ТОКБиК

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

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

«13» 04 2017 г.

Рабочая программа дисциплины

Введение в криптоанализ

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 «Введение в криптоанализ» являются ознакомление студентов с основными задачами криптографического анализа; ознакомление с основными идеями и методами классического и современного криптографического анализа; овладение основными методами анализа криптосистем, основанных на перестановках и подстановках; овладение основными методами анализа линейных криптографических систем; овладение основными методами анализа систем с открытым ключом; ознакомление с основными идеями линейного и дифференциального криптоанализа современных стандартов шифрования.

Курс «Введение в криптоанализ» позволяет студентам овладеть фундаментальными понятиями и методами классической и современной теории криптографического анализа, без знания которых невозможна полноценная оценка современных систем защиты информации. При освоении данного курса у студентов формируются навыки грамотной оценки стойкости рассматриваемой криптографической системы, навыки решения практических задач с учётом этой оценки.

2.Место дисциплины в структуре ООП

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

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Алгебра», «Геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов», «Основы информационной безопасности», «Криптографические методы защиты информации», «Методы программирования», «Алгоритмы алгебры и теории чисел», «Теоретико-числовые методы в криптографии».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими профессиональными и профессионально-специализированными компетенциями:

- способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПК-4);
- способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы (ПК-8);
- способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов (ПСК-2.3).

В рамках указанных компетенций обучающийся должен

• Знать:

– основные понятия, задачи и алгоритмы криптографического анализа симметричных и ассиметричных криптосистем.

• Уметь:

– формулировать основные и промежуточные задачи по криптографическому анализу в конкретных условиях.

• Владеть:

– основными методами криптографического анализа.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 180 часов.

№ 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**
1	Основные задачи криптоанализа	10	1-5	43	10	10	23	Опрос на 2-й неделе
2	Анализ симметричных шифров		6-11	46	11	11	24	Опрос на 6-й неделе
3	Криптоанализ системы RSA		11-16	46	11	11	24	Опрос на 13-й неделе Контрольная работа на 15-й неделе
	Промежуточная аттестация							Экзамен
	ИТОГО			**180**	**32**	**32**	**71**	**45**

Основные задачи криптоанализа. Оценка секретных систем. Основные виды криптоатак. Четыре основных задачи криптоанализа (по Фридману). Пять основных класса методов криптоанализа.

Анализ симметричных шифров.

1) Анализ перестановки с периодом T. Правило Казиски для вычисления длины ключа. Теорема о разложении подстановки на циклы. Число моноциклических перестановок из n символов. Анализ шифра перестановки при известной длине периода на основе вспомогательной таблицы.

2) Анализ шифров подстановки. Частотный анализ простой подстановки.

Анализ шифра Виженера:

- Атака на основе открытого текста и шифротекста;
- Атака Фридмана, Индекс совпадения, Теорема 1 (об индексе совпадения), Теорема 2 (формула вычисления математического ожидания индекса совпадения). Теорема 3 (о среднем индексе совпадения). Теорема 4 (геометрическая оценка среднего индекса совпадения). Атака Фридмана на основе среднего индекса совпадения для вычисления периода шифра подстановки.
- Статистический метод вычисления длины периода гаммы в шифре гаммирования.
- Метод БШ.

Методы вычисления ключа при известной длине ключа:

- Метод чтения по колонкам;
- Метод протяжки вероятного слова;
- Атака по словарю;
- Метод Симпсона;
- Метод Томаса Якобсена.

Анализ шифра Хилла:

- Атака на основе выбранного открытого текста;
- Атака на основе известного открытого текста;
- Атака на основе только шифрограммы.

Криптоанализ системы RSA

Анализ на основе задачи разложения составного числа на множители:

- Метод пробного деления;
- ρ-метод Полларда;
- $(p-1)$-метод Полларда;
- Метод квадратов (метод Ферма);
- Метод Диксона;
- Метод непрерывных дробей (в алгоритме Диксона);
- Метод квадратичного решета (в алгоритме Диксона);

Оценка безопасности системы RSA:

- Лемма о задаче разложения и вычисления функции Эйлера;
- Теорема о задаче вычисления секретного ключа в RSA;
- Алгоритм разложения на множители по известным показателям RSA.

Атаки на криптосистему RSA, не требующие разложения:

- Атака на основе теоремы Винера;
- Атака на основе Греко-китайской теоремы;
- Атака на основе «частично известных» открытых текстов:

a) Алгоритм нахождения линейно зависимых текстов для случая $e = 3$;

b) Алгоритм нахождения линейно зависимых текстов для произвольного e.

- Атака на RSA при малом порядке открытого показателя e по модулю $\varphi(n)$;

- Атака на RSA при малом порядке показателя e по модулю $p - 1$ или $q - 1$.

План лабораторных занятий

На лабораторных занятиях студенты решают задачи, связанные с созданием программного обеспечения, в частности с использованием языков программирования C++, C#, Java, обслуживающего исполнение поставленных перед ними задач выше перечисленных разделов и подразделов.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1–8	Анализ симметричных шифров	№№ 1–11
9–16	Криптоанализ системы RSA	№№ 12–20

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе при реализации компетентностного подхода таких активных и интерактивных формы проведения занятий как интерактивный опрос; модельный метод обучения – моделирование в процессе обучения тех или иных ситуаций; кейс-стади – имитация в учебном процессе реального события для демонстрации того или иного изучаемого явления, студентам предлагается рассмотреть случай, который требует решения тех или иных задач текущей темы; метод проектов – распределение заданий между учащимися, предполагающий сбор и анализ информации; метод Делфи – метод поиска быстрых решений в группе; эвристические технологии генерирования идей: «мозговой штурм», синектика, ассоциации; тренинг – активное овладение и развитие знаний, умений и навыков.

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 изучают дополнительную литературу по предмету (при чтении лекций по соответствующим разделам

дисциплины даются ссылки на источники, в которых рассматривается материал, не вошедший в основной курс), готовятся к лабораторным занятиям.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, 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
10	10	10	0	20	0	20	40	100

Программа оценивания учебной деятельности студента

10 семестр

Лекции

Посещаемость, опрос, активность и др. за семестр – от 0 до 10 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий в течение семестра – от 0 до 10 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Выполнение заданий в рамках самостоятельной работы – от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрены.

Другие виды учебной деятельности

Контроль выполнения контрольной работы, грамотность в оформлении, правильность выполнения – от 0 до 20 баллов.

Промежуточная аттестация

Промежуточная аттестация проходит в виде письменного экзамена.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 31 до 40 баллов;

ответ на «хорошо» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за десятый семестр по дисциплине «Введение в криптоанализ» составляет 100 баллов.

Таблица 2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Введение в криптоанализ» в оценку (экзамен)

86-100 баллов	«отлично»
76-85 баллов	«хорошо»
61-75 баллов	«удовлетворительно»
0-60 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М. М. Глухов [и др.]. - Москва : Лань, 2011. - 394 с. : табл. - (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-1116-0 : Б. ц. URL: https://e.lanbook.com/book/1540 (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

б) дополнительная литература:

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) Смарт, Н. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо. - Москва : Техносфера, 2006. - 525, [3] с. : рис., табл. - (Мир программирования). - ISBN 5-94836-043-1. - ISBN 0077099877 (англ.).

4) Фомичев, В.М. Дискретная математика и криптология [Текст] : курс лекций / В. М. Фомичев ; общ. ред. Н. Д. Подуфалов. - Москва : ДИАЛОГ-МИФИ, 2003. - 397, [3] с. - Библиогр.: с. 386-390 (86 назв.). - ISBN 5-86404-185-8 (в пер.).

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

6) Виноградов, И. М. (1891-1983). Основы теории чисел [Текст] : учеб. пособие / И. М. Виноградов. - 12-е изд., стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2009. - 176 с. : табл. - (Лучшие классические учебники) (Классическая учебная литература по математике) (Учебники для вузов. Специальная литература). - ISBN 978-5-8114-0535-0 (в пер.).

в) программное обеспечение:

1) Лицензионное программное обеспечение: Visual Studio 2012, Visual Studio 2013.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима аудитория на 40-60 посадочных мест, в которой имеются учебные доски (большого размера) для визуализации информации. Также в ходе лекционных занятий применяются учебно-демонстрационные мультимедийные презентации, которые обеспечиваются следующим техническим оснащением: компьютер (в комплекте с колонками); мультимедийный проектор; экран.

Для проведения лабораторных занятий необходим компьютерный класс на 10-20 посадочных мест с установленным необходимым инструментальным программным обеспечением.

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

Доцент кафедры теоретических основ компьютерной безопасности и криптографии, к.ф.-м.н.  В.Е. Новиков

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