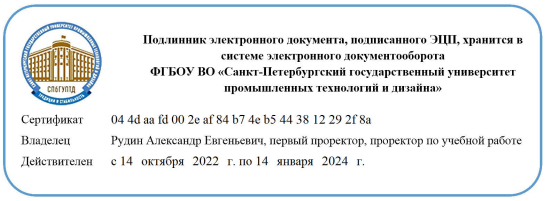
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)


Подлинник электронного документа, подписанного ЭЦП, хранится в системе электронного документооборота
ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна»
Сертификат 04 4d aa fd 00 2e af 84 b7 4e b5 44 38 12 29 2f 8a
Владелец Рудин Александр Евгеньевич, первый проректор, проректор по учебной работе
Действителен с 14 октября 2022 г. по 14 января 2024 г.

УТВЕРЖДАЮ
Первый проректор, проректор по УР
_____А.Е. Рудин
«31»____10____ 2023 года

Рабочая программа дисциплины

Б1.О.09 Криптографические средства защиты информации

Учебный план: 2024-2025 10.04.01 ИИТА ПСЗИнП ОО №2-1-159.plx

Кафедра: 20 Интеллектуальных систем и защиты информации

Направление подготовки: (специальность) 10.04.01 Информационная безопасность

Профиль подготовки: (специализация) Проектирование систем защиты информации на предприятии

Уровень образования: магистратура

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся			Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия	Лаб. занятия				
2	УП	17	17	34	41,5	34,5	4	Экзамен
	РПД	17	17	34	41,5	34,5	4	
Итого	УП	17	17	34	41,5	34,5	4	
	РПД	17	17	34	41,5	34,5	4	

Санкт-Петербург
2023

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утверждённым приказом Минобрнауки России от 26.11.2020 г. № 1455

Составитель (и):

кандидат технических наук, Доцент	_____	Васильева И.Н.
От кафедры составителя: Заведующий кафедрой интеллектуальных систем и защиты информации	_____	Макаров Авинир Геннадьевич
От выпускающей кафедры: Заведующий кафедрой	_____	Макаров Авинир Геннадьевич

Методический отдел:

_____

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: сформировать компетенции обучающихся в области криптографической защиты информации, обеспечить студентам знания в области теоретической криптографии и ее прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности.

1.2 Задачи дисциплины:

- раскрыть основные математические методы криптографии.
- сформировать подходы к выполнению самостоятельных исследований студентами в области криптографических методов и средств защиты информации

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Организационно-правовые механизмы обеспечения информационной безопасности

Экономика защиты информации

Специальные главы математики

Защита электронного документооборота

Технологии обеспечения информационной безопасности

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
Знать: криптографические протоколы, методы атаки на криптографические шифры, области их применения при организации систем обеспечения безопасности
Уметь: использовать основные математические методы, используемые в анализе типовых криптографических алгоритмов
Владеть: навыками применения инструментальных программных средств для анализа эффективности криптографических средств защиты информации

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа			СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)	Лаб. (часы)			
Раздел 1. Основные классы шифров и их свойства	2						О
Тема 1. Введение в криптографию		2			2,5	ИЛ	
Тема 2. Модели шифров и открытых сообщений. Практическое занятие: Модели шифров и открытых текстов Лабораторная работа №1: Алгебраические модели шифров. Лабораторная работа №2: Вероятностные модели шифров.		2	3	10	7		
Тема 3. Криптографическая стойкость шифров. Практическое занятие: Имитостойкость и помехоустойчивость шифров		2	2		4		

Раздел 2. Принципы построения криптографических алгоритмов							
Тема 4. Принципы построения симметричных криптографических алгоритмов. Практическое занятие: Виды симметричных шифров. Особенности программной и аппаратной реализации. Практическое занятие: Современные блочные криптоалгоритмы.Принципы построения поточных шифров Лабораторная работа №3: Принципы построения блочных шифров. Сеть Файстеля		1	4	4	8		О
Тема 5. Принципы построения асимметричных криптографических алгоритмов Лабораторная работ №4: Математические основы асимметричной криптографии		2		2	4		
Тема 6. Методы анализа криптографических алгоритмов Лабораторная работа №5 Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уравнений шифрования, бесключевые методы.		1		2	1	АС	
Раздел 3. Построение сетей с засекреченной связью							О
Тема 7. Организация распределения ключей в сетях засекреченной связи Практическое занятие: Протоколы распределения ключей Лабораторная работа №6: Передача ключей с использованием симметричного шифрования Лабораторная работа №7: Передача ключей с использованием асимметричного шифрования		2	2	6	4		
Тема 8. Организация сетей засекреченной связи Практическое занятие: Методы применения шифрования данных в локальных вычислительных сетях Лабораторная работа №8: Особенности использования вычислительной техники в криптографии		1	2	4	3		
Тема 9. Криптографические хэш-функции Лабораторная работа №9: Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП) Практическое занятие: Ключевые и бесключевые функции хэширования		2	2	4	4	ИЛ	

Тема 10. Электронная подпись Практическое занятие: Алгоритмы электронной подписи Фиата, Фейге, Шамира, Эль-Гамаля Лабораторная работа №10: Ассиметричные алгоритмы электронной подписи на основе RSA		2	2	2	4		
Итого в семестре (на курсе для ЗАО)		17	17	34	41,5		
Консультации и промежуточная аттестация (Экзамен)		10			24,5		
Всего контактная работа и СР по дисциплине		78			66		

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ОПК-1	Перечисляет методы атаки на криптографические шифры, области их применения при организации систем обеспечения безопасности Анализирует типовые криптографические алгоритмы, используя основные математические методы. Оценивает эффективность криптографических средств защиты информации с использованием современных программно-аппаратных средств	вопросы для устного собеседования и практико - ориентированные задания

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявившему творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание.	не предусмотрена

4 (хорошо)	Выставляется обучающемуся, обнаружившему полное знание материала изученной дисциплины, успешно выполняющему предусмотренные задания, усвоившему основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнивший практическое задание, но допустивший при этом непринципиальные ошибки.	не предусмотрена
3 (удовлетворительно)	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившему другие практические задания из того же раздела дисциплины..	не предусмотрена
2 (неудовлетворительно)	Выставляется обучающемуся, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка неудовлетворительно ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине.	не предусмотрена

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 2	
1	Краткая история развития криптографических методов.
2	Основные понятия криптографии.
3	Характер криптографической деятельности.
4	Модели шифров и открытых текстов.
5	Алгебраические модели шифров.
6	Вероятностные модели шифров.
7	Математические модели открытых сообщений.

8	Криптографическая стойкость шифров.
9	Теоретико-информационный подход к оценке криптостойкости шифров.
10	Практическая стойкость шифров.
11	Имитостойкость и помехоустойчивость шифров.
12	Практические вопросы повышения надежности.
13	Виды симметричных шифров. Особенности программной и аппаратной реализации.
14	Принципы построения блочных шифров.
15	Базовые шифрующие преобразования.
16	Сеть Файстеля.
17	Современные блочные криптоалгоритмы.
18	Принципы построения поточных шифров.
19	Синхронизация поточных шифрсистем.
20	Режимы использования шифров.
21	Математические основы асимметричной криптографии.
22	Примеры современных асимметричных шифров.
23	Блочно-итерационные и шаговые функции.
24	Ключевые функции хэширования.
25	Бесключевые функции хэширования.
26	Схемы использования ключевых и бесключевых функций.
27	Задачи и особенности электронной подписи.
28	Ассиметричные алгоритмы электронной подписи на основе RSA.
29	Алгоритм электронной подписи Фиата – Фейге – Шамира.
30	Алгоритм электронной подписи Эль-Гамаля.
31	Симметричные (одноразовые) цифровые подписи.
32	Протоколы распределения ключей.
33	Передача ключей с использованием симметричного шифрования.
34	Передача ключей с использованием асимметричного шифрования.
35	Открытое распределение ключей.
36	Предварительное распределение ключей.
37	Схемы разделения секрета.
38	Способы распределения ключей для конференц-связи.
39	Особенности использования вычислительной техники в криптографии.
40	Методы применения шифрования данных в локальных вычислительных сетях.
41	Обеспечение секретности данных при долгосрочном хранении.
42	Задачи обеспечения секретности и целостности данных и ключей при краткосрочном хранении.
43	Обеспечение секретности ключей при долгосрочном хранении.
44	Защита от атак с использованием побочных каналов.
45	Основные методы криптоанализа.
46	Перспективные направления в криптографии.

5.2.2 Типовые тестовые задания

не предусмотрены

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Зашифровать/ расшифровать текст с помощью шифра Виженера
2. Вычислить произведение двух элементов над полем Галуа FG(2^8)
3. Вычислить сумму двух элементов над полем Галуа FG(2^8)
4. Зашифровать/ расшифровать значение с помощью алгоритма RSA
5. Сформировать общий ключ с помощью алгоритма Диффи-Хеллмана
6. Сформировать шаги протокола Шамира
7. Вычислить число, обратное заданному по модулю
8. Вычислить значение степени числа по модулю
9. Вычислить значение рациональной дроби по модулю
10. Проверить корректность цифровой подписи RSA
11. Проверить корректность цифровой подписи Эль-Гамаля
12. Определить последовательность операций для вычисления кратной точки эллиптической кривой
13. Определить сингулярность эллиптической кривой над конечным полем простой характеристики >3
14. Зашифровать съемный носитель информации с помощью BitLocker ToGo
15. Зашифровать отдельные файлы/ папки файловой системы NTFS
16. Определить корневой центр сертификации веб-сайта

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная	+	Письменная		Компьютерное тестирование		Иная	

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Обучающийся тянет билет, в котором два теоретических вопроса и практическое задание. После этого готовится в течении как минимум 20 минут с использованием конспекта лекций. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. После ответа на теоретический вопрос обучающийся приступает к решению практического задания, гарантированно на решение задачи времени дается 30 минут, решение, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Басалова, Г. В.	Основы криптографии	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	http://www.iprbookshop.ru/89455.html
Лапонина, О. Р., Сухомлина, В. А.	Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	http://www.iprbookshop.ru/97571.html
Косолапов, Ю. В.	Криптографические протоколы на основе линейных кодов	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета	2020	http://www.iprbookshop.ru/100176.html
6.1.2 Дополнительная учебная литература				
Жиль, Земор, Шуликовская, В. В.	Курс криптографии	Москва, Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований	2019	http://www.iprbookshop.ru/91941.html
Петров, А. А.	Компьютерная безопасность. Криптографические методы защиты	Саратов: Профобразование	2019	http://www.iprbookshop.ru/87998.html
Кикин А. Б.	Информационная безопасность. Основы криптографии	СПб.: СПбГУПТД	2019	http://publish.sutd.ru/tp_ext_inf_publish.php?id=201932

6.2 Перечень профессиональных баз данных и информационно-справочных систем

www.gpntb.ru/ Государственная публичная научно-техническая библиотека.
www.nlr.ru/ Российская национальная библиотека.
www.nns.ru/ Национальная электронная библиотека.
www.intuit.ru/ Образовательный сайт
www.osp.ru/ Журнал «Открытые системы»

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional
Microsoft Windows
Python

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

Аудитория	Оснащение
Компьютерный класс	Специализированная мебель; компьютерная техника; наборы демонстрационного оборудования, служащие для представления учебной информации (стационарное мультимедийное оборудование) - мультимедийная проекционная система (мультимедиа проектор и экран). Рабочие станции, программно-аппаратные комплексы ЗИ; локальная вычислительная сеть с выходом в Интернет