обеспечения защиты информации.

Задачи изучения учебной дисциплины:

- изучение технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации;
- получение знаний об аппаратных и аппаратно-программных устройствах, а также о программном обеспечении, предназначенных для обеспечения целостности (неизменности), конфиденциальности, доступности и сохранности защищаемых сведений и основанных на использовании криптографических преобразований передаваемой информации;
- изучение принципов построения и функционирования современных симметричных (одноключевых) и асимметричных (двухключевых) систем криптографической за-

щиты информации, а также криптосистем с депонированием ключа, удовлетворяющих требованиям действующих стандартов по информационной безопасности.

В результате изучения учебной дисциплины «Криптографическая защита информации» формируются следующие компетенции:

академические:

- уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;
- владеть исследовательскими навыками;
- уметь работать самостоятельно;
- быть способным порождать новые идеи (обладать креативностью);
- иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;
- использовать основные законы естественно-научных дисциплин в профессиональной деятельности;
- владеть основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;
- на научной основе организовывать свой труд, самостоятельно оценивать результаты своей деятельности;

социально-личностные:

- обладать способностью к межличностным коммуникациям;
- быть способным к критике и самокритике;
- уметь работать в команде;

профессиональные:

- эксплуатировать средства криптографической защиты информации;
- принимать и осваивать средства криптографической защиты информации;
- настраивать, испытывать и обслуживать аппаратно-программные средства криптографической защиты информации;
- совершенствовать, модернизировать и улучшать технико-экономические показатели средств криптографической защиты информации;
- контролировать качество функционирования систем криптографической защиты информации;
- анализировать научно-техническую информацию, отечественный и зарубежный опыт в области построения и функционирования систем криптографической защиты информации;
- собирать и анализировать исходные данные для проектирования систем и средств криптографической защиты информации;
- выполнять сравнительный технико-экономический анализ вариантов построения и практического применения систем криптографической защиты информации;
- применять методы анализа, синтеза и оптимизации структуры систем криптографической защиты информации;

- разрабатывать и использовать методы математического моделирования в процессе исследования и оптимизации параметров отдельных элементов и систем криптографической защиты информации в целом;
- анализировать и прогнозировать показатели качества функционирования и другие параметры систем криптографической защиты информации;
- владеть современными средствами криптографической защиты информации;
- оценивать конкурентоспособность и экономическую эффективность разрабатываемого и эксплуатируемого оборудования систем криптографической защиты информации.

В результате изучения учебной дисциплины студент должен:

знать:

- основные принципы построения современных симметричных (одноключевых) и асимметричных (двухключевых) систем криптографической защиты информации, а также криптосистем с депонированием ключа;
- особенности функционирования систем обработки документов, представленных в электронной форме, основанных на использовании электронной цифровой подписи;
- современные методы управления криптографическими ключами;

уметь:

- настраивать, испытывать и обслуживать аппаратные, аппаратно-программные и программные средства криптографической защиты информации;
- выполнять сопоставительный анализ вариантов построения и практического применения систем криптографической защиты информации;
- применять современные методы управления криптографическими ключами;

владеть:

- практическими навыками разработки систем криптографической защиты информации.

Перечень учебных дисциплин, усвоение которых необходимо для изучения данной учебной дисциплины.

№ п.п.	Название учебной дисциплины	Раздел, темы
1	Введение в информационную безопасность	Все разделы

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
1	2	3
Раздел 1. Основы защиты информации криптографическими методами		
1	Методология криптографической защиты информации	Криптографические системы связи с секретным и открытым ключом. Типы и особенности реализации криптоаналитических атак. Аппаратно-программные средства защиты компьютерной информации. Нормативно-правовая база Республики Беларусь в области криптографической защиты информации
2	Традиционные (классические) методы шифрования симметричных криптосистем	Шифры перестановки, простой и сложной замены. Шифрование методом гаммирования
Раздел 2. Симметричные алгоритмы и стандарты шифрования данных		
3	Американский стандарт шифрования данных DES	Схемы шифрования и расшифрования данных. Схема вычисления функции шифрования. Режимы работы и области применения алгоритма DES. Комбинирование блочных алгоритмов DES
4	Алгоритм шифрования данных IDEA	Схемы шифрования и расшифрования данных. Преимущества алгоритма IDEA перед алгоритмом DES
5	Стандарт шифрования данных ГОСТ 28147-89	Схемы шифрования и расшифрования в режимах простой замены, гаммирования, гаммирования с обратной связью и выработки имитовставки
6	Блочные и поточные шифры	Блочное и поточное шифрование и расшифрование данных. Блочное шифрование данных с обратной связью
7	Криптосистема с депонированием ключа на базе американского стандарта EES	Спецификации стандарта EES. Метод вычисления поля LEAF. Схемы зашиты телефонных переговоров и дешифрования перехваченных шифртекстов. Генерация и обслуживание ключей
Раздел 3. Асимметричные алгоритмы и стандарты шифрования данных		
8	Криптосистемы с открытым ключом	Особенности построения и безопасность асимметричных криптосистем. Однонаправленные функции шифрования на основе дискретного логарифмирования и факторизации больших чисел. Необратимые функции с «потайным ходом». Схемы применения однонаправленных функций шифрования для контроля целостности данных
9	Алгоритм шифрования данных RSA	Шифрование и расшифрование пользовательских данных. Надежность, безопасность и быстродействие криптосистемы RSA.

1	2	3
10	Криптографическая система Рабина	Этапы реализации, шифрование и расшифрование пользовательских данных. Надежность, безопасность и эффективность криптосистемы
11	Криптографическая система Полига-Хеллмана	Шифрование и расшифрование пользовательских данных. Надежность, безопасность и эффективность криптосистемы
12	Криптографическая система Эль Гамаля	Шифрование и расшифрование пользовательских данных. Надежность, безопасность и эффективность криптосистемы. Комбинированный метод шифрования и расшифрования
13	Алгебраические структуры	Группы и подгруппы. Циклические группы и подгруппы. Теорема Лагранжа о порядках групп и подгрупп. Кольца и поля
14	Алгебраические поля Галуа GF(2^n)	Алгебраические структуры полей Галуа для n-битовых слов. Криптографические операции на полиномах. Нахождение мультипликативной инверсии в поле Галуа GF (2^n) с использованием расширенного алгоритма Евклида. Эффективный алгоритм умножения полиномов в полях Галуа.
15	Криптосистемы на основе метода эллиптических кривых над конечными полями	Эллиптические кривые в вещественных числах и в поле Галуа GF (p). Шифрование и расшифрование пользовательских данных в криптографической системе Эль Гамаля на основе метода эллиптических кривых над конечным полем Галуа GF (p). Безопасность и эффективность криптосистемы на основе метода эллиптических кривых над конечным полем Галуа GF (p).
Раздел 4. Идентификация, проверка подлинности и авторизация объектов на основе криптографических операций		
16	Идентификация и аутентификация пользователей компьютерных систем	Идентификация, аутентификация, авторизация и методы защиты объектов. Типовые схемы идентификации и аутентификации пользователей. Особенности применения пароля для аутентификации пользователей. Биометрическая идентификация и аутентификация пользователей. Взаимная проверка подлинности пользователей компьютерных систем
17	Протокол идентификации с нулевой передачей знаний Фейге-Фиата-Шамира	Генерирование открытого и секретного ключей. Процедура аккредитации
18	Протокол параллельной идентификации с нулевой передачей знаний	Генерирование открытого и секретного ключей. Процедура аккредитации

1	2	3
19	Протокол идентификации с нулевой передачей знаний Гиллоу-Куискуотера	Генерирование открытого и секретного ключей. Процедура аккредитации
20	Электронная цифровая подпись	Формирование электронной цифровой подписи. Аутентификация автора документа и самого документа. Однонаправленные хэш-функции на основе симметричных алгоритмов шифрования блочного типа
21	Алгоритм электронной цифровой подписи RSA	Генерирование открытого и секретного ключей. Формирование электронной цифровой подписи и проверка с ее помощью подлинности сообщения
22	Алгоритм электронной цифровой подписи Эль Гамаля	Генерирование открытого и секретного ключей. Формирование электронной цифровой подписи и проверка с ее помощью подлинности сообщения
23	Алгоритм электронной цифровой подписи DSA	Генерирование открытого и секретного ключей. Формирование электронной цифровой подписи и проверка с ее помощью подлинности сообщения
24	Алгоритм электронной цифровой подписи ГОСТ Р 34.10-94	Генерирование открытого и секретного ключей. Формирование электронной цифровой подписи и проверка с ее помощью подлинности сообщения. Обеспечение конфиденциальности документа с электронной цифровой подписью
25	Электронные цифровые подписи с дополнительными функциональными свойствами	Схемы слепой и неоспоримой электронных цифровых подписей Д. Чома. Генерация и верификация электронной цифровой подписи с дополнительными функциональными свойствами
26	Аутентификация пользователей и программных кодов с применением паролей и цифровых сертификатов	Аутентификация пользователей с использованием одноразового и многоразового паролей и цифровых сертификатов. Первичная аутентификация пользователей в сертифицирующей организации. Классы цифровых сертификатов. Инфраструктура с открытыми ключами PKI. Аутентификация программных кодов на основе аутентикода

1	2	3
Раздел 5. Управление криптографическими ключами		
27	Генерация и хранение ключей	Схемы генерации и модификации ключей. Способы безопасного хранения ключей. Концепция иерархии ключей
28	Распределение ключей для симметричных и асимметричных криптосистем	Распределение ключей для симметричных и асимметричных криптосистем с применением соответственно центров распределения ключей и сертификатов открытых ключей. Система открытого распределения ключей Диффи-Хеллмана. Протокол управления криптоключами SKIP
29	Квантово-криптографические схемы распределения ключей	Элементная база систем квантовой криптографии. Схемы квантового распределения ключа с поляризационным кодированием на основе протокола BB84 и с фазовым кодированием на основе интерферометра Маха-Цендера. Схема высокоскоростного распределения ключа с использованием двух взаимно ортогональных состояний фотонов и спектрального уплотнения каналов

2. Информационно-методический раздел

2.1 Литература

2.1.1 Основная

2.1.1.1 Бабаш, А.В. Криптография / А.В. Бабаш, Г.П. Шангин; под ред. А.П. Шерстюка и Э.А. Применко. – М.: СОЛОН-ПРЕСС, 2007. – 512 с.

2.1.1.2 Мельников, В.П. Информационная безопасность и защита информации: учебное пособие для студентов вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 3-е изд. – М.: Издательский центр «Академия», 2008. – 336 с.

2.1.1.3 Стохастические методы и средства защиты информации в компьютерных системах и сетях / М.А. Иванов [и др.]. - М.: Кудиц-пресс, 2009. – 512с.

2.1.1.4 Голиков, В.Ф. Безопасность информации и надежность компьютерных систем: учебное пособие в 2 ч. / В.Ф. Голиков. – Минск: БНТУ, 2010. – Ч. 1. – 86 с.

2.1.1.5 Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов [и др.]. - СПб.: Лань, 2011. - 400 с.

2.1.2 Дополнительная

2.1.2.1 Завгородний, В.И. Комплексная защита информации в компьютерных системах: учебное пособие / В.И. Завгородний. – М.: Логос, 2001. - 264 с.

2.1.2.2 Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. – 2-е изд. – М.: Радио и связь, 2001. – 376 с.

2.1.2.3 Смарт, Н. Криптография / Н. Смарт. – М.: Техносфера, 2005. – 528 с.

2.1.2.4 Ярочкин, В.И. Информационная безопасность: учебник для вузов / В.И. Ярочкин. – М.: Академический Проспект: Трикста, 2005. – 544 с.

2.1.2.5 Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик [и др.]; под ред. Н.И. Синадского. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для выполнения лабораторных работ

2.2.1 Компьютерные программы для проведения лабораторных работ

2.2.1.1 Стандарт шифрования данных ГОСТ 28147-89 в режиме простой замены.

2.2.1.2 Стандарт шифрования данных ГОСТ 28147-89 в режиме гаммирования.

2.2.1.3 Стандарт шифрования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью.

2.2.1.4 Стандарт шифрования данных DES.

2.2.1.5 LospCryptoLab

2.2.1.6 Алгоритм шифрования данных RSA

2.2.1.7 Криптографическая система Рабина

2.2.1.8 Схема шифрования Эль Гамаля

2.2.1.9 Протокол Фейге-Фиата-Шамира

2.2.1.10 Протокол идентификации с нулевой передачей знаний

2.2.1.11 Протокол идентификации Гиллоу-Куискуотера

2.2.1.12 Алгоритм электронной цифровой подписи RSA

2.2.1.13 Алгоритм электронной цифровой подписи DSA

2.2.2 Методические указания для проведения лабораторных работ

2.2.2.1 Голиков, В.Ф. Криптографическое кодирование информации: методические указания к лабораторным работам / В.Ф. Голиков, А.В. Курилович. – Мн.: БГУИР, 2002. – 24 с.

2.2.2.2 Голиков, В.Ф. Безопасность информации и надежность компьютерных систем: учебное пособие в 2 ч. / В.Ф. Голиков. – Минск: БНТУ, 2010. – Ч. 1. – 86 с.

2.2.2.3 Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик [и др.]; под ред. Н.И. Синадского. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

2.2.3 Оборудование для проведения лабораторных работ

2.2.3.1 Персональные компьютеры

2.2.3.2 Аппаратно-программный комплекс «КриптоЛаб»

2.3 Перечень тем практических занятий, их название

Целью практических занятий является закрепление теоретического курса, приобретение навыков решения задач, активизация самостоятельной работы студентов.

№ темы по п.1	Название практического занятия	Содержание	Обеспеченность по пункту 2.2
1	2	3	4
9	Изучение основных используемых в криптографии арифметических операций	Бинарные операции в криптографии. Операция деления в арифметике целых чисел. Нахождение наибольшего общего делителя двух положительных целых чисел с использованием алгоритма Евклида. Применение расширенного алгоритма Евклида для решения линейных диофантовых уравнений	2.2.2.2, 2.2.2.3
10	Оператор сравнения в модульной арифметике	Оператор по модулю n и система наименьших вычетов Zn. Оператор сравнения и система вычетов. Линейные уравнения с оператором сравнения	2.2.2.2, 2.2.2.3
13	Оператор инверсии в модульной арифметике	Аддитивная и мультипликативная инверсии. Нахождение мультипликативной инверсии с использованием расширенного алгоритма Евклида. Сложение и умножение таблиц в отображении Zn	2.2.2.2, 2.2.2.3
15	Криптографические операции с матрицами вычетов	Использование матриц в модульной арифметике. Операции и уравнения для матриц. Аддитивная и мультипликативная инверсии матриц. Матрицы вычетов и сравнимые матрицы по модулю n	2.2.2.2, 2.2.2.3
16	Простые числа в модульной арифметике	Испытание простоты чисел. Phi-функция Эйлера $\varphi(n)$. Применения теорем Ферма и Эйлера в криптографии. Китайская теорема об остатках	2.2.2.2, 2.2.2.3
17	Квадратичное сравнение в модульной арифметике	Решения квадратичных сравнений по простому и по составному модулям. Квадратичные вычеты и невычеты по модулю p	2.2.2.2, 2.2.2.3

2.4 Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

№ темы по п.1	Наименование лабораторной работы	Содержание	Обеспеченность по пункту 2.2
1	2	3	4
3	Стандарт шифрования данных DES	Изучение обобщенной схемы алгоритма, реализации функции шифрования и алгоритма вычисления ключей	2.2.1.4, 2.2.2.2, 2.2.3.1
5	Стандарт шифрования данных ГОСТ 28147-89 в режиме простой замены	Изучение схем шифрования и расшифрования данных в режиме простой замены	2.2.1.1, 2.2.1.5, 2.2.2.1, 2.2.3.1, 2.2.3.2
5	Стандарт шифрования данных ГОСТ 28147-89 в режиме гаммирования	Изучение схем шифрования и расшифрования данных в режиме гаммирования	2.2.1.2, 2.2.1.5, 2.2.2.1, 2.2.3.1, 2.2.3.2
5	Стандарт шифрования данных ГОСТ 28147-89 в режиме гаммирования с обратной связью	Изучение схем шифрования и расшифрования данных в режиме гаммирования с обратной связью	2.2.1.3, 2.2.1.5, 2.2.2.1, 2.2.3.1, 2.2.3.2
9	Алгоритм шифрования данных RSA	Изучение схем шифрования и расшифрования данных	2.2.1.6, 2.2.2.3, 2.2.3.1, 2.2.3.1
10	Криптографическая система Рабина	Изучение схем шифрования и расшифрования данных	2.2.1.7, 2.2.3.1
12	Криптографическая система Эль Гамаля	Изучение схем шифрования и расшифрования данных	2.2.1.8, 2.2.3.1
17	Протокол Фейге-Фиата-Шамира	Изучение процедур генерирования открытого и секретного ключей и аккредитации	2.2.1.9, 2.2.3.1
18	Протокол параллельной идентификации с нулевой передачей знаний	Изучение процедур генерирования открытого и секретного ключей и аккредитации	2.2.1.10, 2.2.3.1
19	Протокол идентификации Гиллоу-Куискуотера	Изучение процедур генерирования открытого и секретного ключей и аккредитации	2.2.1.11, 2.2.3.1
21	Алгоритм электронной цифровой подписи RSA	Изучение принципов формирования электронной цифровой подписи и проверки с ее помощью подлинности сообщения	2.2.1.12, 2.2.3.1
23	Алгоритм электронной цифровой подписи DSA	Изучение принципов формирования электронной цифровой подписи и проверки с ее помощью подлинности сообщения	2.2.1.13, 2.2.3.1

3.1 Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
1	2	3	4	5	6	7
	Семестр 7					
	Раздел 1. Основы защиты информации криптографическими методами	**10**			**20**	
1	Методология криптографической защиты информации	4			10	текущий опрос
2	Традиционные (классические) методы шифрования симметричных криптосистем	6			10	текущий опрос, доклады
	Раздел 2. Симметричные алгоритмы и стандарты шифрования данных	**22**	**16**		**28**	
3	Американский стандарт шифрования данных DES	4	4		5	оценивание на основе деловой игры, отчет по лаб. зан.
4	Алгоритм шифрования данных IDEA	4			5	текущий опрос
5	Стандарт шифрования данных ГОСТ 28147-89	6	12		5	текущий опрос, отчет по лаб. зан.
6	Блочные и поточные шифры	2			5	текущий опрос
7	Криптосистема с депонированием ключа на базе американского стандарта EES	6			8	контрольный опрос
	Текущая аттестация					зачет
	Итого в 7 семестре	**32**	**16**		**48**	
	Семестр 8					
	Раздел 3. Асимметричные алгоритмы и стандарты шифрования данных	**22**	**12**	**10**	**36**	
8	Криптосистемы с открытым ключом	2			4	текущий опрос
9	Алгоритм шифрования данных RSA	2	4	4	4	отчет по лаб. зан.
10	Криптографическая система Рабина	2	4	2	4	отчет по лаб. зан., доклады

1	2	3	4	5	6	7
11	Криптографическая система Полига-Хеллмана	2			4	доклады
12	Криптографическая система Эль Гамаля	2	4		4	доклады
13	Алгебраические структуры	4		2	4	доклады
14	Алгебраические поля Галуа $GF(2^n)$	4			4	текущий опрос
15	Криптосистемы на основе метода эллиптических кривых над конечными полями	4		2	8	текущий опрос, доклады
	Раздел 4. Идентификация, проверка подлинности и авторизация объектов на основе криптографических операций	**28**	**20**	**6**	**48**	
16	Идентификация и аутентификация пользователей компьютерных систем	4		2	4	текущий опрос
17	Протокол идентификации с нулевой передачей знаний Фейге-Фиата-Шамира	2	4	4	4	отчет по лаб. зан.
18	Протокол параллельной идентификации с нулевой передачей знаний	2	4		4	отчет по лаб. зан.
19	Протокол идентификации с нулевой передачей знаний Гиллоу-Куискуотера	2	4		4	отчет по лаб. зан.
20	Электронная цифровая подпись	2			4	доклады
21	Алгоритм электронной цифровой подписи RSA	2	4		4	отчет по лаб. зан.
22	Алгоритм электронной цифровой подписи Эль Гамаля	2			4	доклады
23	Алгоритм электронной цифровой подписи DSA	2	4		4	отчет по лаб. зан.
24	Алгоритм электронной цифровой подписи ГОСТ Р 34.10-94	4			4	текущий опрос
25	Электронные цифровые подписи с дополнительными функциональными свойствами	2			4	текущий опрос, доклады
26	Аутентификация пользователей и программных кодов с применением паролей и цифровых сертификатов	4			8	текущий опрос, доклады
	Раздел 5. Управление криптографическими ключами	**12**			**22**	
27	Генерация и хранение ключей	4			6	текущий опрос
28	Распределение ключей для симметричных и асимметричных криптосистем	4			6	текущий опрос
29	Квантово-криптографические схемы распределения ключей	4			10	контрольный опрос
	Текущая аттестация					зачет
	Итого в 8 семестре	**62**	**32**	**16**	**106**	
	Всего по учебной дисциплине	**94**	**48**	**16**	**154**	

4. Рейтинг-план

Рейтинг-план учебной дисциплины
«Криптографическая защита информации»
Специальность 1-98 01 02 Защита информации в телекоммуникациях
курс 4, семестр 7
Количество часов по учебному плану 96, в т.ч. аудиторная работа 48, самостоятельная работа 48.
Преподаватель: А.М. Тимофеев, кандидат технических наук, доцент
Кафедра защиты информации

Рекомендовано на заседании кафедры защиты информации
Протокол № 13 от «31» марта 2016 г.

Зав. кафедрой ЗИ Л.М. Лыньков

Преподаватель А.М. Тимофеев

Выставление отметки по текущей аттестации допускается по результатам итогового рейтинга студента

Виды учебной деятельности студентов	Модуль 1 (весовой коэффициент 1/2)		Модуль 2 (весовой коэффициент 1/2)		Итоговый рейтинг
	календарный срок сдачи	весовой коэффициент отметки	календарный срок сдачи	весовой коэффициент отметки	
1	2	3	4	5	6
1. Лекционные занятия	15.10	3/5	15.12	4/6	
Темы 1-3	15.10	3/5			
Темы 4-7			15.12	4/6	
2. Лабораторные работы	15.10	2/5	15.12	2/6	
№ 1, 2	15.10	2/5			
№ 3, 4			15.12	2/6	
Модульный контроль		МР1		МР2	ИР

Рейтинг-план учебной дисциплины
«Криптографическая защита информации»
Специальность 1-98 01 02 Защита информации в телекоммуникациях
курс 4, семестр 8
Количество часов по учебному плану 216, в т.ч. аудиторная работа 110, самостоятельная работа 106.
Преподаватель: А.М. Тимофеев, кандидат технических наук, доцент
Кафедра защиты информации

Рекомендовано на заседании кафедры защиты информации
Протокол № 13 от «31» марта 2016 г.
Зав. кафедрой ЗИ Л.М. Лыньков
Преподаватель А.М. Тимофеев

Выставление отметки по текущей аттестации допускается по результатам итогового рейтинга студента

Виды учебной деятельности студентов	Модуль 1 (весовой коэффициент 1/2)		Модуль 2 (весовой коэффициент 1/2)		Итоговый рейтинг
	календарный срок сдачи	весовой коэффициент отметки	календарный срок сдачи	весовой коэффициент отметки	
1	2	3	4	5	6
1. Лекционные занятия	10.02	8/15	10.03	14/21	
Темы 8-15	10.02	8/15			
Темы 16-29			10.03	14/21	
2. Лабораторные работы	10.02	4/15	10.03	4/21	
№ 5-8	10.02	4/15			
№ 9-12			10.03	4/21	
3. Практические (семинарские) занятия	10.02	3/15	10.03	3/21	
№ 1-3	10.02	3/15			
№ 4-6			10.03	3/21	
Модульный контроль		МР1		МР2	ИР

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Код и наименование специальности	Выпускающая кафедра	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Подпись заведующего выпускающей кафедрой с указанием номера протокола и даты заседания кафедры
1	2	3	4
1-98 01 02 Защита информации в телекоммуникациях	Кафедра защиты информации	изменения не требуются	_____Л.М.Лыньков протокол № 13 от 31.03.2016 г.

Заведующий кафедрой
защиты информации _____ Л.М. Лыньков