МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по образовательной деятельности
_____ В.Г. Шубаева
«24» мая 2023 г.

Методы и средства криптографической защиты информации

Рабочая программа дисциплины

Направление подготовки/ *Специальность*	*10.03.01 Информационная безопасность*
Направленность (профиль) программы/ *Специализация*	*Безопасность компьютерных систем (в экономике и управлении)*
Уровень высшего образования	*Бакалавриат*
Форма обучения	*очная*
Год набора	*2023*

Составитель*(и)*:

к.физмат.н, Васильева Ирина Николаевна

Часов по учебному плану	144	**Виды контроля в семестрах:**
в том числе:		
контактная работа	98	Экзамен: семестр 6 Курсовая работа: семестр 6
самостоятельная работа	10	
практическая подготовка	0	
часов на контроль	36	

Распределение часов дисциплины:

Семестр:	6
Вид занятий	Часы
Лекционные занятия	38
Практические занятия	60
Лабораторные работы	0
Итого аудиторных часов	**98**
Самостоятельная работа	10
Часы на контроль	36
Итого академических часов	**144**
Общая трудоемкость в зачетных единицах	**4**

Санкт-Петербург
2023

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 3

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 3

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ* 4

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 5

5.1 Рекомендуемая литература 6

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства 6

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД) 6

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 7

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 9

8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 10

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ 11

1.1 Контрольные вопросы и задания к промежуточной аттестации 11

1.2 Темы письменных работ 12

1.3 Контрольные точки 13

1.4 Другие объекты оценивания 13

1.5 Самостоятельная работа обучающегося 13

1.6 Шкала оценивания результата 13

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель:	Формирование представлений о современных алгоритмах, методах и средствах криптографической защиты информации, используемых для решения проблем компьютерной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.О Методы и средства криптографической защиты информации относится к обязательной части Блока 1.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции выпускника	**Код и наименование индикатора достижения компетенций**	**Планируемые результаты обучения по дисциплине**
ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.03 - Способен осуществлять выбор и использование методов и средств криптографической защиты информации в компьютерных системах и сетях	Знать: криптографические алгоритмы блочного шифрования, режимы работы блочных шифров, криптографические алгоритмы с открытым ключом, алгоритмы цифровой подписи, функции хэширования, основные принципы и методы криптоанализа. Уметь: производить выбор и настройку параметров криптографических алгоритмов и режимов их работы для решения практических задач криптографической защиты информации в компьютерных системах и сетях. Владеть: навыками применения криптографических методов и средств для обеспечения конфиденциальности и целостности защищаемой информации.
ОПК-12 - Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.01 - Способен анализировать исходные данные для проектирования средств обеспечения защиты информации, формировать требования безопасности и производить выбор методов и средств криптографической защиты информации	Знать: принципы построения и теоретические основы криптографической защиты информации; современные российские и зарубежные криптографические стандарты. Уметь: определять необходимые функции и формулировать требования безопасности к подсистеме криптографической защиты информации. Владеть: навыками анализа, сравнения и обоснования выбора методов и средств криптографической защиты информации при проектировании системы защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*

Номер и наименование тем и/или разделов/тем	Содержание дисциплины	Объем дисциплины (академические часы)			
		Контактная работа			СРО
		ЗЛТ	ПЗ	ЛР	
Раздел I. Криптосистемы с секретным ключом.					
Тема 1. Основные понятия криптографии. Классические шифры.	Основные понятия и определения криптографии. История криптографии. Классические шифры. Шифры замены и перестановки. Классические шифры перестановки. Блочные и потоковые шифры. Методы криптоанализа классических шифров перестановки. Классические шифры замены. Шифр Виженера. Методы криптоанализа классических шифров замены. Шифры гаммирования, шифр Вернама (одноразовый шифровальный блокнот). Механизация криптографии, шифр Энигмы. Теория К.Шеннона. Формальные модели классических шифров. Расстояние единственности шифра. Идеальные криптосистемы. Теоретическая стойкость шифров. Совершенные криптосистемы.	4	8		
Тема 2. Симметричные блочные шифры.	Композиционные шифры. Методы синтеза симметричных блочных шифров. Сети Фейстеля. Алгоритм шифрования DES. Алгоритм «Магма» ГОСТ 34.12-2018. Подстановочно-перестановочные сети. Шифр AES. Алгоритм «Кузнечик» ГОСТ 34.12-2018. Основные режимы работы блочных шифров ГОСТ 34.13-2018. Алгоритмы дополнения блока. Специальные режимы работы блочных шифров.	8	8		2
Тема 3. Криптоанализ блочных шифров.	Практическая стойкость криптоалгоритмов. Классификация атак на алгоритмы шифрования. Методы криптоанализа блочных шифров: полный перебор, метод встречи посередине, линейный, дифференциальный криптоанализ, слайдовые атаки, атаки на связанных ключах. Атаки, использующие утечки по побочным каналам.	2	4		2
Тема 4. Потоковые системы шифрования.	Потоковые криптосистемы. Синхронные и асинхронные потоковые шифры. Генераторы ключевой гаммы на регистрах сдвига с линейной обратной связью LSFR. Нелинейные потоковые шифры. Атаки на потоковые криптосистемы. Алгоритм Берлекэмпа-Месси. Примеры потоковых криптосистем, ChaCha20.	4	6		2
Раздел II. Криптосистемы с открытым ключом.					
Тема 5. Математические основы криптографии с открытым ключом.	Основные концепции криптографии с открытым ключом. Сложные вычислительные задачи. Пример криптосистемы с открытым ключом - система Диффи-Хеллмана. Математические основы асимметричной криптографии. Теорема Ферма, теорема Эйлера, Китайская теорема об остатках. Вычислительные алгоритмы криптографии с открытым ключом. Расширенный алгоритм	4	4		

	Евклида, алгоритм быстрого возведения в степень по модулю. Алгоритмы проверки чисел на простоту. Генерация простых чисел.				
Тема 6. Асимметричные шифры.	Шифр Шамира. Шифр Эль-Гамаля. Атаки на криптосистемы, основанные на сложности задачи дискретного логарифмирования. Шифр RSA. Атаки на алгоритм RSA, требования к выбору параметров шифра. Семантическая стойкость. Вероятностное шифрование (система Блюма-Гольдвассер).	2	6		2
Тема 7. Функции хэширования и системы цифровой подписи.	Бесключевые функции хэширования. Функция хэширования ГОСТ 34.11-2018. Конструкция HMAC. Использование хэш-функций для выработки псевдослучайных последовательностей. Электронная цифровая подпись. Детерминированная цифровая подпись RSA. Рандомизированные цифровые подписи: схема Рабина, схема Эль-Гамаля, схема Шнорра. Создание скрытого канала в электронной подписи.	4	6		2
Тема 8. Цифровые сертификаты.	Проблема компрометации открытого ключа при передаче. Цифровые сертификаты. Модели доверия на основе цепей сертификации. Инфраструктура открытых ключей PKI.	2	4		
Тема 9. Криптография на эллиптических кривых.	Основы теории эллиптических кривых. Использование эллиптических кривых в криптографии. Шифрование и криптосистема Диффи-Хеллмана на эллиптических кривых. Цифровая подпись на эллиптических кривых. Цифровая подпись ГОСТ 34.10-2018. Выбор параметров цифровой подписи.	4	8		
Раздел III. Вопросы практической криптографии.					
Тема 10. Реализация криптографических средств защиты информации.	Программные и аппаратные шифраторы. Реализация шифрования информации при ее хранении. Примеры программных реализаций средств криптографической защиты информации: криптографический прикладной интерфейс в ОС Windows, шифрующая файловая система EFS, полнодисковое шифрование BitLocker. Полнодисковое шифрование LUKS.	2	6		
Тема 11. - Криптография в эпоху квантовых вычислений.	Основные концепции квантовой криптографии. Протоколы квантовой передачи ключа и вопросы их практической реализации. Проблема потери стойкости традиционных криптосистем в эпоху квантовых вычислений. Подходы к построению систем постквантовой криптографии.	2			
Контроль:					**36**
Всего по дисциплине:		**38**	**60**	**0**	**10**

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Рекомендуемая литература

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	Электронные ресурсы
1. Васильева И. Н. Криптографические методы защиты информации : Учебник и практикум - Москва : Юрайт, 2019.	https://www.urait.ru/bcode/433610
2. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации : Учебник / 2-е изд. - Москва : Юрайт, 2019.	https://www.urait.ru/bcode/431164
3. Бабаш А. В. Криптографические методы защиты информации : Учебно-методическое пособие: Том 1 : ВО - Бакалавриат. / Национальный исследовательский университет "Высшая школа экономики" - Москва : Издательский Центр РИОР, 2018.	http://new.znanium.com/go.php?id=960001
4. Фомичёв В. М., Мельников Д. А. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : Учебник - Москва : Юрайт, 2018.	https://www.urait.ru/bcode/422364
5. Фомичёв В. М., Мельников Д. А. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : Учебник / под ред. Фомичёва В.М. - Москва : Юрайт, 2018.	https://www.urait.ru/bcode/422366

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства

- 7-Zip
- Oracle VM VirtualBox
- ОС Альт образование 10
- LibreOffice

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)

№	Наименование СПБД/ ИСС
1.	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2.	Научная электронная библиотека eLIBRARRY – www.elibrary.ru
3.	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4.	База данных ПОЛПРЕД Справочники – www.polpred.com
5.	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary www.oecd-ilibrary.org
6.	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
7.	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)

8.	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
9.	Электронная библиотечная система BOOK.ru - www.book.ru
10.	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
11.	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
12.	Электронная библиотека СПбГЭУ– opac.unecon.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование учебных аудиторий, перечень	**Адрес (местоположение) учебных аудиторий**
Ауд. 1066 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 74 посадочных места, рабочее место преподавателя, доска меловая - 1 шт., стол - 1 шт., кафедра - 1 шт., Smart Телевизор LE43K6500U Размер экрана-42" - 1 шт. Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»
Ауд. 2057 лаборатория Инженерно-технической защиты, лаборатория Программно-аппаратной защиты.Специализированная мебель и оборудование: Учебная мебель на 30 посадочных мест (Парта двухместная – 11 шт., стол – 8 шт., стулья- 30 шт.); 2 рабочих места преподавателя (2 стола, 2 стула); стол – 1 шт.; трибуна для выступлений – 1 шт.; шкаф для документов – 1 шт.; стенды настенные пробковые – 2 шт.; шкаф настенный со стеклянными створками – 4 шт.; доска для маркеров двухсторонняя – 1 шт.; персональный компьютер IBM	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

PC-совместимый (i5-3470/RAM 8Gb/HDD 500Gb/Win7pro) – 7 шт.; персональный компьютер IBM PC-совместимый (i3-2100/RAM 8Gb/HDD 500Gb/Win7pro) – 8 шт.; коммутатор Cisco для организации локальной сети лаборатории с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации – 1 шт.; шкаф серверный 42U – 1 шт.; шкаф телекоммуникационный 20U – 1 шт.; проектор NEC ME-401X – 1 шт.; экран для проектора Screen Media Goldview 244*244MW настенный – 1шт.; акустическая система марка Microlab модель Pro2– 1 шт.; коммутатор консольный Trend Net TK-803R – 1 шт.; разветвитель видеосигнала Aten VS-92A – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЭ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ОЦТ-МР» – 1 шт.; лабораторный стенд НПП «Учтех-Профи» «ФОЭ-НР» – 1 комплект; комплект плакатов НПП «Учтех-Профи» – 1 шт.; генератор акустического шума ЛГШ-301 АО «Лаборатория ППШ» – 1 шт.; виброгенератор ЛГШ-403 в комплекте с вибропреобразователями ЛВП-2о, ЛВП-2Т АО «Лаборатория ППШ» – 1 шт.; фильтр сетевой однофазный ЛФС-10-1Ф АО «Лаборатория ППШ» – 1 шт.; генератор шума по цепям электропит., заземл. и ПЭМИ ЛГШ-503 АО «Лаборатория ППШ» – 1 шт.; устройство защиты телефонных линий Гранит-8 абонентское АО «Лаборатория ППШ» – 1 шт.; сервер HP-DL – 5 шт.; Коммутатор Cisco Small Business SF302-08 – 4 шт.; Коммутатор Cisco 2950 – 3 шт.; Коммутатор Cisco 3560 – 1 шт.; Беспроводной маршрутизатор TP-Link TL - WR941 ND; Электронные ключи Guardant – 16 шт.; огнетушитель ОУ-5 – 1 шт.; огнетушитель ОП-4(3)-ВСЕ – 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	
Ауд. 2021 Лаборатория "Лабораторный комплекс"Специализированная мебель и оборудование: Учебная мебель на 22 посадочных места (22 компьютерных стола, черных кресел 22шт.) Учебная мебель на 42 посадочных мест (парт 21 шт.,) рабочее место преподавателя (компьютерный стол 1шт.)доска, меловая 3-х секционная 1шт., доска маркерная на колесиках 1 ш., часы 1 шт., кафедра 1шт., стол 1шт., тумбочка 1шт., стул изо 4шт., вешалка стойка 2шт., жалюзи 3шт. Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Установка демонстрационных учебных фильмов - 1 шт., Компьютер в комплектации системный блок Intel pentium x2 g3250 клавиатура+мышь L (жесткий диск500gb,монитор philips 21.5') - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»
Ауд. 2034 Компьютерный класс (для проведения практических занятий, курсового проектирования (выполнения курсовых работ) с применением вычислительной техники). Оборудован мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 25 посадочных мест, рабочее место преподавателя (стол 1шт., кресло 1шт.), доска маркерная 1 шт., вешалки стойки 2шт., стульев 3шт.Компьютер I5-7400/8Gb/1Tb/DELL S2218H - 21 шт., Сетевой коммутатор Cisco WS-C2960-	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

48TT-L (Catalyst2960) 48портов 10/100Мбит/с+2п - 1 шт., Коммутатор Cisco Catalyst 2960 24 WS-C2960-24PC-L - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

– учебно-методической документацией;

– локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;

– графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

- фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
- базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
- профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
- индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные

профессиональные специализированные области знаний, определяемые представителями рынка труда;

– метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

8. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Контрольные вопросы и задания к промежуточной аттестации

1 Криптографическая система. Схема, основные понятия и принципы построения.
2 Классические шифры: классификация и примеры.
3 Шифры гаммирования и колонной замены.
4 Алгебраическая и вероятностная модель шифра. Определение апостериорной информации о ключе, открытом тексте.
5 Расстояние единственности шифра.
6 Теоретическая стойкость шифров. Совершенные и близкие к совершенным шифры.
7 Композиционные шифры: принципы синтеза и основные схемы.
8 Алгоритм шифрования DES.
9 Лавинный эффект блочных шифров.
10 Режимы работы блочных шифров: простой замены (ECB) и простой замены с зацеплением (CBC).
11 Режимы работы блочных шифров: гаммирование с зацеплением (CFB).
12 Режимы работы блочных шифров: гаммирования (CTR) и гаммирование с обратной связью (OFB).
13 Режимы работы блочных шифров: полнодисковое шифрование.
14 Режимы работы блочных шифров: аутентифицированное шифрование.
15 Алгоритм "Кузнечик" ГОСТ 34.12-2018.
16 Алгоритм "Магма" ГОСТ 34.12-2018.
17 Алгоритм AES.
18 Вычислительная стойкость криптоалгоритмов. Требования, предъявляемые к алгоритмам шифрования и длине ключа.
19 Цели и классификация атак на алгоритмы шифрования.
20 Методы криптоанализа блочных шифров: «грубой силы» и «встреча посередине».
21 Методы криптоанализа блочных шифров: линейный, дифференциальный криптоанализ и его модификации.
22 Методы криптоанализа блочных шифров: слайдовая атака и атака на связанных ключах.
23 Атаки на шифраторы, использующие утечки по побочным каналам.
24 Потоковое шифрование, методы генерации ключевой гаммы. Синхронные и асинхронные потоковые шифры.
25 Генераторы ключевой гаммы на регистрах сдвига с линейной обратной связью LSFR. Нелинейные потоковые шифры.
26 Криптоанализ потоковых криптосистем.
27 Потоковый шифр Salsa20.
28 Управление криптографическими ключами: хранение и распределение ключей.
29 Управление криптографическими ключами: генерация ключей. BBS-генератор.
30 Линейные и нелинейные ключевые пространства, слабые и эквивалентные ключи, проблемы слабых процедур расширения ключа.
31 Имитостойкость и помехоустойчивость шифров. Коды аутентификации MAC, HMAC.
32 Типы криптосистем по ключу. Симметричные и асимметричные криптосистемы: основные принципы построения, теоретическое обоснование и свойства.
33 Криптосистема Диффи-Хеллмана.
34 Алгоритм быстрого возведения в степень по модулю.

35 Числа, обратные по модулю. Условие существования. Расширенный алгоритм Евклида, вычисление числа, обратного по модулю.
36 Алгоритмы проверки чисел на простоту.
37 Шифр Шамира.
38 Шифр Эль-Гамаля.
39 Криптосистема RSA: теоретическое обоснование, обеспечение конфиденциальности и аутентичности сообщений
40 Требования к параметрам и атаки на шифр RSA.
41 Понятие семантической стойкости. Система вероятностного шифрования Блюма-Гольдвассер.
42 Бесключевые хэш-функции. Стандарты и принципы построения.
43 Функция хэширования ГОСТ 34.11-2018.
44 Электронная подпись: свойства, детерминированные и вероятностные подписи. Система электронной подписи RSA.
45 Система электронной подписи Эль-Гамаля.
46 Система электронной подписи Шнорра.
47 Эллиптические кривые: определение, вид, уравнение, операции с точками.
48 Эллиптические кривые: применение в криптографии, аналог схемы Диффи-Хэллмана на эллиптических кривых, требования к параметрам кривой.
49 Стандарт цифровой подписи ГОСТ 34.10-2018, выбор параметров кривой, подписание сообщений и проверка подписи.
50 Основные принципы и проблемы практической реализации квантовой криптографии.

1.2 Темы письменных работ

1 Алгоритм шифрования Blowfish.
2 Алгоритм шифрования Camellia.
3 Алгоритм шифрования CAST.
4 Алгоритм шифрования CRYPTON.
5 Алгоритм шифрования DES.
6 Алгоритм шифрования FEAL.
7 Алгоритм шифрования IDEA.
8 Алгоритм шифрования KASUMI.
9 Алгоритм шифрования Khafre, Khufu.
10 Алгоритм шифрования ГОСТ Р 34.12-2015 Кузнечик.
11 Алгоритм шифрования LOKI97.
12 Алгоритм шифрования Lucifer.
13 Алгоритм шифрования MADRYGA.
14 Алгоритм шифрования ГОСТ Р 34.12-2015 Магма.
15 Алгоритм шифрования MARS.
16 Алгоритм шифрования Rinjdael (AES).
17 Алгоритм шифрования RC5.
18 Алгоритм шифрования RC6.
19 Алгоритм шифрования SAFER.
20 Алгоритм шифрования Serpent.
21 Алгоритм шифрования Skipjack.
22 Алгоритм шифрования TEA, XTEA.
23 Алгоритм шифрования Twofish.
24 Алгоритм шифрования DEAL.
25 Алгоритм шифрования NUSH.

1.3 Контрольные точки

Номер контрольной точки	Тип контрольной точки	Способ проведения	Номера тем
1	Индивидуальное задание	с помощью технических средств и информационных систем	1
2	Индивидуальное задание	с помощью технических средств и информационных систем	6-7
3	Текущий контроль	с помощью технических средств и информационных систем	1-11

1.4 Другие объекты оценивания

Рабочей программой дисциплины не предусмотрено.

1.5 Самостоятельная работа обучающегося

Наименования самостоятельной работы	Номера тем
Курсовое проектирование	1-4
Подготовка к лекционным и практическим занятиям	1-10
Подготовка к экзамену	1-11

1.6 Шкала оценивания результата

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.

Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся**:

Формой итогового контроля по дисциплине является экзамен (или дифференцированный зачет), итоговая оценка формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
<=54	неудовлетворительно
55-69	удовлетворительно
70-84	хорошо
>=85	отлично

Шкала оценивания результата

2 (балл до 54)	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
3 (балл 55-69)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.
4 (балл 70-84)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
5 (балл 85-100)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.