МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Прикладная криптография

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **25.05.03 Техническая эксплуатация транспортного радиооборудования**
Направленность (профиль) / специализация: **Техническая эксплуатация радиоэлектронного оборудования воздушных судов и аэропортов**
Форма обучения: **очная**
Факультет: **РКФ, Радиоконструкторский факультет**
Кафедра: **КИПР, Кафедра конструирования и производства радиоаппаратуры**
Курс: **4**
Семестр: **8**
Учебный план набора 2018 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	8	8	часов
4	Всего аудиторных занятий	54	54	часов
5	Самостоятельная работа	54	54	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачет: 8 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 20.12.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск

Согласована на портале № 47714

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «21» 5 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 25.05.03 Техническая эксплуатация транспортного радиооборудования , утвержденного 12.09.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. КИБЭВС _____ Е. Ю. Костюченко

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РКФ _____ Д. В. Озеркин

Заведующий выпускающей каф. КИПР _____ В. М. Карабан

Эксперты:

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

Доцент кафедры конструирования и производства радиоаппаратуры (КИПР) _____ Н. Н. Кривин

Согласована на портале № 47714

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Основная цель дисциплины «Прикладная криптография» — 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.Б.32) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Математика.

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-6 способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;

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
		8 семестр
Аудиторные занятия (всего)	54	54
Лекции	28	28
Практические занятия	18	18
Лабораторные работы	8	8
Самостоятельная работа (всего)	54	54
Оформление отчетов по лабораторным работам	12	12
Проработка лекционного материала	18	18
Подготовка к практическим занятиям, семинарам	18	18
Подготовка к тесту	6	6
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

Согласована на портале № 47714

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
8 семестр						
1 Криптографические протоколы: общие понятия.	6	3	4	12	25	ОПК-6
2 Протоколы распределения ключей.	6	5	0	8	19	ОПК-6
3 Инфраструктура открытого ключа.	4	4	0	7	15	ОПК-6
4 Протоколы идентификации и аутентификации.	4	0	4	9	17	ОПК-6
5 Безопасный канал обмена сообщениями.	4	0	0	3	7	ОПК-6
6 Практические аспекты реализации средств криптографической защиты информации.	4	6	0	15	25	ОПК-6
Итого за семестр	28	18	8	54	108	
Итого	28	18	8	54	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
8 семестр			
1 Криптографические протоколы: общие понятия.	Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы.	6	ОПК-6
	Итого	6	
2 Протоколы распределения ключей.	Управление секретными ключами. Распределение секретных ключей.	6	ОПК-6
	Итого	6	
3 Инфраструктура открытого ключа.	Принципы инфраструктуры открытого ключа. Сертификат открытого ключа. Основные компоненты инфраструктуры открытого ключа.	4	ОПК-6
	Итого	4	
4 Протоколы идентификации и аутентификации.	Протоколы идентификации и аутентификации с использованием симметричной криптографии. Протоколы идентификации и аутентификации с использованием	4	ОПК-6

Согласована на портале № 47714

	асимметричной криптографии.		
	Итого	4	
5 Безопасный канал обмена сообщениями.	Создание безопасного канала обмена сообщениями. Использование безопасного канала обмена сообщениями. Основные атаки на безопасный канал обмена сообщениями.	4	ОПК-6
	Итого	4	
6 Практические аспекты реализации средств криптографической защиты информации.	Применение рассмотренных методов в рамках реализации комплексных систем защиты информации.	4	ОПК-6
	Итого	4	
Итого за семестр		28	

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 Математика	+	+	+	+	+	+
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-6	+	+	+	+	Отчет по лабораторной работе, Зачет, Тест

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
8 семестр			

Согласована на портале № 47714

1 Криптографические протоколы: общие понятия.	Установка и настройка Active Directory Certificate Services.Целью данной лабораторной является ознакомление с процессом установки службы Active Directory Certificate Services (службы сертификации) и особенностями работы с сертификатами.	4	ОПК-6
	Итого	4	
4 Протоколы идентификации и аутентификации.	Рассматриваются технические меры повышения защищенности систем. Изучаются методы, лежащие в основе соответствующих средств и механизмов в аспектах идентификации и аутентификации.	4	ОПК-6
	Итого	4	
Итого за семестр		8	

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
8 семестр			
1 Криптографические протоколы: общие понятия.	Анализ уязвимостей простейших протоколов	3	ОПК-6
	Итого	3	
2 Протоколы распределения ключей.	Анализ уязвимостей простейших протоколов распределения ключей	5	ОПК-6
	Итого	5	
3 Инфраструктура открытого ключа.	Структура сертификатов открытого ключа	4	ОПК-6
	Итого	4	
6 Практические аспекты реализации средств криптографической защиты информации.	Удостоверяющие центры	6	ОПК-6
	Итого	6	
Итого за семестр		18	

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
8 семестр				
1 Криптографические протоколы: общие понятия.	Подготовка к практическим занятиям, семинарам	3	ОПК-6	Зачет, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	3		

Согласована на портале № 47714

	Оформление отчетов по лабораторным работам	6		
	Итого	12		
2 Протоколы распределения ключей.	Подготовка к практическим занятиям, семинарам	5	ОПК-6	Зачет, Тест
	Проработка лекционного материала	3		
	Итого	8		
3 Инфраструктура открытого ключа.	Подготовка к практическим занятиям, семинарам	4	ОПК-6	Зачет, Тест
	Проработка лекционного материала	3		
	Итого	7		
4 Протоколы идентификации и аутентификации.	Проработка лекционного материала	3	ОПК-6	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	6		
	Итого	9		
5 Безопасный канал обмена сообщениями.	Проработка лекционного материала	3	ОПК-6	Зачет, Тест
	Итого	3		
6 Практические аспекты реализации средств криптографической защиты информации.	Подготовка к тесту	6	ОПК-6	Зачет, Тест
	Подготовка к практическим занятиям, семинарам	6		
	Проработка лекционного материала	3		
	Итого	15		
Итого за семестр		54		
Итого		54		

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
8 семестр				
Зачет			20	20
Отчет по лабораторной	10	10	20	40

Согласована на портале № 47714

работе				
Тест			40	40
Итого максимум за период	10	10	80	100
Нарастающим итогом	10	20	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. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М. : Гелиос АРВ, 2004. - 143[1] с. : ил. - Загл. обл. : Криптография в упражнениях и задачах. - Загл. на корешке : Криптография в упражнениях и задачах. - Библиогр.: с. 139. - ISBN 5-85438-009-9 : 52.25 р. (наличие в библиотеке ТУСУР - 50 экз.)

2. Криптография : учебник для вузов: пер. с англ. / Н. Смарт ; пер. С. А. Кулешов, ред. пер. С. К. Ландо. - М. : Техносфера, 2005. - 525[3] с. : ил. - (Мир программирования ; VIII-05). - Предм. указ.: с. 524-525. - ISBN 5-94836-043-1 : 402.00 р. (наличие в библиотеке ТУСУР - 11 экз.)

12.2. Дополнительная литература

1. Основы криптографии : учебное пособие для вузов / А. П. Алферов [и др.]. - 3-е изд., испр. и доп. - М. : Гелиос АРВ, 2005. - 479, [1] с. : ил. - Библиогр.: с. 469-475. - ISBN 5-85438-137-0 (наличие в библиотеке ТУСУР - 30 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации [Электронный ресурс]: методические указания для выполнения практических и самостоятельных работ [Электронный ре-

Согласована на портале № 47714

сурс]. — 2014. [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf (дата обращения: 21.06.2019).

2. Евсютин О.О. Прикладная криптография [Электронный ресурс]: методические указания для выполнения лабораторных и самостоятельных работ [Электронный ресурс]. — 2014. [Электронный ресурс]. — Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_pk.pdf (дата обращения: 21.06.2019).

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. Рекомендуется использовать информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

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

Учебная аудитория

учебная аудитория для проведения занятий практического типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 403 ауд.

Описание имеющегося оборудования:

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение не требуется.

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.);

Согласована на портале № 47714

- 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:
– MaxPatrol Education

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.

Согласована на портале № 47714

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

Согласована на портале № 47714

- 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

Согласована на портале № 47714

- 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. 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.

14.1.3. Темы лабораторных работ

Установка и настройка Active Directory Certificate Services.Целью данной лабораторной является ознакомление с процессом установки службы Active Directory Certificate Services (службы сертификации) и особенностями работы с сертификатами.

Рассматриваются технические меры повышения защищенности систем. Изучаются методы, лежащие в основе соответствующих средств и механизмов в аспектах идентификации и аутентификации.

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	Решение дистанционных тестов,	Преимущественно дистанционными

Согласована на портале № 47714

опорно-двигательного аппарата	контрольные работы, письменные самостоятельные работы, вопросы к зачету	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.

Согласована на портале № 47714