МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Введение в специальность

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Дисциплина "Введение в специальность" обеспечивает приобретение начальных профессиональных знаний и умений в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности "10.05.01-Компьютерная безопасность" (уровень специалитета), содействует развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является

1) ознакомление обучаемых с основными задачами в области обеспечения информационной безопасности;

2) ознакомление обучаемых с криптографическими методами решения основных задач в области обеспечения информационной безопасности;

3) ознакомление обучаемых с основными этапами истории развития криптографических методов решения основных задач в области обеспечения информационной безопасности;

4) ознакомление обучаемых с математическим аппаратом, используемым в современной криптографии.

2. Место дисциплины в структуре ОП специалитета

Дисциплина "Введение в специальность" относится к дисциплине специализации блока Б.1. Она играет важную роль для общепрофессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении математических дисциплин “Алгебра”, "Теория чисел" и "Информатика". Знания, умения и навыки, полученные при изучении дисциплины "Введение в специальность", используются обучаемыми при изучении общепрофессиональных и специальных дисциплин математического и компьютерного циклов.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП специалитета

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	И-ОПК-1.3. Знает понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; **И-ОПК- 1.4** Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации	**Знать:** основные понятия, проблемы и методы их решения в области обеспечения информационной безопасности; основные подходы к решению проблем обеспечения конфиденциальности, целостности и аутентификиации. **Уметь**: использовать современные алгоритмы шифрования, ЭЦП. **Владеть навыками:** криптоанализа шифров; реализации современных математических методов защиты информации
ОПК- 3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	И-ОПК-3.5. Знает необходимые математические методы для решения задач обеспечения защиты информации. И-ОПК-3.6. Уметь: применять совокупность необходимых математических методов для решения задач обеспечения защиты информации. И- ОПК-3.7. Наделен навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации**.**	**Знать:** основные понятия, проблемы и методы их решения в области обеспечения информационной безопасности; основные подходы к решению проблем обеспечения конфиденциальности, целостности и аутентификации. **Уметь**: использовать современные алгоритмы шифрования, ЭЦП. **Владеть навыками:** криптоанализа шифров; реализации современных математических методов защиты информации

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет _2_ зачетных единиц, _72_ акад.часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	**Введение.** Место специальности "Компьютерная безопасность" в системе высшего образования РФ. Основные задачи в области обеспечения информационной безопасности, решаемые криптографическими методами.	2	1					1	Устный опрос
2	**Краткий исторический обзор криптографических методов защиты информации.** Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр Плейфейра, шифр Хилла. Решетка Кардано, книжный шифр, шифр Виженера, гаммирование, дисковый шифратор Т.Джефферсона, шифр Вернама и др.		1	1				3	Задания для самостоятельной (домашней) работы Устный опрос
3	**Криптология и криптоанализ.** Принцип Керкгоффса. Математическая модели открытых текстов. Критерии на открытый текст. Понятие шифра, алгебраическая и		1					2	Устный опрос

	вероятностная модели шифра. Классификация шифров. Понятие цифровой подписи.								
4	**Простейшие исторические шифры и их анализ.** Простейшие шифры замены и их криптоанализ. Индекс совпадения Фридмана. Простейшие шифры перестановки и их анализ. Шифры гаммирования и их анализ. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой. Табличное и модульное гаммирование. Дисковые шифраторы многоалфавитной замены.		1	1				4	Задания для самостоятельной (домашней) работы Устный опрос
5	**Основные этапы становления криптографии.** Роль К.Шеннона и отечественные достижения в области защиты информации. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления подлежащей шифрованию информации (оцифровка).		1					2	Устный опрос
6	**Общее понятие шифра, алгебраическая и вероятностная модели шифра** Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система		1					2	Устный опрос

	шифра. Основные требования к шифрам. Общее понятие криптосистемы. Симметричные и асимметричные системы шифрования								
7	**Основные классы шифров и их свойства.** Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки. Одноалфавитные и многоалфавитные шифры замены. Шифрвеличины и шифробозначения. Распределители.		1	2				2	Задания для самостоятельной (домашней) работы Устный опрос
8	**Поточные системы шифрования.** Поточные шифры и принципы их построения. Типовые генераторы псевдослучайных последовательностей и их свойства. Линейные рекуррентные последовательности, их периодичность. Методы усложнения линейных рекуррентных последовательностей. Шифрование в европейской системе мобильной телефонии шифрсистема А5.		1	4				3	Задания для самостоятельной (домашней) работы Устный опрос
9	**Блочные системы шифрования.** Блочные шифры и принципы их построения. S-P-сеть. Выбор линейных и нелинейных блоков. Ознакомление с современными стандартами блочных шифров USA: DES, AES, РФ: ГОСТ 28147-89, ГОСТ Р		2	2		1		3	Задания для самостоятельной (домашней) работы Устный опрос

	34.12-2015. XSL-структура алгоритмов шифрования. Режимы использования блочных шифров ГОСТ Р 34.13-2015. Межгосударственные стандарты ГОСТ 34.12-2018 и ГОСТ 34.13.2018.								
10	**Функции хэширования.** Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций. Использование хеш-функций и блочных шифров в системах аутентификации сообщений. Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC. Ознакомление с современными стандартами функций хэширования ГОСТ Р 34.11-2012 и ГОСТ 34-11-2018		1	2		1		1	Задания для самостоятельной (домашней) работы Устный опрос
11	**Системы шифрования с открытым ключом.** Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы с открытым ключом - асимметричные системы шифрования. Вычислительно сложные задачи математики. Криптосистема RSA и ее анализ. Криптосистемы Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана.		2	2		1		2	Задания для самостоятельной (домашней) работы Устный опрос

	Электронная подпись документов. Цифровая подпись Фиата-Шамира и подпись Эль-Гамаля. ГОСТ Р 34.10-2012 и ГОСТ 34.10-2018.								
12	**Протоколы распределения ключей.** Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos. Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей. Открытое распределение ключей. Предварительное распределение ключевых материалов. Возможные атаки на протоколы распределения ключей. Управление ключами.		1	2		1		2	Задания для самостоятельной (домашней) работы Устный опрос
13	**Схемы разделения секрета.** Доказательства с нулевым разглашением.		1					1	
14	**Некоторые практические аспекты использования шифрсистем** Проблемы реализации криптографической подсистемы и системы управления ключами .		1					1	
			16	16		4		35,7	
							0,3		зачет
	Всего		**16**	**16**		**4**	**0,3**	**35,7**	

Содержание разделов программы дисциплины "Введение в специальность" :

1. Введение.

Место специальности "Компьютерная безопасность" в системе высшего образования РФ.

Основные задачи в области обеспечения информационной безопасности, решаемые криптографическими методами.

2. Краткий исторический обзор криптографических методов защиты информации.

Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр Плейфейра, шифр Хилла. Решетка Кардано, книжный шифр, шифр Виженера, гаммирование, дисковый шифратор Т.Джефферсона, шифр Вернама и др.

3. Криптология и криптоанализ.

Принцип Керкгоффса.

Математическая модели открытых текстов. Критерии на открытый текст.

Классификация шифров.

Понятие цифровой подписи.

4. Простейшие исторические шифры и их криптоанализ.

Простейшие шифры замены и их криптоанализ. Индекс совпадения Фридмана. Простейшие шифры перестановки и их анализ. Шифры гаммирования и их анализ. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой. Табличное и модульное гаммирование. Дисковые шифраторы многоалфавитной замены.

5. Основные этапы становления криптографии. Роль К.Шеннона и отечественные достижения в области защиты информации.
Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию (оцифровка).

6. Общее понятие шифра, алгебраическая и вероятностная модели шифра

Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Общее понятие криптосистемы. Симметричные и асимметричные системы шифрования

7. Основные классы шифров и их свойства.

Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки.

Одноалфавитные и многоалфавитные шифры замены. Шифрвеличины и шифробозначения. Распределители.

8. Поточные системы шифрования.

Поточные шифры и принципы их построения. Типовые генераторы псевдослучайных последовательностей и их свойства. Линейные рекуррентные последовательности, их периодичность. Методы усложнения линейных рекуррентных последовательностей. Шифрование в европейской системе мобильной телефонии - шифрсистема А5.

9. Блочные системы шифрования.

Блочные шифры и принципы их построения. S-P-сеть. Выбор линейных и нелинейных блоков. Ознакомление с современными стандартами блочных шифров USA: DES, AES, РФ ГОСТ 28147-89, ГОСТ Р 34.12-2015. XSL-структура алгоритмов шифрования. Режимы использования блочных шифров ГОСТ Р 34.13-2015. Межгосударственные стандарты ГОСТ 34.12-2018 и ГОСТ 34.13-2018.

10. Функции хэширования.

Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций. Использование хеш-функций и блочных шифров в системах аутентификации сообщений. Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC. Ознакомление с современными стандартами хеш-функций ГОСТ Р 34.11-2012 и ГОСТ 34.11-2018.

11. Системы шифрования с открытым ключом.

Понятие односторонней функции и односторонней функции с «лазейкой».

Криптосистемы с открытым ключом - асимметричные системы шифрования. Вычислительно сложные задачи математики. Криптосистема RSA и ее анализ. Криптосистемы Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана.

Электронная подпись документов. Цифровая подпись Фиата-Шамира и подпись Эль-Гамаля. ГОСТ Р 34.10-2012 и ГОСТ 34.10-2018.

12. Протоколы распределения ключей.

Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.

Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.

Открытое распределение ключей.

Предварительное распределение ключевых материалов.

Возможные атаки на протоколы распределения ключей. Управление ключами.

13. Схемы разделения секрета.

Доказательства с нулевым разглашением.

14. Некоторые практические аспекты использования шифрсистем

Проблемы реализации криптографической подсистемы и системы управления ключами .

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости)

В процессе осуществления образовательного процесса используются:
-программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:
- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
- Microsoft OfficeSTD 2013;
- MikTeX (свободно распространяемое ПО).

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

7. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2005. 480 с.
2. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов. / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. М., Горячая линия - Телеком, 2006. 544 с.
3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] :учебное пособие / С.А. Нестеров. - Электрон. дан. - Санкт-Петербург : Лань, 2017. - 324 с. - Режим доступа: https://e.lanbook.com/book/90153.

б) дополнительная литература

1. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
2. Кукина Е.Г. Введение в криптографию [Электронный ресурс] : сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков. - Электрон. текстовые данные. - Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. - 91 с. - 978-5-7779-1588-7. - Режим доступа: http://www.iprbookshop.ru/24876.html

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

3.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list) представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:
-учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров), в том числе лаборатория программно-аппаратных средств обеспечения информационной безопасности;
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
-помещения для самостоятельной работы;
-помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы):

Профессор, доктор физ.-матем. наук Дурнев В.Г.

Приложение №1 к рабочей программе дисциплины
«Введение в специальность»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 2 **"Краткий исторический обзор криптографических методов защиты информации. "**

Задания для самостоятельного решения № 32 - 41 из параграфа 6 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 4 **"Простейшие исторические шифры и их анализ."**

Задания для самостоятельного решения № 22 - 30 из параграфа 3 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 7 "**Основные классы шифров и их свойства. "**

Задания для самостоятельного решения № 31 - 38 из параграфа 4 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 9 **" Блочные системы шифрования. "**

Задания для самостоятельного решения № 185 - 191 из параграфа 22 и № 195 - 200 из параграфа 24 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 10 **" Функции хэширования. "**

Задания для самостоятельного решения № 192 - 194 из параграфа 23 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 11 **" Системы шифрования с открытым ключом. "**

Задания для самостоятельного решения № 86 - 99 из параграфа 9 и № 100 - 123 из параграфа 10 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Домашние задания по теме № 12 " **Протоколы распределения ключей."**

Задания для самостоятельного решения № 171 - 173 из параграфа 18 сборника задач Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.

Контрольная работа "Блочные системы шифрования."

1) Блочные шифры и принципы их построения. S-P-сеть.
2) Выбор линейных и нелинейных блоков.
3) Сравнение современных стандартов блочных шифров DES, ГОСТ 28147-89, AES, ГОСТ Р 34.12-2015 и ГОСТ 34.12-2018.
4) Режимы использования блочных шифров. ГОСТ Р 34.13-2015 и ГОСТ 34.13.2018.

Темы рефератов

1. Исторические шифры и их криптоанализ.
2. Идея шифрования с открытым ключом на основе однонаправленной функции с секретом.
3. Математическая модель открытых текстов.
4. Критерии на открытый текст.
5. Алгебраическая модель шифра.
6. Вероятностная модель шифра.
7. Шифры замены, классификация и анализ.
8. Шифры перестановки, классификация и анализ.
9. Шифры гаммирования. Криптоанализ шифра Виженера.
10. Шифры гаммирования. Неравновероятная гамма.
11. Шифры гаммирования. Повторное использование гаммы.
12. Дисковые шифраторы многоалфавитной замены.
13. Дисковые шифраторы гаммирования.
14. Практическая стойкость шифров.
15. Вопросы имитостойкости шифров.
16. Коды аутентификации
17. Помехоустойчивость шифров. Теорема Маркова.
1. Поточные шифры и принципы их построения.
2. Генераторы псевдослучайных последовательностей и их характеристики.
3. Методы усложнения линейных рекуррентных последовательностей.
4. Блочные шифры и принципы их построения.
5. Режимы использования блочных шифров. ГОСТ Р 34.13-2015 и ГОСТ 34.13.2018.
6. Стандарт шифрования DES.
7. Стандарт шифрования ГОСТ-28147-89.
8. Стандарт шифрования ГОСТ Р 34.12-2015 и ГОСТ 34.12.2018.
9. XSL-структура алгоритмов шифрования.
10. Стандарт шифрования AES.
11. Криптосистемы на основе открытого ключа. "Сложные" проблемы математики.
12. Криптосистема RSA и выбор параметров.
13. Понятие цифровой подписи. ГОСТ Р 34.10-2012 и ГОСТ 34.10-2018.
14. Методы анализа протокола RSA.

15. Основные методы дискретного логарифмирования.
16. Криптосистема Эль-Гамаля.
17. Понятие хеш-функции, способы их построения.
18. Ключевые хеш-функции и связь с кодами аутентификации.
19. Бесключевые хеш-функции, парадокс дней рождений.
20. Российский стандарт хеш-функции. ГОСТ Р 34.11-2012 и ГОСТ 34.11.2018.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету по дисциплине
"Введение в специальность"

1. Основные задачи в области обеспечения информационной безопасности, решаемые криптографическими методами.

2.Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр Плейфейра, шифр Хилла. Решетка Кардано, книжный шифр, шифр Виженера, гаммирование, дисковый шифратор Т.Джефферсона, шифр Вернама и др.

3. Криптология и криптоанализ. Принцип Керкгоффса.

4. Математическая модели открытых текстов. Критерии на открытый текст.

5. Классификация шифров.

6. Простейшие шифры замены и их криптоанализ. Индекс совпадения Фридмана.

7. Простейшие шифры перестановки и их анализ.

8. Шифры гаммирования и их анализ. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой. Табличное и модульное гаммирование.

9. Дисковые шифраторы многоалфавитной замены.

10. Основные этапы становления криптографии. Роль К.Шеннона и отечественные достижения в области защиты информации.

11. Способы представления информации, подлежащей шифрованию (оцифровка).

12. Общее понятие шифра, алгебраическая и вероятностная модели шифра Определение шифра и его математические модели. Ручные и машинные шифры.

13. Ключевая система шифра. Основные требования к шифрам.

14. Общее понятие криптосистемы. Симметричные и асимметричные системы шифрования

15.Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки.

16. Одноалфавитные и многоалфавитные шифры замены. Шифрвеличины и шифробозначения. Распределители.

17. Поточные шифры и принципы их построения.

18. Типовые генераторы псевдослучайных последовательностей и их свойства.

19. Линейные рекуррентные последовательности, их периодичность. Методы усложнения линейных рекуррентных последовательностей.

20. Шифрование в европейской системе мобильной телефонии - шифрсистема А5.

21. Блочные шифры и принципы их построения. S-P-сеть. Выбор линейных и нелинейных блоков.

22. Современные стандарты блочных шифров USA: DES, AES, РФ: ГОСТ 28147-89, ГОСТ Р 34.12-2015. ГОСТ 34.12-2018. XSL-структура алгоритмов шифрования.

23. Режимы использования блочных шифров. ГОСТ Р 34.13-2015. ГОСТ 34.13.2018.

24. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций.

25. Использование хеш-функций и блочных шифров в системах аутентификации сообщений. Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC.

26. Современные стандарты функций хэширования . ГОСТ Р 34.11-2012. ГОСТ 34.11-2018.

27. Системы шифрования с открытым ключом ключом - асимметричные системы шифрования.

Понятие односторонней функции и односторонней функции с «лазейкой».

28. Использование в ассиметричной криптографии вычислительно сложных задач математики.

29. Криптосистема RSA и ее анализ.

30. Криптосистемы Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана.

31. Электронная подпись документов. Цифровая подпись Фиата-Шамира и подпись Эль-Гамаля. ГОСТ Р 34.10-2012. ГОСТ 34.10-2018.

32. Протоколы распределения ключей.
Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.

33. Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.

34. Открытое распределение ключей.

35. Предварительное распределение ключевых материалов.

36. Возможные атаки на протоколы распределения ключей. Управление ключами.

37. Схемы разделения секрета.

Доказательства с нулевым разглашением.

38. Некоторые практические аспекты использования шифрсистем.

Проблемы реализации криптографической подсистемы и системы управления ключами.

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине "Введение в специальность"

1. Основные задачи в области обеспечения информационной безопасности, решаемые криптографическими методами.

2. Исторические примеры шифров: шифр Цезаря, квадрат Полибия, шифр Хилла. Решетка Кардано, книжный шифр, шифр Виженера, гаммирование, дисковый шифратор Т.Джефферсона, шифр Вернама и др.

3. Криптология и криптоанализ. Принцип Керкгоффса.

4. Математическая модели открытых текстов. Критерии на открытый текст.

5. Классификация шифров.

6. Простейшие шифры замены и их криптоанализ. Индекс совпадения Фридмана.

7. Простейшие шифры перестановки и их анализ.

8. Шифры гаммирования и их анализ. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой. Табличное и модульное гаммирование.

9. Дисковые шифраторы многоалфавитной замены.

10. Основные этапы становления криптографии. Роль К.Шеннона и отечественные достижения в области защиты информации.

11. Способы представления информации, подлежащей шифрованию (оцифровка).

12. Общее понятие шифра, алгебраическая и вероятностная модели шифра
Определение шифра и его математические модели. Ручные и машинные шифры.

13. Ключевая система шифра. Основные требования к шифрам.

14. Общее понятие криптосистемы. Симметричные и асимметричные системы шифрования

15.Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки.

16. Одноалфавитные и многоалфавитные шифры замены. Шифрвеличины и шифробозначения. Распределители.

17. Поточные шифры и принципы их построения.

18. Типовые генераторы псевдослучайных последовательностей и их свойства.

19. Линейные рекуррентные последовательности, их периодичность. Методы усложнения линейных рекуррентных последовательностей.

20. Шифрование в европейской системе мобильной телефонии - шифрсистема А5.

21. Блочные шифры и принципы их построения. S-P-сеть. Выбор линейных и нелинейных блоков.

22. Современные стандарты блочных шифров USA: DES, AES, РФ: ГОСТ 28147-89, ГОСТ Р 34.12-2015. ГОСТ 34.12-2018. XSL-структура алгоритмов шифрования.

23. Режимы использования блочных шифров. ГОСТ Р 34.13-2015. ГОСТ 34.13-2018.

24. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Конструкции хеш-функций.

25. Использование хеш-функций и блочных шифров в системах аутентификации сообщений. Коды аутентификации сообщений MAC и коды обнаружения ошибок MDC и MIC.

26. Современные стандарты функций хэширования. ГОСТ Р 34.11-2012. ГОСТ 34.11.2018.

27. Системы шифрования с открытым ключом ключом - асимметричные системы шифрования.

Понятие односторонней функции и односторонней функции с «лазейкой».

28. Использование в ассиметричной криптографии вычислительно сложных задач математики.

29. Криптосистема RSA и ее анализ.

30. Криптосистемы Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана.

31. Электронная подпись документов. Цифровая подпись Фиата-Шамира и подпись Эль-Гамаля. ГОСТ Р 34.10-2012. ГОСТ 34.10.2018.

32. Протоколы распределения ключей.

Передача ключей с использованием симметричной системы шифрования. Двусторонние и трехсторонние протокола. Протокол Kerberos.

33. Передача ключей с использованием асимметричной системы шифрования. Сертификаты открытых ключей.

34. Открытое распределение ключей.

35. Предварительное распределение ключевых материалов.

36. Возможные атаки на протоколы распределения ключей. Управление ключами.

37. Схемы разделения секрета.

Доказательства с нулевым разглашением.

38. Некоторые практические аспекты использования шифрсистем.

Проблемы реализации криптографической подсистемы и системы управления ключами.

Оценка устного ответа на зачете

Устный ответ на зачете оценивается по 2 балльной системе: ***«зачтено», «незачтено».***

Оценка ***«зачтено»*** ставится, если:

- демонстрируемые студентом знания отличаются достаточной глубиной и содержательностью,
- дается достаточно полный ответ, как на основные вопросы, так и на дополнительные;
- студент достаточно свободно владеет терминологией;

- ответ студента не содержит принципиальных ошибок.

Оценка ***«незачтено»*** ставится, если:

- обнаружено незнание или непонимание студентом основных разделов дисциплины;
- студент допускает существенные фактические ошибки, которые он не может исправить самостоятельно;
- на значительную часть дополнительных вопросов студент затрудняется дать правильный ответ.

Оценивание контрольных работ:

Каждая из четырёх задач оценивается следующими баллами:
0 (задача не сделана), 1 (сделано кое-что), 2 (сделана приблизительно наполовину), 3 (сделана с некоторыми недочетами), 4 (сделана полностью). Общее число баллов за все 4 задания составляет 16. Оценка за работу студента ставится в зависимости от набранного им числа баллов:
0 – 4 балла – неудовлетворительно,
5 – 8 баллов – удовлетворительно,
9 – 12 баллов – хорошо
13 – 16 баллов – отлично.

Приложение №2 к рабочей программе дисциплины
«Введение в специальность»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине "Введение в специальность" являются лекции, что связано, прежде всего, с новизной материала для обучаемых. По большинству тем предусмотрены практические занятия, целью которых является закрепление лекционного материала путем решения специальным образом подобранных задач и упражнений.

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора хорошо подобранных задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы криптографических методов обеспечения информационной безопасности. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на практических занятиях и контрольной работы. Также проводятся консультации (при необходимости) по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

В конце изучения дисциплины студенты сдают зачет. Зачет проводится на основании выполнения домашних заданий, контрольной работы и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать учебную литературу, указанную в разделе 7

Для подбора дополнительного материала, особенно при написании рефератов, рекомендуется использовать интернет-ресуры:

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
2. Электронно-библиотечная система «Юрайт https://www.biblio-online.ru/
3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru)
4. Электронно-библиотечная система «Лань» http://e.lanbook.com/