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 - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	10	10	часов
3	Лабораторные работы	24	24	часов
4	Всего аудиторных занятий	52	52	часов
5	Самостоятельная работа	56	56	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 7 семестр

Томск

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. КИБЭВС _____ А. Ю. Якимук

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

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

1.2. Задачи дисциплины

- сформировать представление об основных проблемах, связанных с практическим использование криптографических методов защиты информации;
- изучить основные криптографические протоколы;
- изучить инфраструктуру открытого ключа

2. Место дисциплины в структуре ОПОП

Дисциплина «Прикладная криптография» (Б1.В.03.02) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность сетей ЭВМ, Криптографические методы защиты информации, Основы информационной безопасности.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ;
- ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач ;
- ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ;
- ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ;

В результате изучения дисциплины обучающийся должен:

- **знать** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.
- **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.
- **владеть** навыками использования типовых криптографических алгоритмов.

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
		7 семестр
Аудиторные занятия (всего)	52	52
Лекции	18	18
Практические занятия	10	10
Лабораторные работы	24	24

Самостоятельная работа (всего)	56	56
Оформление отчетов по лабораторным работам	34	34
Проработка лекционного материала	12	12
Подготовка к практическим занятиям, семинарам	10	10
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	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., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
7 семестр						
1 Криптографические протоколы: общие понятия.	2	2	10	14	28	ОПК-7, ПК-13, ПК-2, ПК-6
2 Протоколы распределения ключей.	2	2	2	10	16	ОПК-7, ПК-13, ПК-2, ПК-6
3 Инфраструктура открытых ключей.	6	4	12	16	38	ОПК-7, ПК-13, ПК-2, ПК-6
4 Протоколы идентификации и аутентификации.	4	0	0	4	8	ОПК-7, ПК-13, ПК-2, ПК-6
5 Безопасный канал обмена сообщениями.	2	2	0	6	10	ОПК-7, ПК-13, ПК-2, ПК-6
6 Практические аспекты реализации средств криптографической защиты информации.	2	0	0	6	8	ОПК-7, ПК-13, ПК-2
Итого за семестр	18	10	24	56	108	
Итого	18	10	24	56	108	

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, ч	Формируемые компетенции
7 семестр			
1 Криптографические протоколы: общие	Понятие криптографического протокола. Роль криптографических протоколов в си-	2	ОПК-7, ПК-13, ПК-6

понятия.	стемах защиты информации. Основныеатаки на криптографические протоколы		
	Итого	2	
2 Протоколы распределения ключей.	Управление секретными ключами. Распределение секретных ключей.	2	ПК-13, ПК-2, ПК-6
	Итого	2	
3 Инфраструктура открытых ключей.	Понятие электронной подписи. Управление открытыми ключами. Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа	6	ОПК-7, ПК-13, ПК-2, ПК-6
	Итого	6	
4 Протоколы идентификации и аутентификации.	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-7, ПК-13, ПК-2, ПК-6
	Итого	4	
5 Безопасный канал обмена сообщениями.	Построение безопасного коммуникационного канала на основе криптографических алгоритмов.	2	ОПК-7, ПК-13, ПК-2, ПК-6
	Итого	2	
6 Практические аспекты реализации средств криптографической защиты информации.	Проблемы реализации криптографических алгоритмов. Генерация случайных чисел. Защита от утечки информации.	2	ОПК-7, ПК-13, ПК-2
	Итого	2	
Итого за семестр		18	

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	6
Предшествующие дисциплины						
1 Безопасность сетей ЭВМ					+	+
2 Криптографические методы защиты информации	+	+	+	+	+	+
3 Основы информационной безопасности	+			+		+
Последующие дисциплины						

1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+

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.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-7	+	+	+	+	Отчет по лабораторной работе, Зачёт, Тест, Отчет по практическому занятию
ПК-2	+	+	+	+	Отчет по лабораторной работе, Зачёт, Тест, Отчет по практическому занятию
ПК-6	+	+	+	+	Отчет по лабораторной работе, Зачёт, Тест, Отчет по практическому занятию
ПК-13	+	+	+	+	Отчет по лабораторной работе, Зачёт, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Криптографические протоколы: общие понятия.	Криптографические файловые системы. Шифрованная файловая система Windows	2	ПК-13, ПК-2, ПК-6
	Криптографические файловые системы. Шифрование диска BitLocker	2	
	Шифрование дисков VeraCrypt	4	
	Криптографические файловые системы. Шифрованная файловая система Linux	2	
	Итого	10	
2 Протоколы распределения ключей.	Средства криптографической защиты информации	2	ПК-13, ПК-2
	Итого	2	
3 Инфраструктура открытых ключей.	Настройка удостоверяющего центра.	4	ПК-13, ПК-6
	Кросс-сертификация удостоверяющих центров	4	

	Построение иерархической модели доверия удостоверяющих центров.	4	
	Итого	12	
Итого за семестр		24	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
7 семестр			
1 Криптографические протоколы: общие понятия.	Анализ уязвимостей простейших криптографических протоколов.	2	ОПК-7, ПК-13, ПК-2, ПК-6
	Итого	2	
2 Протоколы распределения ключей.	Применение ИОК на автоматизированном рабочем месте	2	ОПК-7, ПК-13, ПК-2
	Итого	2	
3 Инфраструктура открытых ключей.	Применение ИОК в клиентах электронной почты	2	ОПК-7, ПК-13, ПК-2, ПК-6
	Структура сертификатов открытого ключа	2	
	Итого	4	
5 Безопасный канал обмена сообщениями.	Изучение протокола IPsec	2	ПК-13, ПК-2, ПК-6
	Итого	2	
Итого за семестр		10	

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, ч	Формируемые компетенции	Формы контроля
7 семестр				
1 Криптографические протоколы: общие понятия.	Подготовка к практическим занятиям, семинарам	2	ПК-13, ПК-2, ПК-6, ОПК-7	Зачёт, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	10		
	Итого	14		
2 Протоколы распределения ключей.	Проработка лекционного материала	2	ОПК-7, ПК-13, ПК-2, ПК-6	Зачёт, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Итого	10		

3 Инфраструктура открытых ключей.	Подготовка к практическим занятиям, семинарам	2	ОПК-7, ПК-13, ПК-2, ПК-6	Зачёт, Отчет по лабораторной работе, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Оформление отчетов по лабораторным работам	12		
	Итого	16		
4 Протоколы идентификации и аутентификации.	Подготовка к практическим занятиям, семинарам	2	ОПК-7, ПК-13, ПК-2, ПК-6	Зачёт, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	4		
5 Безопасный канал обмена сообщениями.	Подготовка к практическим занятиям, семинарам	4	ОПК-7, ПК-13, ПК-2, ПК-6	Зачёт, Отчет по практическому занятию, Тест
	Проработка лекционного материала	2		
	Итого	6		
6 Практические аспекты реализации средств криптографической защиты информации.	Проработка лекционного материала	2	ОПК-7, ПК-13, ПК-2	Зачёт, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	6		
Итого за семестр		56		
Итого		56		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	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			20	20
Отчет по лабораторной работе	20	10	15	45
Отчет по практическому занятию	5	10	10	25
Тест			10	10

Итого максимум за период	25	20	55	100
Нарастающим итогом	25	45	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	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)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. 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 [Электронный ресурс]: 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. — Режим доступа: https://e.lanbook.com/book/111097 (дата обращения: 12.02.2021).

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

12.2. Дополнительная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты [Электронный ресурс]: 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 — Режим доступа: https://urait.ru/bcode/450820 (дата обращения: 12.02.2021).

2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты [Электронный ресурс]: 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 — Режим доступа:

https://urait.ru/bcode/451486 (дата обращения: 12.02.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации [Электронный ресурс] [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ [Электронный ресурс]. — 2014. — Режим доступа: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf (дата обращения: 12.02.2021).
2. Евсютин О.О. Прикладная криптография [Электронный ресурс] [Электронный ресурс]: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. — Режим доступа: — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf (дата обращения: 12.02.2021).

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. http://www.elibrary.ru - научная электронная библиотека;
2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

12.5. Периодические издания

1. Информация и безопасность [Электронный ресурс]: научный журнал. - Воронеж : ВГТУ . - Журнал выходит с 1998 г. — Режим доступа: https://elibrary.ru/title_about.asp?id=8748 (дата обращения: 12.02.2021).

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 практических занятий

Аудитория информатики, технологий и методов программирования

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard 78" с ПО ActivInspire;
- Проектор ViewSonic PJD5154 DLP;
- Компьютеры: DEPO Neos 235/ A8-7650K/ DDR3 4G/ 1Tb / мышь/ клавиатура/ монитор (10 шт.);
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– VirtualBox

13.1.3. 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:

- Моноблок: Asus V222GAK-BA021D: Intel J5005/ DDR4 4G/ 500Gb/ WiFi / мышь/ клавиатура (30шт.);
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Аппаратные средства аутентификации пользователя «eToken Pro»;
- Программно-аппаратный комплекс защиты информации: ПАК ViPNet Coordinator HW100 C 4.x, ПАК ViPNet Coordinator HW1000 4.x, ПАК Аккорд;

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;
- межсетевые экраны: ИКС Lite, Positive Technologies Application Firewall Education, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- системы обнаружения компьютерных атак: Snort, Suricata, СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap;
- системы защиты от утечки данных: Контур информационной безопасности SearchInform;
- средства мониторинга состояния автоматизированных систем: система мониторинга Zabbix;
- средства сканирования защищенности компьютерных сетей: сканер безопасности Xspider Education, система анализа защищенности сети MaxPatrol Education.

Устройства чтения смарт-карт и радиометок: Адаптер компьютерный для считывания и передачи в ПК серийных номеров бесконтактных идентификаторов IronLogic Z-2 USB;

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– VirtualBox

– Аппаратно-программные средства управления доступом к данным, шифрования: КриптоПро CSP

– Дистрибутив Kali Linux

– Криптографическое средство защиты информации КриптоПро CSP

13.1.4. 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.

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

По принципу Керкгоффса в криптосистеме секретным должно быть:

- ключ
- время шифрования
- сложность алгоритма
- длина ключа

Победитель конкурса AES (Advanced Encryption Standard)?

- DES
- RC6
- Rijndael

- Twofish
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.
Каким свойством должен обладать канал передачи информации в схеме Диффи-Хеллмана
- защищенный от подмены
- защищенный от прослушивания
- закрытый канал
- открытый канал
Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? (использует одностороннюю функцию)
- Разбиение входного массива
- Хеширование
- Сжатие
- Сдвиг
Виды симметричных криптосистем:
- поточные шифры
- ЭЦП
- криптосистемы с открытым ключом
- нет ответа
Advanced Encryption Standard (AES), также известный как Rijndael имеет размер блока (в битах):
- 64
- 128
- 192
- 256
Advanced Encryption Standard (AES), также известный как Rijndael может иметь ключ (в битах):
- 128
- 192
- 256
- все выше перечисленные
Какая схема лежит в основе DES и ГОСТ 28147-89?
- Цезаря
- Кантора
- Фейстеля
- Виженера
Какие из следующих алгоритмов являются ассимметричными?
- DES
- Эль-Гамаль
- ГОСТ 28147-89
- RC4
На какой труднорешаемой задаче основан алгоритм RSA?
- Факторизации чисел
- Нахождения большого простого числа
- Вычислении обратного элемента
- Дискретного логарифмирования
Какая длина ключа в ГОСТ 28147-89(Магма)? (ответ в битах)
- 64
- 128
- 192
- 256

Что обычно в себя включает схема электронной подписи?
- алгоритм генерации ключевых пар пользователя
- функцию проверки подписи
- ничего из вышеперечисленного
- все из вышеперечисленного
Метод полиалфавитного шифрования буквенного текста с использованием ключевого слова (текстового):
- Шифр Гронсфельда
- Шифр Виженера
- Шифр Цезаря
- Шифр Вернама
Какой ключ доступен всем для проверки цифровой подписи под документом?
- закрытый
- открытый
- внутренний
- общий
Какой шрифт более стойкий к взлому?
- Симметричный
- Асимметричный
- Псевдосимметричный
- Нет правильного ответа
Какой алгоритм шифрования стал прообразом для отечественного ГОСТ28147-89?
- DES
- DSA
- Rijndael
- IDEA
В чем преимущество симметричных систем над асимметричными?
- скорость шифрования
- простота реализации
- изученность
- все ответы правильные
Что подразумевается под термином аутентичность информации?
- Целостность информации
- Невозможность отказа от авторства
- Подлинность авторства
- все ответы правильные
Выберите правильный вариант, зашифрованной с помощью шифра цезаря, строки: шифр цезаря
- ъйхс чёибсб
- щйхс чёибса
- ъкцт шжйвсб
- юоъц ькнёцж

14.1.2. Вопросы для подготовки к практическим занятиям, семинарам

Анализ уязвимостей простейших криптографических протоколов.
Применение ИОК в клиентах электронной почты
Применение ИОК на автоматизированном рабочем месте
Изучение протокола IPsec
Структура сертификатов открытого ключа

14.1.3. Зачёт

Понятие криптографического протокола.
Роль криптографических протоколов в системах защиты информации.
Основные атаки на криптографические протоколы.
Понятие электронной подписи.
Управление открытыми ключами.

Основные компоненты инфраструктуры открытых ключей.

Понятие сертификата открытого ключа.

Удостоверяющий центр.

Архитектура инфраструктуры открытого ключа.

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.

Построение безопасного коммуникационного канала на основе криптографических алгоритмов.

Проблемы реализации криптографических алгоритмов.

Генерация случайных чисел.

Защита от утечки информации.

14.1.4. Темы лабораторных работ

Настройка удостоверяющего центра.

Кросс-сертификация удостоверяющих центров

Построение иерархической модели доверия удостоверяющих центров.

Криптографические файловые системы. Шифрованная файловая система Windows

Криптографические файловые системы. Шифрование диска BitLocker

Шифрование дисков VeraCrypt

Криптографические файловые системы. Шифрованная файловая система Linux

Средства криптографической защиты информации

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.