МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы криптографии

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Специализация: **Экономико-правовое обеспечение экономической безопасности**
Направленность (профиль): **Регламентация работы персонала организации при обеспечении экономической и информационной безопасности**
Форма обучения: **заочная**
Факультет: **ЗиВФ, Заочный и вечерний факультет**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **8, 9**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	2	4	6	часов
2	Лабораторные работы	4	8	12	часов
3	Всего аудиторных занятий	6	12	18	часов
4	Из них в интерактивной форме	2	4	6	часов
5	Самостоятельная работа	30	56	86	часов
6	Всего (без экзамена)	36	68	104	часов
7	Подготовка и сдача зачета	0	4	4	часов
8	Общая трудоемкость	36	72	108	часов
				3.0	З.Е.

Контрольные работы: 9 семестр - 1
Зачет: 9 семестр

Томск 2018

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «15» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. БИС _____ О. О. Евсютин

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ЗиВФ _____ И. В. Осипов

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент каф. КИБЭВС _____ К. С. Сарин

Доцент каф. КИБЭВС _____ Е. Ю. Костюченко

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Основы криптографии» 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

- дать представление о криптографических методах защиты информации;
- изучить современные стандарты симметричного шифрования;
- изучить криптографические функции хеширования;
- изучить основные криптографические алгоритмы с открытым ключом;
- дать общее представление об инфраструктуре открытых ключей.

2. Место дисциплины в структуре ОПОП

Дисциплина «Основы криптографии» (Б1.В.ДВ.3.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы криптографии, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности.

Последующими дисциплинами являются: Основы криптографии.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

В результате изучения дисциплины обучающийся должен:

- **знать** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.
- **уметь** навыками использования типовых криптографических алгоритмов.
- **владеть** криптографическими методами и средствами защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		8 семестр	9 семестр
Аудиторные занятия (всего)	18	6	12
Лекции	6	2	4
Лабораторные работы	12	4	8
Из них в интерактивной форме	6	2	4
Самостоятельная работа (всего)	86	30	56
Оформление отчетов по лабораторным работам	24	8	16
Проработка лекционного материала	14	6	8
Самостоятельное изучение тем (вопросов) теоретической части курса	40	16	24
Выполнение контрольных работ	8	0	8

Всего (без экзамена)	104	36	68
Подготовка и сдача зачета	4	0	4
Общая трудоемкость, ч	108	36	72
Зачетные Единицы	3.0		

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., час.	Лаб. раб.,	Сам. раб.,	Всего (без	Формируемые компетенции
8 семестр					
1 Основные цели и задачи криптографии	1	0	2	3	ПК-20
2 Симметричное шифрование	1	4	28	33	ПК-20
Итого за семестр	2	4	30	36	
9 семестр					
3 Хеширование	1	0	10	11	ПК-20
4 Криптография с открытым ключом	1	0	14	15	ПК-20
5 Электронная подпись	2	8	32	42	ПК-20
Итого за семестр	4	8	56	68	
Итого	6	12	86	104	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ак. часов	Формируемые компетенции
8 семестр			
1 Основные цели и задачи криптографии	Основная криптографическая терминология. Основные криптографические методы защиты информации: шифрование, хеширование, электронная подпись	1	ПК-20
	Итого	1	
2 Симметричное шифрование	ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. AES.	1	ПК-20
	Итого	1	
Итого за семестр		2	
9 семестр			
3 Хеширование	Криптографические хеш-функции. ГОСТ Р 34.11-2012.	1	ПК-20
	Итого	1	
4 Криптография с открытым ключом	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA.	1	ПК-20
	Итого	1	
5 Электронная подпись	Электронная подпись. ГОСТ Р 34.10-2012. Инфраструктура открытого ключа.	2	ПК-20

	Итого	2	
Итого за семестр		4	
Итого		6	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин				
	1	2	3	4	5
Предшествующие дисциплины					
1 Основы криптографии	+	+	+	+	+
2 Организационное и правовое обеспечение информационной безопасности	+				
3 Основы информационной безопасности	+				
Последующие дисциплины					
1 Основы криптографии	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	Контрольная работа, Защита отчета, Проверка контрольных работ, Отчет по лабораторной работе, Зачет, Тест

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий приведены в таблице 6.1.

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные лабораторные занятия, ч	Интерактивные лекции, ч	Всего, ч
8 семестр			
IT-методы	2		2
Итого за семестр:	2	0	2
9 семестр			
IT-методы	2	2	4
Итого за семестр:	2	2	4
Итого	4	2	6

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, (часы)	Формируемые компетенции
8 семестр			
2 Симметричное шифрование	Шифрованная файловая система Windows	2	ПК-20
	Средство криптографической защиты информации Secret Disk	2	
	Итого	4	
Итого за семестр		4	
9 семестр			
5 Электронная подпись	Работа с криптопровайдерами	8	ПК-20
	Итого	8	
Итого за семестр		8	
Итого		12	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, (часы)	Формируемые компетенции	Формы контроля
8 семестр				
1 Основные цели и задачи криптографии	Проработка лекционного материала	2	ПК-20	Зачет, Контрольная работа, Проверка контрольных работ, Тест
	Итого	2		
2 Симметричное шифрование	Самостоятельное изучение тем (вопросов) теоретической части курса	16	ПК-20	Зачет, Защита отчета, Контрольная работа, Отчет по лабораторной работе, Проверка контрольных работ, Тест
	Проработка лекционного материала	4		
	Оформление отчетов по лабораторным работам	8		
	Итого	28		
Итого за семестр		30		
9 семестр				
3 Хеширование	Самостоятельное изучение тем (вопросов) теоретической части курса	8	ПК-20	Зачет, Контрольная работа, Проверка контрольных работ, Тест
	Проработка лекционного материала	2		

	Итого	10		
4 Криптография с открытым ключом	Выполнение контрольных работ	4	ПК-20	Зачет, Контрольная работа, Проверка контрольных работ, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	8		
	Проработка лекционного материала	2		
	Итого	14		
5 Электронная подпись	Выполнение контрольных работ	4	ПК-20	Зачет, Защита отчета, Контрольная работа, Отчет по лабораторной работе, Проверка контрольных работ, Тест
	Самостоятельное изучение тем (вопросов) теоретической части курса	8		
	Проработка лекционного материала	4		
	Оформление отчетов по лабораторным работам	16		
	Итого	32		
Итого за семестр		56		
	Подготовка и сдача зачета	4		Зачет
Итого		90		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется.

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2016. — 232 с. — Загл. с экрана. [Электронный ресурс] - Режим доступа: https://e.lanbook.com/book/111098 (дата обращения 28.06.2018)

12.2. 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 - 51 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ. [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf (дата обращения:

28.06.2018).

2. Евсютин О.О. Прикладная криптография: методические указания для выполнения лабораторных и самостоятельных работ. [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf (дата обращения: 28.06.2018).

12.3.2. 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.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://edu.tusur.ru/ – Научно-образовательный портал ТУСУР.
2. http://fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования.
3. eLIBRARY.RU – Российская научная электронная библиотека, интегрированная с Российским индексом научного цитирования (РИНЦ).
4. Scopus – библиографическая и реферативная база данных.
5. SpringerLink – хранилище электронных копий научных книг и журналов, издаваемых компанией Springer.
6. IEEE Xplore – электронная платформа, содержащая полные тексты публикаций из журналов, материалов конференций, стандартов, издаваемых IEEE и IEE (Institution of Electrical Engineers).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. 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 количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория "Интернет-технологий и информационно-аналитической деятельности"учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb (15

шт.);

- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– VirtualBox
– Visual Studio

13.1.3. 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.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

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

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными 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 зрениями** 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.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

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

3. 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

4. Какова длина секретного ключа в шифре «Кузнечик»?

а) 64 бита
б) 128 бит
в) 256 бит
г) 512 бит

5. 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

6. 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

7. Какой из перечисленных шифров относится к классу асимметричных шифров?

а) Магма
б) Кузнечик
в) RSA
г) AES

8. 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

9. Почему асимметричные криптосистемы затруднительно использовать для непосредственного шифрования видеотрафика?
а) В связи с недостаточной криптографической стойкостью асимметричных криптосистем
б) В связи с отсутствием соответствующих стандартов
в) В связи с недостаточным быстродействием асимметричных криптосистем
г) Асимметричные криптосистемы используются для непосредственного шифрования видеотрафика

10. 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

11. На какой вычислительной задаче основана криптосистема RSA?
а) Нахождение наибольшего общего делителя
б) Вычисление модулярно обратного элемента
в) Целочисленная факторизация
г) Дискретное логарифмирование

12. 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

13. 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

14. 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

15. 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

16. 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

17. 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

18. Для чего служит инфраструктура открытого ключа?

а) Обеспечение аутентичности закрытых ключей
б) Обеспечение конфиденциальности закрытых ключей
в) Обеспечение аутентичности открытых ключей
г) Обеспечение конфиденциальности открытых ключей

19. Что не относится к функциям удостоверяющего центра?

а) Подтверждение личности пользователей
б) Выдача пользователями сертификатов
в) Шифрование пользовательских данных
г) Отзыв выданных сертификатов

20. Что требуется пользователю для проверки цифрового сертификата?

а) Аутентичный открытый ключ соответствующего удостоверяющего центра
б) Аутентичный закрытый ключ соответствующего удостоверяющего центра
в) Аутентичный открытый ключ пользователя – владельца сертификата
г) Аутентичный закрытый ключ пользователя – владельца сертификата

14.1.2. Темы контрольных работ

Решение задач информационной безопасности с помощью криптографических методов защиты информации

14.1.3. Зачёт

1. Цели и задачи криптографии. Основные понятия.
2. Простейшие шифры: простой замены, перестановочный, аффинный.
3. ГОСТ Р 34.12–2015.
4. AES.
5. Режимы работы симметричных блочных шифров.
6. Криптография с открытым ключом.
7. Криптосистема RSA.
8. Криптосистема Эль-Гамаля.
9. Криптосистема Рабина.
10. Протокол Диффи-Хеллмана.
11. Понятие хеш-функции. Свойства криптографических хеш-функций.
12. ГОСТ Р 34.11-2012.
13. Код аутентичности сообщений.
14. Электронная подпись.
15. ГОСТ Р 34.10-2012.

16. Инфраструктура открытого ключа.

14.1.4. Темы лабораторных работ

Шифрованная файловая система Windows
Средство криптографической защиты информации Secret Disk
Работа с криптопровайдерами

14.2. 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 14.

Таблица 14 – 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 исходя из состояния обучающегося на момент проверки

14.3. 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, 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.