МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АЛГОРИТМЫ ШИФРОВАНИЯ ИНФОРМАЦИИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	8

Магнитогорск
2019 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
ст. преподаватель кафедры ИиИБ, канд. техн. наук

_____ М.В. Коновалов

Рецензент:
начальник УИТиАСУ , канд. техн. наук _____ К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 01 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Алгоритмы шифрования информации» является формирование у студентов понятий об основных методах шифрования, криптографических протоколах, базовых алгоритмах, применяемых в криптосистемах, алгоритмах шифрования с симметричным и несимметричным ключом.Овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Алгоритмы шифрования информации входит в вариативную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Математическая логика и теория алгоритмов

Дискретная математика

Теория информации

Организация ЭВМ и вычислительных систем

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Научно-исследовательская работа

Подготовка к защите и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Алгоритмы шифрования информации» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать	Классификацию методов шифрования сообщений. Основы теории засекреченной связи. Математические операции, применяемые при шифровании данных.
Уметь	Применять алгоритмы блочного шифрования при разработке ПО. Применять алгоритмы симметричного шифрования при разработке ПО
Владеть	Навыками частотного анализа; Навыками применения метода полного перебора; Навыками атаки на закрытое и открытое сообщение.
ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	

Знать	Системы блочного шифрования. Системы симметричного шифрования Хеш-функции; Протоколы обмена ключами.
Уметь	Реализовывать на языках высокого уровня алгоритмы шифров однозначной замены; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров; Реализовывать на языках высокого уровня алгоритмы омофонических шифров; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров.
Владеть	Навыками разработки защищенного программного обеспечения с применением шифров гаммирования; Навыками разработки защищенного программного обеспечения с применением комбинированных шифров; Навыками разработки защищенного программного обеспечения с применением шифров с открытым ключом;

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

– контактная работа – 87,8 акад. часов:

– аудиторная – 85 акад. часов;

– внеаудиторная – 2,8 акад. часов

– самостоятельная работа – 92,2 акад. часов;

Форма аттестации - курсовая работа, зачет с оценкой

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Введение в шифрование								
1.1 Шифры замены и перестановки. Типы атак на примитивные шифры.	8	2		7/4И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа	ПК-9, ПК-10
Итого по разделу		2		7/4И	13			
2. Симметричные криптографические системы								
2.1 Блочные шифры. Составные шифры. Атаки на блочные шифры.	8	2		7/3И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9, ПК-10
Итого по разделу		2		7/3И	13			
3. Потоковые шифры и генераторы ГСПЧ								

3.1 Общие сведения. Принципы использования ГСПЧ. Классификация потоковых шифров. Шифр A5. Шифр RC4.	8	2		7/3И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9, ПК-10
Итого по разделу		2		7/3И	13			
4. Блочное симметричное шифрование данных (DES)								
4.1 Принципы построения алгоритма DES. Анализ алгоритма DES. Безопасность DES.	8	7		8/3И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9, ПК-10
Итого по разделу		7		8/3И	13			
5. ГОСТ 28147-89								
5.1 Математический базис ГОСТ 28147-89. Режимы работы алгоритма ГОСТ 28147-89. Безопасность ГОСТ 28147-89.	8	7		8/3И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9, ПК-10
Итого по разделу		7		8/3И	13			
6. AES								

6.1 Математический базис AES. Формат данных AES. Структура алгоритма и раундов AES. Стойкость AES	8	7		7/3И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9, ПК-10
Итого по разделу		7		7/3И	13			
7. IDEA								
7.1 Структура алгоритма IDEA. Шифрование данныхIDEA. БезопасностьIDEA.	8	7		7/3И	13	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к тестированию.	семинарское занятие, контрольная работа, проверка ИДЗ	ПК-9, ПК-10
Итого по разделу		7		7/3И	13			
8. Зачет с оценкой								
8.1 Подготовка к зачету с оценкой	8					Подготовка к зачету с оценкой	Зачет с оценкой	ПК-9, ПК-10
Итого по разделу					1,2			
Итого за семестр		34		51/22И	91		зао,кр	
Итого по дисциплине		34		51/22И	92,2		курсовая работа, зачет с оценкой	ПК-9,ПК-10

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Алгоритмы шифрования информации» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

Формы учебных занятий с использованием традиционных технологий:

• обзорные лекции – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;

• информационные – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;

• лекции-визуализации – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;

• Семинар.

• Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала

проблемная - для развития исследовательских навыков и изучения способов решения задач.

лекции с заранее запланированными ошибками – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Технологии проектного обучения

Творческий проект – учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/441493 (дата обращения: 13.04.2020)

б) Дополнительная литература:

1. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 13.04.2020)

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва :ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.:. - ISBN 978-5-16-106992-9. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/987215 (дата обращения: 13.04.2020)

3. Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - Москва : ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/544713 (дата обращения: 13.04.2020)

4. Ларин, Д. А. Криптографическая деятельность в России от Полтавы до Бородина : монография / Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2019. — 282 с. — (Научная мысль). — https://doi.org/10.12737/5285. - ISBN 978-5-16-102175-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1010795 (дата обращения: 13.04.2020)

5. Овчинский, В. С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. - Москва : Норма : ИНФРА-М, 2020. -352 с. - ISBN 978-5-16-106320-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1059377 (дата обращения: 13.04.2020)

6. Баранкова И. И. Теория информации. Кодирование [Электронный ресурс] : учеб-ное пособие / И. И. Баранкова, М. В. Коновалов ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=3313.pdf&show=dcatalogues/1/1137756/3313.pdf&view=true. - Макрообъект. - ISBN 978-5-9967-1073-7

в) Методические указания:

Представлены в приложении 3

Текст : электронный. - URL: https://new.znanium.com/catalog/product/515181 (дата обращения: 13.04.2020)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	свободно распространяемое ПО	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
Atom Editor	свободно распространяемое ПО	бессрочно
NotePad++	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio 2013 Professional(для класса)	Д-1227-18 от 08.10.2018	11.10.2021
Adobe Reader	свободно распространяемое ПО	бессрочно
FAR manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Международная справочная система «Полпред» polpred.com отрасль «Образование, наука»	URL: http://education.polpred.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Федеральная служба по техническому и экспортному контролю	URL: http://www.fstec.ru/
Федеральное агентство по техническому регулированию и метрологии	URL: https://www.rst.gov.ru/portal/gost

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитории - Мультимедийные средства хранения, передачи и представления информации

Компьютерные классы - персональные компьютеры с установленным ПО

Аудитории для самостоятельной работы - персональные компьютеры с установленным ПО

ПРИЛОЖЕНИЕ 1

По дисциплине «Алгоритмы шифрования информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерный индивидуальные домашние задания

Модуль 1. Введение в шифрование.

1. Дан шифротекст «ШДЁЮЧЖЪХЩЖАЮВЕБХВЪГЪВ». Необходимо получить открытое сообщение.

2. Дан шифротекст и открытый текст. Определить ключ, если известно что использован шифр Виженера.

Шифротекст

ЮУТПЕФОЪХЯНФЭЕЭЧАЛТВЯХНРЩТМЯЪКЛСТЦРЙТСЫАЬЫКУЭЦОРЩШЙНЧХОФЦТЙЭЫЖЦЯЫРЧРЮЖЫЗМГРУЙПЙЫЦЦМТШЕЮЯОЧЦРЩРТЬЮЙНСЯЫТЦФДФГЯАЬАВЫНЩЦРЫОБОИДЕЪОУКХЪВТМЬЧАУНЖЬДХЧНЯАСЩШЕФЦТЙЕМНЮТТЛРЩЫСЮЧНМУОЗНОУИГЬЧСЕБТЙУДУЭСЩУККЯМЕГНМЭЕЦЧПЫЖЬБЫЕГЩИЦЗШНМАЩФОЬДЪЦУШОЫТЧЖСВЩИЪБЫБЯПВКНЦЪЧХТОУЬЪЛУЗЗЦЕЮКЖЭПСЙКВЯТЖЪАПРЦЮТХЕМЕОТТМШПНЪЪЕВЩДШЧЮПДУЮУПКРИСШГЫБПЗЙЖЦХСГЧСЕТТЕЖЗУРВФНВАСЕЩШЖЮГРРГЫБМДЫКСКРИЭЪЯРОЫАФАЮЮПНВПТСЫАРУФРФТЪАЬСУОТЛХКЧФВИЦСВТЧЙИУЗНОЖЮБНЯЬЕЬЗРФЪЭАЩГВЫЕДУЗШНУЬТТЯМГСУДТДХКЦЕГРИХЩЛЭУУОУЬБШНЕУМТД

Открытый текст

НеспокойныевременанасталидляГалактическойРеспубликиНалогообложение торговых путей к отдаленным солнечным системам сталопричиной раздоров В стремлении добиться своего обуянная алчностьюТорговая Федерация с помощью мощных боевых кораблей взяла в кольцоблокады маленькую планету Набу лишив её всех поставок В то время какчлены Конгресса Республики ведут напряженные дебаты в связи стревожными событиями Верховный канцлер втайне от всех поручил двумрыцарям джедай хранителям мира и справедливости в Галактикеурегулировать конфликт

Модуль 2. Симметричные криптографические системы

1. Укажите различия между современными и традиционнымишифрами с симметричным ключом.

2. Объясните, почему современные блочные шифры спроектированы как шифры подстановки вместо того, чтобы применятьшифры транспозиции.

3. Перечислите компоненты современного блочного шифра.

4. Определите P-блок и назовите его три варианта. Какой вариант является обратным?

5. Сообщение имеет 1500 символов для представления, которых используются ASCII коды. Это сообщение будет зашифрованоблочным шифром длиной 64 бита. Найдите размер дополнениями количество зашифрованных блоков.

6. Покажите P-блок, определенпоследовательностью: 81234567.

Модуль 3. Потоковые шифры и генераторы ГСПЧ

1. Определите последовательность из первых десяти чисел и период линейного конгруэнтного ГПСЧ для a=5, b=7 и c=17 (k0принять равным – 0).

2. Определите последовательность из десяти чисел, генерируемой методом Фибоначчи с задержкой, начиная с kаприа = 3, b = 1, k0=0,6, k1=0,3, k2 =0,5.

3. Вычислить псевдослучайную двоичную последовательность длиной 12 бит по методу генерации ПСЧ BBS, если: p = 19, q = 23, x = 3.

Модуль 4. Блочное симметричное шифрование данных (DES)

1. Значение последовательности входных данных в DESравно:1234567890ABCDEF16. Определить значение последовательности навыходе блока IP-перестановки.

2. Значение последовательности R0 в DES равно: R0 =F0AAE8A516.Определить значение последовательности на выходе Е-блока перестановки и расширения.

3. Значение последовательности R1в DES равно: R1 =116BA13316. Определить значение последовательности на выходе Е-блока перестановки и расширения.

Модуль 5. ГОСТ 28147-89

1. В регистре N1 алгоритма ГОСТ 28147-89 находятся данные:N1 – 191A2AB816, в N2 – 434665B216. Ключ для шифрования k0=EB8A715916, k2=7CE5D63D16, k3=4AC1D6E016, k4=BAFE473116, k5=A3DEB02516, k6=8BB389AC16, k7=10D3B61A16, k8=E9AC340F16. Цикл шифрования – 25. Что будет находится в N1 и N2 после завершения цикла. Использовать структуру режима простой замены.

Модуль 6. AES

1. Произвести сложение двух элементов конечного поля x7 + x3 + x + 1 и x6 + x3 + x2 + 1.

2. Определить аддитивную инверсию многочлена длиной в один байт из конечного поля GF(28) x6+x3+x2+1.

3. Значения байтов матрицы состояния данных на входе функции SubBytes()AES-128 равны A49C7FF2689F352B6B5BEA43026A504916. Определить значения байтов матрицы состояния данных на выходе функции SubBytes().

Модуль 7. IDEA

1. Начальный ключ алгоритма IDEA – последовательность длиной 128 битов, которая равна K = 3F424CDC105CA00D7B3DBE8C96A2978E16. Сформировать раундовые ключи для второго раунда шифрования.

2. Определить результат этапа перестановки (трансформации) первого раунда шифрования алгоритмом IDEA, если входные данные равны: M = 3D550F51D71EE0AA16. Раундовые ключи шифрования: k1=3F4216, k2=4CDC16, k3=105C16, k4=A00D16.

Курсовая работа выполняется обучающимся самостоятельно под руководство преподавателя. При выполнении курсовой работы обучающийся должен показать свое умение работать с нормативным материалом и другими литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В начале изучения дисциплины преподаватель предлагает обучающимся на выбор перечень тем курсовых работ. Обучающийся самостоятельно выбирает тему курсовой работы. Совпадение тем курсовых работ у обучающихся одной учебной группы не допускается. Утверждение тем курсовых работ проводится ежегодно на заседании кафедры.

После выбора темы преподаватель формулирует задание по курсовой работе и рекомендует перечень литературы для ее выполнения. Исключительно важным является использование информационных источников, а именно системы «Интернет», что даст возможность обучающимся более полно изложить материал по выбранной им теме.

В процессе написания курсовой работы обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

Преподаватель, проверив работу, может возвратить ее для доработки вместе с письменными замечаниями. Обучающийся должен устранить полученные замечания в установленный срок, после чего работа окончательно оценивается.

Курсовая работа должна быть оформлена в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления».

Примерный перечень тем курсовых работ и пример задания представлены в разделе «Оценочные средства для проведения промежуточной аттестации».

ПРИЛОЖЕНИЕ 2

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-9. Способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать	Классификацию методов шифрования сообщений. Основы теории засекреченной связи. Математические операции, применяемые при шифровании данных.	1.Сформулируйте необходимое и достаточное условия для совершенной секретности криптографической системы. 2. Дайте объяснение сущности рассеивания данных в процессе их шифрования. 3. Что является целью перемешивания данных в процессе их шифрования? 4. Что такое криптографическая атака? 5. Какие типы криптографических атак существуют? 6. Дайте характеристику атаки только на зашифрованный текст. Объясните сущность атаки “грубой силы”. 7. Дайте характеристику атаки только на зашифрованный текст. Объясните сущность статистической атаки. 8. Дайте характеристику атаки только на зашифрованный текст. Объясните сущность атаки по образцу. 9. Дайте характеристику атаки на известный входной текст. 10. Дайте характеристику атаки на выбранный входной текст. 11. Дайте характеристику атаки на выбранный зашифрованный текст.
Уметь	Применять алгоритмы блочного шифрования при разработке ПО. Применять алгоритмы симметричного шифрования при разработке ПО	1. S-блок подстановки производит операцию xor с нечетными битами, чтобы получить левый бит выхода, и xor с четными битами, чтобы получить правый бит выхода. Определить значение на выходе блока если на входе блока 1100102 2. Крайний левый бит S-блока подстановки размером4x3определяет смещение других трех бит. Если крайний левый бит равен 0, то три других бита перемещаются вправо на один бит. Если крайний левый бит равен 1, то три других бита перемещаются влево на один бит. Определить результат на выходе блока если на входе последовательность 10112.

Владеть	Навыками частотного анализа; Навыками применения метода полного перебора; Навыками атаки на закрытое и открытое сообщение.	1. Файл содержит сообщение зашифрованное шифром перестановки. Дешифровать сообщение при помощи метода полного перебора, и опираясь на статистические свойства сообщения. 2. Файл содержит открытое и закрытое сообщение, зашифрованное при помощи шифра перестановки. Определить ключ, используемый при шифровании.
ПК-10.способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности		
Знать	Комбинированное шифрование; Шифрование с открытым ключом; Хеш-функции; Протоколы обмена ключами.	1.Схема режима шифрования DES-ECB. 2. Схема режима шифрования DES-CBC. 3. Схема режима шифрования DES-CPB и DES-OFB. 4. Тройной DES. Сферы применения различных режимов DES. 5. Схема режима шифрования простой замены ГОСТ 28147-89. 6. Шифрование с открытым ключом. Основные понятия. 7. Алгоритм шифрования на основе эллиптических кривых.

Уметь	Реализовывать на языках высокого уровня алгоритмы шифров однозначной замены; Реализовывать на языках высокого уровня алгоритмы полиалфавитных шифров;	Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи полибианского квадрата. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифрующей системы Тримесуса. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи биграммного шифра Порты. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра Хилла. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра Виженера. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи совмещенного шифра. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра маршрутной перестановки. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра «Перекресток». Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи решетки Кардано. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощи шифра RC4. Реализовать на языке C# алгоритм шифрования/дешифрования текстового сообщения при помощишифра ADFGX
Владеть	Навыками разработки защищенного программного обеспечения с применением шифров гаммирования; Навыками разработки защищенного программного обеспечения с применением комбинированных шифров; Навыками разработки защищенного программного обеспечения с применением шифров с открытым ключом;	1.Реализовать на языке C# программное средство осуществляющее шифрование изображения представленного в формате BMP при помощи Вернама. 2. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-ECB. 3. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-CBC. 4. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-CPB. 5. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму DES-OFB. 5. Разработка криптографической программы, осуществляющей шифрование и дешифрование данных по алгоритму тройной DES.

Примерный перечень тем курсовых работ

1. Разработать ПО для криптоанализа простого шифра замены с использованием лозунга и без.
2. Разработать ПО для криптоанализа шифров простой перестановки. Размер блока определен в диапазоне +/-5символов.
3. Разработать ПО для криптоанализа шифров маршрутной перестановки.
4. Разработать ПО для шифрования/дешифрования текстовых файлов при помощи шифра Хилла с матрицей 7x7.
5. Программная реализация сети Фейстиля для шифрования изображений.
6. Разработать ПО для шифрования/дешифрования аудиофайлов при помощи алгоритма шифрования Люцифер.
7. Разработать ПО для шифрования/дешифрования изображений при помощи алгоритма шифрования DES.
8. Разработать ПО для поточного шифрования/дешифрования аудио потока данных при помощи шифра Вермана
9. Разработать ПО для шифрования/дешифрования файлов про помощи алгоритма IDEA
10. Разработка ПО для шифрования/дешифрования файлов про помощи алгоритма RSA.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета и экзамена.

Показатели и критерии оценивания зачета с оценкой:

– на оценку «отлично» (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку «хорошо» (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку «удовлетворительно» (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

«не зачтено» – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, не может показать знания на уровне воспроизведения и объяснения информации.

Показатели и критерии оценивания курсовой работы:

– на оценку «отлично» (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «хорошо» (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку «удовлетворительно» (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку «неудовлетворительно» (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

ПРИЛОЖЕНИЕ 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Рекомендации направлены на оказание методической помощи студентам при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности студентов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы студент демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.