

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 08.11.2023 10:01:43
Уникальный программный ключ:
69e375c64f7e9754e8870e7b4fc2ad11bf35f08

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

Утверждаю:
Руководитель ООП
Н.А. Семькина


« 4 » 09 
МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
УНИВЕРСИТЕТ

Рабочая программа дисциплины (с аннотацией)

Криптографические протоколы

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»


Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:

Семькина Н. А.



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 проектирования и построения криптографических протоколов, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

- 1) получение базовых знаний и умений, связанных с основными понятиями криптографических протоколов;
- 2) формирование навыков решения прикладных задач, решаемых с помощью криптопротоколов и умения применять различные методы и алгоритмы построения криптографических протоколов.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Организационное и правовое обеспечение информационной безопасности», «Криптографические методы защиты информации», «Теоретико-числовые методы в криптографии».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 ч., в т.ч. практическая подготовка – 0 часов;

практические занятия – 34 ч., в т.ч. практическая подготовка – 7 ч.;

самостоятельная работа: 40 ч.

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-9. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей | ОПК-9.2 Проводит анализ криптографических протоколов, в том числе с использованием автоматизированных средств |
| ОПК-10. Способен анализировать тенденции развития методов и средств | ОПК-10. Разворачивает инфраструктуру открытых ключей для решения криптографических задач |

| | |
|--|--|
| криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности | ОПК-10.4 Применяет различные подходы к разработке и анализу безопасности криптографических протоколов |
|--|--|

5. Форма промежуточной аттестации и семестр прохождения – зачет в 9 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 | |
| 1 Раздел Основные понятия | 20 | 4 | 4 | 0 | 12 |
| 2 Раздел Криптографические протоколы | 78 | 30 | 23 | 7 | 28 |
| ИТОГО | 108 | 34 | 27 | 7 | 40 |

III. Образовательные технологии

| Учебная программа – наименование разделов и тем | Вид занятия | Образовательные технологии |
|---|----------------------------|--|
| 1 Раздел. Основные понятия | лекция практическое | Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция. |

| | | |
|--|----------------------------|--|
| 2 Раздел Криптографические протоколы | лекция практическое | Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления |
|--|----------------------------|--|

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения текущей аттестации

Примерные задания для практических (семинарских) занятий

1 Раздел.

Задание 1 (ОПК-10.4): Приведите классификацию протоколов.

Задание 2 (ОПК-10.4): Определить тип протокола по решаемой задаче.

2 Раздел.

Задание 1 (ОПК-9.2; ОПК-10.2): Опишите схему протокола генерации ключей Диффи Хелмана.

Задание 2 (ОПК-9.2; ОПК-10.2): Модифицируйте протокол обеспечения свойства конфиденциальности и целостности передачи сообщений для предварительного обмена сессионным ключом симметричной схемы шифрования.

Оценочные материалы для проведения промежуточной аттестации

Проверяемые индикаторы достижения компетенций: ОПК-9.2; ОПК-10.2; ОПК-10.4

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к зачету

1. Понятие и назначение криптографических протоколов.
2. Классификация протоколов (по видам, по выполняемой задаче, по способу генерации ключевой информации)
3. Атаки на протоколы
4. Протоколы идентификации
5. Протоколы аутентификации
6. Парольные схемы разграничения доступа.
7. Протоколы генерации и распределения ключей
8. Рекомендации X.509
9. Протоколы разделения секрета (общая схема)
10. (n, k) пороговые схемы разделения секрета (идеальные СРС, способы их математического описания)
11. Схема Шамира разделения секрета
12. Протоколы с нулевым разглашением*
13. Д-во нулевого разглашения*
14. Протоколы игры в покер.*

15. Однонаправленные функции
16. Хеш-функции
17. Неоспоримые цифровые подписи
18. Управление ключами

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 выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 2-х баллов.

3 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется полное верное решение задачи, включающее правильный ответ.

2 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Дано верное решение задачи, но в решении имеются неверные записи И/ИЛИ арифметические ошибки.

1 балл:

Ответ демонстрирует знание и корректное использование терминологии. Решение содержит фактические ошибки, не искажающие общего смысла.

0 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Решение не дано ИЛИ дано неверное решение.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Лапони́на, О.Р. Криптографические основы безопасности / О.Р. Лапони́на. - 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>.

Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1716-6>. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1899016>

б) Дополнительная литература:

Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2021. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469758>

Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие для СПО / Б. А. Фороузан ; под редакцией А. Н. Берлина. — Саратов : Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102192.html>

2) Программное обеспечение

| | |
|--|---|
| Adobe Acrobat Reader DC - Russian | бесплатно Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009 |
| Cadence SPB/OrCAD 16.6 | бесплатно |
| 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 Акт предоставления прав ИС00000027 от 16.09.2011; Акт предоставления прав № Us000311 от 25.09.2012; |
| Mathcad 15 M010 | бесплатно |
| MATLAB R2012b | бесплатно |
| 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 договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»; |
| Origin 8.1 Sr2 | бесплатно |
| 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. Репозиторий ТвГУ <http://eprints.tversu.ru>

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

<https://cyberleninka.ru/> научная электронная библиотека «Киберленинка».
www.fstec.ru Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

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 оценивается в 100 баллов, которые распределяются между двумя 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 |

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 |
|--|---|--|
| <p>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)</p> <p>Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации,</p> | <p>Столы, стулья, переносной ноутбук, проектор</p> <p>Столы, стулья, переносной ноутбук, проектор</p> | <p>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 IC00000027 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» ;</p> |

| | | |
|--|---|--|
| <p>Учебная аудитория № 203 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)</p> <p>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 № 314 (Корпус 3, 170002, Тверская обл., г.Тверь, пер. Садовый, дом 35)</p> | <p>Стол, стулья, переносной ноутбук, проектор</p> | <p>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.</p> <p>Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО- бесплатно</p> |
|--|---|--|

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 обеспечение дисциплины | Обновление списков ПО. Обновление ссылок из ЭБС. | Протокол № 1 от 1.09.2023 |