Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *ФПМ*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
21.05.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации

Направление подготовки *10.03.01 Информационная безопасность*

Профиль подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
5	**144 / 4**	**32**		**48**	**5,2**	**0,35**	**85,55**	**22,8**	**Экз.(35,65)**
Итого	**144 / 4**	**32**		**48**	**5,2**	**0,35**	**85,55**	**22,8**	**35,65**

Муром, 2024 г.

1. Цель освоения дисциплины

Цель дисциплины: формирование у студентов основных навыков по разработке и использованию симметричных и асимметричных криптографических алгоритмов.

Задачи дисциплины: дать обучаемому арсенал типовых приемов для решения задач, возникающих при разработке и использовании криптографических алгоритмов; приобретение студентами умений пользоваться основными понятиями, законами и моделями криптографии, основными криптографическими методами защиты информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Методы и средства криптографической защиты информации» является дисциплиной по направлению 10.03.01 «Информационная безопасность» (бакалавриат). Дисциплина «Методы и средства криптографической защиты информации» базируется на знаниях, полученных в рамках изучения следующих дисциплин: «Теория информации», «Математика».

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.2 Применяет методы и средства криптографической защиты информации для решения задач профессиональной деятельности	Знать методы и приемы формализации и типовые алгоритмы решения прикладных задач (ОПК-9.2) Уметь использовать существующие алгоритмы, языки и системы программирования для решения специальных задач (ОПК-9.2)	тест

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Симметричные криптосистемы	5	10		16					3	тестирование
2	Асимметричные криптосистемы	5	8		8					4	тестирование
3	Проверка подлинности	5	6		12					4	тестирование
4	Электронная цифровая подпись	5	8		12					11,8	тестирование
Всего за семестр		144	32		48			5,2	0,35	22,8	Экз.(35,65)
Итого		144	32		48			5,2	0,35	22,8	35,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 5

Раздел 1. Симметричные криптосистемы

Лекция 1.

Принципы криптографической защиты информации (2 часа).

Лекция 2.

Традиционные симметричные криптосистемы (2 часа).

Лекция 3.

Шифры перестановки (2 часа).

Лекция 4.

Шифры замены (2 часа).

Лекция 5.

Традиционные симметричные криптосистемы (2 часа).

Раздел 2. Асимметричные криптосистемы

Лекция 6.

Шифры сложной замены (2 часа).

Лекция 7.

Шифрование гаммированием (2 часа).

Лекция 8.

Современные симметричные криптосистемы (2 часа).

Лекция 9.

Система DES (2 часа).

Раздел 3. Проверка подлинности

Лекция 10.

Система IDEA (2 часа).

Лекция 11.

Современные асимметричные криптосистемы (2 часа).

Лекция 12.

Идентификация и проверка подлинности (2 часа).

Раздел 4. Электронная цифровая подпись

Лекция 13.

Протоколы с нулевой передачей данных (2 часа).

Лекция 14.

Схема идентификации Гиллоу-Куискуотера (2 часа).

Лекция 15.

Электронная цифровая подпись. Алгоритмы цифровой подписи RSA, Эль Гамаля (2 часа).

Лекция 16.

Электронная цифровая подпись. Алгоритмы цифровой подписи DSA, отечественный стандарт (2 часа).

4.1.2.2. Перечень практических занятий

Не планируется.

4.1.2.3. Перечень лабораторных работ

Семестр 5

Раздел 1. Симметричные криптосистемы

Лабораторная 1.

Принципы криптографической защиты информации (4 часа).

Лабораторная 2.

Традиционные симметричные криптосистемы (4 часа).

Лабораторная 3.

Шифры перестановки. Шифры замены (4 часа).

Лабораторная 4.

Традиционные симметричные криптосистемы (4 часа).

Раздел 2. Асимметричные криптосистемы

Лабораторная 5.

Шифры сложной замены.Шифрование гаммированием (4 часа).

Лабораторная 6.

Современные симметричные криптосистемы (4 часа).

Раздел 3. Проверка подлинности

Лабораторная 7.

Система DES. Система IDEA (4 часа).

Лабораторная 8.

Современные асимметричные криптосистемы (4 часа).

Лабораторная 9.

Идентификация и проверка подлинности. Протоколы с нулевой передачей данных (4 часа).

Раздел 4. Электронная цифровая подпись

Лабораторная 10.

Схема идентификации Гиллоу-Куискуотера (4 часа).

Лабораторная 11.

Электронная цифровая подпись. Алгоритмы цифровой подписи RSA, Эль Гамаля (4 часа).

Лабораторная 12.

Электронная цифровая подпись. Алгоритмы цифровой подписи DSA, отечественный стандарт (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Обеспечения информационной безопасности на законодательном уровне.
2. Теоретические вопросы обеспечения информационной безопасности.
3. Обеспечения информационной безопасности на административном уровне.
4. Обеспечения информационной безопасности на процедурном уровне.
5. Обеспечения информационной безопасности на программно-техническом уровне.
6. Основные инструментальные средства поддержки разработки политики информационной безопасности.
7. Основные инструментальные средства анализа рисков.
8. Основные экономические аспекты обеспечения информационной безопасности.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении работ применяется имитационный или симуляционный подход. Шаги решения задач студентам демонстрируются при помощи мультимедийной техники. В дальнейшем студенты самостоятельно решают аналогичные задания.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. - https://www.iprbookshop.ru/89455.html

2. Жиль, Земор Курс криптографии / Земор Жиль ; перевод В. В. Шуликовская. — Москва, Ижевск : Регулярная и хаотическая динамика, Институт компьютерных исследований, 2019. — 256 c. - https://www.iprbookshop.ru/91941.html

3. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 c. - https://www.iprbookshop.ru/102017.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Майстренко, Н. В. Основы теории информации и криптографии : учебное пособие / Н. В. Майстренко, А. В. Майстренко. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2018. — 81 c. - https://www.iprbookshop.ru/94362.html

2. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2016. — 256 c. - https://www.iprbookshop.ru/90248.html

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

yandex.ru

google.com

Программное обеспечение:

Mathcad Education – University Edition (100 pack) v.15 (Государственный контракт №1 от 10.01.2012 года)

Google Chrome (Лицензионное соглашение Google)

Mozilla Firefox (MPL)

Free Commander XE (Лицензионное соглашение FreeCommander)

РЕД ОС (Соглашение №140/05-21У от 18.05.2021 года о сотрудничестве в области науки, развития инновационной деятельности)

Oracle VirtualBox (GNU GPL)

OpenStego (GNU GPL)

gpg4win (GNU GPL)

Sysinternals Suite (Лицензионное соглашение Sysinternals)

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Pascal PascalABC.NET (GNU Lesser General Public License v.3)

Apache OpenOffice (Apache License)

Lazarus (GNU GPL, GNU LGPL)

Microsoft Access (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft Visio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft Project (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Microsoft SQL Server (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru
mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория технической защиты информации

Подавитель телефона Троян Х6-В; генератор шума Штора-1; блок помех генераторный SEL SP-157G с вибрационным преобразователем и колонкой; комбинированное устройство защиты от утечки информации ЛГШ-513; детектор жучков Баг Хантер «Профессионал»; сканер отпечатков пальцев Eikon; сканер глаза EyeLock; офисный электронный замок EM-Marine, PROXIMITY (125kHz) AYT 930-6-DI; дубликатор KeyMaster PRO 4 RF (с комплектом ключей); аппаратно-программный модуль доверенной загрузки "Соболь" с сертификатом ФСТЭК; квадрокоптер DJI Phantom 3 Professional (в комплекте дисплей-планшет Samsung Galaxy Tab 4 10.1 SM-T530 16Gb; пульт управления и рюкзак); камера D-Link DCS-930L; IP камера Beward BD2570; анализатор спектра; система видеонаблюдения Orient; видеопроектор NEC Projector V260XG (переносной); ноутбук ASUS (переносной); экран мобильный Classic Solution Premier Vela Express; ПК ПЭВМ «Хопер» -2 шт.; ПК - 5 шт.;ПК:(mATX350W;IC2,8;1Gb;DVD-R;3,5"S775PCI-E;К-ра PS/2;М/Опт.PS/2;19"TFT)-1 шт.. Доступ к сети Интернет.

Защищаемое помещение

Помещение оборудовано для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений , составляющих государственную тайну

Библиотека литературы ограниченного доступа

Помещение оборудовано для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторная работа проводятся в компьютерном классе. Обучающиеся выполняют индивидуальную задачу компьютерного моделирования в соответствии с заданием на лабораторную работу. Полученные результаты исследований сводятся в работе, которая проверяется. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы приведены в методических указаниях, размещенных на информационно-образовательном портале института.: https://www.mivlgu.ru/iop/course/view.php?id=3307

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *10.03.01 Информационная безопасность* и профилю подготовки *Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)*
Рабочую программу составил *к.т.н., доцент, Штыков Р. А.*_____

Программа рассмотрена и одобрена на заседании кафедры *ФПМ*

протокол № 21 от 02.05.2024 года.
Заведующий кафедрой *ФПМ* _____*Орлов А.А.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 9 от 17.05.2024 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине

Методы и средства криптографической защиты информации

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Вопросы к экзамену:

1 Основные угрозы безопасности АСОИ
2 Обеспечение безопасности АСОИ
3 Традиционные симметричные криптосистемы
4 Шифры перестановки
5 Шифры простой замены
6 Шифры сложной замены
7 Шифрование методом гаммирования
8 Методы генерации псевдослучайных последовательностей чисел
9 Идентификация и проверка подлинности
10 Идентификация и механизмы подтверждения подлинности пользователя
11 Взаимная проверка подлинности пользователе
12 Протоколы идентификации с нулевой передачей знаний
13 Проблема аутентификации данных и электронная цифровая подпись
14 Однонаправленные хэш-функции
15 Алгоритм безопасного хеширования SHA
16 Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
17 Отечественный стандарт хэш-функции
18 Алгоритмы электронной цифровой подписи
19 Особенности функционирования межсетевых экранов
20 Основные компоненты межсетевых экранов
21 Основные схемы сетевой защиты на базе межсетевых экранов
22 Применение межсетевых экранов для организации виртуальных корпоративных сетей
23 Программные методы защиты
24 Признаки личности в системах защиты информации
25 Устройства для снятия биометрических характеристик
26 Системы распознавания личности
27 Программы с потенциально опасными последствиями
28 Вирус
29 Люк
30 Троянский конь
31 Правовые аспекты информационной безопасности

Темы докладов:

1. Алгоритм шифрования DES
2. Алгоритм шифрования IDEA
3. Алгоритм шифрования ГОСТ 28147-89
4. Алгоритм шифрования RSA
5. Алгоритм шифрования Эль Гамаля
6. Стандарт шифрования AES
7. Алгоритм шифрования PGP
8. Алгоритм шифрования CAST
9. Алгоритм шифрования Lucipher
10. Алгоритм шифрования FEAL-1
11. Алгоритм шифрования B-Crypt
12. Алгоритм шифрования Диффи-Хеллмана DH
13. Алгоритм шифрования Camellia

14. Алгоритм шифрования Twofish
15. Алгоритм шифрования Blowfish
16. Алгоритм шифрования RC4
17. Алгоритм шифрования ГОСТ Р 34.10-2001
18. Алгоритм хэш-функций MD4
19. Алгоритм хэш-функций SHA-1

1. Зашифровать произвольное сообщение методом простой перестановки
2. Зашифровать произвольное сообщение с помощью шифрующих таблиц
3. Зашифровать произвольное сообщение с помощью простой замены
4. Зашифровать произвольное сообщение методом гаммирования
5. Зашифровать произвольное сообщение с помощью схемы идентификации с нулевой передачей данных
6. Зашифровать произвольное сообщение с помощью схемы идентификации Гиллоу-Куискуотера
7. Зашифровать произвольное сообщение с помощью схемы аутентификации Эль Гамаля
8. Зашифровать произвольное сообщение с помощью схемы аутентификации Шнорра
9. Зашифровать произвольное сообщение с помощью кодов Хэмминга

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	тесты	15
Рейтинг-контроль 2	тесты	15
Рейтинг-контроль 3	тесты	15
Посещение занятий студентом		5
Дополнительные баллы (бонусы)		5
Выполнение семестрового плана самостоятельной работы		5

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

Пример заданий для выполнения тестов:

1) Верны ли утверждения?

A) Алгоритм шифрования DES состоит из чередующейся последовательности перестановок и подстановок.

B) Алгоритм шифрования DES осуществляет шифрование 20-битных блоков с помощью 20-битного ключа.

Подберите правильный ответ.

A – да, B - нет
A – да, B - да
A – нет, B - нет
A – нет, B - да

2)Верны ли утверждения?

A) Алгоритм шифрования 3-DES используется в ситуациях, когда надежность алгоритма DES считается недостаточной.

B) Алгоритм шифрования 3-DES имеет меньшую криптостойкость, чем DES.

Подберите правильный ответ.

A – да, B - нет
A – да, B - да
A – нет, B - нет
A – нет, B - да

3)Верны ли утверждения?

A) Алгоритм шифрования ГОСТ 28147-89 предназначен только для аппаратной реализации.

B) Алгоритм шифрования ГОСТ 28147-89 представляет собой 64-битный блочный алгоритм с 256-битным ключом.

Подберите правильный ответ.

A – нет, B - да
A – да, B - нет
A – да, B - да
A – нет, B - нет

4)На рисунке представлена обобщенная схема шифрования в алгоритме _____.

DES
RSA
ГОСТ 28147-89
MD5

5)На рисунке представлена обобщенная схема шифрования в алгоритме _____.

ГОСТ 28147-89
RSA
DES
MD5

Методические материалы, характеризующие процедуры оценивания

Индивидуальный семестровый рейтинг студента формируется на основе действующего в ВУЗе Положения "О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся".

В течение семестра студент получает баллы успеваемости за выполнение всех видов учебных поручений: посещение лекций, выполнение практических работ. Зачет выставляется в случае, если итоговая оценка студента составляет не менее 50 баллов.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их	***Высокий уровень***

		выполнения оценено числом баллов, близким к максимальному	
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

Примеры заданий в тестовой форме для контроля остаточных знаний:

1) Соотнесите размер блока и ключа соответствующему алгоритму шифрования. Выберите верную последовательность:

- размер блока 64 бит, ключ 256 бит
- размер блока 64 бит, ключ 128 бит
- размер блока 128 бит, ключ 128/192/256 бит
- размер блока 128 бит, ключ 256 бит

2) Найти соответствие метода шифрования и его длины ключа:

- Кузнечик
- RC-5
- DES

3) Что такое пространство ключей k?

- длина ключа
- нет правильного ответа
- набор возможных значений ключа

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?courseid=2936&cat=31182%2C100062

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.