ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 03.11.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.23 Криптографические методы защиты информации
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 03.11.2021

А. Н. Соколов

Разработчик программы,
д.физ.-мат.н., доц., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зюляркина Н. Д.
Пользователь: ziuliarkinand
Дата подписания: 03.11.2021

Н. Д. Зюляркина

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является формирование у студентов общих представлений о содержании криптографических методов защиты информации и о подходах к оценке эффективности таких методов. Задачи дисциплины: дать представление об информационной безопасности, как сфере профессиональной деятельности; раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии; ознакомить с основными видами шифров; ознакомить с современными стандартами криптографической защиты; дать представление об атаках на криптографические системы.

Краткое содержание дисциплины

В рамках данной дисциплины исследуются основные типы шифров, проводится анализ их криптостойкости, изучаются основные типы атак и методы противодействия им.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать:криптографические стандарты и их использование в информационных системах
	Уметь:применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
	Владеть:навыками использования типовых криптографических алго
ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать:требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; принципы построения криптографических алгоритмов
	Уметь:эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах
	Владеть:криптографической терминологией
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать:требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры
	Уметь:эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах
	Владеть:навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров
ПК-14 способностью проводить контрольные проверки работоспособности применяемых	Знать:требования к шифрам и основные характеристики шифров

программно-аппаратных, криптографических и технических средств защиты информации	Уметь:уметь пользоваться научно-технической литературой в области криптографии
	Владеть:криптографической терминологией; навыками использования ПЭВМ в анализе простейших шифров
ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	Знать:основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки; модели шифров и математические методы их исследования
	Уметь:использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки; применять математические методы исследования моделей шифров
	Владеть:навыками использования ЭВМ в анализе простейших шифров; навыками математического моделирования в криптографии

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.33 Математические основы криптологии	Б.1.34 Криптографические протоколы, Б.1.30.01 Разработка защищенных автоматизированных систем

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.33 Математические основы криптологии	Знать основные алгебраические структуры-группы, кольца, поля. Уметь производить вычисления в группах, конечных полях и кольцах вычетов. Владеть навыками программирования в пакете GAP.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32

Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	60	60
Подготовка к практическим занятиям. Выполнение домашних заданий	36	20
Подготовка к экзамену	12	12
Написание программ, реализующих заданные криптоалгоритмы	12	12
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение в криптографию	4	2	2	0
2	Криптосистемы с секретным ключом	14	4	10	0
3	Криптосистемы с открытым ключом	16	4	12	0
4	Надежность шифров	2	2	0	0
5	Алгоритмы цифровой подписи	10	2	8	0
6	Современные стандарты шифрования	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
2	1	Исторический обзор. Открытые сообщения и их характери-стики. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. Основные задачи и понятия криптографииПеречень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы.	2
4	2	Поточные шифры замены Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, анализ шифра Виженера. Шифры перестановки Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы анализа шифров перестановки.	2
5	2	Шифры Хилла. Шифры на основе псевдослучайных последовательностей. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная слож-ность псевдослучайной последовательности. Алгоритм Берлекемпа-Месси.	2
8	3	«Public key cryptography»: Принцип построения шифрсистем с открытым ключом. Протокол Диффи-Хеллмана. Шифрсистема на основе задачи об “укладке рюкзака”. Шифрсистема RSA. Шифрсистема Эль-Гамаля.	2
10	3	Шифрсистема Нидеррайтера. Криптосистемы на основе эллиптических кривых.	2
13	4	Основы теории К.Шеннона Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ.	2
16	5	Общие требования к цифровой подписи. Цифровые подписи на основе	2

		шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стан-дарты цифровой подписи.	
17	6	Современные блочные шифрсистемы. Сети Фейстеля. Криптоалгоритм DES. Криптоалгоритм RIJNDAEL. Криптоалгоритм ГОСТ-28147-89	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Шифры замены. Шифр Виженера. Перестановочные шифры. Шифры Хилла	2
2	2	Контрольная работа по симметричным криптосистемам	1
3	2	Шифры на основе линейных рекуррентных последовательностей. Сети Фейстеля.	6
4	2	Контрольная работа по теме "Линейные рекуррентные последовательности"	2
5	2	Контрольная работа по теме "Сети Фейстеля"	1
6	3	Криптосистема на основе задачи о рюкзаке. Криптосистема RSA	4
7	3	Криптосистема Эль-Гамаля. Эллиптические кривые. Шифрсистемы на основе эллиптических кривых	4
8	3	Контрольная работа по асимметричным системам шифрования.	2
9	3	Элементы криптографического анализа.	1
10	3	Контрольная работа по теме "Криптографический анализ"	1
11	5	Цифровая подпись Эль-Гамаля.	4
12	5	Цифровая подпись Фиата-Шамира. Цифровая подпись Шнорра.	2
13	5	Контрольная работа по теме "Цифровые подписи"	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Подготовка к практическим занятиям. Выполнение домашних заданий.	Основная печатная литература: п.1 (разделы 1-3), ЭУМД: п.1 осн.лит. (разделы 2-3).	36
Подготовка к экзамену	Основная печатная литература: п.1 (разделы 1-3), ЭУМД: п.1 осн.лит. (разделы 2-3), п1 доп.лит.(раздел 1)	12
Написание программ, реализующих заданные криптоалгоритмы	Основная печатная литература: п.1 (разделы 1-3), ЭУМД: п.1 осн.лит. (разделы 2-3), п2 доп.лит.(разделы 3-4)	12

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
не предусмотрены	Лабораторные		0

	занятия		

Собственные инновационные способы и методы, используемые в образовательном процессе

Инновационные формы обучения	Краткое описание и примеры использования в темах и разделах
не предусмотрены	не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ОПК-2 способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	контрольная работа	1
Все разделы	ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы	реферат и выступление с докладом	2
Все разделы	ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	контрольная работа	3
Все разделы	ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы	зачет	3
Все разделы	ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	зачет	3

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
контрольная работа	проверка выполненного задания	Отлично: все поставленные задачи решены правильно Хорошо: почти все поставленные задачи решены правильно, есть незначительные ошибки Удовлетворительно: более

		половины задач решено верно, имеются значительные ошибки Неудовлетворительно: менее половины заданий решено верно, есть значительные ошибки
реферат и выступление с докладом	проверка написанного реферата и сделанного доклада	Зачтено: тема доклада раскрыта, на дополнительные вопросы получены правильные ответы Не зачтено: тема доклада не раскрыта
зачет	Зачет проводится в форме устного опроса по теоретическому материалу. Допуск к зачету получают студенты, не имеющие долгов по контрольным работам. В аудитории, где проводится зачет, должно одновременно присутствовать не более 6-8 студентов. Каждому студенту задается по одному вопросу или заданию из каждой темы. При неправильном ответе студенту могут быть заданы уточняющие или новые вопросы из этой темы. Тема считается освоенной, если студент смог ответить на 2 вопроса, заданных по этой теме	Зачтено: Получены правильные ответы на большинство заданных вопросов. Не зачтено: Правильные ответы получены менее чем на половину заданных вопросов

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
контрольная работа	методкрипто33.doc
реферат и выступление с докладом	темы докладов.docx
зачет	1. Определение криптографической системы. Виды криптографических систем. 2. Перестановочные шифры. 3. Шифры простой замены. 4. Шифр Цезаря и его модификации. 5. Шифр Вернама. 6. Шифр Хилла. 7. Криптосистема на основе задачи о рюкзаке. 8. Криптосистема RSA. 9. Криптосистема Эль-Гамаля. 10. Криптосистема Нидеррайтера.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Зюляркина Н.Д. Криптографические методы защиты информации. Методические указания по проведению практических занятий

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Глухов М.М. Введение в теоретико-числовые методы в криптографии. -- СПб. : Лань, 2011. — 400 с. http://e.lanbook.com/
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. http://e.lanbook.com/
3	Основная литература	Электронно-библиотечная система издательства Лань	Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. http://e.lanbook.com/

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лабораторные занятия	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2

Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.