Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 08.11.2023 10:02:15
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2021 г.

Рабочая программа дисциплины (с аннотацией)

Методы и средства криптографической защиты информации

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 4 курса ОФО

Составитель:
Никонов В. В.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области использования и проектирования и средств криптографической защиты информации, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

- получение базовых знаний и умений, связанных с основными понятиями средств криптографической защиты информации;
- получение теоретических знаний о роли и назначении различных криптографических систем;
- обучения студентов общим принципам и методам построения криптографических систем;

получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью средств криптографической защиты информации.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Языки программирования», «Алгебра», «Теоретико-числовые методы в криптографии».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Методы алгебраической геометрии в криптографии», «Криптографические протоколы», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 7 зачетные единицы, 252 академических часов, в том числе:

контактная аудиторная работа: лекции – 64 ч., в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 47 ч., практические занятия – 17 ч., в т.ч. практическая подготовка – 8 ч.;

самостоятельная работа: 124 ч., в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**ОПК-8.1** Применяет основы теории чисел в криптографии и других дисциплинах

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	**ОПК-9.1** Использует криптографические алгоритмы на практике при решении задач криптографическими методами
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**ОПК-10.1** Использует методы построения быстрых вычислительных алгоритмов алгебры и теории чисел
	ОПК-10.2 Разворачивает инфраструктуру открытых ключей для решения крипто-графических задач
	ОПК-10.4 Применяет различные подходы к разработке и анализу безопасности криптографических протоколов

5. Форма промежуточной аттестации и семестр прохождения – зачет в 7 семестре, экзамен в 8 семестре.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
Раздел 1. Основные понятия криптографии. Простейшие шифры	80	22	22	0	36
Раздел 2. Симметричные шифры	94	20	20	4	50
Раздел 3. Ассиметричные системы	86	22	22	4	38
ИТОГО	252	64	64	8	124

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1. Основные понятия криптографии. Простейшие шифры	Лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления
Раздел 2. Симметричные шифры		
Раздел 3. Ассиметричные системы	Лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

ОПК-8.1; ОПК-9.1; ОПК-10.1; ОПК-10.2; ОПК-10.4

Оценочные материалы для проведения текущей аттестации

Примерные задания для практических (семинарских) занятий

Раздел 1.

Задание 1 (ОПК-8.1; ОПК-9.1): Опишете алгебраическую модель шифра Цезаря.

Задание 2 (ОПК-8.1; ОПК-9.1): Расшифровать фразу, зашифрованную столбцовой перестановкой "ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО".

Задание 3 (ОПК-8.1; ОПК-9.1): Опишете алгебраическую модель шифра гаммирования.

Задание 4 (ОПК-8.1; ОПК-9.1): Написать реферат на тему «Квадрат Полибия».

Раздел 2.

Задание 1 (ОПК-10.1; ОПК-10.2; ОПК-10.4): Зашифровать по алгоритму DES-ECB сообщение, состоящее из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв шифруемого сообщения

Задание 2 (ОПК-10.1; ОПК-10.2; ОПК-10.4): Произвести кодирование текстового файла при помощи блочного алгоритма шифрования TEA (блочный алгоритм шифрования типа "Сеть Фейштеля"). Стандартное количество раундов сети Фейштеля равно 64 (32 цикла).

Раздел 3.

Задание 1 (ОПК-10.1; ОПК-10.2; ОПК-10.4): Известны значения модуля шифрования $N = 1517$, открытого ключа $e = 193$ и открытого текста «сон». Зашифровать сообщение по алгоритму RSA с помощью открытого ключа *(N, e)*.

Задание 2 (ОПК-10.1; ОПК-10.2; ОПК-10.4): Используемая хеш-функция – умножение. Построить статистическое распределение вероятности P(n)

формирования цепочек длины n для каждого из текстов при A = 0.618 и m = 512, 701, 1024, 1579, 2048.

Задание 3 (ОПК-10.1; ОПК-10.2; ОПК-10.4): Реализовать две хеш-функции: деление с остатком и умножение. Построить и сравнить статистические распределения вероятности P(n) формирования цепочек длины n для каждого из текстов. Параметры хеш-функций:

– деление с остатком: m = 1579;

– умножение: m = 1579, A = 0.618.

Оценочные материалы для проведения <u>промежуточной аттестации</u>

Проверяемые индикаторы достижения компетенций: ОПК-8.1; ОПК-9.1; ОПК-10.1; ОПК-10.2; ОПК-10.4

Каждый студент отвечает на вопросы теста и дает развернутый ответ на теоретический вопрос.

Примерные вопросы к зачету

1) Предмет криптографии, основные понятия. Общая схема симметричного шифрования.
2) История криптографии.
3) История русской криптографии.
4) Определение шифра, простейшие примеры.
5) Шифры замены, основные понятия.
6) Алгебраические модели шифров.
7) Вероятностные модели шифров.
8) Понятие блочного шифра.
9) Понятие итерированного шифра
10) Шифр Фейстеля, определение и свойства.
11) Алгоритм DES.
12) Режимы DES.
13) Теоретическая стойкость шифров.
14) Практическая стойкость.
15) ГОСТ 28147-89.

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения **зачета** необходимо ответить на вопросы теста и дать ответ на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется решение теста верное от 85 – 100% всех заданий.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Верно даны ответы на 70-84% тестовых заданий.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Правильные решения тестовых заданий составляют от 41-69%.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Правильные тестовые ответы составляют менее 40%.

Примерные вопросы к экзамену

1. Предмет криптографии, основные понятия. Общая схема симметричного шифрования.
2. История криптографии (Шифратор Джеферсона, Шифр Виженера, Диск Альберти, Шифры Порта, Шифры Кардано, Книжный шифр,).
3. История русской криптографии.
4. Определение шифра, простейшие примеры. Шифры замены, основные понятия.
5. Алгебраические модели шифров.
6. Вероятностные модели шифров.
7. Понятие блочного и итерированного шифров.
8. Шифр Фейстеля, определение и свойства.
9. Алгоритм DES.
10. Режимы и модификации DES.
11. Операторы, используемые при построении блочных шифров.
12. Требования к шифрам.
13. Теоретическая стойкость шифров.
14. Практическая стойкость.
15. Частотный криптоанализ.
16. Дифференциальный криптоанализ.
17. ГОСТ 28147-89.
18. CAST-256.
19. Rijndael.
20. RC5.
21. Blowfish.
22. Совершенные шифры.
23. Криптосистемы с открытым ключом.
24. Стойкость криптосистем с открытым ключом.
25. Крипто система RSA.
26. Параметры RSA.
27. Вероят. Шифр. СОК Блюма-Голдвассера.
28. Ранцевые криптоситемы.
29. DSA.
30. Генераторы ПСП и ПСЧ и их применение в криптографии.

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **5** баллов. Для получения **экзамена** необходимо ответить на вопросы теста и дать ответ на теоретический вопрос с суммарной оценкой не менее 2-х балов.

5 баллов:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется решение теста верное от 85 – 100% всех заданий.

4 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Верно даны ответы на 70-84% тестовых заданий.

3 балла:

Ответ демонстрирует знание и корректное использование терминологии. Правильные решения тестовых заданий составляют от 41-69%.

0-2 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Правильные тестовые ответы составляют менее 40%.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87998.html

Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092

б) Дополнительная литература:

Донгак, Ш. М. Криптография: Практикум : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163935

2) Программное обеспечение

Adobe Acrobat Reader DC - Russian	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Git version 2.5.2.2	бесплатно
Google Chrome	бесплатно

Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011;
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012;
Многофункциональный редактор ONLYOFFICE	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
MySQL Workbench 6.3 CE	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;
PostgreSQL 9.6	бесплатно
Python 3.4.3	бесплатно
Visual Studio 2010 Prerequisites - English	Акт на передачу прав №785 от 06.08.2021 г.
WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
WinPcap 4.1.3	бесплатно
Wireshark 2.0.0 (64-bit)	бесплатно
R studio	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.

2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.

3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.

4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.

5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозитарий ТвГУ http://eprints.tversu.ru

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

www.fstec.ru Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

http://www.intuit.ru/ Национальный Открытый Университете «ИНТУИТ»

http://www.cisco.com/c/ru_ru/index.html Сетевой Академии Cisco

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения распределяются между 4 модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	50	18	12	20
2	50	18	12	20
3	30	15	-	15
4	30	15	-	15

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:

https://tversu.ru/sveden/files/204-R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория. Математический кабинет № 213 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Столы, стулья, переносной ноутбук, проектор	Adobe Acrobat Reader DC - Russian-бесплатно; Cadence SPB/OrCAD 16.6-Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009; Git version 2.5.2.2-бесплатно; Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus 1.4.0-бесплатно; Mathcad 15 M010-Акт предоставления прав ИС00000027 от 16.09.2011; MATLAB R2012b-Акт предоставления прав № Us000311 от 25.09.2012; Многофункциональный редактор ONLYOFFICE -бесплатно;
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, Учебная аудитория № 203 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)	Столы, стулья, переносной ноутбук, проектор	ОС Linux Ubuntu бесплатное ПО-бесплатно; Microsoft Web Deploy 3.5-бесплатно; MiKTeX 2.9-бесплатно; MSXML 4.0 SP2 Parser and SDK-бесплатно; MySQL Workbench 6.3 CE-бесплатно; NetBeans IDE 8.0.2-бесплатно; Notepad++-бесплатно; Origin 8.1 Sr2-договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд» ; PostgreSQL 9.6 -бесплатно; Python 3.4.3-бесплатно; Visual Studio 2010 Prerequisites - English-Акт на передачу прав №785 от 06.08.2021 г. ; WCF RIA Services V1.0 SP2-бесплатно; WinDjView 2.1-бесплатно; WinPcap 4.1.3-бесплатно; Wireshark 2.0.0 (64-bit)-бесплатно; R studio-бесплатно.

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы.	Протокол № 11 от 26.06.2013
2.	VII. Методические указания для обучающихся по освоению дисциплины	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 10 от 24.06.2014
3.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
4.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
5.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
6.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2018
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
8.	V. Учебно-методическое и информационное	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023

	обеспечение дисциплины		