

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Галунин Сергей Александрович  
Должность: проректор по учебной работе  
Дата подписания: 27.03.2023 14:17:41  
Уникальный программный ключ:  
08ef34338325bdb0ac5a47baa5472ce36cc3fc3b

Приложение к ОПОП  
«Информационные системы и  
технологии в таможенной дея-  
тельности»



**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

**«БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ»**

для подготовки магистров

по направлению

09.04.02 «Информационные системы и технологии»

по программе

**«Информационные системы и технологии в таможенной деятельности»**

Санкт-Петербург

2022

## **ЛИСТ СОГЛАСОВАНИЯ**

Разработчики:

профессор, д.т.н., профессор Молдовян Н.А.

Рабочая программа рассмотрена и одобрена на заседании кафедры ИС  
21.02.2022, протокол № 2

Рабочая программа рассмотрена и одобрена учебно-методической комиссией  
ФКТИ, 24.02.2022, протокол № 2

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

## **1 СТРУКТУРА ДИСЦИПЛИНЫ**

Обеспечивающий факультет    ФКТИ

Обеспечивающая кафедра    ИС

Общая трудоемкость (ЗЕТ)    6

Курс    1

Семестр    1

### **Виды занятий**

Лекции (академ. часов)    34

Практические занятия (академ. часов)    51

Иная контактная работа (академ. часов)    1

Все контактные часы (академ. часов)    86

Самостоятельная работа, включая часы на контроль  
(академ. часов)    130

Всего (академ. часов)    216

### **Вид промежуточной аттестации**

Дифф. зачет (курс)    1

## **2 АННОТАЦИЯ ДИСЦИПЛИНЫ**

### **«БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ»**

Целью дисциплины является изучение вопросов теории проектирования информационных технологий и систем в безопасном исполнении, включающем механизмы обеспечения информационной безопасности как инструмента исследования и проектирования безопасных информационных технологий и систем (БИТС). Рассматриваются основы теории компьютерной безопасности, защиты информации и их приложения в проектировании современных БИТС. Рассматриваются как устоявшиеся теоретические вопросы проектирования защищенных систем, так и новые аспекты, мало отраженные в отечественной и переводной литературе, включая электронные носители. Обсуждаются аспекты метода защиты информации на технологическом уровне и применяемые алгоритмы в рамках этого метода. Показано место аппарата теории чисел и его применение для реализации механизмов обеспечения информационной безопасности, встраиваемых в информационные системы на этапе их проектирования. Отражается взаимное влияние развития информационных технологий и современной криптографии, основные методы, алгоритмы, протоколы и роль последней как источника новых информационных технологий. Полученные знания позволяют заложить в проектируемые информационные системы расширенную функциональность в плане заложенных внутренних функций по обеспечению информационной безопасности в различных областях применения информационных систем.

#### **SUBJECT SUMMARY**

#### **«SECURE INFORMATION TECHNOLOGIES AND SYSTEMS»**

The purpose of the discipline is to study the issues of the theory of designing information technologies and systems in a safe execution, including mechanisms for

providing information security as a tool for research and design of secure information technologies and systems (SITS). The basics of the theory of computer security, information security and their applications in the design of modern SITS are considered. We consider both the well-established theoretical issues of the design of protected systems, and new aspects, which are little reflected in the domestic and translated literature, including electronic media. The aspects of the method of protecting information at the technological level and the algorithms used in this method are discussed. The place of the apparatus of number theory and its application for the implementation of information security mechanisms embedded in information systems at the design stage is shown. It reflects the mutual influence of the development of information technologies and modern cryptography, the main methods, algorithms, protocols and the role of the latter as a source of new information technologies. The knowledge gained will allow the projected information systems to provide enhanced functionality in terms of internal functions to ensure information security in various fields of information systems.

### **3 ОБЩИЕ ПОЛОЖЕНИЯ**

#### **3.1 Цели и задачи дисциплины**

1. Целью освоения дисциплины является приобретение знаний и формирование навыков создания информационных технологий и систем с встроенными механизмами обеспечения информационной безопасности.
2. Задачами освоения дисциплины являются:
  - освоение принципов и способов реализации механизмов защиты информационных технологий и систем;
  - получение навыков конструирования защищенных информационных технологий и систем;
  - освоение процесса проектирования информационных технологий и систем в защищенном исполнении.
3. Получение знаний элементов математических основ алгоритмического обеспечения защиты информации.  
Усвоение основ современных криптографических алгоритмов и протоколов для обеспечения информационной безопасности.
4. Умения применять криптографические алгоритмы и протоколы для решения задач обеспечения аутентификации и защиты информации в информационных технологиях и системах.
5. Получение навыков практического использования криптографических механизмов обеспечения защищенности информации в информационных технологиях и системах.

#### **3.2 Место дисциплины в структуре ОПОП**

Дисциплина изучается на основе знаний, полученных при освоении программы бакалавриата или специалитета.

и обеспечивает изучение последующих дисциплин:

1. «Технологии распределенной обработки данных»
2. «Современные методы и средства проектирования информационных систем»

### **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:

<b>Код компетенции/ индикатора компетенции</b>	<b>Наименование компетенции/индикатора компетенции</b>
ПК-1	Способен разрабатывать и исследовать модели объектов профессиональной деятельности, предлагать и адаптировать методики, определять качество проводимых исследований, составлять отчеты о проделанной работе, обзоры, готовить публикации
ПК-1.1	<i>Знает основные методы разработки и исследования объектов профессиональной деятельности; основы управления качеством; основные стандарты по оформлению результатов исследований и технической документации</i>
ПК-3	Способен вести сдачу проекта, собирать и анализировать мнения и замечания заказчика по выполнению проекта и предлагать соответствующие решения
ПК-3.3	<i>Владеет методами сбора, анализа и представления необходимой информации</i>

## **4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ**

### **4.1 Содержание разделов дисциплины**

#### **4.1.1 Наименование тем и часы на все виды нагрузки**

<b>№ п/п</b>	<b>Наименование темы дисциплины</b>	<b>Лек, ач</b>	<b>Пр, ач</b>	<b>ИКР, ач</b>	<b>СР, ач</b>
1	Введение.	2	0	0	0
2	Механизмы обеспечения конфиденциальности информации	9	12	0	32
3	Способы и механизмы защиты от отказов от электронных сообщений и документов.	7	15	0	33
4	Комплексный подход к проектированию защищенных информационных технологий и систем.	9	12	1	33
5	Решении задач обеспечения анонимности и неотслеживаемости пользователей в распределенных информационных системах специальных типов.	7	12	0	32
Итого, ач		34	51	1	130
Из них ач на контроль		0	0	0	0
Общая трудоемкость освоения, ач/зе		216/6			

#### **4.1.2 Содержание**

<b>№ п/п</b>	<b>Наименование темы дисциплины</b>	<b>Содержание</b>
1	Введение.	Основные термины и определения. Концепции проектирования защищенных информационных технологий и систем.
2	Механизмы обеспечения конфиденциальности информации	Понятие криптографического преобразования.. Криптографическое преобразование по разделяемому секретному ключу. Криптографическое преобразование по открытому ключу. Гибридные шифры. Технология прозрачного шифрования.
3	Способы и механизмы защиты от отказов от электронных сообщений и документов.	Понятие электронной цифровой подписи (ЭЦП). Системы ЭЦП с открытыми ключами. Базовые алгоритмы реализации механизмов ЭЦП в защищенных информационных системах. Потенциальные атаки на схемы ЭЦП и защита от них.

<b>№ п/п</b>	<b>Наименование темы дисциплины</b>	<b>Содержание</b>
4	Комплексный подход к проектированию защищенных информационных технологий и систем.	Конфиденциальность, целостность и доступность информации и сервисов информационных систем. Использование среды общего доступа для реализации защищенных каналов проектируемых систем. Распределенные средства обеспечения информационной защищенности информационных технологий и систем.
5	Решении задач обеспечения анонимности и неотслеживаемости пользователей в распределенных информационных системах специальных типов.	Задача анонимности и неотслеживаемости в информационных технологиях и системах специальных типов. Протоколы слепой цифровой подписи. Понятие слепой подписи. Технология электронных денег. Системы тайного электронного голосования. Виды протоколов слепой подписи.

## **4.2 Перечень лабораторных работ**

Лабораторные работы не предусмотрены.

## **4.3 Перечень практических занятий**

<b>Наименование практических занятий</b>	<b>Количество ауд. часов</b>
1. Алгоритмы аутентификации пользователей.	12
2. Алгоритмы и протоколы ЭЦП.	15
3. Алгоритмы открытого шифрования.	12
4. Протоколы слепой ЭЦП.	12
<b>Итого</b>	<b>51</b>

## **4.4 Курсовое проектирование**

Курсовая работа (проект) не предусмотрены.

## **4.5 Реферат**

**Исходные данные и требования:** Выполняется реферат по одной из предложенных тем.

Студент выбирает механизм и дает по нему теоретическую справку с указанием методик работы, плюсов, минусов и дополнительных сведений о выбранном механизме. Проводит поиск и анализ научных публикаций и готовит

презентацию информации по заданной теме, на основе собранных данных выполняет расчеты, составляет схемы и модели.

Отчёт оформляется по шаблону, представленном на сайте СПбГЭТУ "ЛЭТИ".

Количество страниц -от 5 до 15.

Количество использованных источников -от 2 до 5.

Файл с отчетом должен иметь название в виде: РЕФ+nnnn+Фамилия+Имя , где nnnn

Отчет сдается преподавателю в электронном виде.

Темы:

№ п/п	Название темы	Перевод темы
1	Механизмы обеспечения конфиденциальности информации в системах беспилотного транспорта	
2	Постквантовые механизмы цифровой подписи	
3	Специальные режимы блочного шифрования	

#### **4.6 Индивидуальное домашнее задание**

Титульный лист отчета должен содержать название ВУЗа, номер группы, фамилию, имя и отчество (при наличии) студента полностью, название работы, дату готовности отчета.

Шрифт Times new Roman 14пт. с межстрочным интервалом 1.5

Файл с отчетом должен иметь название в виде: УБИ+nnnn+Фамилия+Имя , где nnnn номер группы студента.

Готовый отчет сдаётся преподавателю в электронном виде

#### **Задание 1. Исследование угроз безопасности информации**

После названия работы необходимо уточнить перечень из трех исследуемых угроз (указать их идентификаторы). Для каждого студента перечень будет уникален. Исследуемые угрозы необходимо выбирать из списка угроз, приведенного на сайте ФСТЭК России (<https://bdu.fstec.ru/threat>). Номера исследуемых

угроз для каждого студента определяются следующим образом. Для первой группы: Нс+5, Нс + 55, Нс + 115, где Нс - номер студента по списку. Для второй группы: Нс+35, Нс +92, Нс + 155. Например, для студента под 9-м номером из списка первой группы в отчете название ПЗ будет выглядеть так: «Угрозы безопасности информации. УБИ.014, УБИ.064, УБИ.124».

Отчет должен содержать идентификатор, наименование угрозы, описание угрозы, источник угрозы (характеристику и потенциал нарушителя), объект воздействия, возможные последствия реализации угрозы (нарушение конфиденциальности, целостности, доступности информации).

Для каждой угрозы указать меры по ее нейтрализации.

### **Задание 2. Средства защиты от несанкционированного доступа**

После установки СЗИ НСД на ЭВМ для четкой идентификации студента, выполняющего задание, сформировать с ФИО студента двух пользователей с логинами а) adm\_Фамилия\_Имя и б) user\_Фамилия\_Имя. Прописать соответственно полномочия администратора и обычного пользователя.

Отчет необходимо сопровождать скриншотами все операции по настройке и эксперименты с СЗИ НСД. В скриншотах должны четко читаться фамилия исполнителя.

После освоения документации по СЗИ Аура, провести тестовые испытания выбранного студентом самостоятельно набора функций (не менее 5) СЗИ НСД и описать результаты

#### **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, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

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.

Самостоятельное изучение студентами теоретических основ дисциплины обеспечено необходимыми учебно-методическими материалами (учебники, учебные пособия, конспект лекций и т.п.), выполненными в печатном или электронном виде.

Изучение студентами дисциплины сопровождается проведением регулярных консультаций преподавателей, обеспечивающих практические занятия по дисциплине, за счет бюджета времени, отводимого на консультации (внеаудиторные занятия, относящиеся к разделу «Самостоятельные часы для изучения

дисциплины»).

Текущая СРС	Примерная трудоемкость, ач
Работа с лекционным материалом, с учебной литературой	10
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	10
Самостоятельное изучение разделов дисциплины	10
Выполнение домашних заданий, домашних контрольных работ	25
Подготовка к лабораторным работам, к практическим и семинарским занятиям	22
Подготовка к контрольным работам, коллоквиумам	22
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	20
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	11
<b>ИТОГО СРС</b>	<b>130</b>

## **5 Учебно-методическое обеспечение дисциплины**

### **5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины**

<b>№ п/п</b>	<b>Название, библиографическое описание</b>	<b>К-во экз. в библ.</b>
<b>Основная литература</b>		
1	Дернова, Евгения Сергеевна. Криптографические протоколы [Текст] : учеб. пособие / Е.С. Дернова, Д.Н. Молдовян, Н.А. Молдовян, 2010. -99 с	неогр.
2	Молдовян, Александр Андреевич. Практичные протоколы цифровых мультиподписей [Электронный ресурс] : электрон. учеб. пособие / А. А. Молдовян, А. Н. Березин, Д. Н. Молдовян, 2018. -1 эл. опт. диск (CD-ROM)	неогр.
<b>Дополнительная литература</b>		
1	Дубенецкий, Владислав Алексеевич. Проектирование корпоративных информационных систем [Текст] : [монография] / В. А. Дубенецкий, Б. Я. Советов, В. В. Цехановский, 2013. -189, [1] с.	10
2	Молдовян, Дмитрий Николаевич. Расширение функциональности стандартов цифровой подписи [Электронный ресурс] : электрон. учеб. пособие / Д. Н. Молдовян, А. Н. Березин, Н. А. Молдовян, 2018. -1 эл. опт. диск (CD-ROM)	неогр.

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

<b>№ п/п</b>	<b>Электронный адрес</b>
1	Стеганографические и криптографические методы защиты ин-формации: учебное пособие. Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. [Электронный ресурс] : учеб. пособие — Элек-трон. дан. — Режим доступа: <a href="http://e.lanbook.com/book/90963">http://e.lanbook.com/book/90963</a>
2	Криптографические методы защиты информации <a href="http://e.lanbook.com/book/92914">http://e.lanbook.com/book/92914</a>

### **5.3 Адрес сайта курса**

Адрес сайта курса: <https://vec.etu.ru/moodle/course/view.php?id=11261>

## **6 Критерии оценивания и оценочные материалы**

### **6.1 Критерии оценивания**

Для дисциплины «Безопасные информационные технологии и системы» предусмотрены следующие формы промежуточной аттестации: зачет с оценкой.

#### **Зачет с оценкой**

<b>Оценка</b>	<b>Описание</b>
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач

## **Особенности допуска**

Допуском к зачету является выполнение и защита ИДЗ и реферата.

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

### **Вопросы к дифф.зачету**

<b>№ п/п</b>	<b>Описание</b>
1	Понятие конфиденциальности.
2	Понятие цифровой подписи
3	Основные типы криптографических алгоритмов
4	Проблема аутентификации открытых ключей
5	Постквантовая криптография
6	Программные, аппаратные и универсальные шифры
7	Зависимость стойкости криптографических алгоритмов и протоколов от уровня развития вычислительных технологий
8	Концепции проектирования защищенных информационных технологий и систем
9	Криптографическое преобразование по разделяемому секретному ключу. Криптографическое преобразование по открытому ключу
10	Гибридные шифры. Технология прозрачного шифрования
11	Электронная цифровая подпись. Алгоритмы реализации механизмов ЭЦП
12	Распределенные средства обеспечения информационной защищенности информационных технологий и систем
13	Понятие цифровой подписи. Алгоритм ЭЦП Эль-Гамаля
14	Режимы использования блочных шифров

### **Форма билета**

Министерство науки и высшего образования Российской Федерации  
ФГАОУ ВО «Санкт-Петербургский государственный электротехнический  
университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

---

### **БИЛЕТ № 1**

**Дисциплина Безопасные информационные системы и технологии ФК-ТИ**

1. Раскрыть понятие цифровой подписи. Алгоритм ЭЦП Эль-Гамаля.
2. Режимы использования блочных шифров.

**УТВЕРЖДАЮ**

Заведующий кафедрой

В.В. Цехановский

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**

<b>Неделя</b>	<b>Темы занятий</b>	<b>Вид контроля</b>
1	Механизмы обеспечения конфиденциальности информации Способы и механизмы защиты от отказов от электронных сообщений и документов.	
2		
3		
4		
5		Реферат
6	Способы и механизмы защиты от отказов от электронных сообщений и документов.	
7		
8		ИДЗ / ИДРГЗ / ИДРЗ
9	Решение задач обеспечения анонимности и неотслеживаемости пользователей в распределенных информационных системах специальных типов.	
10		
11		ИДЗ / ИДРГЗ / ИДРЗ

### **6.4 Методика текущего контроля**

#### **На лекционных занятиях**

Текущий контроль включает в себя контроль посещаемости (не менее **80** % занятий), по результатам которого студент получает допуск на дифф. зачет.

#### **На практических (семинарских) занятиях**

Текущий контроль включает в себя контроль посещаемости (не менее **80** % занятий), а также выполнение ИДЗ, по результатам которых студент получает допуск на дифф. зачет.

ИДЗ и Реферат оцениваются по системе "зачтено-незачтено":

"зачтено" - ИДЗ/реферат считается выполненным, если студент верно сформулировал все необходимые понятия и положения, а также дал полные выводы по указанным в требованиях пунктам;

"не зачтено" выставляется, если отсутствуют ответ на задание на вопросы или содержание ответа не совпадает с поставленным заданием, в ответе имеются существенные ошибки.

Задания защищаются студентами индивидуально. Каждый студент полу-

чает вопрос по теме работы. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов. В случае если студент демонстрирует достаточное знание вопроса, работа считается защищенной.

В ходе проведения семинарских и практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.

### **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**

<b>Тип занятий</b>	<b>Тип помещения</b>	<b>Требования к помещению</b>	<b>Требования к программному обеспечению</b>
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, требуется доска, компьютер и проектор не обязательны	Программа для демонстрации компьютерных презентаций
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя. 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
Самостоятельная работа	Помещение для самостоятельной работы	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

## **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**

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