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

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **25.05.03 Техническая эксплуатация транспортного радиооборудования**
Направленность (профиль) / специализация: **Информационно-телекоммуникационные системы на транспорте и их информационная защита**
Форма обучения: **очная**
Факультет: **Радиоконструкторский факультет (РКФ)**
Кафедра: **Кафедра конструирования и производства радиоаппаратуры (КИПР)**
Курс: **4**
Семестр: **7**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Практические занятия	18	18	часов
в т.ч. в форме практической подготовки	10	10	часов
Самостоятельная работа	64	64	часов
Общая трудоемкость (включая промежуточную аттестацию)	100	100	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	7

Томск

1. Общие положения

1.1. Цели дисциплины

1. Формирование у студентов общих представлений о криптографических методах защиты информации.
2. Формирование у студентов представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

1.2. Задачи дисциплины

1. Дать представление о криптографических методах защиты информации.
2. Изучить математические основы современной криптографии.
3. Сформировать представление об основных проблемах, связанных с практическим использованием криптографических методов защиты информации.
4. Изучить основные криптографические протоколы.
5. Изучить инфраструктуру открытого ключа.
6. Изучить основные криптографические алгоритмы (симметричные, асимметричные, бесключевые).

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль специализации (major).
Индекс дисциплины: Б1.В.02.04.
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		

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает методики сбора и обработки информации, актуальные российские и зарубежные источники информации для решения поставленных задач, а также методы системного анализа	Знает основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности.
	УК-1.2. Умеет применять методики поиска, сбора и обработки информации, осуществлять критический анализ и синтез информации, полученной из разных источников	Умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.
	УК-1.3. Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации, методикой системного подхода для решения поставленных задач; способен генерировать различные варианты решения поставленных задач	Владеет навыками использования средств криптографической защиты информации для обеспечения информационной безопасности.
Общепрофессиональные компетенции		
-	-	-
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 3 зачетных единиц, 100 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
		7 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	36	36
Лекционные занятия	18	18
Практические занятия	18	18
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	64	64
Подготовка к зачету	26	26
Подготовка к тестированию	18	18
Написание отчета по практическому занятию (семинару)	20	20
Общая трудоемкость (в часах)	100	100
Общая трудоемкость (в з.е.)	3	3

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
7 семестр					
1 Общие понятия криптографии	8	8	26	42	УК-1
2 Инфраструктура открытых ключей	6	4	18	28	УК-1
3 Механизмы управления ключами	2	4	10	16	УК-1
4 Практические аспекты криптографической защиты информации	2	2	10	14	УК-1
Итого за семестр	18	18	64	100	
Итого	18	18	64	100	

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
7 семестр			

1 Общие понятия криптографии	Основные цели и задачи криптографии. Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.	2	УК-1
	Математические основы 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.	2	УК-1
	Историческая криптография. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.	1	УК-1
	Симметричное шифрование. DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, эммитовставка. AES.	1	УК-1
	Поточное шифрование. Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Критерии качества псевдослучайных чисел.	1	УК-1
	Хеширование. Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.	1	УК-1
	Итого	8	
2 Инфраструктура открытых ключей	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема ЭльГамаля. Криптосистема Рабина.	2	УК-1
	Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа	4	УК-1
	Итого	6	

3 Механизмы управления ключами	Изучение стандарта ISO/IEC 11770. Механизмы, использующие симметричные методы. Механизмы, использующие асимметричные методы. Механизмы, основанные на слабых секретах. Управление групповыми ключами. Формирование ключей.	2	УК-1
	Итого	2	
4 Практические аспекты криптографической защиты информации	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы. Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ». Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.	2	УК-1
	Итого	2	
Итого за семестр		18	
Итого		18	

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
7 семестр			
1 Общие понятия криптографии	Криптографические файловые системы. Шифрованная файловая система Windows	4	УК-1
	Криптографические файловые системы. Шифрование диска BitLocker	4	УК-1
	Итого	8	
2 Инфраструктура открытых ключей	Применение ИОК в клиентах электронной почты	4	УК-1
	Итого	4	
3 Механизмы управления ключами	Применение ИОК на автоматизированном рабочем месте	4	УК-1
	Итого	4	
4 Практические аспекты криптографической защиты информации	Применение криптопровайдеров	2	УК-1
	Итого	2	
Итого за семестр		18	
Итого		18	

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
7 семестр				
1 Общие понятия криптографии	Подготовка к зачету	10	УК-1	Зачёт
	Подготовка к тестированию	8	УК-1	Тестирование
	Написание отчета по практическому занятию (семинару)	8	УК-1	Отчет по практическому занятию (семинару)
	Итого	26		
2 Инфраструктура открытых ключей	Подготовка к зачету	8	УК-1	Зачёт
	Подготовка к тестированию	6	УК-1	Тестирование
	Написание отчета по практическому занятию (семинару)	4	УК-1	Отчет по практическому занятию (семинару)
	Итого	18		
3 Механизмы управления ключами	Подготовка к зачету	4	УК-1	Зачёт
	Подготовка к тестированию	2	УК-1	Тестирование
	Написание отчета по практическому занятию (семинару)	4	УК-1	Отчет по практическому занятию (семинару)
	Итого	10		
4 Практические аспекты криптографической защиты информации	Подготовка к зачету	4	УК-1	Зачёт
	Подготовка к тестированию	2	УК-1	Тестирование
	Написание отчета по практическому занятию (семинару)	4	УК-1	Отчет по практическому занятию (семинару)
	Итого	10		
Итого за семестр		64		
Итого		64		

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.	
УК-1	+	+	+	Зачёт, Тестирование, 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
7 семестр				
Зачёт	0	0	30	30
Тестирование	5	5	10	20
Отчет по практическому занятию (семинару)	20	20	10	50
Итого максимум за период	25	25	50	100
Нарастающим итогом	25	50	100	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

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] [Электронный ресурс]: монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия Телеком, 2016. — 232 с. — Загл. с экрана. — Режим доступа: [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111098.

2. Осипян В. О. Криптография в задачах и упражнениях. - М. : Гелиос АРВ , 2004. - 143[1] с. (наличие в библиотеке ТУСУР - 50 экз.).

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 - 51 экз.).

3. 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, 2020. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/450820.

4. 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, 2020. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/451486.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — 2014. — Режим доступа: [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/kmzi/practice.pdf.

2. Евсютин О.О. Прикладная криптография [Электронный ресурс]: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. — Режим доступа: [Электронный ресурс]: — Режим доступа: https://disk.fb.tusur.ru/crypto/laboratory_work.pdf.

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

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

Аудитория моделирования, проектирования и эксплуатации информационных и аналитических систем: учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 407 ауд.

Описание имеющегося оборудования:
- Интерактивная доска TraceBoard TS-408L;
- Проектор ViewSonic PJD5154 DLP;
- 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 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 Общие понятия криптографии	УК-1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Инфраструктура открытых ключей	УК-1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
3 Механизмы управления ключами	УК-1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий

4 Практические аспекты криптографической защиты информации	УК-1	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий

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
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. По принципу Керкгоффса в криптосистеме секретным должно быть:
   - ключ
   - время шифрования
   - сложность алгоритма
   - длина ключа
2. Победитель конкурса AES (Advanced Encryption Standard)?
   - DES
   - RC6
   - Rijndael
   - Twofish
3. Что такое диффузия?
   - Влияние одного знака открытого ключа на значительное количество знаков шифротекста.
   - Влияние одного знака закрытого ключа на значительное количество знаков шифротекста.
   - Влияние одного знака открытого текста на значительное количество знаков шифротекста.
   - Влияние алгоритма защиты информации на значительное количество знаков шифротекста.
4. Каким свойством должен обладать канал передачи информации в схеме Диффи-Хеллмана
   - защищенный от подмены
   - защищенный от прослушивания
   - закрытый канал
   - открытый канал
5. Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? (использует одностороннюю функцию)
   - Разбиение входного массива
   - Хеширование
   - Сжатие
   - Сдвиг
6. Виды симметричных криптосистем:
   - поточные шифры
   - ЭЦП
   - криптосистемы с открытым ключом
   - нет ответа
7. Advanced Encryption Standard (AES), также известный как Rijndael имеет размер блока (в битах):
   - 64

- 128
- 192
- 256

8. Advanced Encryption Standard (AES), также известный как Rijndael может иметь ключ (в битах):
   - 128
   - 192
   - 256
   - все выше перечисленные
9. Какая схема лежит в основе DES и ГОСТ 28147-89?
   - Цезаря
   - Кантора
   - Фейстеля
   - Виженера
10. Какие из следующих алгоритмов являются ассимметричными?
    - DES
    - Эль-Гамаль
    - ГОСТ 28147-89
    - RC4
11. На какой труднорешаемой задаче основан алгоритм RSA?
    - Факторизации чисел
    - Нахождения большого простого числа
    - Вычислении обратного элемента
    - Дискретного логарифмирования
12. Какая длина ключа в ГОСТ 28147-89(Магма)? (ответ в битах)
    - 64
    - 128
    - 192
    - 256
13. Что обычно в себя включает схема электронной подписи?
    - алгоритм генерации ключевых пар пользователя
    - функцию проверки подписи
    - ничего из вышеперечисленного
    - все из вышеперечисленного
14. Метод полиалфавитного шифрования буквенного текста с использованием ключевого слова
    (текстового):
    - Шифр Гронсфельда
    - Шифр Виженера
    - Шифр Цезаря
    - Шифр Вернама
15. Какой ключ доступен всем для проверки цифровой подписи под документом?
    - закрытый
    - открытый
    - внутренний
    - общий
16. Какой шрифт более стойкий к взлому?
    - Симметричный
    - Асимметричный
    - Псевдосимметричный
    - Нет правильного ответа
17. Какой алгоритм шифрования стал прообразом для отечественного ГОСТ28147-89?
    - DES
    - DSA
    - Rijndael
    - IDEA
18. В чем преимущество симметричных систем над асимметричными?

- скорость шифрования
- простота реализации
- изученность
- все ответы правильные

19. Что подразумевается под термином аутентичность информации?
    - Целостность информации
    - Невозможность отказа от авторства
    - Подлинность авторства
    - все ответы правильные
20. Выберите правильный вариант, зашифрованной с помощью шифра цезаря, строки: шифр Цезаря
    - ъйхс чёибсб
    - щйхс чёибса
    - ъкцт шжйвсб
    - юоъц ьknёцж

9.1.2. Перечень вопросов для зачета

1. Понятие криптографического протокола.
2. Роль криптографических протоколов в системах защиты информации.
3. Основные атаки на криптографические протоколы.
4. Понятие электронной подписи.
5. Управление открытыми ключами.
6. Основные компоненты инфраструктуры открытых ключей.
7. Понятие сертификата открытого ключа.
8. Удостоверяющий центр.
9. Архитектура инфраструктуры открытого ключа.
10. Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ».
11. Понятие протоколов интерактивного доказательства и доказательства знания.
12. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.
13. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.
14. Проблемы реализации криптографических алгоритмов.
15. Защита от утечки информации.

9.1.3. Темы практических занятий

1. Криптографические файловые системы. Шифрованная файловая система Windows
2. Криптографические файловые системы. Шифрование диска BitLocker
3. Применение ИОК в клиентах электронной почты
4. Применение ИОК на автоматизированном рабочем месте
5. Применение криптопровайдеров

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:

– 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, 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.

ЛИСТ СОГЛАСОВАНИЯ

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

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИПР	Н.Н. Кривин	Согласовано, 61bb81d6-898a-4d50-b92b-bf79399fcfac
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Начальник учебного управления	Е.В. Саврук	Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c

ЭКСПЕРТЫ:

Доцент, каф. КИПР	А.А. Чернышев	Согласовано, 72a81577-12a0-4023-8fe9-e3b84d6716fc
Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	А.Ю. Якимук	Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc