Приложение к ОПОП
«Разработка программно-информационных систем»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)**

РАБОЧАЯ ПРОГРАММА

дисциплины

«КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ»

для подготовки бакалавров

по направлению

09.03.04 «Программная инженерия»

по профилю

«Разработка программно-информационных систем»

Санкт-Петербург

2022

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

к.т.н., доцент Племянников А.К.

Рабочая программа рассмотрена и одобрена на заседании кафедры ИБ 07.09.2022, протокол № 7

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 29.09.2022, протокол № 7

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИБ
Общая трудоемкость (ЗЕТ)	4
Курс	4
Семестр	7
Виды занятий	
Лекции (академ. часов)	17
Лабораторные занятия (академ. часов)	17
Практические занятия (академ. часов)	17
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	52
Самостоятельная работа, включая часы на контроль (академ. часов)	92
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	4

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ»

Дисциплина формирует знания и умения, необходимые для разработки криптографических модулей и исследования их стойкости к компьютерным атакам.

В рамках дисциплины изучаются следующие основные темы: симметричные блочные шифры, включая зарубежные и отечественные стандарты, атаки на симметричные блочные шифры, хэш функции и атаки на них, коды аутентификации, поточные шифры и атаки на них, способы распределения секретных ключей, ассиметричные шифры, алгоритмы создания и проверки электронной цифровая подписи, управление сертификатами открытых ключей, стандарты инфраструктуры отрытых ключей, отечественные средства криптографической защиты информации, приложения криптографии.

Практические часть курса, в составе лабораторных и практических работ нацелена на изучение криптомодулей и анализ их стойкости к атакам с использованием приложения CrypTool.

SUBJECT SUMMARY

«DATA PROTECTION CRYPTOGRAPHY METHODS AND TOOLS»

The discipline is aimed at studying the issue of the fundamental principles of data protection using cryptographic methods and applying examples of implementation of these methods in practice.

Course content introduces students to the contemporary history of cryptography and its current trends, reveals the details of the main cryptographic transformations for concealment and control of data integrity. Syllabus assesses resistance of these transformations to attack intruders from the standpoint of modern methods of cryptanalysis.

The discipline enables the acquisition of knowledge and skills in the field of cryptographic protection of information in accordance with state educational standards.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Цель дисциплины: приобретение теоретических знаний и практических навыков анализа и разработки криптографических преобразований для обеспечения конфиденциальности и целостности данных для решения задач профессиональной деятельности. Теоретический базис дисциплины основывается на знаниях из теории чисел, дискретной математики, теории кодирования, теории алгоритмов.

2. Задачи дисциплины:
-изучение криптографических модулей, входящих в состав компьютерных систем;
-освоение методов исследования стойкости к компьютерным атакам криптографических модулей, входящих в состав компьютерных систем;
-приобретение практических навыков разработки программных средств криптографической защиты данных.

3. Дисциплина обеспечивает получение знаний, необходимых для разработки криптографических модулей, входящих в состав компьютерных систем.

4. Дисциплина вырабатывает умения исследования стойкости к компьютерным атакам криптографических модулей, входящих в состав компьютерных систем.

5. Результатом освоения дисциплины является приобретение практических навыков разработки программных средств криптографической защиты данных.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Алгебраические структуры»

2. «Дискретная математика и теоретическая информатика»

3. «Комбинаторика и теория графов»

4. «Математическая логика и теория алгоритмов»

и обеспечивает изучение последующих дисциплин:

1. «Производственная практика (научно-исследовательская работа)»

2. «Производственная практика (преддипломная практика)»

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ОПК-3.1	*Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*
ОПК-3.2	*Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*
ОПК-3.3	*Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	Лаб, ач	ИКР, ач	СР, ач
1	Ведение	1	0	0	0	0
2	Эволюция криптографии	2	2	2	0	10
3	Методы симметричного шифрования	3	5	5	0	18
4	Методы контроля целостности и подлинности данных	2	2	2	0.25	12
5	Потоковые шифры и генераторы случайных последовательностей	2	0	0	0	10
6	Методы ассиметричного шифрования	2	4	4	0	20
7	Электронная цифровая подпись	2	2	2		10
8	Распределение открытых ключей	2	2	2	0.25	12
9	Заключение	1			0.5	
	Итого, ач	17	17	17	1	92
	Из них ач на контроль	0	0	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4				

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Ведение	Структура рабочей программы курса. Методика контроля знаний. Цели информационной безопасности. Место криптографии среди других наук. Угрозы в фокусе криптографии. Задачи криптографии. Введение в криптоанализ. Виды атак.

№ п/п	Наименование темы дисциплины	Содержание
2	Эволюция криптографии	Интуитивная криптография: Шифр Сцитала, Шифр Изгороди. Шифр Цезаря. Формальная криптография: аффинный шифр, шифр моноалфавитной подстановки, омофонический шифр, комбинированный шифр ADFGVX, шифр Вернама, требования к одноразовому блокноту. Шифровальная машина. Принципы Керкгоффса. Научная криптография: Обзор теории секретной связи Шеннона. Классическая схема секретной системы связи. Совершенная секретная система. Принципы построения блочных шифров. Сеть Фейстеля. подстановочно-перестановочная сеть. Обзор теории сложности вычислений. Вехи отечествен-ной криптографии XX века Компьютерная криптография. Модель симметричной криптосистемы. Свойства симметричной криптосистемы. Блочный шифр. Поточный шифр. Модель асимметричной криптосистемы. Свойства асимметричной криптосистемы. Сравнение криптосистем. Модель гибридной криптосистемы.
3	Методы симметричного шифрования	Стандарт шифрования данных DES. Дифференциальный и линейный криптоанализ. Проблемы DES. Режимы работы блочных шифров. Шифр Triple DES. Атака встреча посредине. Конкурс AES. Шифр Rijndael и другие финалисты. Криптоанализ AES. Достоинства AES. ГОСТ 28147-89 ”Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”, криптоанализ этого алгоритма. ГОСТ Р 34.12–2015 ”Информационная технология. Криптографическая защита информации. Блочные шифры”. ГОСТ Р 34.13–2015 ”Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров”.
4	Методы контроля целостности и подлинности данных	Односторонняя хэш-функция. Модель идеальной хэш-функции. Анализ модели на основе проблем дня рождения. Атаки на хэш-функции. Хэш-функция MD5. Пример атаки на MD5 методом радужных таблиц. Хэш-функции SHA-1 и SHA-2. ГОСТ Р 34.11-12 ”Информационная технология. Криптографическая защита информации. Функция хэширования” Конкурс SHA-3. Хэш-функция Keccak и ее свойства. Коды обнаружения модификации: MAC, HMAC, CMAC.

№ п/п	Наименование темы дисциплины	Содержание
5	Потоковые шифры и генераторы случайных последовательностей	Требования к криптостойким генераторам. Специальные реализации: по-токовый шифр A5/1 и его криптоанализ, аддитивные генераторы, потоковый шифр RC4 и его криптоанализ. Реализации на основе вычислительно сложных задач: генератор RSA, генератор с квадратичным остатком, генератор Blum-Micali. Реализация на основе шифров: режим счетчика, режим обратной связи по выходу, режим обратной связи по шифру. Генератор ключей стандарта ANSI X9.17. Тестирование псевдослучайных последовательностей. NIST Statistical Test Suite.
6	Методы ассиметричного шифрования	Модель асимметричной криптосистемы. Свойства асимметричной крипто-системы. Требования к шифрам с открытым ключом. Односторонняя функция с секретом. Шифр RSA, примеры атак на RSA. Рекомендации по выбору параметров RSA. Шифр Эль-Гамаля, примеры атак на шифр. Введение в эллиптическую криптографию. Моделирование криптосистемы Эль-Гамаля. Свойства метода с использованием эллиптической кривой. Гибридные криптосистемы. Атака по побочным каналам на гибридную криптосистему
7	Электронная цифровая подпись	Сравнение рукописных и цифровых подписей. Виды подделок цифровой подписи. Цифровая подпись RSA, подделка цифровой подписи. Цифровая подпись Эль-Гамаля, подделка цифровой подписи. Цифровая подпись DSA. Сравнительный анализ подписей. ГОСТ Р 34.10-94 ”Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.”. Цифровая подпись ECDSA. ГОСТ Р 34.10─2012 ”Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи”
8	Распределение открытых ключей	Распределение открытых ключей. Понятие сертификата открытого ключа. Структура сертификата стандарта X.509. Инфраструктура открытых ключей (PKI). Компоненты PKI: удостоверяющий центр, политика применения сертификатов, регистрационный центр, репозиторий, архив сертификатов. Понятие архитектуры PKI. Путь сертификации. Строго иерархическая архитектура. Сетевая архитектура. Гибридная архитектура. Стандарты PKI, стандарт X.509, стандарты PKCS, стандарты PKIX. Приложения основанные на PKI.
9	Заключение	Основные направления развития современной криптографии. Обзор криптографических средств защиты.

4.2 Перечень лабораторных работ

Наименование лабораторной работы	Количество ауд. часов
1. Исследование свойств классических шифров	2
2. Исследование свойств шифра DES и его модификаций	2
3. Исследование свойств симметричных шифров–финалистов конкурса AES	3
4. Исследование свойств хэш-функций	2
5. Исследование свойств асимметричных шифров	4
6. Исследование свойств электронной цифровой подписи	4
Итого	17

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Применение классических шифров для зашифровки и расшифровки сообщений	2
2. Применение симметричных шифров для зашифровки и расшифровки сообщений	5
3. Применение хэш-функций для контроля целостности сообщений	2
4. Применение ассиметричных шифров для зашифровки и расшифровки сообщений	4
5. Применение эллиптических кривых для создания и проверки цифровой подписи	4
Итого	17

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал презентации, представленной на лекции. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины и дополнить ими представленную на лекции презентацию.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	16

Текущая СРС	Примерная трудоемкость, ач
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	8
Самостоятельное изучение разделов дисциплины	0
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	20
Подготовка к контрольным работам, коллоквиумам	13
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	92

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Дернова, Евгения Сергеевна. Элементы теоретических основ криптографии [Текст] : учеб. пособие / Е.С. Дернова, Н.А. Молдовян, П.А. Молдовяну, 2009. -91 с.	77
2	Коржик, Валерий Иванович. Основы криптографии [Текст] : учеб. пособие по направлениям подгот. бакалавров и магистров: 10.04.01, 10.03.01 ”Информационная безопасность”, 43.03.01 ”Сервис”, 11.03.02, 11.04.02 ”Инфокоммуникационные технологии и системы связи”, по специальности 210403 ”защищенные системы связи” / В. И. Коржик, В. А. Яковлев, 2017. -294 с.	29
3	Столлингс, Вильям. Криптография и защита сетей. Принципы и практика [Текст] : монография / В.Столлингс; [Пер. с англ. А.Г.Сивака, А.А.Шпака], 2001. -669 с.	42
Дополнительная литература		
1	Гашков, Сергей Борисович. Криптографические методы защиты информации [Текст] : учеб. пособие для вузов по направлению ”Прикладная математика и информатика” и ”Информац. технологии” / С. Б. Гашков, Э. А. Применко, М. А. Черепнев, 2010. -297, [1] с.	5

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Портал сообщества IT-специалистов: раздел информационная безопасность, защита данныхhttps://habr.com/ru/hub/infosecurity/
2	Сайт Национального Открытого Университета ”ИНТУИТ”: раздел безопасностьhttps://intuit.ru/studies/courses?service=0&option_id=9&service_path=1

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=13923

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Криптография и защита информации» предусмотрены следующие формы промежуточной аттестации: экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	Выставляется студенту, продемонстрировавшему существенные пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий.
Удовлетворительно	Выставляется студенту, продемонстрировавшему знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой, обладающему необходимыми знаниями, но допустившему неточности в ответах на аттестационном испытании и при выполнении учебных заданий
Хорошо	Выставляется студенту, продемонстрировавшему полное знание учебного материала, успешно выполнившему предусмотренные программой задачи, освоившему основную рекомендованную литературу, показавшему систематический характер знаний по дисциплине и способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности.
Отлично	Выставляется студенту, продемонстрировавшему всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, освоившему основную литературу и ознакомившемуся с дополнительной литературой, рекомендованной рабочей программой дисциплины, усвоившему взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании, изложении и использовании учебного материала.

Особенности допуска

Для допуска к экзамену обучающийся должен иметь положительные оценки по двум коллоквиумам, проводимым в ходе изучения учебной дисциплины, и одному итоговому тесту.

Наличие у обучающегося задолженности (получена оценка «неудовлетворительно») по результатам хотя бы одного коллоквиума, является основанием для принятия решения о его недопуске к экзамену по данной учебной дисциплине.

Текущая аттестация обучающегося по результатам всех коллоквиумов только на «отлично» является основанием для преподавателя о ходатайстве перед заведующим кафедрой об освобождении обучающегося от промежуточной аттестации по дисциплине с выставлением ему оценки «отлично».

Экзамен проводится с целью проверки и определения уровня знаний, полученных обучающимися, умений применять их в решении практических задач, а также полноты и уровня овладения практическими умениями и навыками в объеме требований рабочей программы по дисциплине. На экзамене в зависимости от оценок по отдельным вопросам выставляется итоговая оценка. Обязательным условием положительной оценки являются правильный (или с незначительными ошибками) ответ на практическое задание к вопросу в билете.

Экзамен в устной форме. Билет к экзамену по дисциплине состоит из трех теоретических вопросов. Ответ на каждый из вопросов оценивается отдельно с учетом дополнительных вопросов по теме билета. Обучающемуся предоставить возможность самостоятельно выбрать билет. По истечении отведенного на ответ времени (20 минут или по готовности досрочно) проводится индивидуальная собеседование по вопросам билета. Дополнительно обучающемуся предоставляется ещё 10 минут для выполнения практического задания по теме одного из вопросов в билете. В итоге совокупно оцениваются все ответы обучающегося.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к экзамену

№ п/п	Описание
1	Формальная криптография: Шифр Хилла: принцип зашифровки и расшифровки, схема работы, ключ, свойства матрицы-ключа. Пример атаки на основе открытого текста
2	Формальная криптография: Шифр Вернама. Требования к одноразовому блокноту. Атака на двухразовый блокнот. Принципы Керкгоффса.
3	Научная криптография; Обзор научного вклада в криптографию В.А. Котельникова и К. Шеннона. Классическая схема секретной системы связи. Понятие совершенно секретной системы.
4	Научная криптография: Принципы построения блочных шифров. Сеть Фейстеля: схема работы, доказательство обратимости сети Фейстеля.
5	Шифр ”Магма” ГОСТ Р 34.12–2015 ”Информационная технология. Криптографическая защита информации. Блочные шифры”.: Структура. Раунды. S-блоки. Генерация раундовых ключей. Основные отличия шифра «Магма» от DES и AES.
6	Шифр ”Кузнечик” ГОСТ Р 34.12–2015 ”Информационная технология. Криптографическая защита информации. Блочные шифры”. : Структура. Раундовое преобразование. Подстановка и линейное преобразование. Генерация раундовых ключей.
7	Режимы работы блочных шифров по ГОСТ Р 34.13–2015: Режим простой замены. Режим простой замены с зацеплением. Режим выработки имитовставки.
8	Атака предсказания дополнения (Padding Oracle Attack) на блочные шифры (CBC mode) Цель атаки. Структурная схема режима расшифрования. Действия нарушителя. Меры противодействия атаки.
9	Поточные шифры: Схема зашифровки и расшифровки. Свойства синхронных и самосинхронизирующихся шифров
10	Коды для проверки подлинности и целостности: MDC-код обнаружения модификации. MAC -код установления подлинности сообщения. HMAC -код , основанный на хэшировании. CMAC -код на основе шифровании базового сообщения.
11	Итерированная хэш-функция на примере MD5: Общая схема. Модуль HMD5. Цикл модуля HMD5. Свойства MD5. Пример атаки «радужных таблиц»
12	Атака на хэш-функцию с использованием «радужных таблиц»: цель, создание таблиц, поиск строки с заданным хэш-кодом
13	ГОСТ 34.11-12 ””Информационная технология. Криптографическая защита информации. Функция хэширования” Основные этапы преобразований. Функция сжатия g и функция шифрования E.
14	Хэш-функция Keccak: Внутреннее состояние. Бесключевая псевдослучайная перестановка. Оценка криптостойкости. Масштабируемость Keccak, как универсальный криптопримитив.
15	Шифр RSA: Базовые принципы. Генерация ключей. Протокол Зашифрование и расшифрования. Атака посредника. Доказательство корректности расшифрования.
16	Вероятностный Шифр Голдвассера-Микали (GM). Базовые принципы. Генерация ключей. Зашифрование. Расшифрование. Основные свойства. Вероятностная модель шифра RSA.

17	Протокол Диффи-Хелмана на эллиптических кривых. Атака посредника.
18	ГОСТ Р 34.10─2012 ”Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи” Общие сведения о стандарте. Генерация ключей. Подписание и проверка. Сложность подделки цифровой подписи
19	Распределение открытых кючей. Понятие архитектуры PKI. Путь сертификации. Иерархическая, сетевая и гибридная архитектуры.
20	ФЗ №63 «Об электронной подписи». Основные определения. Виды электронных подписей. Процесс расшифрования и проверки целостности электронного документа.

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический

университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

_____

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

Дисциплина **Криптография и защита информации** ФКТИ

1. Научная криптография: Обзор теория секретной связи Клода Шеннона. Классическая схема секретной системы связи Понятие совершенно секретной системы. Принципы построения блочных шифров.

2. Шифр ГОСТ Р 34.12–2015: Структура. Раундовое преобразование. Подстановка и линейное преобразование. Генерация раундовых ключей.

3. Цифровая подпись ГОСТ Р 34.10─2012. Общие сведения о стандарте. Генерация ключей. Подписание и проверка. Сложность подделки цифровой подписи

УТВЕРЖДАЮ

Заведующий кафедрой Е. Г. Воробьёв

Образцы задач (заданий) для контрольных (проверочных) работ

Примерные вопросы к коллоквиумам:

Коллоквиум по теме ”Симметричная криптография”:

1. Как расшифровать перехваченное сообщение при известном шифре и ключе?

2. Как оценить вычислительную сложность атаки на перехваченное зашифрованное сообщение при известном шифре?

3. Что подается на вход и снимается с выхода заданного симметричного блочного шифра?

4. Какие основные раундовые криптопреобразования используются в заданном симметричном блочном шифре?

5 Как выбрать режим работы симметричного блочного шифра в условиях поставленной задачи сокрытия информации?

6. Как контролировать целостность данных при наличии только заданных криптопреобразований?

Коллоквиум по теме ”Асимметричная криптография”:

1. Какая вычислительно сложная задача лежит в основе заданного криптопреобразования?

2. Как провести компьютерную атаку посредника на заданный криптографический протокол?

3. Как обеспечить контроль целостности сообщений участников в заданной модели криптографического протокола

4. Как защититься от компьютерной атаки в заданной модели гибридной криптосистемы?

5. Как убедится в доверии к сертификату открытого ключа в ИОК задан-

ной архитектуры?

6. Как защититься от активного нарушителя в заданной модели компьютерной атаки на гибридную криптоситему?

Пример вопросов итогового теста:

1. При использовании классических криптографических алгоритмов ключ шифрования и ключ расшифрования совпадают и такие криптосистемы называются:

а) простыми криптосистемами

б) гибридными криптосистемами

в) ассиметричными криптосистемами

г) симметричными криптосистемами

2. Чему равна разрядность ключа алгоритма шифрования Магма (ГОСТ 34.12-15)?

а) 58

б) 64

в) 128

г) 256

3. Какой атаке подвержены классические ассиметричные криптосистемы?

а) атака посредника

б) атака ”встреча по середине”

в) атака предсказания дополнения

г) атака ”грубой силы”

4. Что из перечисленного ниже лучше всего описывает цифровую подпись?

а) это метод переноса собственноручной подписи на электронный документ

б) это метод шифрования конфиденциальной информации

в) это метод, обеспечивающий электронную подпись и шифрование

г) это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения

5. Что из перечисленного ниже лучше всего описывает удостоверяющий центр?

а) организация, которая выпускает закрытые ключи и соответствующие алгоритмы

б) организация, которая проверяет цифровые подписи

в) организация, которая проверяет ключи шифрования

г) организация, которая выпускает сертификаты

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
1	Эволюция криптографии	
2		
3		Отчет по лаб. работе
5	Методы симметричного шифрования	
6		
7		Отчет по лаб. работе
8	Методы контроля целостности и подлинности данных	
9		
10		Отчет по лаб. работе
11	Эволюция криптографии Методы симметричного шифрования Методы контроля целостности и подлинности данных	Коллоквиум
12	Методы ассиметричного шифрования	
13		Отчет по лаб. работе
14	Электронная цифровая подпись	
15		Отчет по лаб. работе
16	Методы ассиметричного шифрования Электронная цифровая подпись Распределение открытых ключей	Коллоквиум
17	Заключение	Тест

6.4 Методика текущего контроля

Основной формой текущего контроля являются индивидуальные контрольные собеседования (ИКС), проводимые в рамка коллоквиумов по разделам курса ”Симметричная криптография” и ”Асимметричная криптография”.

Дополнительными формами текущего контроля являются варианты частного контроля по всем видам учебных занятий, а именно:

- на лекционных занятиях

Текущий контроль включает в себя контроль посещаемости в форме ответа на вопрос по существу прочитанной лекции, например:

1. Укажите шифр, который обладает заданными характеристиками

2. Укажите режим работы шифра, который обладает заданными характеристиками

3. Укажите хэш-функцию, которая обладает заданными характеристиками

4. Укажите алгоритм создания ЭЦП, который обладает заданными характеристиками

5. Укажите архитектуру ИОК, которая обладает заданными характеристиками

Результативность работы студента на лекционных занятиях учитывается при оценивании на экзамене в спорных ситуациях.

- на лабораторных занятиях

В процессе обучения по дисциплине студент обязан выполнить 6 лабораторных работ. Под выполнением работ подразумевается подготовка к работе, проведение экспериментальных исследований, подготовка отчета и его защита на коллоквиуме. Предусматривается проведение коллоквиума на 11 и 16 неделях, на которых осуществляется защита отчетов по лабораторным работам в форме индивидуального контрольного собеседования. Выполнение работ студентами осуществляется индивидуально.

Оформление отчета студентами осуществляется индивидуально в соответствии с принятыми в СПбГЭТУ правилами оформления студенческих работ. Отчет оформляется после выполнения экспериментальных исследований и предъявляется преподавателю на проверку. Особое внимание при проверке уделяется разделу заключение, где должны присутствовать лаконичные выводы по всем этапам проделанной работы. После проверки отчет либо возвращается (при наличии существенных замечаний) на доработку, либо принимается к защите.

Лабораторные работы защищаются студентами на коллоквиумах индивидуально. Каждый студент получает вопрос по теоретической части соответствующего раздела учебного курса, или по процедуре проведения эксперимен-

тальных исследований, или по последующей обработке результатов, после чего ему предоставляется время для подготовки ответа. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов.

Критерии оценивания на коллоквиуме:

Тема зачтена, если студент демонстрирует достаточное знание вопроса, показывает: понимание методики криптоанализа и знание особенностей её применения, понимание и умение объяснять особенности применяемых методов криптозащиты, умение давать качественную и количественную оценку полученных экспериментальных результатов, формулировать выводы по всем разделам выполненной практической работы.

Тема не зачтена, если студент, продемонстрировал существенные пробелы в знаниях основного учебного материала по теме коллоквиума, допустил принципиальные ошибки в выполнении предусмотренных учебно-методическим пособием практических заданий, поверхностно сформулировал выводы в заключении отчета по работе.

Текущий контроль включает в себя выполнение, сдачу в срок отчетов по всем лабораторным работам и их успешную защиту на двух коллоквиумах, а также предъявление не менее 60% правильных ответов на вопросы итогового теста (примерные вопросы теста приведены в критериях оценивания). По результатам этих контрольных испытаний студент получает допуск на экзамен.

- на практических занятиях

В процессе обучения студент выполняет практические задания по изучению алгоритмов работы заданных криптопреобразований и сравнивает полученные результаты с эталонными данными, полученные с помощью приложения CrypTool. Результаты расчетов, выполненные вручную, либо запрограммированных, включаются в отчет по лабораторной работе соответствующей тематики и оцениваются вкупе с другими результатами, представленными в от-

чете.

- при выполнении самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя: стол, кресло, компьютер или ноутбук, с выходом в ”Интернет” проектор, экран, разнонаправленный микрофон, меловая или маркерная доска.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше, СДО ”Moodle”
Практические занятия	Аудитория	Количество посадочных мест в соответствии с контингентом, компьютеры или ноутбуки в соответствии с контингентом, рабочее место преподавателя: стол, кресло, меловая или маркерная доска, компьютер или ноутбук, с выходом в ”Интернет”	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3)CrypTool 1 и 2 3) Среда программирования на C/C++, Java, Python
Лабораторные работы	Лаборатория	Количество посадочных мест в соответствии с контингентом, компьютеры или ноутбуки в соответствии с контингентом, рабочее место преподавателя: стол, кресло, меловая или маркерная доска, компьютер или ноутбук, с выходом в ”Интернет”	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3)CrypTool 1 и 2
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше, 3)CrypTool 1 и 2 3) Среда программирования на C/C++, Java, Python

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА