



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



«УТВЕРЖДАЮ»

Проректор по учебно-методической работе

Н.В. Бабина

«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

**ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

**«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ
ИНФОРМАЦИИ»**

Направление подготовки: 10.03.01 Информационная безопасность

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Сухотерин А.И. **Рабочая программа дисциплины:** «Криптографические методы защиты информации». – **Королев МО: «Технологический университет», 2020.**

Рецензент: к.в.н., доцент Соляной В.Н.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переподтверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ОПОП ВО

к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переподтверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

1. Сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности.
2. Освоение студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- ОПК-3: способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;

Профессиональные компетенции:

- ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
- ПК-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
- ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

Основными **задачами** дисциплины являются:

- Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные задачи и понятия криптографии;
- частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
- модели шифров и математические методы их исследования;
- требования к шифрам и основные характеристики шифров;

- основные задачи и понятия криптографии;
- типовые поточные и блочные шифры;
- типовые шифры с открытыми ключами;
- криптоалгоритмы, используемые в современных криптосистемах с открытым ключом;
- криптоалгоритмы, используемые в стандартах шифрования данных;
- методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистемы;
- ключевые системы современных криптосистем и протоколы распределения ключей;

Уметь:

- применять полученные знания к исследованию простых шифров;
- строить и изучать математические модели криптоалгоритмов;
- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
- решать основные задачи на применение криптографических алгоритмов в защите информации.

Владеть:

- навыками использования ЭВМ в анализе простейших шифров;
- криптографической терминологией;
- навыками математического моделирования в криптографии;
- навыками использования типовых криптографических алгоритмов.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Криптографические методы защиты информации» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Аппаратные средства вычислительной техники», «Языки программирования», «Информатика», «Основы информационной безопасности», «Математический анализ», «Основы управления информационной безопасностью» и компетенциях: ОК-5, ОПК-2,4,7 и ПК-2,4,13.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Комплексное обеспечение

защиты информации объекта информатизации (предприятия)», «Организация информационно-аналитического обеспечения финансового мониторинга», «Стандарты информационной безопасности в банковской сфере», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетные единицы, 108 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 7	Семестр 8	Семестр ...	Семестр ...
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	60	60			
КСР	-	-			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	T1; T2	T1; T2			
Вид итогового контроля	Зачет	Зачет			

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Код компетенций
Седьмой семестр				
Раздел 1. Теоретические основы криптографии				
Тема 1. Общие принципы информационной безопасности.	4	8	3	ОПК-3; ПК-1,2,7.

Тема 2. Теоретические основы криптографии.	4	8	3	ОПК-3; ПК-1,2,7.
Раздел 2. Прикладные криптографические методы систем защиты информации и их реализация				
Тема 3. Криптографическ ие протоколы.	4	8	3	ОПК-3; ПК-1,2,7.
Тема 4. Общие принципы РКІ.	4	8	3	ОПК-3; ПК-1,2,7.
Итого:	16	32	12	

4.2. Содержание тем дисциплины

Раздел 1. Теоретические основы криптографии

Тема 1. Общие принципы информационной безопасности

Политика безопасности, уязвимости, угрозы, механизмы и услуги безопасности, превентивные и проактивные методы обеспечения безопасности. Принципы построения систем информационной безопасности: минимизация привилегий, минимальное число доверенных компонент, простота, скептицизм и параноидальный подход к оценке криптостойкости.

Конфиденциальность. Целостность. Подлинность. Неотрекаемость (невозможность отказа). Доступность. Анонимность.

Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (тройские программы, потайные ходы).

Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Тема 2. Теоретические основы криптографии

Формальное определение классической криптосистемы. Условная вероятность и теорема Байеса. Совершенная секретность и теорема Шеннона. Одноразовый блокнот (шифр Вернама). Конечные поля. Мультипликативная группа конечного поля. Дискретная логарифмическая проблема. Теоремы Эйлера и Ферма. Эллиптические кривые. Группа точек эллиптической кривой.

Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) криптосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное

криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB, PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89. Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамала. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность, неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

Свойства хэш-функции. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHA, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Раздел 2. Прикладные криптографические методы систем защиты информации и их реализация

Тема 3. Криптографические протоколы

Анонимность и неотслеживаемость. Проблема «ужинающих криптографов». Протоколы для анонимных чеков на основе «слепой» подписи. Свойства идеальной системы электронных наличных. Платежных систем Payword и Micromint.

Протокол электронного аукциона, отвечающий требованиям Федерального Закона № 94 от 21 июля 2005 года «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».

Принципы квантовой криптографии. Квантовый протокол распределения ключей.

Обзор биометрических методов. Метод биометрической «вуали».

Тема 4. Общие принципы PKI

Генерация ключей. Неравносильные ключи. Распределение. Проверка. Использование. Обновление. Хранение и резервирование. Уничтожение. Жизненный цикл ключа. Определения ключей Vaffine.

Метод полной матрицы. Проблема «квадратного корня». Облегченная схема предварительного распределения ключей KEDYS. Облегченная схема предварительного распределения ключей для кластерной архитектуры EKSYD.

Проблема подлинности открытых ключей – на примере атаки «человек посередине» (man-in-the-middle-attack). Цифровой сертификат (по Конфелдеру).

Сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных сертификатов (COC), приостановление действия сертификата, Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата. Архитектура PKI. Понятие сертификационного пути. Преимущества PKI.

Непосредственный контакт. Удаленный доступ. Разделение функциональности. Расширение функциональности.

Проекты Clipper и Capstone. Стандарт EES. Криптоалгоритм Skipjack.

Проблематика. Промежуточные COC (Delta CRL). Сегментированные COC. Система отзыва сертификатов (CRS). Проверка статуса сертификата при помощи дерева Меркля. Протокол проверки статуса сертификата OCSP.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине.

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Криптографические методы защиты информации» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Бабаш. А.В. Криптографические методы защиты информации. Том 1. Учебно - метод. пособие. – 2-е изд.-М.: ИНФРА-М, 2013.-413.
2. Горбатов В.С. Основы технологии PKI-2-е издание, стереотип. – М. Горячая линия – Телеком, 2011.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебное пособие для вузов.-4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

Дополнительная литература:

1. Афанасьев А.А., Веденньев Л.Т. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

2. Тихонов В.А., Райх В.В.. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.

3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стенографии – 2-е издание –М. Горячая линия – Телеком, 2013.

Рекомендуемая литература:

1. Коваленко Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. – М. Горячая линия – Телеком, 2012.

2. Ищейнов В.Я., Мещатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009.

3. Чепига А.Ф.. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.

4. Словарь криптографических терминов / Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006.

5. Бабаш А.В.. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие/- 2-е изд., стер.-М.: КНОРУС, 2013.

Электронные книги:

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ, 2012.

http://biblioclub.ru/index.php?page=book_view&book_id=231673

2. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. –М. Горячая линия – Телеком,- 2-е изд., стер. 2012.

http://eknigi.org/nauka_i_ucheba/57446-kriptograficheskie-metody-zashhity-informacii.html

3. Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информации // Успехи современного естествознания. – 2010.

www.rae.ru/use/?section=content&op=show_article&article_id=7784920

4. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.-4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.

2. <http://informika.ru/> – образовательный портал.

3. <http://www.academy.it.ru/> – академия АЙТИ.

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.
- **Информационные справочные системы:**
 1. Ресурсы информационно-образовательной среды МГОТУ.
 2. Рабочая программа и методическое обеспечение по дисциплине: «Криптографические методы защиты информации»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
 - рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
 - рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»
(Приложение 1 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-3	способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Тема:1,3,4	типовые шифры с открытыми ключами	анализировать основные задачи и понятия криптографии;	криптографической терминологией
2.	ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Тема:1,3,4	типовые шифры с открытыми ключами	анализировать требования к шифрам и основные характеристик и шифров; типовые поточные и блочные шифры	криптографической терминологией
3.	ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Тема:2,4	требования к шифрам и основные характеристик и шифров;	применять математические методы исследования моделей шифров;	криптографической терминологией
4.	ПК-7	способность проводить анализ исходных данных для проектирования подсистем и	Тема:1,4	типовые поточные и блочные шифры;	применять математические методы исследования моделей шифров;	навыками использования ПК в анализе простейших шифров;

		средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
--	--	---	--	--	--	--

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-3	Доклад в форме презентации	<p>А) полностью сформирована 5 баллов</p> <p>В) частично сформирована 3-4 балла</p> <p>С) не сформирована 2 балла</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> 1. Соответствие представленной презентации заявленной тематике (1 балл). 2. Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3. Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4. Качество самой представленной презентации (1 балл). 5. Оригинальность подхода и всестороннее раскрытие выбранной тематике (1 балл). <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-1	Доклад в форме презентации	<p>А) полностью сформирована 5 баллов</p> <p>В) частично сформирована 3-4 балла</p> <p>С) не сформирована 2 балла</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <ol style="list-style-type: none"> 1. Соответствие представленной презентации заявленной тематике (1 балл). 2. Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).

			<p>4. Качество самой представленной презентации (1 балл).</p> <p>5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-2	Контрольная работа	<p>А) полностью сформирована 5 баллов</p> <p>В) частично сформирована 3-4 балла</p> <p>С) не сформирована 2 балла</p>	<p>Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1. Соответствие представленной презентации заявленной тематике (1 балл).</p> <p>2. Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</p> <p>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</p> <p>4. Качество самой представленной презентации (1 балл).</p> <p>5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ПК-7	Доклад в форме презентации	<p>А) полностью сформирована 5 баллов</p> <p>В) частично сформирована 3-4 балла</p> <p>С) не сформирована 2 балла</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1. Соответствие представленной презентации заявленной тематике (1 балл).</p>

			<p>2. Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</p> <p>3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).</p> <p>4. Качество самой представленной презентации (1 балл).</p> <p>5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.</p>
--	--	--	---

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и асимметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.

10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

11. Информационная безопасность при составление и направление ЭД участником – отправителем.

12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Примерная тематика заданий на контрольную работу:

1. Информационная безопасность модели Интернет - банкинга.
2. Информационная безопасность расчетов банковскими картами в Интернете.
3. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
4. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
5. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
6. Применение и информационная безопасность режима электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту.
7. Режим счетчика (counter). Функция хеширования и асимметричные алгоритмы.
8. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
9. Информационная безопасность электронных платежей с помощью цифровых денег.
10. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
11. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
12. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
13. Информационная безопасность при составление и направление ЭД участником – отправителем.
14. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

15. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Криптографические методы защиты информации» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-3; ПК-1; ПК-2; ПК-7.	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-3; ПК-1; ПК-2; ПК-7.	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная

						оценка – 5 баллов.
Согласно учебному плану	Зачет	ОПК-3; ПК-1; ПК-2; ПК-7.	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: « Зачтено »: <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. « Незачтено »: <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплины и незнание основных понятий; • незнание неумение использовать и применять полученные

					знания на практике; • не работал на практически х занятиях
--	--	--	--	--	---

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

Тестовые задания для контроля остаточных знаний

Вариант № 1

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:

- Криптоанализ
- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем

"ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной

- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 2

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

- Криптология
- Криптография

- Криптостойкость
 - Криптометодология
2. Криптология включает в себя:
- Криптоанализ
 - Криптография
 - Криптосервис
 - Криптостойкость
3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:
- симметричным системам шифрования
 - асимметричным системам шифрования
 - одноключевым системам шифрования
 - ключным системам
4. Простейшим из шифров замены является:
- одноалфавитная подстановка
 - многоалфавитная замена
 - гомофонический шифр
 - малоалфавитная замена
5. Сколько этапов можно условно выделить в истории криптографии?
- 4
 - 3
 - 40
 - 7
6. Для наивной криптографии (до начала XVI в.) характерно использование:
- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
 - формализованных и относительно стойких к ручному криптоанализу шифров
 - криптосистем со строгим математическим обоснованием криптостойкости
 - вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры
7. Когда возникла компьютерная криптография?
- с 1970-х гг.
 - с 1980-х гг.

- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в эталонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования"

- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

Вариант № 3

1. Как называется наука о способах преобразования информации с целью ее защиты от незаконных пользователей?

- Криптология
- Криптография
- Криптостойкость
- Криптометодология

2. Криптология включает в себя:

- Криптоанализ

- Криптография
- Криптосервис
- Криптостойкость

3. Системы шифрования, в которых для шифрования и для расшифрования используется один и тот же ключ относятся к:

- симметричным системам шифрования
- асимметричным системам шифрования
- одноключевым системам шифрования
- ключным системам

4. Простейшим из шифров замены является:

- одноалфавитная подстановка
- многоалфавитная замена
- гомофонический шифр
- малоалфавитная замена

5. Сколько этапов можно условно выделить в истории криптографии?

- 4
- 3
- 40
- 7

6. Для наивной криптографии (до начала XVI в.) характерно использование:

- любых, обычно примитивных, способов запутывания противника относительно содержания шифруемых текстов
- формализованных и относительно стойких к ручному криптоанализу шифров
- криптосистем со строгим математическим обоснованием криптостойкости
- вычислительных средств с производительностью, достаточной для реализации криптосистем, обеспечивающих при большой скорости шифрования на несколько порядков более высокую криптостойкость, чем "ручные" и "механические" шифры

7. Когда возникла компьютерная криптография?

- с 1970-х гг.
- с 1980-х гг.
- с 1990-х гг.
- с 2000-х гг.

8. В системе передачи данных между абонентами с коммутацией пакетов используются два способа передачи:

- дейтаграммный
- виртуальный
- параллельный
- перпендикулярный

9. Сколько уровней в этолонной модели OSI?

- 1
- 13
- 10
- 7

10. В каком году приняты определяющие нормативные правовые акты Российской Федерации: Концепция национальной безопасности Российской Федерации и Доктрина информационной безопасности Российской Федерации?

- 2000
- 1967
- 1998
- 2008

11. Подлежит ли деятельность по распространению шифровальных (криптографических) средств обязательному лицензированию?

- да
- нет
- для государственных учреждений нет, а для коммерческих предприятий да
- только для иностранных компаний, действующих на территории России

12. Какой уровень модели OSI обеспечивает создание, передачу и прием кадров данных? (Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов)

- канальный
- представления
- прикладной
- сеансовый

13. В каком ГОСТ-е дано определение термину "служебная тайна"?

- ГОСТ Р 51624-2000 “Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования”
- ГОСТ Р 51583-2000 “Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения”
- ГОСТ Р ИСО\МЭК 15408
- Common Criteria

14. В Доктрине информационной безопасности РФ важное значение придано системам и сетям России, в том числе по следующим направлениям:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств
- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи
- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации
- развитию свободы слова в Интернете

15. Основными мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- закрытие всех интернет-кафе
- лицензирование деятельности организаций в области защиты информации
- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите

4.2. Типовые вопросы, выносимые на зачет

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Классификация методов криптографического закрытия информации
5. Классические шифры.
6. Шифры гаммирования и колонной замены.
7. Простейшие шифры и их свойства.
8. Композиции шифров.
9. Системы шифрования с открытыми ключами.
10. Криптографическая стойкость шифров.
11. Модели шифров.
12. Основные требования к шифрам.
13. Вопросы практической стойкости.
14. Имитостойкость и помехоустойчивость шифров.
15. Принципы построения криптографических алгоритмов

16. Аппаратные средства. Программные средства, программные реализации шифров.
17. Крипто сервис провайдеры (CSP).
18. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи; ключевые системы.
19. Виртуальные частные сети.
20. Скремблеры.
21. Криптографические параметры узлов и блоков шифраторов.
22. Синтез шифров.
23. Методы получения случайных и псевдослучайных последовательностей.
24. Электронные цифровые подписи (электронные подписи).
25. Криптографические хеш-функции.
26. Криптографические протоколы.
27. Основные подходы к реализации PKI.
28. Компоненты и сервисы инфраструктуры открытых ключей.
29. Архитектура и топология PKI.
30. Стандарты в области PKI 50.
31. Стандарты Internet X.509 PKI (PKIX).
32. Сертификаты открытых ключей X.509.
33. Списки аннулированных сертификатов. Атрибутные сертификаты.
34. Основные требования к политике PKI.
35. Политика применения сертификатов и регламент.
36. Краткая характеристика политики PKI.
37. Набор положений политики PKI.
38. Проблемы формирования политики PKI.
39. Симметричные криптосистемы.
40. Основы теории К. Шеннона.
41. Симметричные методы шифрования.
42. Алгоритмы блочного шифрования.
43. Режимы применения блочных шифров.
44. Поточковые шифры.
45. Комбинированные методы.
46. Односторонние функции и функции ловушки.
47. Асимметричные системы шифрования.
48. Применение асимметричных алгоритмов.
49. Средства криптографической защиты, разработанные компаниями: Инфотекс, Крипто-Про, ОКБ Сапр, Аладдин и Adobe, MS Windows, Cisco.
50. Хранилище сертификатов ОС MS Windows.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»
(Приложение 2 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

- Сформировать представление о современных методах и средствах криптографической защиты информации, используемых, в частности, для решения проблем компьютерной безопасности.
- Освоение студентами основ криптографических методов, оценок систем защиты информации в компьютерных системах и сетях.

Задачи дисциплины:

- Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

2. Указания по проведению практических занятий

Раздел 1. Основы информационной безопасности региона

Тема 1. Общие принципы информационной безопасности. Услуги безопасности. Угрозы. Механизмы

Практическое занятие 1.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных угроз безопасности для информационного объекта.

Основные положения темы занятия:

- базовые составляющие концепции информационной безопасности информационного объекта.
- основные направления обеспечения информационной безопасности.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Конфиденциальность. Целостность. Подлинность.
Неотрекаемость (невозможность отказа). Доступность. Анонимность.

2. Фундаментальные угрозы – утечка информации, нарушение целостности, отказ в обслуживании, незаконное использование. Первичные угрозы – проникновение (маскарад, обход защиты, нарушение полномочий) и внедрение (троянские программы, потайные ходы).

3. Шифрование. Цифровая подпись. Хэш-функция. Взаимосвязь услуг безопасности, механизмов и алгоритмов.

Продолжительность занятия – 8 ч.

Тема 2. Теоретические основы криптографии. Криптографические методы защиты информации. Общие принципы и модели. Симметричные криптосистемы и блочные шифры. Асимметричные криптосистемы. Хэш-функции

Практическое занятие 2.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических методов защиты информации.

Основные положения темы занятия:

- базовые составляющие криптографической защиты информации.
- криптосистемы и блочные шифры.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Базовая модель (отправитель ↔ злоумышленник ↔ получатель). Терминология: секретный/общедоступный ключи, открытый текст, шифртекст, криптоалгоритм, шифр, криптосистема, атака. Одноключевая (симметричная) криптосистема. Двухключевая (асимметричная) криптосистема или криптосистема с общедоступным ключом. Прямое криптографическое преобразование (зашифрование). Обратное криптографическое преобразование (расшифрование). Вычисление и проверка цифровой подписи. Код аутентичности сообщения (MAC). Метод цифрового конверта. Пассивные и активные атаки. Классификация атак.

2. Определение блочного шифра. Принцип итерирования. Конструкция Фейстеля. Режимы шифрования. (ECB, CBC, CFB, OFB, PCBC). Стандарты блочного шифрования – AES, ГОСТ-28147-89. Поточные шифры (на примере RC4). Схема одноразовых паролей (OTP). Минимальная длина ключа симметричной криптосистемы. Экспортные ограничения на длину ключа. Метод расширения ключевого пространства. Принцип несепарабельного шифрования. Многоуровневая криптография.

3. Криптосистема RSA. Практическая криптостойкость RSA: оценки и прогнозы. Криптосистема ЭльГамала. Протокол согласования ключа Диффи-Хэллмана. Свойства цифровой подписи (подлинность, целостность,

неотрекаемость). Федеральные стандарты цифровой подписи – DSS, ГОСТ Р 34.10 2001 (группа точек эллиптической кривой).

4. Свойства хэш-функции. Функция сжатия, как основной метод построения хэш-функций. Ключевые и бесключевые хэш-функции. Алгоритм HMAC. Федеральные стандарты хэш-функций – SHA, ГОСТ Р 34.11-94. MD5 – de facto стандарт Internet. Парадокс «дней рождения». Атаки на основе парадокса «дней рождения».

Продолжительность занятия – 8 ч.

Раздел 2. Оценка криптографических методов систем защиты информации

Тема 3. Криптографические протоколы. Базовые принципы. Финансовая криптография. Электронные аукционы. Квантовая криптография. Биометрия Практическое занятие 3.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки моделирования основных криптографических протоколов защиты информации.

Основные положения темы занятия:

- базовые протоколы криптографической защиты информации.
- квантовая криптография.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Принципы проектирования криптографических протоколов по Нидхему-Шредеру. Протокол «запрос-ответ».
2. Анонимность и неотслеживаемость. Проблема «ужинающих криптографов». Протоколы для анонимных чеков на основе «слепой» подписи. Свойства идеальной системы электронных наличных. Платежных систем Payword и Micromint.
3. Протокол электронного аукциона, отвечающий требованиям Федерального Закона № 94 от 21 июля 2005 года «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд».
4. Принципы квантовой криптографии. Квантовый протокол распределения ключей.
5. Обзор биометрических методов. Метод биометрической «вуали».

Продолжительность занятия – 8 ч.

Тема 4. Управление ключами. Общие принципы. Депонирование ключей. Предварительное распределение ключей. Инфраструктура открытых ключей. Назначение РКІ. Основные понятия. Принципы взаимодействия с УЦ. Список отозванных сертификатов

Практическое занятие 4.

Вид практического занятия: *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки управления ключами.

Основные положения темы занятия:

- Управление ключами.
- Взаимодействие с УЦ.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Генерация ключей. Неравносильные ключи. Распределение. Проверка. Использование. Обновление. Хранение и резервирование. Уничтожение. Жизненный цикл ключа. распределения ключей Vaffine.
2. Метод полной матрицы. Проблема «квадратного корня». Облегченная схема предварительного распределения ключей KEDYS. Облегченная схема предварительного распределения ключей для кластерной архитектуры EKSYD. Проблема подлинности открытых ключей – на примере атаки «человек посередине» (man-in-the-middle-attack). Цифровой сертификат (по Конфелдеру).
3. Сертификат, подписчик, пользователь, выпуск сертификата, аннулирование открытого ключа, отзыв сертификата, список отозванных сертификатов (COC), приостановление действия сертификата, Удостоверяющий Центр (УЦ), Центр регистрации (ЦР), взаимная (перекрестная) сертификация. Жизненный цикл сертификата. Архитектура РКІ. Понятие сертификационного пути. Преимущества РКІ.
4. Непосредственный контакт. Удаленный доступ. Разделение функциональности. Расширение функциональности.

Продолжительность занятия – 8 ч.

3. Указания по проведению лабораторных работ

Лабораторные работы не предусмотрены Учебным планом.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

- 1) расширить представление в области существующих современных аппаратных средств вычислительной техники;
- 2) привить навыки самостоятельного решения нестандартных задач в

области аппаратных средств вычислительной техники.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	Очная форма обучения
	Всего академических часов
Всего часов на самостоятельную работу	60
Вопросы, выносимые на самостоятельное изучение	34
Подготовка к практическим занятиям	8
Подготовка к лабораторным занятиям	-
Подготовка докладов	10
Выполнение практических заданий	8

**Вопросы, выносимые на самостоятельное изучение:
для очной формы обучения:**

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и асимметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
11. Информационная безопасность при составление и направление ЭД участником – отправителем.

12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.

13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	34	Изучение открытых источников
2.	Подготовка к практическим занятиям	8	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	
4.	Тематика докладов	10	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических заданий	8	Разработка аппаратного средства вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.

14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике РКІ.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики РКІ.
18. Набор положений политики РКІ.
19. Проблемы формирования политики РКІ.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Хранилище сертификатов ОС MS Windows.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

Основная:

1. Бабаш. А.В. Криптографические методы защиты информации. Том 1. Учебно - метод. пособие. – 2-е изд.-М.: ИНФРА-М, 2013.-413.

2. Горбатов В.С. Основы технологии РКІ-2-е издание, стереотип. – М. Горячая линия – Телеком, 2011.

3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

Дополнительная:

1. Афанасьев А.А., Веденньев Л.Т. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

2. Тихонов В.А., Райх В.В.. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. - М.: Гелиос АРВ, 2006.

3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стенографии – 2-е издание –М. Горячая линия – Телеком, 2013.

Рекомендуемая:

1. Коваленко Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. – М. Горячая линия – Телеком, 2012.

2. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009.

3. Чепига А.Ф.. Информационная безопасность автоматизированных систем. М.: «Гелиос АРВ», 2010.

4. Словарь криптографических терминов / Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006.

5. Бабаш А.В.. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие/- 2-е изд., стер.-М.: КНОРУС, 2013.

Электронные книги:

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ, 2012.

http://biblioclub.ru/index.php?page=book_view&book_id=231673

2. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. –М. Горячая линия – Телеком,- 2-е изд., стер. 2012.

http://eknigi.org/nauka_i_ucheba/57446-kriptograficheskie-metody-zashhity-informacii.html

3. Жданов О.Н., Золотарев В.В. МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ // Успехи современного естествознания. – 2010.

www.rae.ru/use/?section=content&op=show_article&article_id=778492

4. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Учебное пособие для вузов.: -4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

<http://biblioclub.ru/index.php?page=book&id=253208&sr=1>

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. <http://eup.ru/catalog/all-all.asp> – научно-образовательный портал.
 2. <http://informika.ru/> – образовательный портал.
 3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
 4. www.biblioclub.ru - Универсальная библиотека онлайн.
 5. www.rucont.ru - ЭБС «Руконт».
 6. <http://www.academy.it.ru/> – академия АЙТИ.
 7. <http://www.minfin.ru> - Официальный сайт Министерства финансов Российской Федерации
 8. <http://www.gov.ru> - Официальный сервер органов государственной власти Российской Федерации.
 9. <http://www.fsb.ru/> - Официальный сайт Федеральной Службы Безопасности
- <http://www.fstec.ru/> - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

8. Перечень информационных технологий

Перечень программного обеспечения: *MOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Криптографические методы защиты информации».