Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования

**Пермский национальный исследовательский
политехнический университет**

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Н.В.Лобов
« 11 » декабря 20 20 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Криптографические методы защиты информации
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 216 (6)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем
(наименование образовательной программы)

Пермь 2020

1. Общие положения

1.1. Цели и задачи дисциплины

Изучение дисциплины «Криптографические методы защиты информации» имеет целью овладение основным математическим аппаратом исследования формализованных структур, формирование логического и системного мышления студентов. Целью преподавания дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

В прогрессе изучения дисциплины студент осваивает следующие заданные дисциплинарные компетенции:

1) способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;

2) способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

3) способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.

Задачи дисциплины – дать основы:

1) системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;

2) принципов синтеза и анализа шифров;

3) математических методов, используемых в криптоанализе.

1.2. Изучаемые объекты дисциплины

1) алгоритмы поточного шифрования;
2) алгоритмы блочного шифрования;
3) алгоритмы вероятностного шифрования;
4) криптографические протоколы.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-9	ИД-1ОПК-9	Знать – классические системы шифрования. Знать – системы шифрования с симметричным ключом. Знать – асимметрические системы шифрования. Уметь – использовать основные математические методы, исполь-зуемые в анализе типовых криптографических алгоритмов. Уметь – формулировать постановки задач криптоанализа и находить подходы к их решению. Владеть – методами криптоанализа простейших шифров.	Знает основные характеристики сигналов электросвязи, спектры и виды модуляции; способы кодирования информации; основные задачи и понятия криптографии; модели шифров и математические методы их исследования; технические средства защиты информации	Контрольная работа
ОПК-9	ИД-2ОПК-9	Знать - основные принципы построения криптоалгоритмов. Знать – основные методы дешифрования; стандарты систем шифрования. Знать – теорема Кука, NP-полнота. Знать – вероятностное шифрование. Уметь – строить современные шифрсистемы. Уметь – формулировать постановки задач криптоанализа и нахо-дить подходы к их решению Владеть – криптографической терминологией; методами крипто-анализа простейших шифров; современной научно-технической литературой в области криптографической защиты	Умеет анализировать основные характеристики и возможности телекоммуникационных систем; применять математические методы исследования моделей шифров; использовать типовые криптографические алгоритмы и технические средства защиты информации;	Контрольная работа
ОПК-9	ИД-3ОПК-9	Знать - основные принципы построения криптоалгоритмов. Знать – основные методы	Владеет методами и средствами технической защиты информации	Коллоквиум

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		дешифрования; стандарты систем шифрования. Знать – теорема Кука, NP-полнота. Знать – вероятностное шифрование. Уметь – строить современные шифрсистемы. Уметь – формулировать постановки задач криптоанализа и находить подходы к их решению Владеть – криптографической терминологией; методами крипто-анализа простейших шифров; современной научно-технической литературой в области криптографической защиты		

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	64	64
- лекции (Л)	28	28
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	32	32
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	116	116
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	216	216

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
6-й семестр				
Введение в криптографию	4	0	4	10
Тема 1. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Тема 2. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Тема 3. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.				
Основные классы шифров и их свойства	4	0	4	15
Тема 4. ШИФРЫ ПЕРЕСТАНОВКИ. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Тема 5. ШИФРЫ ЗАМЕНЫ. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). Тема 6. ПОТОЧНЫЕ ШИФРЫ. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Надежность шифров	3	0	4	18
Тема 7. ТЕОРИЯ К.ШЕННОНА. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности. Тема 8. ИМИТОСТОЙКОСТЬ ШИФРОВ. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования. Тема 9. ПОМЕХОУСТОЙЧИВОСТЬ ШИФРОВ. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.				
Принципы построения криптографических алгоритмов	10	0	10	35
Тема 10. РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ. Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров. Тема 11. ВОПРОСЫ СИНТЕЗА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ. Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Проверка построенной последовательности на случайность. Тема 12. Методы усложнения последовательностей псевдослучайных чисел. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнений последовательности. Различные способы задания дискретных функций. Тема 13. Методы анализа криптографических алгоритмов. Понятие криптоатаки. Виды				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
криптоатак. Классификация криптоатак. Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уравнений шифрования, бесключевые методы. Особенности криптоанализа блочных шифров. Криптографические параметры узлов и блоков шифраторов. Основные принципы построения криптоалгоритмов (выбор группы шифра, параметров ПСП, параметров функции усложнения) Тема 14. СИСТЕМЫ ШИФРОВАНИЯ С ОТКРЫТЫМИ КЛЮЧАМИ. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Секретные характеристики в системах с открытым ключом. Преимущества ассиметричных систем шифрования. Вероятностное шифрование.				
Криптографические протоколы	5	0	8	35
Тема 15. МОДЕЛИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ. Сложность криптографических алгоритмов (теорема Кука, NP-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. Тема 16 ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения. Тема 17. Протоколы установления подлинности. Парольные системы разграничения доступа и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и ЭЦП. Тема 18. Протоколы управления ключами. Протоколы сертификации ключей. Протоколы распределения ключей. Открытое распределение ключей Диффи-Хэлмана и его модификация. Протоколы Oakley, ISAKMP.				
Заключение	2	0	2	3
ЗАКЛЮЧЕНИЕ. Проблемы и перспективы исследований в области современной криптографии. Квантовая криптография. Стеганография. Нерешенные задачи. Итоги изучения курса.				
ИТОГО по 6-му семестру	28	0	32	116
ИТОГО по дисциплине	28	0	32	116

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Простейшие шифры и их свойства. Типы атак. Атаки, в основе которых лежит парадокс задачи о днях рождения. Двусторонние атаки. Уровень безопасности. Освоение процессов зашифрования и расшифрования для простейших шифров.
2	Частотные свойства осмысленных сообщений.
3	Криптоанализ шифра однобуквенной простой замены.
4	Криптоанализ шифра «решетка Кардано».
5	Вскрытие шифра Вернама при повторном использовании ключа. Криптоанализ шифра Виженера.
6	Шифры, основанные на алгоритме Файстеля. Функция раунда. Реализация функции раунда. Традиционные симметричные блоч-ные шифры.
7	Расчет метода встречных атак.
8	Канальное и сквозное шифрование. Управление секретными клю-чами. Криптоанализ рассмотренных алгоритмов симметричного шифрования. Размер ключа.
9	Цифровые подписи. Управление ключами. Взлом ключа. Согласо-вание ключей с помощью пароля. Защищенные функции хэширо-вания. HMAC. SHA. MD5. RIPEMD. UMAC.Криптография с от-крытым ключом.
10	Обмен ключами. Схема Диффи-Хеллмана. Протокол обмена клю-чами Oakley, ISAKMP.
11	Серверы ключей. Система Kerberos. Сервис аутентификации X.509.
12	Стохастическое преобразование информации. R-блоки. Гаммирование. Вероятностное шифрование.
13	Изучение системы PGP.

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Пример реализации защиты информации на предприятии (представить свой вариант ПО позволяющего защитить секретные данные от несанк-ционированного копирования, в качестве варианта использовать пред-приятие, работающее на 1С, не исключать использование копирования информации на электронные носители и выход в Интернет).
2	Брандмауэры.
3	Троянские кони. Принцип действия. Защита
4	Черви. Принцип действия. Защита
5	Криптосистемы с открытым ключом (ассиметричные).
6	Свойства конструкции безусловно стойких шифров, названных К.Шенноном совершенными, по отношению к различным криптоатакам.
7	Квантовая криптография.
8	Цифровая подпись. Реализация. Плюсы и минусы ее использования.

№ п.п.	Наименование темы курсовых проектов/работ
9	Вероятностное шифрование.
10	Криптографическое сжатие. Алгоритмы сжатия данных. Арифметическое кодирование.
11	Беспроводные сети. Атаки. Механизмы обеспечения защиты ин-формации. Протокол WEP.
12	Последние разработки в криптографии (разбор современнейших подходов к шифрованию, исключая квантовое).
13	Модель обработки сообщений и защиты пользователя. Управление доступом на основе представлений.
14	Режим сцепления шифрованных блоков. Электронная шифровальная книга.

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Данилов А. Н. Математические основы криптологии и криптографические методы и средства обеспечения информационной безопасности : учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин. - Пермь: Изд-во ПГТУ, 2008.	64
2	Данилов А. Н. Практикум по курсам Математические основы криптологии и Криптографические методы и средства обеспечения информационной безопасности : учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин. - Пермь: Изд-во ПГТУ, 2008.	59
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Гашков С. Б. Криптографические методы защиты информации : учебное пособие для вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва: Академия, 2010.	8
2	Рябко Б. Я. Криптографические методы защиты информации : учебное пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия-Телеком, 2015.	25
3	Смарт Н. Криптография : пер. с англ. / Н. Смарт. - Москва: Техносфера, 2006.	5
2.2. Периодические издания		
1	Вестник УРФО. Безопасность в информационной сфере	10
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
1	Уильям Столлингс "Основы защиты сетей"	5

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	АЛГОРИТМЫ БЛОЧНОЙ КРИПТОГРАФИИ	https://elar.urfu.ru/bitstream/10995/28062/1/978-5-7996-0934-4.pdf	сеть Интернет; свободный доступ
Дополнительная литература	Майстренко, Н. В. Основы теории информации и криптографии : учебное пособие / Н. В. Майстренко, А. В. Майстренко. - Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2018.	http://elib.pstu.ru/Record/iprbooks94362	локальная сеть; авторизованный доступ

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Основная литература	Прохорова О. В. Информационная безопасность и защита информации / Прохорова О. В. - Санкт-Петербург: Лань, 2020.	http://elib.pstu.ru/Record/lanRU-LAN-BOOK-133924	локальная сеть; авторизованный доступ
Учебно-методическое обеспечение самостоятельной работы студентов	Данилов А. Н. Практикум по курсам "Математические основы криптологии" и "Криптографические методы и средства обеспечения информационной безопасности" : учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин. - Пермь: Изд-во ПГТУ, 2008.	http://elib.pstu.ru/Record/RUPNRPUelib2790	локальная сеть; свободный доступ
Учебно-методическое обеспечение самостоятельной работы студентов	Никифоров С. Н. Методы защиты информации. Шифрование данных : учебное пособие / Никифоров С. Н. - Санкт-Петербург: Лань, 2019.	http://elib.pstu.ru/Record/lanRU-LAN-BOOK-114699	локальная сеть; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	MATLAB 7.9 + Simulink 7.4 Academic, ПНИПУ 2009 г.
Прикладное программное обеспечение общего назначения	Microsoft Office Visio Professional 2016 (подп. Azure Dev Tools for Teaching)
Прикладное программное обеспечение общего назначения	PGP v.8 (Freeware)

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных Web of Science	http://www.webofscience.com/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/

Наименование	Ссылка на информационный ресурс
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	проектор	1
Лекция	доска	1
Лекция	компьютер	1
Лекция	проектор	1
Практическое занятие	доска	1

8. Фонд оценочных средств дисциплины

Описан в отдельном документе