МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____П.В. Сенченко
«23» _____12_____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.04 Информационно-аналитические системы безопасности**
Направленность (профиль) / специализация: **Информационная безопасность финансовых и экономических структур**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра безопасности информационных систем (БИС)**
Курс: **3**
Семестр: **6**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	6 семестр	Всего	Единицы
Лекционные занятия	30	30	часов
Практические занятия	30	30	часов
Самостоятельная работа	48	48	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
	4	4	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	6

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 23.12.2020
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 56438

1. Общие положения

1.1. Цели дисциплины

1. Целью дисциплины «Криптографические методы защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

1.2. Задачи дисциплины

1. дать представление о криптографических методах защиты информации.
2. изучить математические основы современной криптографии.
3. изучить современные стандарты симметричного шифрования.
4. изучить основные криптографические алгоритмы с открытым ключом.
5. изучить криптографические функции хеширования.
6. сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль специальности (special hard skills - SHS).
Индекс дисциплины: Б1.О.03.20.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

Согласована на портале № 56438

ОПК-3. Способен на основании совокупности существующих математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает основные понятия математического анализа и алгебры, необходимые для решения задач профессиональной деятельности	Знает основные понятия математического анализа и алгебры, необходимые для решения задач профессиональной деятельности в области реализации криптографического обеспечения
	ОПК-3.2. Умеет применять основные математические методы, а также методы теории вероятностей и математической статистики для решения задач профессиональной деятельности	Умеет применять основные математические методы, а также методы теории вероятностей и математической статистики для решения задач профессиональной деятельности в области анализа и реализации криптографического обеспечения
	ОПК-3.3. Владеет практическими навыками решения математических задач и построения статистических моделей экспериментов при решении прикладных задач в области профессиональной деятельности	Владеет практическими навыками решения математических задач и построения статистических моделей экспериментов при решении прикладных задач в области профессиональной деятельности, связанных с аналитическим и экспериментальным исследованием криптографического обеспечения

Согласована на портале № 56438

ОПК-9. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-9.1. Знает основные понятия криптографии и криптографические методы защиты информации, основные типы средств криптографической защиты информации (СКЗИ) и предъявляемые к ним требования	Знает основные понятия криптографии и криптографические методы защиты информации, необходимые для понимания функционирования профессионального программного обеспечения, реализующего криптографические алгоритмы и протоколы
	ОПК-9.2. Умеет осуществлять обоснованный выбор и использовать СКЗИ при решении задач профессиональной деятельности	Способность обнаруживать уязвимости и противодействовать им, в том числе с применением криптографических методов
	ОПК-9.3. Владеет практическими навыками разработки криптографических алгоритмов механизмов, определяемых национальными стандартами и рекомендациями Российской Федерации и стандартами международной организации по стандартизации	Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности, необходимыми для защиты данных при их передаче по открытым каналам связи
Профессиональные компетенции		
-	-	-

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		6 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	60	60
Лекционные занятия	30	30
Практические занятия	30	30
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	48	48
Подготовка к тестированию	20	20
Написание отчета по практическому занятию (семинару)	28	28
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	144	144

Согласована на портале № 56438

Общая трудоемкость (в з.е.)	4	4

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
6 семестр					
1 Математические основы криптографии	2	16	9	27	ОПК-3, ОПК-9
2 Основные цели и задачи криптографии	4	-	2	6	ОПК-3, ОПК-9
3 Историческая криптография	2	4	9	15	ОПК-3, ОПК-9
4 Симметричное шифрование	6	2	9	17	ОПК-3, ОПК-9
5 Хеширование	2	-	2	4	ОПК-3, ОПК-9
6 Поточное шифрование	2	-	2	4	ОПК-3, ОПК-9
7 ГСПЧ и проверка их качества	2	-	2	4	ОПК-3, ОПК-9
8 Криптография с открытым ключом	4	8	9	21	ОПК-3, ОПК-9
9 Электронная подпись	4	-	2	6	ОПК-3, ОПК-9
10 Протоколы	2	-	2	4	ОПК-3, ОПК-9
Итого за семестр	30	30	48	108	
Итого	30	30	48	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
6 семестр			
1 Математические основы криптографии	Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.	2	ОПК-3, ОПК-9
	Итого	2	

Согласована на портале № 56438

2 Основные цели и задачи криптографии	Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках. Генерация простых чисел. Тест на простоту. Алгоритмы работы с большими числами.	4	ОПК-3, ОПК-9
	Итого	4	
3 Историческая криптография	Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.	2	ОПК-3, ОПК-9
	Итого	2	
4 Симметричное шифрование	DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, эммитовставка. AES.	6	ОПК-3, ОПК-9
	Итого	6	
5 Хеширование	Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.	2	ОПК-3, ОПК-9
	Итого	2	
6 Поточное шифрование	Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Шифр RC-4 как пример поточного алгоритма шифрования.	2	ОПК-3, ОПК-9
	Итого	2	
7 ГСПЧ и проверка их качества	Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Критерии качества псевдослучайных чисел. Виды тестов псевдослучайных последовательностей. Тесты NIST.	2	ОПК-3, ОПК-9
	Итого	2	
8 Криптография с открытым ключом	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистема Рабина.	4	ОПК-3, ОПК-9
	Итого	4	
9 Электронная подпись	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.	4	ОПК-3, ОПК-9
	Итого	4	

Согласована на портале № 56438

10 Протоколы	Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений.	2	ОПК-3, ОПК-9
	Итого	2	
Итого за семестр		30	
Итого		30	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3 – Наименование практических занятий (семинаров)

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
6 семестр			
1 Математические основы криптографии	Алгебраические структуры. Группы. Циклические группы.	4	ОПК-3, ОПК-9
	Кольца, кольца классов вычетов.	4	ОПК-3, ОПК-9
	Конечные поля, поля Галуа.	4	ОПК-3, ОПК-9
	Теоретико-числовые алгоритмы, используемые в криптографии	4	ОПК-3, ОПК-9
	Итого	16	
3 Историческая криптография	Простейшие шифры и их криптоанализ.	4	ОПК-3, ОПК-9
	Итого	4	
4 Симметричное шифрование	Современные симметричные шифры	2	ОПК-3, ОПК-9
	Итого	2	
8 Криптография с открытым ключом	Протокол Диффи-Хеллмана	2	ОПК-3, ОПК-9
	Криптосистема RSA	2	ОПК-3, ОПК-9
	Криптосистема Эль-Гамаля	2	ОПК-3, ОПК-9
	Криптосистема Рабина	2	ОПК-3, ОПК-9
	Итого	8	
Итого за семестр		30	
Итого		30	

5.4. Лабораторные занятия

Не предусмотрено учебным планом

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля

Согласована на портале № 56438

6 семестр				
1 Математические основы криптографии	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Написание отчета по практическому занятию (семинару)	7	ОПК-3, ОПК-9	Отчет по практическому занятию (семинару)
	Итого	9		
2 Основные цели и задачи криптографии	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Итого	2		
3 Историческая криптография	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Написание отчета по практическому занятию (семинару)	7	ОПК-3, ОПК-9	Отчет по практическому занятию (семинару)
	Итого	9		
4 Симметричное шифрование	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Написание отчета по практическому занятию (семинару)	7	ОПК-3, ОПК-9	Отчет по практическому занятию (семинару)
	Итого	9		
5 Хеширование	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Итого	2		
6 Поточное шифрование	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Итого	2		
7 ГСПЧ и проверка их качества	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Итого	2		
8 Криптография с открытым ключом	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Написание отчета по практическому занятию (семинару)	7	ОПК-3, ОПК-9	Отчет по практическому занятию (семинару)
	Итого	9		
9 Электронная подпись	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Итого	2		
10 Протоколы	Подготовка к тестированию	2	ОПК-3, ОПК-9	Тестирование
	Итого	2		
Итого за семестр		48		

Согласована на портале № 56438

	Подготовка и сдача экзамена	36		Экзамен
Итого		84		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Прак. зан.	Сам. раб.	
ОПК-3	+	+	+	Тестирование, Экзамен, Отчет по практическому занятию (семинару)
ОПК-9	+	+	+	Тестирование, Экзамен, Отчет по практическому занятию (семинару)

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
6 семестр				
Тестирование	10	10	10	30
Отчет по практическому занятию (семинару)	10	20	10	40
Экзамен				30
Итого максимум за период	20	30	20	100
Нарастающим итогом	20	50	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Согласована на портале № 56438

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линияТелеком, 2016. — 232 с. — Загл. с экрана. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111098.

7.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с. (наличие в библиотеке ТУСУР - 30 экз.).

2. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2002. — 176 с. (наличие в библиотеке ТУСУР - 6 экз.).

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/489919.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ: [Электронный ресурс]: — Режим доступа: https://cloud.fb.tusur.ru/index.php/s/Htd7FxD8JbxB93D.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

Согласована на портале № 56438

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория программно-аппаратных средств обеспечения информационной безопасности: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 405 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Аппаратные средства аутентификации пользователя "eToken Pro";
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x;
- Устройства чтения смарт-карт и радиометок: адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными

Согласована на портале № 56438

возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Математические основы криптографии	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Основные цели и задачи криптографии	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Историческая криптография	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 56438

4 Симметричное шифрование	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Хеширование	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
6 Поточное шифрование	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
7 ГСПЧ и проверка их качества	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
8 Криптография с открытым ключом	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
9 Электронная подпись	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
10 Протоколы	ОПК-3, ОПК-9	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков

Согласована на портале № 56438

3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какой криптографический метод защиты информации предназначен для обеспечения конфиденциальности информации?
   а) Хеширование
   б) Электронная подпись
   в) Шифрование
   г) Коды аутентичности сообщений
2. Для решения какой задачи обеспечения информационной безопасности предназначено хеширование?
   а) Обеспечение конфиденциальности информации

Согласована на портале № 56438

б) Обеспечение неотказуемости
в) Обеспечение контроля целостности данных
г) Проверка подлинности источника данных

3. Каким свойством обладают элементы a и a^-1 в кольце классов вычетов по модулю n?
   а) a·a^-1 = 0 (mod n)
   б) a·a^-1 = –1 (mod n)
   в) a·a^-1 = 1 (mod n)
   г) a·a^-1 = n (mod n)
4. В каком случае существует значение a^-1 по модулю n?
   а) Если a делит n
   б) Если n делит a
   в) Если НОД(a, n) = 1
   г) Если НОД(a, n) > 1
5. Поставьте в соответствие двоичной последовательности 11001101 элемент поля Галуа GF(2^8), в виде которого можно представить данную последовательность для проведения над ней криптографических преобразований.
   а) x^8 + x^7 + x^4 + x^3 + x
   б) x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1
   в) x^7 + x^6 + x^3 + x^2 + 1
   г) x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1
6. Чем шифр «Магма» отличается от шифра, определенного в стандарте ГОСТ 28147-89?
   а) Длиной ключа
   б) Это два принципиально разных симметричных блочных шифра
   в) Невозможностью использования произвольной таблицы замен
   г) Количеством раундов
7. Какова длина секретного ключа в шифре «Кузнечик»?
   а) 64 бита
   б) 128 бит
   в) 256 бит
   г) 512 бит
8. Какой из режимов работы симметричных блочных шифров не предназначен для обеспечения конфиденциальности информации?
   а) Режим простой замены
   б) Режим простой замены с зацеплением
   в) Режим выработки имитовставки
   г) Режим гаммирования
9. В каком из режимов работы симметричных блочных шифров результат зашифрования очередного блока открытого текста при фиксированном ключе зависит только от порядкового номера данного блока?
   а) Режим простой замены
   б) Режим гаммирования с обратной связью по выходу
   в) Режим гаммирования
   г) Режим гаммирования с обратной связью по шифртексту
10. Какой из перечисленных шифров относится к классу асимметричных шифров?
    а) Магма
    б) Кузнечик
    в) RSA
    г) AES
11. В чем заключается различие между симметричными и асимметричными криптосистемами?
    а) В решаемых задачах защиты информации
    б) В показателях криптографической стойкости
    в) В количестве и назначении используемых ключей
    г) Принципиальных различий нет
12. Почему асимметричные криптосистемы затруднительно использовать для непосредственного шифрования видеотрафика?
    а) В связи с недостаточной криптографической стойкостью асимметричных криптосистем

Согласована на портале № 56438

б) В связи с отсутствием соответствующих стандартов
в) В связи с недостаточным быстродействием асимметричных криптосистем
г) Асимметричные криптосистемы используются для непосредственного шифрования видеотрафика

13. Сопоставьте действующие отечественные криптографические стандарты с перечисленными криптографическими методами защиты информации в порядке их перечисления: шифрование, хеширование, электронная подпись.
    а) ГОСТ Р 34.12–2015, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012
    б) ГОСТ 28147-89, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012
    в) ГОСТ Р 34.12–2015, ГОСТ Р 34.11–2012, ГОСТ Р 34.10–2012
    г) ГОСТ Р 34.12–2015, ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012
14. На какой вычислительной задаче основана криптосистема RSA?
    а) Нахождение наибольшего общего делителя
    б) Вычисление модулярно обратного элемента
    в) Целочисленная факторизация
    г) Дискретное логарифмирование
15. На каком математическом аппарате основана схема электронной подписи, определенная в стандарте ГОСТ Р 34.10–2012?
    а) Кольца классов вычетов
    б) Поля Галуа
    в) Эллиптические кривые
    г) Матричные группы
16. Чем код аутентичности отличается от хеш-кода?
    а) Это синонимы
    б) Хеш-код рассчитывается с использованием секретного ключа, а код аутентичности — без использования секретного ключа
    в) Код аутентичности рассчитывается с использованием секретного ключа, а хеш-код — без использования секретного ключа
    г) Код аутентичности рассчитывается с использованием закрытого ключа, а хеш-код — с использованием открытого ключа
17. Чем код аутентичности отличается от электронной подписи?
    а) Это синонимы
    б) Длиной ключа
    в) Электронная подпись обеспечивает неотказуемость, а код аутентичности — нет
    г) Электронная подпись обеспечивает возможность проверки подлинности источника данных, а код аутентичности — нет
18. Для чего в схемах электронной подписи используются функции хеширования?
    а) Для повышения криптографической стойкости схемы электронной подписи
    б) Для обеспечения контроля целостности подписываемого сообщения
    в) Для представления подписываемого сообщения произвольной длины в виде строки данных фиксированной длины
    г) Для представления подписанного сообщения произвольной длины в виде строки данных фиксированной длины
19. Чем схема электронной подписи, определенная в стандарте ГОСТ Р 34.10-2012, отличается от схемы электронной подписи, определенной в стандарте ГОСТ Р 34.10-2001?
    а) Перечнем решаемых задач
    б) Используемым математическим аппаратом
    в) Длиной подписи
    г) Ничем не отличается
20. Что является основной проблемой криптографии с открытым ключом?
    а) Обеспечение аутентичности закрытых ключей
    б) Обеспечение конфиденциальности закрытых ключей
    в) Обеспечение аутентичности открытых ключей
    г) Обеспечение конфиденциальности открытых ключей

9.1.2. Перечень экзаменационных вопросов

Согласована на портале № 56438

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Кольца. Кольца классов вычетов.
4. Поля. Поля Галуа.
5. Цели и задачи криптографии. Основные понятия.
6. Простейшие шифры: простой замены, перестановочный, аффинный.
7. Шифр Хилла.
8. Генерация простых чисел.
9. Шифры гаммирования. Шифр Вернама (одноразовый блокнот).
10. ГОСТ Р 34.12-2015. Шифр «Магма».
11. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
12. Генерация псевдослучайных последовательностей и их тесты.
13. Поточное шифрование.
14. Стандарт шифрования DES.
15. Стандарт шифрования AES.
16. Криптография с открытым ключом.
17. Ранцевая криптосистема.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамаля.
20. Протокол Диффи-Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. Коды аутентичности сообщений. Электронная подпись.
24. ГОСТ Р 34.10-2012.
25. Протокол передачи бита.
26. Слепые подписи.
27. Протоколы доказательств знания с нулевым разглашением.
28. Протоколы электронного голосования.
29. Протоколы безопасных вычислений.

9.1.3. Темы практических занятий

1. Алгебраические структуры. Группы. Циклические группы.
2. Кольца, кольца классов вычетов.
3. Конечные поля, поля Галуа.
4. Теоретико-числовые алгоритмы, используемые в криптографии
5. Простейшие шифры и их криптоанализ.
6. Современные симметричные шифры
7. Протокол Диффи-Хеллмана
8. Криптосистема RSA
9. Криптосистема Эль-Гамаля
10. Криптосистема Рабина

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

Согласована на портале № 56438

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах,

Согласована на портале № 56438

адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 56438

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры БИС
протокол № 11 от «14» 12 2020 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Заведующий обеспечивающей каф. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

и.о. заведующего кафедрой, каф. БИС	Е.Ю. Костюченко	Разработано, c6235dfe-234a-4234-88f9-e1597aac6463

Согласована на портале № 56438