Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сибирский институт управления – филиал РАНХиГС
Факультет государственное и муниципальное управление

Кафедра информатики и математики

УТВЕРЖДЕНА
кафедрой информатики и математики
Протокол от «28» июня 2019 г. №10

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Б1.В.ДВ.03.02

не устанавливается

по направлению подготовки 38.03.04 Государственное и муниципальное управление направленность (профиль): «Информационные технологии в ГМУ» квалификация выпускника: бакалавр

формы обучения: очная

Год набора – 2021

Новосибирск, 2020

Автор–составитель:

Канд.тех.наук, доцент, доцент кафедры информатики и математики

Осипов Александр Леонидович

Заведующий кафедрой информатики и математики

Рапоцевич Е. А.

СОДЕРЖАНИЕ

1 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.03.02 «Криптографические методы защиты информации» обеспечивает овладение следующими компетенциями:

Таблица 1.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-6	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-6.3	способность применять информационно-коммуникационные технологий с учетом основных требований информационной безопасности

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2.

Профессиональные действия	Код этапа освоения компетенции	Результаты обучения
	ОПК-6.3	на уровне знаний: основ информационной безопасности. на уровне умений: анализировать риски информационной безопасности на уровне навыков: навыками анализа угроз информационной безопасности

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Дисциплина Б1.В.ДВ.03.02 «Криптографические методы защиты информации» изучается на 4 курсе (8 семестр) очной формы обучения.

Количество академических часов, выделенных на контактную работу с преподавателем.

- 44 часов (12 часа лекций, 32 часа практических (семинарских) занятий);

на самостоятельную работу обучающихся – 64 часов.

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

Место дисциплины

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области информационных технологий, а также на приобретенные ранее умения и навыки использования информационных технологий в профессиональной деятельности.

Дисциплина реализуется после изучения: Б1.Б.09 Информационные технологии в управлении.

3. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Таблица 3.

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущ. контроля успеваемости[1], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			л	лр	пз	**КСР**		
Тема 1.	Введение и история криптографии		1		4		8	
Тема 2.	Основы криптографии с открытым ключом		1		4		8	
Тема 3.	Элементы теории чисел		1		4		8	
Тема 4.	Системы с открытым ключом		1		4		8 Б1.В. ДВ.03.	
Тема 5.	Криптографические протоколы		1		4		8	
Тема 6.	Общие методы взлома систем с открытым ключом		1		4		6	
Тема 7.	Блоковые шифры		2		2		6	
Тема 8.	Потоковые шифры		2		4		6	
Тема 9	Криптографические хеш-функции		2		2		6	
Промежуточная аттестация								Зачет
Всего:		108	12		32		64	

1 Формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), практические задания (ПЗ)

Содержание дисциплины

Тема 1. Введение и история криптографии

Актуальность задач, решаемых в криптографии. Классическая схема Шеннона с секретным ключом. История криптографии. Исторические шифры. Шифр Цезаря. Взлом шифра Цезаря.

Тема 2. Основы криптографии с открытым ключом

Односторонние функции. Задача дискретного логарифмирования. Быстрый алгоритм возведения в степень и его сложность. Задача хранения паролей в компьютере. Система «свой – чужой» в авиации. Задача, возникающая в сетях с удаленным доступом.

Тема 3. Элементы теории чисел

Простые числа. Основная теорема арифметики. Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Алгоритм Евклида. Обобщенный алгоритм Евклида и решение диофантова уравнения. Нахождение инверсий по заданному модулю.

Тема 4. Системы с открытым ключом

Система Диффи-Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Односторонняя функция с лазейкой и шифр RSA.

Тема 5. Криптографические протоколы

Протоколы аутентификации и электронной подписи. Электронные деньги. Подбрасывание монеты по телефону. Ментальный покер. Доказательства с нулевым знанием. Электронные деньги. Голосование через Интернет.

Тема 6. Общие методы взлома систем с открытым ключом

«Шаг младенца, шаг великана». Теоретико-числовые алгоритмы. Алгоритм исчисления порядка.

Тема 7. Блоковые шифры

Принципы построения блоковых шифров и требования, предъявляемые к ним. Режимы функционирования блоковых шифров: ECB, CBC, OFB, CTR. Сеть Фейстеля. Шифры DES, ГОСТ, AES. Криптоанализ блоковых шифров. Сценарии атак на шифры. Основные атаки на блоковые шифры: линейный и дифференциальный криптоанализ. Связь блоковых шифров и генераторов псевдослучайных чисел.

Тема 8. Потоковые шифры

Принципы построения и современные требования к потоковым шифрам. Криптографически стойкие генераторы псевдослучайных чисел и потоковые шифры. Классификация потоковых шифров. Основные потоковые шифры.

Тема 9. Криптографические хеш-функции

Принципы построения и современные требования к хеш-функциям. Применение хеш-функций в криптографии. Хеш-функция MD5 и семейство SHA. Хеш-функции, базирующиеся на блоковых шифрах.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.ДВ.03.02 «Криптографические методы защиты информации» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 4.

Тема (раздел)		Методы текущего контроля успеваемости
Тема1.	Введение и история криптографии	Устный ответ на вопросы
Тема 2.	Основы криптографии с открытым ключом	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 3.	Элементы теории чисел	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 4.	Системы с открытым ключом	Устный ответ на вопросы
Тема 5.	Криптографические протоколы	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 6.	Общие методы взлома систем с открытым ключом	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 7.	Блоковые шифры	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 8.	Потоковые шифры	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 9.	Криптографические хеш-функции	Устный ответ на вопросы Выполнение практического задания на компьютере

4.1.2. Зачет проводится в форме устного ответа на вопрос.

4.2. Материалы текущего контроля успеваемости.

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ УСТНОГО (ПИСЬМЕННОГО) ОПРОСА

1.Компоненты защиты информационной безопасности.
2.Комплексный подход к обеспечению информационной безопасности.
3.Сертификация средств защиты информации.
4.Понятие рисков.
5.Что такое векторы угроз?
6.Какие существуют модели защиты?
7.Периметровая защита.
8.Для чего нужна политика безопасности?
9.Какие подразделения участвуют в разработке политики безопасности?
10. Каково содержание политики безопасности?
11. Понятие аутентификации.
12. Средства контроля аутентификации.
13. Аутентификация по сертификатам.
14. Защита ключей в системах аутентификации.
15. Целостность информации.
16. Доступность информации.
17. Вирусы и антивирусы.
18. Классификация МЭ.
19. Шлюзы приложений и контурного уровня.
20. Понятие системы обнаружения атак.
21. Виды систем обнаружения атак.
22. Модель обнаружения аномалий
23. Атаки доступа.
24. Атаки модификации.
25. Переполнение буфера.
26. Распределенные атаки.
27. Понятие частной виртуальной сети.
28. VPN туннели.
29. Протокол IPSec.
30. Средства безопасности беспроводных сетей.
31. Протокол WEP.
32. Протокол WPA.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ РЕФЕРАТОВ

1. Конкурс криптоалгоритмов NESSIE:
2. Конкурс блочных шифров AES:
3. Проект CRYPTREC;
4. Конкурс поточных шифров eStream;
5. Конкурс хеш-функций SHA-3;
6. Блочные шифры;

7. Поточные шифры;
8. Криптоанализ блочных шифров;
9. Криптоанализ поточных шифров;
10. Криптоанализ хеш-функций;
11. Цифровая подпись;
12. Криптосистемы на эллиптических кривых;
13. Криптография в электронной коммерции и электронные деньги;
14. Криптосистемы с открытым ключом;
15. Исторические шифры;
16. Компьютерные вирусы;
17. Антивирусы;
18. Случайные числа;
19. Кодирование информации;
20. Сжатие информации;
21. Криптографические библиотеки в современных языках программирования;
22. Историческая стеганография;
23. Цифровая стеганография;
24. Цифровые водяные знаки
25. Стегоанализ;
26. Коды аутентичности сообщений;
27. Методы генерации простых чисел и проверки чисел на простоту;
28. Спам и методы борьбы с ним;
29. Проблема распределения ключей;
30. Задача разделения секрета;
31. Доказательство с нулевым знанием (с нулевым разглашением);
32. Криптоалгоритмы на графах;
33. Методы факторизации;
34. Методы дискретного логарифмирования;
35. Российские ГОСТы на криптоалгоритмы;

4.3. Оценочные средства промежуточной аттестации

Таблица 5.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ОПК-6	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-6.3	способность применять информационно-коммуникационные технологий с учетом основных требований информационной безопасности

Таблица 6.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ОПК-6.3 способность применять информационно-коммуникационные технологий с учетом основных требований информационной безопасности	Знает нарушения информационной безопасности компьютерной системы и их причины Умеет проводить сертификацию средств защиты информации	Осуществляет политику безопасности компьютерной системы Проводит политику безопасности беспроводных сетей

ТИПОВЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ

1. Описать алгоритм шифра Цезаря.
2. Как провести криптоанализ шифра Цезаря?
3. Что такое односторонняя функция?
4. Что такое дискретное логарифмирование?
5. Описать алгоритм быстрого возведения в степень. Оценить его сложность.
6. Как решаются проблема хранения паролей и проблема ПВО с помощью односторонней функции?
7. Чем отличается криптосистема с открытым ключом от криптосистемы с секретным ключом?

8. Описать первую криптосистему с открытым ключом? Какие проблемы она позволяет решать?
9. Описать алгоритм Евклида и обобщенный алгоритм Евклида.
10. Дать определение инверсии. Как вычислять инверсию, используя алгоритм Евклида?
11. Дать определение функции Эйлера и привести пример ее вычисления.
12. Описать алгоритм «Решето Эратосфена».
13. Описать методы дискретного логарифмирования. Оценить их сложность.
14. Как построить цифровую подпись на басе шифра RSA?
15. Как построить цифровую подпись на басе шифра Эль-Гамаля?

.

4.4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Зачет включает ответы на устные теоретические вопросы.

Ответы на теоретические вопросы могу даваться в устной форме или в форме электронного тестирования.

Для получения положительной оценки на зачете достаточно изучить рекомендуемую основную литературу, а также усвоить умения и навыки в ходе контактной работы с преподавателем путем опроса и выполнения различных практических заданий.

Студент при подготовке к ответу по билету формулирует ответ на вопрос.

При подготовке ответа на вопрос стоит использовать соответствующий дисциплине понятийный аппарат.

Давать односложные ответы нежелательно.

ТИПОВЫЕ БИЛЕТЫ К ЗАЧЕТУ

Билет 1.
Вопрос: Политика безопасности.

Билет 2.
Вопрос: SQL-инъекции.

Ответ на вопрос билета оценивается по системе зачет/не зачет.

Шкала оценивания

Таблица 7

Зачет	Критерии оценки
не зачтено	Этапы компетенций, предусмотренные образовательной программой не сформированы. Недостаточный уровень усвоения понятийного аппарата и наличие фрагментарных знаний по дисциплине. Отсутствие минимально допустимого уровня в самостоятельном решении практических задач. Практические навыки профессиональной деятельности не сформированы.
зачтено	Этапы компетенций, предусмотренные образовательной программой сформированы. Наличие допустимого уровня в усвоении учебного материала, в т.ч. в самостоятельном решении практических задач. Практические навыки профессиональной деятельности сформированы.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При изучении курса «Криптографические методы защиты информации» применяются разнообразные лекции, практические занятия, выполнение практических заданий по темам, самостоятельная работа с источниками и др.).

Студент должен посетить установочные лекции, на которых излагается цель, задачи и содержание курса, приводятся рекомендации и критерии оценивания.

В ходе лекционных занятий раскрываются базовые вопросы в рамках каждого модуля дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала, даются рекомендации по выполнению заданий к практическим занятиям.

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям, а также к промежуточной аттестации по дисциплине.

Практические занятия позволяют более детально проработать наиболее важные темы курса. Целью практических занятий является закрепление теоретических знаний, полученных студентами на лекциях и в процессе самостоятельной работы, контроль за степенью усвоения пройденного материала, ходом выполнения студентами самостоятельной работы и рассмотрение наиболее сложных и спорных вопросов в рамках темы занятия.

Подготовку к занятиям следует начинать с ознакомления с содержанием темы, вопросами к теме, подбора рекомендованной литературы. Затем необходимо перечитать запись лекции, соответствующие разделы учебника, статьи в журналах. При этом перед собой нужно иметь соответствующие нормативные акты в действующей редакции.

Подготовка к практическим занятиям осуществляется студентами самостоятельно с использованием научной и учебной литературы и необходимых правовых источников. На практических занятиях у студентов формируются навыки публичного выступления, анализа материала, умение грамотно и обоснованно отвечать на поставленные вопросы и применять полученные теоретические знания к практическим ситуациям, а также умение решать практические задания (задачи).

Для получения глубоких теоретических знаний и практических навыков студентам рекомендуется посещать лекции, активно участвовать в практических занятиях. Поставленные перед занятиями цели могут быть достигнуты лишь при систематической работе студентов над изучением дисциплины.

При необходимости в период самостоятельной подготовки студенты могут получить индивидуальные консультации преподавателя по учебной дисциплине.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ПОДГОТОВКИ К ОПРОСУ

Опрос в рамках изучаемой темы может проходить как в устной, так и в письменной форме.

Опрос проводится только после изучения материала темы и направлен на ее закрепление.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ РЕШЕНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ

Решение практических заданий нацелено на формирование у студента соответствующих компетентностных практических умений и владений. Поэтому для исключения компиляций результата все задания выполняются на компьютерах.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Рябко Б. Я. Основы современной криптографии для специалистов по информационным технологиям / Б. Я. Рябко, А. Н. Фионов. – М.: Науч. мир, 2004.
2. Введение в криптографию. Новые мат. дисциплины: [учебник] / [В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко и др.]; под ред. В. В. Ященко. – СПб.: МЦНМО : Питер, 2001.
3. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. – М.: Солон-Пресс, 2007.
4. Основы криптографии: учеб. пособие для высш. учеб. заведений по гр. специальностям в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 3-е изд., испр. и доп. – М.: Гелиос АРВ, 2005.

6.2. Дополнительная литература

1. Goldreich O. Foundations of Cryptography [Electronic resource] / O. Goldreich. – Mode of access:
http://eccc.hpi-web.de/eccc-local/ECCC-Books/oded_book_readme.html

2. Menezes A. Handbook of Applied Cryptography [Electronic resource] / A. Menezes, P. van Oorshot, S. Vanstone. – [S.l.]: SRS Press, 1996. – Mode of access: http://www.cacr.math.uwaterloo.ca/hac
3. Ryabko B. Basics of Contemporary Cryptography for IT Practitioners / B. Ryabko, A. Fionov. – [S.l.]: World Scientific, 2005.
4. Смарт Н. Криптография / Н. Смарт. – М.: Техносфера, 2006.
5. Goldwasser S. Lecture notes on cryptography [Electronic resource] / S. Goldwasser, M. Bellare. – Mode of access: http://www-cse.ucsd.edu/users/mihir/crypto-lecnotes.html
6. Schneier B. Self-study course in block cipher cryptanalysis [Electronic resource] // Cryptologia. – 2000. – V. 24. – № 1. – Mode of access: http://www.counterpane.com/self-stady.html
7. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Вильямс, 2004.
8. Шнайер Б. Прикладная криптография / Б. Шнайер. – М.: Триумф, 2002.

6.3. Интернет-ресурсы

1. Бизнес и компьютер [Электронный ресурс]: офиц. сайт. – Режим доступа: http://www.bizcom.ru
2. Университетская библиотека ONLINE [Электронный ресурс]: [электрон.-библиотеч. система] / О-во с огранич. ответственностью «Директ-Медиа». - [М.], 2001 - 2010. - Режим доступа: http://www.biblioclub.ru, требуется авторизация.
3. Университетская информационная система РОССИЯ [Электронный ресурс] : тематич. электрон. б-ка / Науч.-исслед. вычислит. центр МГУ; Автоном. некоммерч. организация «Центр информац. исслед.». – Электрон. дан. – М., 2000 – 2012. - Режим доступа: http://uisrussia.msu.ru, требуется авторизация.

7. Материально – техническая база, информационные технологии, программное обеспечение и информационные справочные системы

7.1. Программное обеспечение

1. Microsoft Visual Studio 2010 и выше.
2. Microsoft SQL Server 2008 и выше.

7.2. Технические средства и материально-техническое обеспечение дисциплины (модуля).

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Учебные аудитории для проведения занятий лекционного типа (ауд. № 219)	экран, компьютер с подключением к локальной сети института, и выходом в Интернет, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Лаборатория личностного и профессионального развития (ауд. № 219)	экран, компьютер с подключением к локальной сети института, и выходом в Интернет, мультимедийный проектор, столы аудиторные, стулья, трибуна настольная, доска аудиторная
Аудитория для самостоятельной работы обучающихся. Центр Интернет-ресурсов (ауд.№ 207, №208)	Мультимедийный проектор – 1шт., Экран проекционный – 1шт., Принтер-1шт. ПК - 11 шт. с подключенным интернетом и к локальной сети института (включая правовые системы) и Интернет, столы аудиторные, стулья, доски аудиторные.
Центр интернет-ресурсов (ауд. № 201)	10 компьютеров с выходом в Интернет, автоматизированную библиотечную информационную систему и электронные библиотечные системы: «Университетская библиотека ONLINE», «Электронно-библиотечная система издательства ЛАНЬ», «Электронно-библиотечная система издательства «Юрайт», «Электронно-библиотечная система IPRbooks»,«Университетская Информационная Система РОССИЯ», «Электронная библиотека диссертаций РГБ», «Научная электронная библиотека eLIBRARY», «EBSCO», «SAGE Premier». Система федеральных образовательных порталов «Экномика. Социология. Менеджмент», «Юридическая Россия», Сервер органов государственной власти РФ, Сайт Сибирского Федерального округа и др. Экран, компьютер с подключением к локальной сети филиала и выходом в Интернет, звуковой усилитель, мультимедийный проектор, столы аудиторные, стулья, трибуна, доска аудиторная. Наборы виртуального демонстрационного оборудования, наглядные учебные пособия.
Библиотека (имеющая места для обучающихся,	компьютеры с подключением к локальной сети филиала и Интернет, Wi-Fi, столы аудиторные,

оснащенные компьютерами с доступом к базам данных и сети Интернет (ауд. № 101, № 102)	стулья