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: **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: **4**
Семестр: **7**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	22	22	часов
Практические занятия	10	10	часов
Лабораторные занятия	32	32	часов
Самостоятельная работа	44	44	часов
Общая трудоемкость (включая промежуточную аттестацию)	108	108	часов
	3	3	з.е.

Формы промежуточной аттестация	Семестр
Зачет	7

Томск

1. Общие положения

1.1. Цели дисциплины

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

1.2. Задачи дисциплины

1. Сформировать представление об основных проблемах, связанных с практическим использованием криптографических методов защиты информации.
2. Изучить основные криптографические протоколы.
3. Изучить инфраструктуру открытого ключа.
4. Изучить механизмы управления ключами.

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.03.25.
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		

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 криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности.
	ОПК-9.2. Умеет осуществлять обоснованный выбор и использовать СКЗИ при решении задач профессиональной деятельности	Умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.
	ОПК-9.3. Владеет практическими навыками разработки криптографических алгоритмов механизмов, определяемых национальными стандартами и рекомендациями Российской Федерации и стандартами международной организации по стандартизации	Владеет навыками использования средств криптографической защиты информации при обеспечении информационной безопасности на автоматизированном рабочем месте.

ОПК-13. Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.1. Знает методологические основы, методы и средства построения информационно-аналитических систем, знает нормативные правовые акты в области защиты информации	Знает основные меры по криптографической защите информации в автоматизированных системах.
	ОПК-13.2. Умеет осуществлять наладку компонентов обеспечивающей части информационно-аналитических систем на всех этапах их жизненного цикла, применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях	Умеет выбирать необходимые средства криптографической защиты информации исходя из типа защищаемой автоматизированной системы; применять средства криптографической защиты информации для обеспечения конфиденциальности и целостности обрабатываемой на автоматизированном рабочем месте информации.
	ОПК-13.3. Владеет методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети, методикой анализа сетевого трафика	Владеет навыками настройки средств криптографической защиты информации, построения инфраструктуры открытых ключей, применения криптопровайдеров и иных программных средств системы защиты информации автоматизированной системы.
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, 108 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	64	64
Лекционные занятия	22	22
Практические занятия	10	10
Лабораторные занятия	32	32
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	44	44
Подготовка к зачету	11	11
Подготовка к лабораторной работе, написание отчета	20	20

Подготовка к тестированию	8	8
Написание отчета по практическому занятию (семинару)	5	5
Общая трудоемкость (в часах)	108	108
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	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Введение в прикладные аспекты криптографической защиты информации	4	4	12	10	30	ОПК-9, ОПК-13
2 Инфраструктура открытых ключей	6	4	16	21	47	ОПК-9, ОПК-13
3 Механизмы управления ключами	8	-	-	6	14	ОПК-13, ОПК-9
4 Практические аспекты криптографической защиты информации	4	2	4	7	17	ОПК-9, ОПК-13
Итого за семестр	22	10	32	44	108	
Итого	22	10	32	44	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
7 семестр			
1 Введение в прикладные 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.	4	ОПК-13, ОПК-9
	Итого	4	

2 Инфраструктура открытых ключей	Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа	6	ОПК-9
	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.	8	ОПК-13, ОПК-9
	Итого	8	
4 Практические аспекты криптографической защиты информации	Проблемы реализации криптографических алгоритмов. Защита от утечки информации. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.	4	ОПК-13
	Итого	4	
Итого за семестр		22	
Итого		22	

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 Введение в прикладные аспекты криптографической защиты информации	Криптографические файловые системы. Шифрование файловой системы Linux	4	ОПК-9
	Итого	4	
2 Инфраструктура открытых ключей	Применение ИОК в клиентах электронной почты	2	ОПК-9
	Применение ИОК на автоматизированном рабочем месте	2	ОПК-9
	Итого	4	
4 Практические аспекты криптографической защиты информации	Применение криптопровайдеров	2	ОПК-9, ОПК-13
	Итого	2	
Итого за семестр		10	
Итого		10	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.
Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Введение в прикладные аспекты криптографической защиты информации	Криптографические файловые системы. Шифрованная файловая система Windows	4	ОПК-9
	Криптографические файловые системы. Шифрование диска BitLocker	4	ОПК-9
	Шифрование дисков VeraCrypt	4	ОПК-9
	Итого	12	
2 Инфраструктура открытых ключей	Установка и настройка служб удостоверяющего центра	4	ОПК-9, ОПК-13
	Изучение функций удостоверяющего центра	4	ОПК-9, ОПК-13
	Кросс-сертификация удостоверяющих центров	4	ОПК-9, ОПК-13
	Построение иерархической архитектуры инфраструктуры открытых ключей	4	ОПК-9, ОПК-13
	Итого	16	
4 Практические аспекты криптографической защиты информации	Средства криптографической защиты информации	4	ОПК-13
	Итого	4	
Итого за семестр		32	
Итого		32	

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 Введение в прикладные аспекты криптографической защиты информации	Подготовка к зачету	2	ОПК-9	Зачёт
	Подготовка к лабораторной работе, написание отчета	4	ОПК-9	Лабораторная работа
	Подготовка к тестированию	2	ОПК-9	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ОПК-9	Отчет по практическому занятию (семинару)
	Итого	10		

2 Инфраструктура открытых ключей	Подготовка к зачету	3	ОПК-9	Зачёт
	Подготовка к лабораторной работе, написание отчета	14	ОПК-9, ОПК-13	Лабораторная работа
	Подготовка к тестированию	2	ОПК-9	Тестирование
	Написание отчета по практическому занятию (семинару)	2	ОПК-9	Отчет по практическому занятию (семинару)
	Итого	21		
3 Механизмы управления ключами	Подготовка к зачету	4	ОПК-13, ОПК-9	Зачёт
	Подготовка к тестированию	2	ОПК-13, ОПК-9	Тестирование
	Итого	6		
4 Практические аспекты криптографической защиты информации	Подготовка к зачету	2	ОПК-9, ОПК-13	Зачёт
	Подготовка к тестированию	2	ОПК-9, ОПК-13	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ОПК-13	Лабораторная работа
	Написание отчета по практическому занятию (семинару)	1	ОПК-9, ОПК-13	Отчет по практическому занятию (семинару)
	Итого	7		
Итого за семестр		44		
Итого		44		

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.	Лаб. раб.	Сам. раб.	
ОПК-9	+	+	+	+	Зачёт, Лабораторная работа, Тестирование, Отчет по практическому занятию (семинару)
ОПК-13	+	+	+	+	Зачёт, Лабораторная работа, 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
Лабораторная работа	15	15	10	40
Тестирование	0	0	10	10
Отчет по практическому занятию (семинару)	5	10	5	20
Итого максимум за период	20	25	55	100
Нарастающим итогом	20	45	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. Осипян В. О. Криптография в задачах и упражнениях. - М. : Гелиос АРВ , 2004. - 143[1] с. (наличие в библиотеке ТУСУР - 50 экз.).

2. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111097.

3. Основы информационной безопасности : Учебное пособие для вузов. - М. : Горячая линия-Телеком , 2006. - 544 с. (наличие в библиотеке ТУСУР - 81 экз.).

7.2. Дополнительная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/450820.

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 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. Прикладная криптография: методические указания для выполнения лабораторных работ / Якимук А.Ю. — 195 с. [Электронный ресурс] - 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 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:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;

8.3. Материально-техническое и программное обеспечение для лабораторных работ

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;
- Аппаратно-программные средства управления доступом к данным, шифрования: КриптоПро CSP;
- Криптографическое средство защиты информации КриптоПро CSP;

8.4. 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.

8.5. 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 Введение в прикладные аспекты криптографической защиты информации	ОПК-9, ОПК-13	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Инфраструктура открытых ключей	ОПК-9, ОПК-13	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Отчет по практическому занятию (семинару)	Темы практических занятий

3 Механизмы управления ключами	ОПК-13, ОПК-9	Зачёт	Перечень вопросов для зачета
		Тестирование	Примерный перечень тестовых заданий
4 Практические аспекты криптографической защиты информации	ОПК-9, ОПК-13	Зачёт	Перечень вопросов для зачета
		Лабораторная работа	Темы лабораторных работ
		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. Независимый программный модуль, позволяющий осуществлять криптографические операции, называется…
   a) Криптооператор
   b) Криптопровайдер
   c) Криптографический клиент
   d) Криптошлюз
2. Какие протоколы входят в IPSec? Выбрать несколько вариантов
   a) ISAKMP
   b) TCP
   c) ESP
   d) Все перечисленные
3. Что такое PIM?
   a) Система для централизованного управления большими массивами данных
   b) Персональный множитель интеграций
   c) Протокол шифрования данных транспортного уровня OSI, входящий в стек протоколов IPSec
   d) Персональный идентификационный номер
4. Равенство значений хеш-функции на двух различных блоках данных называется?
   a) Пересечение эллиптических кривых
   b) Компрометация хэш-алгоритмов
   c) Коллизия хэш-функций
   d) Криптографическая соль
5. Какие средства шифрования из перечисленных являются стандартными в OS Windows?
   a) Bitlocker
   b) Шифрование дисков
   c) VeraCrypt
   d) eCryptfs
6. Что из перечисленного не является программным средством шифрования дисков?
   a) Bitlocker
   b) TPM
   c) VeraCrypt

d) Ни один из вариантов

7. Что не относится к обязательным полям сертификата формата X.509?
   a) Открытый ключ субъекта.
   b) Идентификатор алгоритма подписи.
   c) Имя объекта сертификата.
   d) Имя субъекта сертификата.
8. Что означает аббревиатура KDF?
   a) Функция формирования ключей.
   b) Функция расширения ключей.
   c) Функция извлечения ключей.
   d) Код аутентификации сообщения.
9. Чем занимается сервис конфиденциальности PKI?
   a) Агрегирует все сертификатов, необходимых для формирования полного пути.
   b) Обеспечивает аутентификацию участников коммуникации и аутентификацию источника данных.
   c) Предотвращает преднамеренное или случайное несанкционированное изменение данных.
   d) Обеспечивает защиту от несанкционированного получения информации.
10. Что такое центр перевода ключей?
   a) Доверенная сущность, генерирующая или получающая ключи, и передающая их общающимся группам, а также имеющая уникальный симметричный ключ с каждой такой группой.
   b) Доверенная сущность, осуществляющая расшифрование ключа, сгенерированного и зашифрованного одной сущностью, и последующее зашифрование для другой сущности.
   c) Сущность, ответственная за предоставление проверенных идентификаторов пользователей центру сертификации.
   d) Доверенная сущность, создающая и назначающая сертификаты открытых ключей.
11. Какая из перечисленных ниже технологий Active Directory применяется для организации инфраструктуры открытых ключей?
   a) Доменные службы
   b) Службы сертификации
   c) Службы федерации
   d) Службы управления правами
12. Что не относится к основным функциям, выполняемым центром сертификации?
   a) Формирование собственного секретного ключа и сертификата ЦС.
   b) Формирование сертификатов открытых ключей конечных пользователей.
   c) Формирование списка отозванных сертификатов.
   d) Регистрация новых пользователей центра сертификации.
13. Что из перечисленного ниже не является форматом сертификата?
   a) X.509
   b) PGP
   c) SPKI
   d) MD5
14. Какого этапа нет в жизненном цикле сертификата?
   a) Запрос сертификата
   b) Выдача сертификата
   c) Копирование сертификата
   d) Отзыв сертификата
15. Что из перечисленного ниже является примером ситуации, при которой доверие к сертификату было подорвано до истечения срока его действия?
   a) Смена фамилии владельца сертификата
   b) Потеря ключевого носителя владельцем сертификата
   c) Увольнение из организации владельца сертификата
   d) Все вышеперечисленное
16. Какая из перечисленных ниже моделей доверия иначе называется «hub and spoke»?
   a) Четырехсторонняя модель
   b) Мостовая модель

c) Сетевая модель
d) Иерархическая модель

17. Выберите правильное определение пути сертификации.
    a) Последовательность сертификатов, в которой издатель первого сертификата и субъект последнего сертификата являются конечными субъектами.
    b) Последовательность сертификатов, в которой издатель первого сертификата является пунктом доверия, а субъект последнего сертификата - конечным субъектом.
    c) Последовательность сертификатов, в которой издатель первого сертификата является конечным субъектом, а субъект последнего сертификата - пунктом доверия.
    d) Последовательность сертификатов, в которой издатель первого сертификата и субъект последнего сертификата являются пунктами доверия.
18. Каким образом в приложениях проверяется валидность сертификата в процессе его использования?
    a) По локальному списку отозванных сертификатов.
    b) По значению ключа субъекта сертификата.
    c) По электронной подписи издателя сертификата.
    d) По сроку действия сертификата.
19. В каком виде криптопровайдеры хранятся на компьютере?
    a) В формате исполняемых файлов.
    b) В формате динамически подключаемых библиотек DLL.
    c) В формате параметров реестра.
    d) В виде ключевых контейнеров в корне диска.
20. Какую задачу не выполняет CryptoAPI?
    a) Надежность сокрытия данных.
    b) Расшифровывание полученных конфиденциальных данных.
    c) Дешифровывание полученных конфиденциальных данных.
    d) Обеспечение работы с признанными криптографическими стандартами.

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 лабораторных работ

1. Криптографические файловые системы. Шифрованная файловая система Windows
2. Криптографические файловые системы. Шифрование диска BitLocker
3. Шифрование дисков VeraCrypt
4. Установка и настройка служб удостоверяющего центра
5. Изучение функций удостоверяющего центра
6. Кросс-сертификация удостоверяющих центров
7. Построение иерархической архитектуры инфраструктуры открытых ключей
8. Средства криптографической защиты информации

9.1.4. Темы практических занятий

1. Криптографические файловые системы. Шифрование файловой системы Linux
2. Применение ИОК в клиентах электронной почты
3. Применение ИОК на автоматизированном рабочем месте
4. 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. БИС	Е.Ю. Костюченко	Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463
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. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	К.С. Сарин	Согласовано, 68c81ca0-0954-467a-8d01-f93a0d553669

РАЗРАБОТАНО:

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