МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

«13» 01 2017 г.

Рабочая программа дисциплины
Криптографические методы защиты информации

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2017

1. Цели освоения дисциплины

Целями освоения дисциплины являются овладение основными идеями и методами классической и современной криптографии; знакомство со средствами криптографической защиты информации; знание основополагающих документов в области защиты информации.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к базовой части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся общепрофессиональных и профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Алгебра», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов», «Основы информационной безопасности»,

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Криптографические протоколы», «Теоретико-числовые методы в криптографии», «Модели безопасности компьютерных систем», «Введение в криптоанализ», «Методы алгебраической геометрии в криптографии».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими общепрофессиональными и профессиональными компетенциями:

- способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);
- способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);
- способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-18).

В рамках указанных компетенций обучающийся должен

• Знать:

– основные виды симметричных и асимметричных криптографических алгоритмов;

– математические модели шифров;

– криптографические стандарты;

• Уметь:

– корректно применять симметричные и асимметричные криптографические алгоритмы;

• Владеть:

– криптографической терминологией.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 9 зачетных единиц, 324 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Лабораторные занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
7-ой семестр								
1	Введение	7	1-2	4	4	–	–	Контрольная работа № 1 на 7-й неделе
2	Искусство шифрования		3-8	48	12	18	18	
3	Стандарты шифрования		9-18	56	20	18	18	Опрос на 10-й неделе
	Промежуточная аттестация							Зачет
	ИТОГО в 7-м семестре			**108**	**36**	**36**	**36**	–
8-ой семестр								
4	Криптосистема RSA	8	1-3	33	6	6	21	Опрос на 9-й неделе
5	Хеш-функции и ЭЦП		4-9	45	12	12	21	
6	Доказательства с нулевым разглашением		10-11	25	2	2	21	Контрольная работа № 2 на 16-й неделе
7	Теория информации в криптографии		11-14	34	8	4	22	
8	Средства криптографической защиты информации (СКЗИ)		15-16	34	4	8	22	
	Промежуточная аттестация							Экзамен

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Лабораторные занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
	ИТОГО в 8-м семестре			216	32	32	107	45
	ВСЕГО			324	68	68	143	45

Введение. Общая схема линии связи. Помехоустойчивое кодирование. Физические методы защиты канала связи. Стеганография. Основные понятия криптографии. История криптологии. Правила криптологии.

Искусство шифрования. Перестановочные шифры. Маршрутное шифрование. Шифрование с помощью решеток. Подстановочные шифры. Шифры простой замены и их криптоанализ. Исторические шифры. Модульная арифметика. Блочные шифры. Шифр Виженера. Шифр Хилла. Поточные шифры. Книжные шифры. Шифры с автоключами. Шифр Вернама.

Стандарты шифрования. Шифр DES: общее описание, функция Фейстеля, *S*-боксы. История шифра DES. Шифр Rejndael (AES): описание криптоалгоритма, его программные и аппаратные реализации, структура (неприводимый многочлен, преобразование SubBytes, функция MixColumns, функция ShiftRows). Шифр ГОСТ 28147-89, сравнение с шифром Rejndal.

Криптосистема RSA. Функция Эйлера и ее свойства. Односторонние функции. Система шифрования RSA. Большие простые числа, проверка на простоту. Тест Миллера-Рабина. Алгоритм AKS. Временная сложность алгоритмов. Проблема NP=P.

Функции хеширования и электронные цифровые подписи. Стандарты хеш-функции SHA и ГОСТ Р 34.11-94. Код проверки подлинности сообщения (MAC). Аутентификация. Электронная цифровая подпись (ЭЦП). Протокол ЭЦП Эль-Гамаля. Стандарт ЭЦП ГОСТ Р 34.10-94. Основные понятия об эллиптических кривых. Стандарт ЭЦП Р 34.10-2001. Федеральный закон РФ об ЭЦП. Создание инфраструктуры ЭЦП.

Доказательства с нулевым разглашением. Базовый протокол Кискатера-Гилу. Протокол Фиата-Шамира. Протоколы Блюма, связанные с графами.

Теория информации в криптографии. Эксперименты. Энтропия, условная энтропия, количество информации. Источник сообщения, его энтропия, эргодичность, избыточность. Виды криптоатак. Совершенная

секретность криптосистемы. Теоретико-информационная характеристика совершенной секретности. Теорема о длине ключа. Совершенная секретность шифра Вернама. Неопределенность шифра по ключу. Неравенство для среднего количества ложных ключей. Расстояние единственности.

Средства криптографической защиты информации (СКЗИ). Шифровальные машины SZ-52 и «Энигма». СКЗИ «Верба» и «КриптоПро». Пакет PGP. Виртуальная экскурсия в музей криптографии Агентства национальной безопасности США в Форт-Миде. Космический проект «Пионер».

План лабораторных занятий

На лабораторных занятиях студенты, выполняя предложенные задания, должны практически овладеть основными методами классической и современной криптографии, в частности с использованием языков программирования C++, C#, Java, Python.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
	7 семестр	
1-3	Анаграммные (перестановочные) шифры	1-2
4-5	Шифр Виженера	3
6	Шифр Уитстона- Плейфера	4
7-9	Исторические шифры	5-7
10-12	Поточные шифры	8-10
13	Шифровальная машина *SZ*-52	11
14-18	Стандарты шифрования	12-14
	8 семестр	
1-3	Криптосистема *RSA*	15-18
4-5	ЭЦП	19-20
6-7	Доказательства с нулевым разглашением	21-22
8-9	Теория информации в криптографии	23
10-13	Средства криптографической защиты информации	24
14-15	Пакет *PGP*	25
16	Контрольная работа	

5. Образовательные технологии, применяемые при освоении дисциплины

Рекомендуемые образовательные технологии: встречи с представителями ведущих отечественных фирм по производству криптографической продукции, выступления экспертов и специалистов перед студентами, ознакомительные беседы с представителями потенциальных работодателей, экскурсия в музей регионального Управления ФСБ России, комментированное посещение Интернет-страницы музея криптологии Агентства национальной безопасности США в Форт-Миде.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья и инвалидов, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты должны, творчески освоив представленный на лекциях теоретический материал, составить о нем более углубленное представление и попытаться получить некоторые оригинальные результаты.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольных работ, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачет), вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств дисциплины приведён в приложении 1.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	17	30	0	11	0	12	30	100
8	16	32	0	10	0	10	32	100

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 17 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий, самостоятельность при выполнении работы, правильность выполнения, посещаемость в течение одного семестра – от 0 до 30 баллов.

Практические занятия

Не предусмотрены

Самостоятельная работа

Контроль выполнения заданий в рамках самостоятельной работы, проверка усвоения изученного лекционного материала в рамках опроса, конспект занятий – от 0 до 11 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа № 1 – от 0 до 12 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *зачёт*, проводимый в виде собеседования в устной форме с предварительной подготовкой студента к ответу, или в письменном виде по выбору преподавателя.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 24 до 30 баллов;

ответ на «хорошо» оценивается от 19 до 23 баллов;

ответ на «удовлетворительно» оценивается от 15 до 18 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 14 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за седьмой семестр по дисциплине «Криптографические методы защиты информации» составляет 100 баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Криптографические методы защиты информации» в оценку (зачет)

70 баллов и более	«зачтено»
меньше 70 баллов	«не зачтено»

8 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 16 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий, самостоятельность при выполнении работы, правильность выполнения, посещаемость в течение одного семестра – от 0 до 32 баллов.

Практические занятия

Не предусмотрены

Самостоятельная работа

Контроль выполнения заданий в рамках самостоятельной работы, проверка усвоения изученного лекционного материала в рамках опроса, конспект занятий – от 0 до 10 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа № 2 – от 0 до 10 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический экзамен, проводимый в виде собеседования в устной форме с предварительной подготовкой студента к ответу, или в письменном виде по выбору преподавателя.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 26 до 32 баллов;

ответ на «хорошо» оценивается от 20 до 25 баллов;

ответ на «удовлетворительно» оценивается от 16 до 19 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 15 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за восьмой семестр по дисциплине «Криптографические методы защиты информации» составляет 100 баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Криптографические методы защиты информации» в оценку (экзамен)

80–100 баллов	«отлично»
64–79 баллов	«хорошо»
51–63 баллов	«удовлетворительно»
0–50 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс] : Учебное пособие / В. Н. Салий. - Саратов, 2012. - 42 с. URL: http://library.sgu.ru/uch_lit/622.pdf (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

б) дополнительная литература:

1) Математические и компьютерные основы криптологии [Текст] : учеб. пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. - Минск : Новое знание, 2003. - 381, [3] с. : рис. - Библиогр.: с. 371-378 (196 назв.). - Предм. указ.: с. 379-381. - ISBN 985-475-016-7 (в пер.).

2) Основы криптографии [Текст] : учеб. пособие / А. П. Алфёров [и др.]. - 3-е изд., испр. и доп. - Москва : Гелиос АРВ, 2005. - 479, [1] с. - Библиогр.: с. 469-475. - ISBN 5-84438-137-0 (в пер.).

3) Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире [Текст] = Secrets and Lies / Б. Шнайер ; . - Москва ; Санкт-Петербург [и др.] : Питер, 2003. - 367, [1] с. : ил. - (Классика computer science). - ISBN 0-471-25311-1 (англ.) (в пер.). - ISBN 5-318-00193-9.

в) Интернет-ресурсы:

1) Баричев, С. Г. Основы современной криптографии [Электронный ресурс] : Учебный курс / С. Г. Баричев, Р Е. Серов // Теория кодирования в НГУ [Электронный ресурс]. URL: http://www.codingtheory.gorodok.net/literature/barichev-serov.pdf (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

г) программное обеспечение:

1) Лицензионное программное обеспечение: Visual C++ 4.2, Visual Studio 2010, Visual Studio 2012, Visual Studio 2013, Visual Studio 2015

2) Свободное программное обеспечение: Java Developers Kit, NetBeans IDE, Eclipse, CPython, Jython, IronPython.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных работ необходимо наличие компьютерного класса, оснащенного соответствующим программным обеспечением, с возможностью выхода в сеть Интернет из расчета одна ПЭВМ на одного человека. В целях сохранения результатов работы желательно наличие у студентов носителей информации.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Профессор кафедры теоретических основ компьютерной безопасности и криптографии  В.Н. Салий

Программа разработана в 2012 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «25» мая 2012 года, протокол № 18).

Программа актуализирована в 2017 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «09» января 2017 года, протокол № 10).

Заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, профессор, к.ф.-м.н.  В.Н. Салий

Декан факультета компьютерных наук и информационных технологий, к.ф.-м.н., доцент  А.Г. Федорова