МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ,
МИНИСТЕРСТВО НАУКИ, ВЫСШЕГО ОБРАЗОВАНИЯ И ИННОВАЦИЙ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ

МОО ВО Кыргызско-Российский Славянский университет
имени первого Президента Российской Федерации Б.Н. Ельцина



УТВЕРЖДАЮ

директор Политехнического института

_____ Г.В.Лоцев

_____ 3 сентября 2026 г.

Кодирование и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Высшая школа Цифровых технологий**

Учебный план b010302_26_1 пмии.plx
Направление 01.03.02 - РФ, 510200 - КР Прикладная математика и информатика

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 50
самостоятельная работа 57,9

Виды контроля в семестрах:
зачет с оценкой 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	34	34	34	34
Контактная работа в период теоретического обучения	0,1	0,1	0,1	0,1
Итого ауд.	50	50	50	50
Контактная работа	50,1	50,1	50,1	50,1
Сам. работа	57,9	57,9	57,9	57,9
Итого	108	108	108	108

Программу составил(и):
ст.преп., Шаршекеев У.Ж. _____

Рецензент(ы):
к.т.н., доцент, Хмелева И.В. _____

Согласовано РОП: _____ *Доулбекова С. Б.*

Рабочая программа дисциплины
Кодирование и защита информации

разработана в соответствии с ФГОС 3++:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление 01.03.02 - РФ, 510200 - КР Прикладная математика и информатика

утвержденного учёным советом вуза от 26.06.2026 протокол № 11.

Рабочая программа одобрена на заседании _*Высшей школы цифровых технологий*_

Протокол от 02.09.2026 г. № 1
Срок действия программы: 2026-2030 уч.г. Руководитель подразделения: к.т.н., доцент, Хмелева И.В.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
к рабочей программе дисциплины (модуля)

Кодирование и защита информации

наименование дисциплины

№ п/п	Основание внесения изменения	Раздел/ пункт	Содержание изменения
1.			
2.			
3.			
4.			
5.			

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью освоения дисциплины «Кодирование и защита информации» является формирование у обучающихся теоретических знаний и практических навыков в области кодирования, криптографической и программно-технической защиты информации, изучение современных симметричных и асимметричных криптографических алгоритмов, хэш-функций, электронной подписи, инфраструктуры открытых ключей, методов аутентификации, управления криптографическими ключами и обеспечения конфиденциальности, целостности и подлинности данных в современных информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.1
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Численные методы
2.1.2	Дискретная математика
2.1.3	Спец курс (MATLAB)
2.1.4	Математический анализ
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-3: Способен разрабатывать требования и осуществлять проектирования программного обеспечения, баз данных и программных интерфейсов	
Знать:	
Уровень 1	основные понятия информационной безопасности и криптографии; виды угроз; принципы конфиденциальности, целостности и доступности информации; основные методы кодирования и защиты данных.
Уровень 2	основные понятия информационной безопасности и криптографии; виды угроз; принципы конфиденциальности, целостности и доступности информации; основные методы кодирования и защиты данных.
Уровень 3	принципы работы симметричных и асимметричных криптографических алгоритмов; хэш-функций; кодов аутентификации сообщений; электронной подписи; протоколов обмена ключами.
Уметь:	
Уровень 1	принципы построения защищенных программных и информационных систем; методы управления криптографическими ключами; PKI; современные протоколы защиты информации; методы безопасного хранения и передачи конфиденциальных данных.
Уровень 2	программно реализовывать и исследовать криптографические алгоритмы; применять современные криптографические библиотеки; создавать и проверять электронную подпись.
Уровень 3	программно реализовывать и исследовать криптографические алгоритмы; применять современные криптографические библиотеки; создавать и проверять электронную подпись.
Владеть:	
Уровень 1	навыками использования программных средств шифрования и хэширования информации.
Уровень 2	навыками применения симметричной и асимметричной криптографии, электронной подписи и механизмов аутентификации.
Уровень 3	навыками проектирования и программной реализации механизмов защиты информации, управления ключами, безопасного хранения учетных данных и применения криптографических протоколов.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов, основы инфраструктуры систем, построенных с использованием публичных и секретных ключей;
3.2	**Уметь:**
3.2.1	применять известные методы и средства поддержки информационной безопасности в компьютерных системах, проводить сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах;
3.3	**Владеть:**

3.3.1	применения методов и средств защиты информации и управления правами использования информационных ресурсов при передаче конфиденциальной информации по каналам связи, установлении подлинности передаваемых сообщений, хранении информации (документов, баз данных), встраивании скрытой служебной информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Пр. подг.	Примечание
	Раздел 1. Симметричные алгоритмы							
1.1	Основные понятия и определения информацией /Лек/	8	2	ПК-3	Л1.1 Л1.2 Л1.4Л2.2 Э1			
1.2	Подстановки. Перестановки /Пр/	8	4	ПК-3	Л1.1 Л1.3Л2.2 Э1			
1.3	Сеть Фейстеля /Ср/	8	7,5	ПК-3	Л1.4Л2.3 Э1			
1.4	Стандарт шифрования DES. /Лек/	8	2	ПК-3	Л1.5Л2.4 Э1			активное групповое обсуждение
1.5	Стандарт шифрования DES. /Пр/	8	4	ПК-3	Л1.2Л2.1 Л2.5 Э1			
1.6	Стандарт шифрования DES. /Ср/	8	7,5	ПК-3	Л1.2Л2.1 Л2.5			
1.7	Стандарт шифрования данных ГОСТ 28147-89. /Лек/	8	2	ПК-3	Л1.2 Л1.3Л2.2 Л2.4 Э1			активное групповое обсуждение
1.8	Стандарт шифрования данных ГОСТ 28147-89. /Пр/	8	6	ПК-3	Л1.3Л2.1 Э1			
1.9	Стандарт шифрования данных ГОСТ 28147-89. /Ср/	8	6,4	ПК-3	Л1.3Л2.1			
1.10	Стандарт шифрования данных AES. /Лек/	8	2	ПК-3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1			
1.11	AES. /Пр/	8	4	ПК-3	Л1.2 Л1.4Л2.2 Л2.3 Л2.4 Э1			активное групповое обсуждение
1.12	Конкурс AES /Ср/	8	6,5	ПК-3	Л1.2 Л1.5Л2.2 Л2.3 Л2.4 Э1			
1.13	/КрТО/	8	0,1	ПК-3	Л1.1 Л1.5Л2.2 Л2.3 Л2.4			
	Раздел 2. Асимметричные алгоритмы							
2.1	Алгоритм Диффи-Хеллмана. Протоколы обмена ключами /Лек/	8	2	ПК-3	Л1.1 Л1.2 Л1.5Л2.1 Л2.3 Л2.5 Э1			
2.2	Алгоритм Диффи-Хеллмана. Протоколы обмена ключами /Пр/	8	4	ПК-3	Л1.2 Л1.3Л2.1 Л2.3 Л2.5 Э1			
2.3	риптоанализ алгоритма Диффи -Хеллмана. /Ср/	8	9,5	ПК-3	Л1.2 Л1.3 Л1.5Л2.1 Л2.2 Л2.3 Э1			

2.4	Системы с открытым ключом. Алгоритм шифрования RSA /Лек/	8	2	ПК-3	Л1.2 Л1.3 Л1.4Л2.3 Л2.4 Л2.5 Э1			
2.5	Криптосистема Эль-Гамаля. Вычислительные аспекты реализации алгоритма RSA. /Пр/	8	4	ПК-3	Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Э1			тестирование на криптостойкость
2.6	Вопросы стойкости. Криптосистемы на основе эллиптических уравнений. /Ср/	8	9,5	ПК-3	Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Э1			
	Раздел 3. Цифровая подпись							
3.1	Проблема аутентификации данных и электронная цифровая подпись /Лек/	8	4	ПК-3	Л1.3Л2.2 Л2.4 Э1			
3.2	Проблема аутентификации данных и электронная цифровая подпись /Пр/	8	2	ПК-3	Л1.3Л2.2 Л2.4 Э1			активное групповое обсуждение
3.3	Проблема аутентификации данных и электронная цифровая подпись /Ср/	8	11	ПК-3	Л1.3Л2.2 Л2.4			
3.4	Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. /Пр/	8	2	ПК-3	Л1.3Л2.2 Л2.4 Э1			
3.5	Электронная подпись на основе алгоритма RSA. Алгоритм цифровой подписи Эль-Гамаля (EGSA) /Пр/	8	2	ПК-3	Л1.3Л2.1 Л2.2 Л2.4 Э1			
3.6	Алгоритм цифровой подписи DSA. /Пр/	8	2	ПК-3	Л1.3Л2.1 Л2.2 Л2.4 Э1			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Перечень вопросов к экзамену

Знать:

1. Криптография. Основные разделы современной криптографии.
2. Схемы шифрования и дешифрования. Ключ. Типы криптосистем.
3. Гаммирование.
4. Структура сети Фейстеля.
5. Схема алгоритма DES.
6. DES. Функция шифрования.
7. DES. Функция сжатия.
8. DES. Функция расширения.
9. DES. Генерация ключа.
10. Схема шифрования алгоритма ГОСТ 28147-89.
11. ГОСТ 28147-89.Режим шифрования ключевой информации.
12. ГОСТ 28147-89. Режим гаммирования.
13. ГОСТ 28147-89. Режим гаммирования с обратной связью.
14. ГОСТ 28147-89. Иммитовставка.
15. Условия конкурса алгоритма AES. Победители конкурса.
16. Стандарт AES. Алгоритм Rijndal. Схема.
17. AES. Преобразование ByteSub.
18. AES. Преобразование ShiftRow.
19. AES. Преобразование MixColumn.
20. AES. Преобразование AddRoundKey. Последняя итерация.
21. AES. Алгоритм обработки ключа.
22. Ассиметричные криптосистемы.
23. Криптосистема Эль-Гамаля.
24. Криптосистема Деффи-Хеллмана.
25. Проверка числа на простоту. Тест Ферма

Уметь и владеть:
1. Используя алгоритм Деффи-Хеллмана вычислить ключ, при q=5, p =13.

2. S1=(AS0+C)(modM)
…
SL=(ASL-1+C)(modM)
Где A=1, C =3, S0= 7, M-=256.
Зашифровать открытый текст «EF» (числа в шестнадцатеричной системе счисления) методом гаммирования

3. S1=(AS0+C)(modM)
…
SL=(ASL-1+C)(modM)

Где A=3, C =7, S0= 7, M-=256.
Зашифровать открытый текст «FC» (числа в шестнадцатеричной системе счисления) методом гаммирования

4. S1=(AS0+C)(modM)
…
SL=(ASL-1+C)(modM)

Где A=1, C =5, S0= 11, M-=256.
Зашифровать открытый текст «EA» (числа в шестнадцатеричной системе счисления) методом гаммирования

5. S1=(AS0+C)(modM)
…
SL=(ASL-1+C)(modM)
Где A=5, C =3, S0= 7, M-=256.
Зашифровать открытый текст «7C» (числа в шестнадцатеричной системе счисления) методом гаммирования

6. S1=(AS0+C)(modM)
…
SL=(ASL-1+C)(modM)
Где A=4, C =3, S0= 13, M-=256.
Зашифровать открытый текст «9F» (числа в шестнадцатеричной системе счисления) методом гаммирования.

7. Применяя Тест Ферма проверить число n =12 на простоту, t=3. В ответе: вывод, вероятность ошибки
8. Применяя Тест Ферма проверить число n =13 на простоту, t=3. В ответе: вывод, вероятность ошибки
9. Применяя Тест Ферма проверить число n =11 на простоту, t=3. В ответе: вывод, вероятность ошибки
10. Применяя Тест Ферма проверить число n =9 на простоту, t=3. В ответе: вывод, вероятность ошибки
11. Применяя Тест Ферма проверить число n =14 на простоту, t=3. В ответе: вывод, вероятность ошибки
12. Применяя функцию сжатия DES преобразовать число «FFAE»
13. Применяя функцию расширения DES преобразовать число «FFAE»

пример:
«КОДИРОВАНИЕ И ЗАЩИТА ИНФОРМАЦИИ»

Факультет: Естественно-технический.
Специальность: Прикладная математика и Информатика.

Экзаменационный билет №1
Знать:
1. Криптография. Основные разделы современной криптографии.
2. ГОСТ 28147-89. Иммитовставка.
Уметь и владеть:
3. Используя алгоритм Деффи-Хеллмана вычислить ключ, при q=5, p =13.

5.2. Темы курсовых работ (проектов)

не предусмотрены

5.3. Фонд оценочных средств

Вопросы с собеседованию по теме "Симметричные алгоритмы":
1. Криптография. Основные разделы современной криптографии.
2. Схемы шифрования и дешифрования. Ключ. Типы криптосистем.
3. Требования к криптосистемам.

4. Криптоанализ. Уровни атак. Криптостойкость.
5. Классы симметричных криптосистем.
6. Блочные шрифты. Перестановки.
7. Системы подстановок.
8. Подстановка Цезаря.
9. Многоалфавитные подстановки.
10. Гаммирование.
11. Структура итерации сети Фейстеля.
12. Схема алгоритма DES.
13. DES. Функция сжатия.
14. DES. Функция расширения.
15. DES. Генерация ключа.
16. Схема шифрования алгоритма ГОСТ 28147-89.
17. ГОСТ 28147-89.Режим шифрования ключевой информации.
18. ГОСТ 28147-89. Режим гаммирования.
19. ГОСТ 28147-89. Режим гаммирования с обратной связью.
20. Стандарт AES. Алгоритм Rijndal. Схема.
21. AES. Преобразование ByteSub.
22. AES. Преобразование ShiftRow.
23. AES. Преобразование MixColumn.
24. AES. Преобразование AddRoundKey. Последняя итерация.
25. AES. Алгоритм обработки ключа.

Вопросы с собеседованию по теме "Асимметричные алгоритмы":
1. Ассиметричные криптосистемы.
2. Криптосистема Эль-Гамаля.
3. Криптосистема RSA.
4. Цифровые подписи.
5. Функция хеширования MD5.
6. Функция Хэширования ГОСТ Р 34.11.

Темы рефератов:
Блочные шифры
Blowfish
Создатель - автор наиболее популярной книги по криптографии "Applied Cryptography", Bruse Schneier. Длинна ключа 32 -448 бит. Длинна обрабатываемых блоков - 64 бит. Число раундов - 16. Считается одним из наиболее сильных криптоалгоритмов. Для выработки ключей используется 521 цикл шифрования, что значительно затрудняет атаку приямым перебором. Эта же особенность делает затруднительной и возможность применения алгоритма в системах, где ключи меняются очень часто.
CAST
Авторы - Carlisle Adams и Stafford Taveres. Алгоритм очень похож на Blowfish. Длинна ключа 40...64 бит. Количество проходов 8. Известна related key атака на 64-битный CAST, открытая David Wagner, John Kelsey, и Bruce Schneier. Других атак кроме прямого перебора нет. Вариант алгоритма CAST-256 был выставлен на конкурс AES, но до финала не дошел. Запатенотован, но (!) открыт для свободного использования.
CMEA
Алгоритм, который используется в сотовых телефонах для шифрования служебных каналов. Был взломан by David Wagner, John Kelsey, and Bruce Schneier of Counterpane Systems.
CRYPTON
DEAL
Интересный алгоритм, который был предложен на конкурс AES. Оперирует 128-битовыми блоками данных и ключами длинной 128, 192 и 256 бит. Использует DES во внутренних итерациях. Для обеспечения сносной криптостойкости требуется не менее 8 итераций. Существуют атаки, которые успешно вскрывают шифр, если количество итераций меньше указанного значения.
ECC
Несимметричный криптоалгоритм на основе эллиптических кривых. Более быстр и стоек чем RSA, алгоритм Диффи-Хеллмана или DSA.
FEAL
Крайне ненадежный криптоалгоритм. Взломан! Разработан by the Nippon Telephone & Telegraph более быстрая, но менее надежная альтернатива DES. Известно множество атак, каждая из которых требует минимума информации.
FROG
Goatboy's Encryption Algorithm
Неплохой алгоритм, но его название служит ему плохую службу. (GoatBoy's - козлиный)
IDEA
International Decryption-Encryption Algorithm - разработанный в Щвейцарии (Цюрих) считается очень стойким криптоалгоритмом, хотя полной проверки еще не прошел. Авторы: Xuejia Lai, James Massey.Размер блока данных 64 бит. Длинна ключа 128 бит. Число раундов - 8. Оперирует 16-битовыми подблоками. Оптимизирован для 16-битных процессоров. Запатентован в США, Европе и Японии. Свободен для некоммерческого применения. В остальных случаях необходима лицензия компании Аском (владелец патента)

LOKI 89/91/97
MAGENTA
MARS
Новый симметричный блочный алгоритм от создателей DES. Один из 5ти финалистов AES. Разработан исследователями фирмы IBM. Оперирует 128-битовыми блоками. Длинна ключа переменная. Скорость работы - 65 Мбит/с на Pentium Pro 200 и 85 Мбит на 200MHz Power PC. Есть аппаратные реализации данного алгоритма.
RC2
Блочный шифр разработанный Роном Ривестом для RSA Data Security. Криптостойкость считается очень высокой. Размер блока 64 бит. Длинна ключа переменная. Скорость работы примерно вдвое быстрее чем DES. Является собственностью RSA Data Security.
RC5
Мощный и быстрый блочный симметричный криптоалгоритм разработанный Ривестом для RSA Data Security. Оперирует блоками данных длинной 32, 64 или 128 бит. Длинна ключа переменна. Количество проходов 0...255. Длинна ключа 0...2048 бит. Скорость алгоритма обусловлена применением только трех простых и быстрых операций - сложения, XOR и чередования (rotation). Был объявлен конкурс на взлом этого алгоритма. За три года были взломаны только слабо зашифрованные тексты (с малыми длинной ключа и количеством проходов). Собственность RSA Data Security.
RC6
Safer
Safer+
Serpent
128 битный алгоритм designed by Ross Anderson, Eli Biham and Lars Knudsen. Скорость в 5 раз быстрее DES.
Skipjack
Разработка АНБ США. До недавнего времени был секретным. Достаточно стоек. Размер блока 64 бит. Длина ключа 80 бит. 32 нелинейных комплексных раунда. Создан чип, который шифрует данные по этому алгоритму.
Обзор на английском: http://www.austinlinks.com/Crypto/skipjack-review.shtml
Twofish
Великолепный алгоритм, пришедший на смену Blowfish. Автор - все тот же Брюс Шайнер. Скорость работы может меняться в зависимости от глубины проведенной перекомпиляции ключа.
Tripple DES
Это ответ на вопрос "что будет если несколько раз зашифровать/расшифровать данные с разными кллючами?" Этот алгоритм позволяет используя DES увеличить его криптостойкость путем дифрования/дешифрования/шифрования по алгоритму DES с разными ключами. Объединение этих ключей в один дает длинну 3*56=168 бит. Но DES он и в Африке DES...
Потоковые шифры:
RC4
Байт-ориентированный потоковый шифр. Ключ переменного размера. Примерно в 10 раз быстрее DES. Является конфиденциальным алгоритмом, которым владеет RSA Data Security.
SEAL
Sapphire
Хэш-функции и алгоритмы генерации ПСЧ:
MD2
Самая медленная хэш-функция. Оптимизирована для 8-битных машин.
MD4
Самая быстрая хэш-функция. Оптимизирована для 32-битных машин.
MD5
Наиболее распространенная из семейства MD хэш-функция. Считается очень стойкой и безопасной. Похожа на MD4, но имеет несколько дополнительных средств для повышения безопасности, что замедляет ее примерно на треть по сравнению с MD4.
RIPEMD
SHA1
Secure Hash Algorithm. Создает 160-битовое значение хэш-функции из исходных данных переменного размера. Предложена NIST и принята правительством США как стандарт. Используется в стандарте DSS.
ГОСТ Р34.11-94
Электронные подписи
Предназначение - проверка целостности данных. Не для шифрования. Может добавляться к сообщению и шифроваться вместе с ним.
DSA
Digital Signature Authorization. Алгоритм, использующий открытые ключи для создания электронной подписи. Секретное создание хэш-значения и публичная проверка ее - только один человек может создать хэш-значение сообщения, но любой может проверить ее корректность. Основан на вычислительной сложности взятия логарифмов в конечных полях.
RSA
Отправитель создает хэш-функцию сообщения, а затем шифрует ее с использованием своего секретного ключа. Получатель использует открытый ключ отправителя для расшифровки хэша, сам рассчитывает хэш для сообщения, и сравнивает эти два хэша. Запатентовано RSA Data Security.
MAC (Код аутентификации сообшения)
Электронная подпись, использующая схемы хэширования, аналогичные MD или SHA, но хэш-значение вычисляется с использованием как данных сообщения, так и секретного ключа.
DTS (служба электронных временных меток)

Выдает пользователям временные метки, связанные с данными документа, криптографически стойким образом.

5.4. Перечень видов оценочных средств

Собеседование
Реферат
Контрольные вопросы.

ШКАЛА ОЦЕНИВАНИЯ Приложение 2.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Потемкин В.Г.	МАТЛАБ: среда проектирования инженерных приложений: Учебное пособие	М.: Диалог-МИФИ 2008
Л1.2	Мельников В.П., Клейменов С.А., Клейменов С.А., Петраков А.М.	Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений	М.: Издательский центр "Академия" 2008,2012
Л1.3	Артемов А.В.	Информационная безопасность : Электрон. текстовые данные	Межрегиональная Академия безопасности и выживания (МАБИВ) 2014
Л1.4	Сычев В.Н., Сычева Н.А.	Практикум по объектно-ориентированному программированию на базе языка С++: учебно-методическое пособие	Бишкек: Изд-во КРСУ 2017
Л1.5	Павловская Т.А.	С++. Программирование на языке высокого уровня. Для магистров и бакалавров: учебник	СПб.: Питер 2013

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	А.Ю. Щербаков, А.В. Домашев	Прикладная криптография. Использование и синтез криптографических интерфейсов	Москва .: Русская Редакция 2003
Л2.2	Фергюсон Н., Шнайер Б.	Практическая криптография: Учебное пособие	М.: Издательский дом Вильямс 2005
Л2.3	Столлингс В.	Криптография и защита сетей: принципы и практика: пер. с англ.	М.: Издательский дом "Вильямс" 2001
Л2.4	Вельшенбах М.	Криптография на Си и С++ в действии: Учебное пособие	М.: Издательство "Триумф" 2004
Л2.5	Жельников В.	Криптография от папируса до компьютера: научное издание	М.: АВГ 1996

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Васильев В.И. Интеллектуальные системы защиты информации: учебное пособие / Васильев В.И.—М.: Машиностроение, 2013. 172—с	http://www.iprbookshop.ru/18519

6.3. Перечень информационных и образовательных технологий

6.3.1 Компетентностно-ориентированные образовательные технологии

6.3.1.1	Изучение дисциплины студентами осуществляется в форме лекций, практических занятий в аудиторных условиях (компьютерные классы) и в процессе самостоятельной работы, контроля знаний.
6.3.1.2	Теоретическая информация, по мере возможности, представляется в виде компьютерных презентаций с использованием мультимедийных средств.
6.3.1.3	Практические занятия проводятся в компьютерных классах, оснащенных персональными компьютерами необходимыми параметрами и с установленным необходимым программным обеспечением. Используется Интернет для получения дополнительной информации. Используется дискуссионный метод проведения занятий, где студенты могут высказать свое мнение по обсуждаемой проблеме.
6.3.1.4	Защита практических работ проводится в виде собеседования с преподавателем по теории и программной реализации работы.
6.3.1.5	При изучении материала третьего модуля студентам предлагается написать и защитить реферат.
6.3.1.6	Защита реферата выполняется в форме дискуссии

6.3.2 Перечень информационных справочных систем и программного обеспечения

6.3.2.1	операционная система Microsoft Windows , пакет программ Microsoft Office 2010, языки программирования высокого уровня, установленные на компьютерах, учебно-методические комплексы по разделам дисциплины, размещенные на серверах компьютерных классов

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебная компьютерная лаборатория:
7.2	ПК-10шт.
7.3	Сервер-1.
7.4	Локальная сеть кафедры ЕПМ КРСУ.
7.5	Интернет со скоростью 70 Мбит/сек.
7.6	Зона WI-FI.
7.7	Интерактивная доска, проектор, обычная доска, 15 посадочных мест.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

технологическую карту дисциплины Приложение1

Рекомендации по организации самостоятельной работы студента
1. Советы по планированию и организации времени, необходимого для изучения дисциплины. Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:
Изучение конспекта лекции в тот же день, после лекции – 10-15 минут.
Изучение конспекта лекции за день перед следующей лекцией – 10-15 минут.
Изучение теоретического материала по учебнику и конспекту – 1 час в неделю.
Подготовка к практическому занятию – 2 час.
Всего в неделю – 3 часа 30 минут.

2. Описание последовательности действий студента
Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:
2.1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня (10-15 минут).
2.2. При подготовке к лекции следующего дня, нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции (10-15 минут).
2.3. В течение недели выбрать время (1-час) для работы с рекомендуемой литературой в библиотеке.
2.4. При подготовке к практическим занятиям следующего дня, необходимо сначала прочитать основные понятия и подходы по теме домашнего задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи.

Рекомендации по написанию реферата.
1. Тема реферата выбирается в соответствии с Вашими интересами и не обязательно должна соответствовать приведенному ниже примерному перечню. Важно, чтобы в реферате: во-первых, были освещены как естественнонаучные, так и социальные стороны проблемы; а во-вторых, представлены как общетеоретические положения, так и конкретные примеры. Особенно приветствуется использование собственных примеров из окружающей Вас жизни.
2. Реферат должен основываться на проработке нескольких дополнительных к основной литературе источников. Как правило, это специальные монографии или статьи. Во многих регионах регулярно издаются Доклады о состоянии окружающей среды. Рекомендуется использовать также в качестве дополнительной литературы научно-популярные журналы, а также газеты специализирующиеся на природоохранной тематике.
3. План реферата должен быть авторским. В нем проявляется подход автора, его мнение, анализ проблемы.
4. Все приводимые в реферате факты и заимствованные соображения должны сопровождаться ссылками на источник информации. Например: ... Нас заинтересовало снижение рождаемости, зарегистрированное в последнее время в России (Население России, 2008)... или ... Установлено, что в крупных городах, таких как Москва, уровень загрязнения воздуха в некоторые часы может превышать предельно допустимые концентрации в 10 и более раз (Лихачева, Смирнова, 2006) ...
5. Недопустимо просто скомпоновать реферат из кусков заимствованного текста. Все цитаты должны быть представлены в кавычках с указанием в скобках источника и страницы. Отсутствие кавычек и ссылок означает плагиат и, в соответствии с установившейся научной этикой, считается грубым нарушением авторских прав.
6. Реферат оформляется в виде текста на листах стандартного формата (А- 4). Начинается с титульного листа, в котором указывается название вуза, учебной дисциплины, тема реферата, фамилия и инициалы студента, номер академической группы или название кафедры, год и географическое место местонахождения вуза. Затем следует оглавление с указанием страниц разделов. Сам текст реферата желательно подразделить на разделы: главы, подглавы и озаглавить их. Приветствуется использование в реферате количественных данных и иллюстраций (графики, таблицы, диаграммы, рисунки).
7. Завершают реферат разделы "Заключение" и "Список использованной литературы". В заключении представлены основные выводы, ясно сформулированные в тезисной форме и, обычно, пронумерованные.

8. Список литературы должен быть составлен в полном соответствие с действующим стандартом (правилами), включая особую расстановку знаков препинания. Для этого достаточно использовать в качестве примера любую книгу изданную крупными научными издательствами: "Наука", "Прогресс", "Мир", "Издательство МГУ" и др.

Указания по организации работы с контрольно-измерительными материалами, по выполнению домашних заданий.
При выполнении домашних заданий необходимо сначала прочитать основные понятия и подходы по теме задания. При выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи, а затем приступить к расчетам и сделать качественный вывод.

Советы по подготовке к рубежному и промежуточному контролям. Дополнительно к изучению конспектов лекции необходимо пользоваться учебником. Кроме «заучивания» материала, очень важно добиться состояния понимания изучаемых тем дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?.
При подготовке к промежуточному контролю нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить несколько типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.

Рекомендации по работе с литературой. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги. Легче освоить курс, придерживаясь одного учебника и конспекта. Рекомендуется, кроме «заучивания» материала, добиться состояния понимания изучаемой темы дисциплины. С этой целью рекомендуется после изучения очередного параграфа выполнить несколько простых упражнений на данную тему. Кроме того, очень полезно мысленно задать себе следующие вопросы (и попробовать ответить на них): о чем этот параграф?, какие новые понятия введены, каков их смысл?, что даст это на практике?.