

Документ подписан простой электронной подписью.

Информация о владельце:

ФИО: Кандрашина Елена Александровна

Должность: И.о. ректора ФГАОУ ВО «Самарский государственный экономический университет»

Дата подписания: 11.07.2025 11:49:17

Уникальный программный ключ:

2db64eb9605ce27edd3b8e8fdd32c70e0674ddd2

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

УТВЕРЖДЕНО

Ученым советом Университета

(протокол № 10 от 22 мая 2025 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.10 Криптографическая защита информации

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа
Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2025

Содержание (рабочая программа)

Стр.

- 1 Место дисциплины в структуре ОП
- 2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе
- 3 Объем и виды учебной работы
- 4 Содержание дисциплины
- 5 Материально-техническое и учебно-методическое обеспечение дисциплины
- 6 Фонд оценочных средств по дисциплине

Содержание (ФОС)

Стр.

- 6.1 Контрольные мероприятия по дисциплине
- 6.2 Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе
- 6.3 Паспорт оценочных материалов
- 6.4 Оценочные материалы для текущего контроля
- 6.5 Оценочные материалы для промежуточной аттестации
- 6.6 Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Криптографическая защита информации входит в часть, формируемая участниками образовательных отношений блока Б1. Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Вычислительные системы, сети и телекоммуникации, Основы проектной деятельности, Современные технологии и языки программирования, Теория информационной безопасности и методология защиты информации, Правовая защита информации, Технологии защищенного документооборота

Последующие дисциплины по связям компетенций: Разработка профессиональных приложений, Проектный практикум, Управление информационной безопасностью, Специализированные ИТ в правоохранительной деятельности, Управление информационными проектами реализации комплексной безопасности

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Криптографическая защита информации в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-2	ПК-2.1: Знать: особенности защиты автоматизированных систем с помощью типовых программных средств	ПК-2.2: Уметь: оценивать защищенность автоматизированных систем с помощью типовых программных средств

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	56.3/1.56
Занятия лекционного типа	18/0.5
Занятия семинарского типа	36/1
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	53.7/1.49
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации:	
Экзамен	Экз
Общая трудоемкость (объем части образовательной программы): Часы	144
Зачетные единицы	4

очно-заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	6.3/0.18
Занятия лекционного типа	2/0.06
Занятия семинарского типа	2/0.06
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	103.7/2.88
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации:	
Экзамен	Экз
Общая трудоемкость (объем части образовательной программы): Часы	144
Зачетные единицы	4

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Криптографическая защита информации представлен в таблице.

Разделы, темы дисциплины и виды занятий Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				
1.	Введение в криптографию. Основные классы шифров и их свойства	6	12	0,1		13,7	ПК-2.1, ПК-2.2, ПК-2.3
2.	Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	6	12	0,1		20	ПК-2.1, ПК-2.2, ПК-2.3
3.	Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения	6	12	0,1		20	ПК-2.1, ПК-2.2, ПК-2.3
	Контроль	34					
	Итого	18	36	0.3	2	53.7	

очно-заочная форма

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по
		Лекции	Занятия семинарского типа	ИКР	ГКР		
			Практич. занятия				

							образовательной программе	
1.	Введение в криптографию. Основные классы шифров и их свойства	0,5	0,5	0,1		23,7	ПК-2.1, ПК-2.2, ПК-2.3	
2.	Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	0,5	0,5	0,1		40	ПК-2.1, ПК-2.2, ПК-2.3	
3.	Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения	1	1	0,1		40	ПК-2.1, ПК-2.2, ПК-2.3	
	Контроль	34						
	Итого	2	2	0.3	2	103.7		

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Введение в криптографию. Основные классы шифров и их свойства Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	лекция	История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Критерии распознавания открытого текста. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование.
лекция		Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Дисковые шифраторы колонной замены.	
лекция		Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89. Криптоалгоритм AES.	

			Режимы использования блочных шифров
2.	Введение в криптографию. Основные классы шифров и их свойства Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	лекция	Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии. Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры
лекция		Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки. Примеры имитостойких и неимитостойких шифров. Методы имитозащиты неимитостойких шифров. Имитовставки. Коды аутентификации. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков. Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Особенности режимов использования блочных шифров. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров.	
лекция		Строение поточных шифрсистем. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел. Линейные рекуррентные последовательности (ЛРП) над полем. Фильтрующие и комбинирующие генераторы, и их свойства. Композиции линейных регистров сдвига. Подходы к анализу алгоритмов шифрования. Особенности криптоанализа алгоритмов блочного шифрования. Особенности анализа программных реализаций криптографических алгоритмов.	
3.	Введение в криптографию. Основные классы шифров и их свойства	лекция	Шифрсистема RSA. Шифрсистема Эль-Гамала. Шифрсистема Мак-Элиса. Шифрсистема на основе задачи об “укладке рюкзака”. Анализ шифрсистемы RSA. Практические аспекты использования шифрсистем с открытым ключом. Общие положения. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамала. Стандарты цифровой подписи.

		лекция	Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением. Алгоритмы передачи ключей (с использованием и без использования цифровой подписи). Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.
		лекция	Общие сведения о хеш-функциях. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции. Целостность данных и аутентификация источника данных. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC.

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Введение в криптографию. Основные классы шифров и их свойства Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом Введение в криптографию. Основные классы шифров и их свойства Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	практическое занятие	История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Критерии распознавания открытого текста.
		практическое занятие	Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование.
		практическое занятие	Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. Разновидности шифров перестановки: маршрутные и геометрические перестановки.
		практическое занятие	Элементы криптоанализа шифров перестановки. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Дисковые шифраторы колонной замены.
		практическое занятие	Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана.
		практическое занятие	Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритм DES.

			Криптоалгоритм ГОСТ-28147-89. Криптоалгоритм AES. Режимы использования блочных шифров
2.	<p>Введение в криптографию. Основные классы шифров и их свойства Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом</p> <p>Введение в криптографию. Основные классы шифров и их свойства Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом</p>	практическое занятие	Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии.
практическое занятие		Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры	
практическое занятие		Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки. Примеры имитостойких и неимитостойких шифров. Методы имитозащиты неимитостойких шифров. Имитовставки. Коды аутентификации. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков.	
практическое занятие		Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Особенности режимов использования блочных шифров. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров.	
практическое занятие		Строение поточных шифрсистем. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел. Линейные рекуррентные последовательности (ЛРП) над полем. Фильтрующие и комбинирующие генераторы, и их свойства	
практическое занятие		Композиции линейных регистров сдвига. Подходы к анализу алгоритмов шифрования. Особенности криптоанализа алгоритмов блочного шифрования. Особенности анализа программных реализаций криптографических алгоритмов	
3.	<p>Введение в криптографию. Основные классы шифров и их свойства</p>	практическое занятие	Шифрсистема RSA. Шифрсистема Эль-Гамала. Шифрсистема Мак-Элиса. Шифрсистема на основе задачи об “укладке рюкзака”. Анализ шифрсистемы RSA. Практические аспекты использования шифрсистем с открытым ключом. Общие положения.

	практическое занятие	Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамала. Стандарты цифровой подписи.
	практическое занятие	Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением.
	практическое занятие	Алгоритмы передачи ключей (с использованием и без использования цифровой подписи). Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.
	практическое занятие	Общие сведения о хеш-функциях. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции.
	практическое занятие	Целостность данных и аутентификация источника данных. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC.

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Введение в криптографию. Основные классы шифров и их свойства	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN

978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560804>

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561432>

Дополнительная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560977>

2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536453>

3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560426>

Литература для самостоятельного изучения

1.

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС ; ОС "Альт Рабочая станция" 10; ОС "Альт Образование" 10

2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный, МойОфис Стандартный 3, МойОфис Профессиональный 3

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - <http://www.gov.ru/>)

2. Государственная система правовой информации «Официальный интернет-портал правовой информации» (<http://pravo.gov.ru/>)

3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - <https://www.minfin.ru/ru/>)

4. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - <http://www.gks.ru/>)

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. справочно-правовая система «Консультант Плюс»

2. справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения	Комплекты ученической мебели

практических занятий (занятий семинарского типа)	Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

5.6 Лаборатории и лабораторное оборудование

Лаборатория информационных технологий в профессиональной деятельности	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ Лабораторное оборудование
---	---

6. Фонд оценочных средств по дисциплине Криптографическая защита информации:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Оценка докладов	+
	Тестирование	+
	Лабораторные работы	+
Промежуточный контроль	Экзамен	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Профессиональные компетенции (ПК):

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по программе	Планируемые результаты обучения по дисциплине		
	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств
Пороговый	некоторые особенности защиты автоматизированных систем	оценивать защищенность автоматизированных систем	навыками защищенности автоматизированных систем
Стандартный (в дополнение к пороговому)	некоторые особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность компонент автоматизированных систем с помощью типовых программных средств	навыками защищенности компонент автоматизированных систем с помощью типовых программных средств
Повышенный (в дополнение к пороговому, стандартному)	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Введение в криптографию. Основные классы шифров и их свойства	ПК-2.1, ПК-2.2, ПК-2.3	Тестирование Практические задачи	Экзамен
2.	Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	ПК-2.1, ПК-2.2, ПК-2.3	Тестирование Практические задачи	Экзамен
3.	Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения	ПК-2.1, ПК-2.2, ПК-2.3	Тестирование Практические задачи	Экзамен

6.4.Оценочные материалы для текущего контроля

Ссылка на текущую академическую активность, точки текущего контроля для всех оценочных материалов, размещенных в БРСО ЭИОС СГЭУ: <https://lms2.sseu.ru/course/index.php?categoryid=1918>

Примерная тематика докладов

Раздел дисциплины	Темы
Введение в криптографию. Основные классы шифров и их свойства	Простейшие криптографические протоколы. Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Многоалфавитные шифры замены. Дисковые шифраторы колонной замены
Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	Характеристики имитостойкости шифров и их оценки. Коды аутентификации. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров.
Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения	Шифрсистема RSA. Шифрсистема Эль-Гамала. Шифрсистема Мак-Элиса. Шифрсистема на основе задачи об “укладке рюкзака”. Анализ шифрсистемы RSA Цифровые подписи на основе шифрсистем с открытым ключом. Стандарты цифровой подписи.

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)

1. Что понимается под безопасностью сети?

+защита ее от вмешательства в процесс функционирования;
защита сети от атак;
защита сети от вирусов;
защита информации от искажения

2. В чём отличие санкционированного (СД) и несанкционированного (НСД) доступа к информации?

+СД не нарушает установленные правила разграничения доступа;
НСД не нарушает установленные правила;
СД обеспечивает конфиденциальность информации;
СД обеспечивает целостность информации.

3. Конфиденциальность данных (информации) это?

внутреннее свойство информации;
+статус, представляемый данным и определяющий степень их защиты;
значительные объемы информации; информация, предназначенная для передачи.

4. Субъект информационной системы это?

пользователь системы; +активный компонент системы, который может стать причиной потока информации от объекта к субъекту;
отправитель сообщения; получатель сообщения.

5. Объект информационной системы это?

межсетевой экран; шифратор;
+пассивный компонент системы, хранящий, принимающий или передающий информацию;

скремблер.

6. Целостность информации это:

скрытность информации;
важность информации;
+подлинность информации;
объем информации.

7. Угроза безопасности сети это:

+возможные разрушительные воздействия на сеть;
нарушение работоспособности сети;
отказ каналообразующего оборудования;
отказ коммутационного оборудования.

8. Уязвимость сети это:

отсутствие межсетевых экранов в сети;
+неудачное свойство сети, провоцирующее возникновение и реализацию угрозы;
отсутствие средств активной защиты;
отсутствие средств анализа защищенности

9. Атака на сеть это:

нарушение конфиденциальности;
нарушение целостности;
нарушение доступности;
+реализация угрозы безопасности.

10. Политика безопасности это:

организационно-правовое обеспечение информационной безопасности;
административные меры обеспечения информационной безопасности;
+нормы, правила и практические рекомендации, регламентирующие работу средств защиты сетей;
технические средства обеспечения информационной безопасности.

11. Дискреционная политика безопасности основана на:

симметричном шифровании; асимметричном шифровании; электронной цифровой подписи;
+множестве заданных администратором разрешенных отношений доступа субъектов к объектам.

12. Полномочная политика безопасности основана на:

алгоритме распределения ключей;
+представлении доступа в зависимости от метки конфиденциальности информации и уровня доверия пользователя;
протоколах идентификации;
протоколах аутентификации.

13. Цель процедуры идентификации заключается в:

+предъявлении субъектом своего уникального имени по запросу системы;
доказательстве подлинности;
доказательстве целостности;
применении электронной цифровой подписи.

14. Цель процедуры аутентификации заключается в:

управлении криптографическими ключами;
антивирусной защите;
+доказательстве подлинности;
противодействию угрозам безопасности.

15. Назначение средств авторизации заключается в:

распределении ключей;

+контроле доступа легальных пользователей к ресурсам системы;
построении VPN;
криптографической защите данных.

16. Назначение технологии аудита в информационной системе:
обеспечение целостности;
обеспечение конфиденциальности;
+фиксация в системном журнале событий, связанных с доступом к защищаемым ресурсам;
устранение уязвимостей.

17. Симметричная криптосистема основана на применении:
+криптоалгоритма и одного секретного ключа;
одного секретного ключа; двух секретных ключей;
электронной цифровой подписи.

18. Асимметричная криптосистема основана на применении:
защищенного канала;
+криптоалгоритма, открытого и секретного ключей;
алгоритма скрытой передачи ключей; алгоритмов аутентификации.

19. Основные функции управления криптографическими ключами:
шифрование ключей;
распределение ключей;
+генерация, хранение и распределение ключей;
сертификация ключей.

20. Цель сертификации открытых ключей:
повышение защищенности системы;
повышение надежности системы;
+обеспечение целостности открытых ключей;
повышение быстродействия системы.

21. Классической сетью Фейстеля называется:
корпоративная сеть;
виртуальная частная сеть VPN;
+методика обратимых преобразований данных;
инфраструктура открытых ключей РКІ.

22. Размер ключа стандарта ГОСТ 28147-86:
128;
512;
+256;
64.

23. Количество раундов стандарта ГОСТ 28147-89:
16;
8;
+32;
64.

24. Имитозащитой называется:
идентификация;
аутентификация;
+защита системы связи от навязывания ложных данных;
генерация ключей.

25. Поточным шифрованием называется:

стандарт DES;
стандарт ГОСТ 28147-89;
+посимвольное шифрование;
блочное шифрование.

26. Какое многократное шифрование позволяет увеличить длину результирующего ключа:
шифрование DES;
+шифрование 3DES;
шифрование ГОСТ 28147-89;
шифрование RSA.

27. Криптосистема RSA относится:
к симметричным криптосистемам;
+к асимметричным криптосистемам;
к системам двукратного шифрования;
к системам трехкратного шифрования.

28. Комбинированный метод шифрования предназначен для:
формирования ЭЦП;
проверки ЭЦП;
+скрытого (защищенного) распределения секретных ключей по открытому каналу;
идентификации и аутентификации.

29. Протокол Гиллоу-Куискуотера предназначен для:
шифрования данных;
расшифрования данных;
+идентификации с нулевой передачей знаний;
авторизации.

30. Электронная цифровая подпись (ЭЦП) предназначена для:
шифрования данных;
идентификации абонентов;
+аутентификации отправителя и контроля целостности электронного сообщения;
обеспечения конфиденциальности

Практические задачи (min 20, max 50 + ссылку на ЭИОС с электронным изданием, если имеется)

Раздел дисциплины	Задачи
Введение в криптографию. Основные классы шифров и их свойства	<ol style="list-style-type: none">1. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Критерии распознавания открытого текста.2. Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование.3. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы. Разновидности шифров перестановки: маршрутные и геометрические перестановки.4. Элементы криптоанализа шифров перестановки. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Дисковые шифраторы колонной замены.

	<p>5. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана.</p> <p>6. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры. Криптоалгоритм DES. Криптоалгоритм ГОСТ-28147-89. Криптоалгоритм AES. Режимы использования блочных шифров.</p>
<p>Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом</p>	<p>1. Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. О теоретико-информационном подходе в криптографии.</p> <p>2. Энтропия и количество информации. “Ненадёжность шифра”, “ложные ключи” и “расстояние единственности”. Практически стойкие шифры</p> <p>3. Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки. Примеры имитостойких и неимитостойких шифров. Методы имитозащиты неимитостойких шифров. Имитовставки. Коды аутентификации. Понятие о помехоустойчивости шифра. Шифры, не размножающие искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков.</p> <p>4. Принципы построения алгоритмов блочного шифрования. Выбор базовых преобразований. Особенности режимов использования блочных шифров. Принципы построения алгоритмов поточного шифрования. Режимы использования поточных шифров.</p> <p>5. Строение поточных шифрсистем. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел. Линейные рекуррентные последовательности (ЛРП) над полем. Фильтрующие и комбинирующие генераторы, и их свойства</p> <p>6. Композиции линейных регистров сдвига. Подходы к анализу алгоритмов шифрования. Особенности криптоанализа алгоритмов блочного шифрования. Особенности анализа программных реализаций криптографических алгоритмов</p>
<p>Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения</p>	<p>1. Шифрсистема RSA. Шифрсистема Эль-Гамала. Шифрсистема Мак-Элиса.</p> <p>2. Шифрсистема на основе задачи об “укладке рюкзака”. Анализ шифрсистемы RSA. Практические аспекты использования шифрсистем с открытым ключом. Общие положения.</p> <p>3. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамала. Стандарты цифровой подписи.</p> <p>4. Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением.</p> <p>5. Алгоритмы передачи ключей (с использованием и без использования цифровой подписи). Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.</p>

	<p>6. Общие сведения о хеш-функциях. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функции.</p> <p>7. Целостность данных и аутентификация источника данных. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC.</p>
--	--

Тематика контрольных работ

Раздел дисциплины	Темы
Введение в криптографию. Основные классы шифров и их свойства	Отечественный стандарт цифровой подписи Классификация угроз информационной безопасности корпоративных сетей. Методы генерации ключей. Понятие политики безопасности и ее основные виды: дискреционная и мандатная. Алгоритм открытого распределения ключей Диффи-Хеллмана Базовые технологии информационной безопасности:
Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом	Комбинирование блочных алгоритмов. Схема двукратного и трехкратного алгоритмов DES. Цели аутентификации электронного документа. Электронная цифровая подпись. Пути реализации угроз безопасности информационных систем. Блочные и поточные шифры. Алгоритм шифрования ГОСТ 28147-89. Режим простой замены. Концепция криптосистемы с открытым ключом. Однонаправленные функции
Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения	Алгоритм шифрования DES. Режим CFB Комбинированный метод шифрования. Алгоритм шифрования DES. Режим OFB. Схема шифрования Полига-Хеллмана.

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме экзамена

Раздел дисциплины	Вопросы
Введение в криптографию. Основные классы шифров и их свойства	<ol style="list-style-type: none"> 1. Основные понятия информационной безопасности передачи данных: безопасность сети, санкционированный и несанкционированный доступ, конфиденциальность и целостность данных. 2. Требования, предъявляемые к процедуре распределения ключей. Протокол Kerberos 3. Понятия субъект и объект информационной системы, угроза и ущерб безопасности, уязвимость сети, атака на сеть. 4. Отечественный стандарт цифровой подписи 5. Классификация угроз информационной безопасности корпоративных сетей. 6. Хэш-функции на основе симметричных блочных алгоритмов. 7. Защищенный канал. Защита на канальном уровне. Основные протоколы. 8. Методы генерации ключей. 9. Понятие политики безопасности и ее основные виды: дискреционная и мандатная. 10. Алгоритм открытого распределения ключей Диффи-Хеллмана 11. Базовые технологии информационной безопасности: идентификация, аутентификация, авторизация, аудит, технология защищенного виртуального канала. 12. Цифровая подпись с дополнительными функциональными

	<p>свойствами. Схемы слепой и неоспоримой подписи. 13. Принципы криптографической защиты данных. 14. Концепция иерархии ключей. 15. Обобщенная схема симметричной криптосистемы. 16. Типовые схемы идентификации и аутентификации пользователей. 17. Обобщенная схема асимметричной криптосистемы. 18. Алгоритм цифровой подписи Эль Гамала. 19. Защищенный канал. Защита на сетевом уровне. Протокол защиты содержимого пакетов ESP 20. Основные принципы, используемые в практических шифрах, и пути их реализации.</p>
<p>Надёжность шифров. Методы синтеза и анализа криптографических алгоритмов с секретным ключом</p>	<ol style="list-style-type: none"> 1. Отечественный стандарт хэш-функции. 2. Классическая сеть Фейстеля. 3. Хранение ключей и основные носители ключевой информации. 4. Американский стандарт шифрования DES. Основные характеристики. Структурная схема. 5. Однонаправленные хэш-функции. 6. Комбинирование блочных алгоритмов. Схема двукратного и трехкратного алгоритмов DES. 7. Цели аутентификации электронного документа. Электронная цифровая подпись. 8. Пути реализации угроз безопасности информационных систем. 9. Защищенный канал. Защита на сетевом уровне. Архитектура стека протоколов IPsec. 10. Блочные и поточные шифры. 11. Алгоритм шифрования ГОСТ 28147-89. Режим простой замены. Концепция криптосистемы с открытым ключом. Однонаправленные функции
<p>Методы синтеза и анализа криптографических алгоритмов с открытым ключом. Хэш-функции и их криптографические приложения</p>	<ol style="list-style-type: none"> 1. Алгоритм шифрования DES. Режим ECB 2. Криптосистема шифрования данных RSA. 3. Алгоритм шифрования DES. Режим CBC 4. Процедура шифрования и расшифрования в криптосистеме RSA. 5. Алгоритм шифрования DES. Режим CFB 6. Комбинированный метод шифрования. 7. Алгоритм шифрования DES. Режим OFB. 8. Схема шифрования Полига-Хеллмана. 9. Системы централизованного контроля доступа. Система TACACS. 10. Схема шифрования Эль Гамала. 11. Протокол аутентификации и распределения ключей Kerberos 12. Основные понятия и концепции аутентификации и идентификации. Требования защиты при обмене сообщениями. 13. Защита данных в Web. Размещение средств защиты Web. Протокол SSL. 14. Основные типовые схемы идентификации и аутентификации пользователей. 15. Классическая сеть Фейстеля 16. Взаимная аутентификация пользователей. Процедура рукопожатия. 17. Схема шифрования Эль Гамала 18. Упрощенная схема идентификации с нулевой передачей знаний. 19. Алгоритм DES. Схема вычисления функции шифрования 20. Параллельная схема идентификации с нулевой передачей знаний. 21. Защищенный канал. Установление защищенного канала. Протокол IKE 22. Схема идентификации Гиллоу-Куискуотера. 23. Сущность проблемы управления криптографическими ключами. 24. Алгоритм цифровой подписи RSA.

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	Критерии оценивания для мероприятий контроля с применением 4-х балльной системы
«отлично»	Повышенный ПК-2.1, ПК-2.2, ПК-2.3
«хорошо»	Стандартный ПК-2.1, ПК-2.2, ПК-2.3
«удовлетворительно»	Пороговый ПК-2.1, ПК-2.2, ПК-2.3
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне