Токбик

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

Факультет компьютерных наук и информационных технологий

«УТВЕРЖДАЮ»
«23» 01 2017

Рабочая программа дисциплины
Криптографические свойства булевых функций

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 использование аппарата теории булевых функций для создания эффективных методов и алгоритмов, повышающих стойкость криптографических средств или помехоустойчивость кодов.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к вариативной части Блока 1 «Дисциплины (Модули)» ООП, является дисциплиной по выбору и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Алгебра», «Математическая логика и теория алгоритмов», «Дискретная математика».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими общепрофессиональными компетенциями:

- способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

В рамках указанных компетенций обучающийся должен

- Знать:

– арифметику конечных полей и полиномов;

– криптографические свойства булевых функций и отображений;

– некоторые классы максимально нелинейных функций и их свойства;

– методы построения корреляционно-иммунных функций и устойчивых отображений;

– построение булевых функций, удовлетворяющих лавинному критерию;

- Уметь:

– применять аппарат теории булевых функций к проблемам анализа и синтеза дискретных устройств, осуществляющих обработку и преобразование информации;

- Владеть:

– простейшими подходами к анализу безопасности криптографических протоколов, используя в конструкциях подходящие формы булевых функций.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 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)
				Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
5-ый семестр								
1	Арифметика конечных полей и полиномов	5	1-5	10	–	–	7	Контрольная работа № 1 на 5-й неделе
2	Булевы функции. Числовые и метрические характеристики		6-8	6	–	–	7	Коллоквиум на 11-й неделе
3	Криптографические свойства булевых функций.		9-11	6	–	–	7	
4	Коды Рида-Маллера и их криптографические параметры.		12-15	8	–	–	7	
5	Использование алгоритмов деко-дирования кодов Рида-Маллера при построении методов криптографического анализа.		16-18	6	–	–	8	
	Промежуточная аттестация							Зачёт
	ИТОГО в 5-м семестре			**36**	–	–	**36**	–
6-ый семестр								
6	Нелинейность как мера криптографического качества. Максимально нелинейные булевы функции.	6	1-2	4	2	–	5	Контрольная работа № 2 на 8-й неделе

№ 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)
				Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
7	Корреляционная иммунность и устойчивость булевых функций как средство противостоять корреляционному методу анализа.		3-4	4	2	–	5	
8	Генерация корреляционно-иммун-вых булевых функций. Наследова- ние свойств при сужениях.		5-6	4	4	–	5	
9	Нелинейность корреляционно-иммунных и устойчивых булевых функций.		7-8	4	4	–	5	
10	Почти совершенно нелинейные и почти бент-отображения. Теоретико-кодовый подход.		9-10	4	4	–	6	
11	Лавинные критерии и критерии распространения		11-12	4	4	–	6	
12	Применение криптографических свойств булевых функций при создании узлов замен		13-14	4	6	–	6	
13	Применение криптографических свойств булевых функций при разработке методов криптоанализа		15-16	4	6	–	6	
	Промежуточная аттестация							Экзамен
	ИТОГО в 6-м семестре			**32**	**32**	–	**44**	**36**
	ВСЕГО			**68**	**32**	–	**80**	**36**

Раздел 1. Арифметика конечных полей и полиномов

1. Алгебраические основы
2. Строение конечных полей
3. Полиномы над конечными полями

Раздел 2. Булевы функции. Числовые и метрические характеристики

1. Основные понятия и определения
2. Числовые и метрические характеристики
3. Групповая алгебра булевых функций

Раздел 3. Криптографические свойства булевых функций

Принципы построения криптографических функций:

- рассеивание;
- запутывание;
- перемешивание.

Раздел 4. Коды Рида-Маллера и их криптографические параметры

1. Общие свойства кодов Рида-Маллера
2. Алгоритм декодирования Рида
3. Коды Рида-Маллера первого, второго и третьего порядка

Раздел 5. Использование алгоритмов декодирования кодов Рида - Маллера при построении методов криптографического анализа..

Раздел 6. Нелинейность как мера криптографического качества. Максимально-нелинейные булевы функции

1. Максимально-нелинейные булевы функции и их свойства
2. Платовидные функции и частично определенные максимально-нелинейные булевы функции.

Раздел 7. Корреляционная иммунность и устойчивость булевых функций как средство противостоять корреляционному методу анализа.

Раздел 8. Генерация корреляционно-иммунвых булевых функций. Наследование свойств при сужениях.

Раздел 9. Нелинейность корреляционно-иммунвых и устойчивых булевых функций.

Раздел 10. Почти совершенно нелинейные и почти бент-отображения. Теоретико-кодовый подход.

1. Почти совершенно нелинейные и почти бент - отображения.
2. Теоретико-кодовый подход к изучению свойств APN- и AB-отображений.

Раздел 11. Лавинные критерии и критерии распространения

1. Лавинные критерии и критерии распространения.
2. Построение булевых функций, удовлетвояющих критерию распространения.
3. Глобальные лавинные характеристики булевых функций.

Раздел 12. Применение криптографических свойств булевых функций при создании узлов замен.

Раздел 13. Применение криптографических свойств булевых функций при разработке методов криптоанализа.

1. Алгоритм Берлекемпа-Месси. Линейная сложность.

2. Принципы статистического метода криптоанализа.
3. Принципы корреляционного метода криптоанализа.
4. Принципы линейного метода криптоанализа.
5. Принципы дифференциального метода криптоанализа.

План лабораторных занятий

На лабораторных занятиях студенты строят алгоритмы кодирования - декодирования, используя криптографические свойства булевых функций, в частности с использованием языков программирования C++, C#, Java, Python.

№ занятия	Тема	Задания для лабораторного практикума
1-3	Коды Рида-Маллера. Использование параметров RM (r,m) – кодов в криптологии	1
4-5	Выколотый RM^* (r,m) – код. Криптографические свойства RM^* (r,m) – кодов	2
6-10	Алгоритм декодирования Рида. .Его применение в криптоанализе.	3
11-12	Алгоритм декодирования Берлекемпа-Месси в виде регистра сдвига с линейной обратной связью.. Тестирование линейных рекуррентных последовательностей на случайность.	4
13-14	Линейный метод криптоанализа. Алгоритмы определения ключа методом линейного криптоанализа..	5
15-16	Статистический криптоанализ блочных шифров	6

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как промежуточное тестирование, перекрестный опрос, использование методических материалов сайта кафедры теоретических основ компьютерной безопасности и криптографии, технологии анализа конкретных ситуаций. В рамках учебного курса предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

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;
- занимаются научно-исследовательской работой.

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 (зачёт), 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
5	26	0	0	28	0	30	16	100
6	20	20	0	20	0	20	20	100

Программа оценивания учебной деятельности студента

5 семестр

Лекции

Оценивается посещаемость, активность – от 0 до 26 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Оценивается качество и количество выполненных работ, грамотность в оформлении, правильность выполнения – от 0 до 28 баллов.

Автоматизированное тестирование

Не предусмотрено

Другие виды учебной деятельности

Контрольная работа – от 0 до 30 баллов

Промежуточная аттестация

Проводится в форме теоретического зачета путем устного ответа на вопросы для проведения промежуточной аттестации (зачет)

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 13 до 16 баллов;

ответ на «хорошо» оценивается от 10 до 12 баллов;

ответ на «удовлетворительно» оценивается от 7 до 9 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 6 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за пятый семестр по дисциплине «Криптографические свойства булевых функций» составляет 100 баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Криптографические свойства булевых функций» в оценку «зачет».

30 баллов и более	«зачтено»
меньше 30 баллов	«не зачтено»

6 семестр

Лекции

Оценивается посещаемость, активность – от 0 до 20 баллов.

Лабораторные занятия

Самостоятельность при выполнении работы, грамотность в оформлении, Правильность выполнения и т.д. – от 0 до 20 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Оценивается качество и количество выполненных домашних работ, грамотность в оформлении, правильность выполнения и т.д. – от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрено

Другие виды учебной деятельности

Контрольная работа – от 0 до 20 баллов

Промежуточная аттестация

Проводится в форме теоретического экзамена путем устного ответа на вопросы для проведения промежуточной аттестации (экзамен).

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 16 до 20 баллов;

ответ на «хорошо» оценивается от 12 до 15 баллов;

ответ на «удовлетворительно» оценивается от 9 до 11 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 8 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за шестой семестр по дисциплине «Криптографические свойства булевых функций» составляет 100 баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Криптографические свойства булевых функций» в оценку (экзамен)

70–100 баллов	«отлично»
50–69 баллов	«хорошо»
30–40 баллов	«удовлетворительно»
0–29 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Глухов, М. М. Математическая логика. Дискретные функции. Теория алгоритмов : учеб. пособие [Электронный ресурс] / М. М. Глухов , А. Б. Шишков. - Москва : Лань, 2012. - 416 с. - ISBN 978-5-8114-1344-7 : Б. ц. URL: https://e.lanbook.com/book/4041 (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

б) дополнительная литература:

2) Гамова, А. Н. Сложность вычислений [Текст] : учебное пособие для студентов и магистров факультета компьютерных наук и информационных технологий / А. Н. Гамова ; Сарат. гос. ун-т им. Н. Г. Чернышевского. - Саратов : Издательство Саратовского университета, 2015. - 79, [4] с. : ил., табл. - Библиогр.: с. 81 (6 назв.). - ISBN 978-5-292-04343-0.

в) 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 выполнения лабораторных работ необходим компьютерный класс с установленным необходимым 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., доцент _____ А.Н. Гамова

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