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

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/Шубаева В.Г./
«28» августа 2020 г.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Рабочая программа дисциплины

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составитель:
_____/к.ф.-м.н., доцент Васильева И.Н.

Санкт-Петербург
2020

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ 3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 3
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ 4
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ 4
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 6
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 7
7.1. Методические указания для обучающегося по освоению дисциплины **7**
7.2. Организация самостоятельной работы **7**
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 8
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8
9.1 Учебно-методическое и информационное обеспечение дисциплины **8**
9.2. Материально-техническое обеспечение учебного процесса **9**
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 9
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 10

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: формирование представлений о современных алгоритмах, методах и средствах криптографической защиты информации, используемых для решения проблем компьютерной безопасности.

Задачи:

- приобретение теоретических знаний, касающихся математических основ современной криптографии, исторических и современных методов шифрования и криптоанализа, электронной подписи и криптографических методов контроля целостности;
- формирование представление о роли математических методов при решении задач криптографии и криптоанализа, способов их реализации в современных программных комплексах;
- формирование умения формулировать количественные и качественные требования по криптографической защите информации;
- выработка практических навыков использования криптографических методов для обеспечения конфиденциальности, целостности и аутентичности защищаемой информации;
- выработка практических навыков программной реализации алгоритмов современной криптографии;
- формирование навыков работы с современными средствами криптографической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.Б. Криптографические методы защиты информации относится к базовой части дисциплин Блока 1 является обязательной для освоения обучающимся вне зависимости от направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
ОПК-7 – способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных	Третий уровень (продвинутый) (ОПК-7)-3	Декомпозиция I Знать: предмет, цели и задачи криптографии и криптоанализа, принципы построения криптографических алгоритмов; криптографические стандарты, профессиональные требования к симметричным и асимметричным криптосистемам. З3 (I)(ОПК-7) Уметь: решать задачи, связанные с шифрованием и цифровой подписью сообщений; осуществлять выбор необходимых криптографических методов, алгоритмов и режимов работы криптоалгоритмов для решения практических задач информационной безопасности. У3(I) (ОПК-7) Владеть: методами имитозащиты, обеспечения конфиденциальности, аутентификации и проверки

процессов и особенностей функционирования объекта защиты		целостности с помощью криптографических алгоритмов и функций; приемами управления ключевой информацией и построения сетей засекреченной связи. В3 (I)(ОПК-7)
ПСК-1.1 – способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	Третий уровень (продвинутый) (ПСК-1.1) – З	Декомпозиция II Знать: структуру, принципы построения и основные элементы криптографических алгоритмов, криптографические алгоритмы шифрования, обеспечения целостности и электронной подписи З3 (II)(ПСК-1.1) Уметь: проводить анализ и построение структурных схем криптографических алгоритмов, реализовывать вычислительные алгоритмы криптографии с помощью программных инструментальных средств У3(II) (ПСК-1.1) Владеть: приемами и навыками программной реализации и анализа криптографических алгоритмов в современных программных комплексах В3 (II)(ПСК-1.1)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, из которых 36 часов самостоятельной работы обучающегося отводится на подготовку и защиту экзамена.

Форма промежуточной аттестации: экзамен – 6 семестр, курсовая работа – 6 семестр.

Распределение фонда времени по темам по очной форме обучения представлено в таблице 4.1

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	*2*	*3*	*4*	*5*
Тема 1.1. Основные понятия криптографии. Классические шифры	6	6		6
Тема 1.2. Современные симметричные блочные шифры	10	6		18
Тема 1.3. Потоковые системы шифрования	2	4		8
Тема 1.4. Вопросы практической реализации симметричных криптосистем	4	6		30
Тема 2.1. Асимметричная криптография	10	10		8
Тема 2.2. Цифровая подпись	4	8		8
Тема 2.3. Криптография на эллиптических кривых	4	8		8
Тема 2.4. Квантовая криптография	2			4
Всего по дисциплине:	**42**	**48**		**90**

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

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Раздел 1. Криптосистемы с секретным ключом

Тема 1.1. 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.

Тема 1.2. Современные симметричные блочные шифры

Совершенные и близкие к совершенным шифры. Композиции шифров. Методы синтеза симметричных блочных шифров.

Сети Фейстеля. Алгоритм шифрования DES. Алгоритм «Магма» ГОСТ Р 34.12-2015.

Подстановочно-перестановочные сети. Шифр AES. Алгоритм «Кузнечик» ГОСТ 34.12-2015.

Режимы работы блочных шифров ГОСТ Р 34.13-2015. Специальные режимы работы блочных шифров: полнодисковое шифрование, аутентифицированное шифрование. Режимы работы блочных шифров с преобразованием ключа. Алгоритмы экспорта и импорта ключа.

Практическая стойкость криптоалгоритмов. Атаки на алгоритмы шифрования. Методы криптоанализа блочных шифров. Требования, предъявляемые к современным блочным алгоритмам шифрования.

Тема 1.3. Потоковые системы шифрования

Потоковые криптосистемы. Генераторы ключевой гаммы на регистрах сдвига с линейной обратной связью LSFR. Нелинейные потоковые шифры. Синхронные и асинхронные потоковые шифры. Атаки на потоковые криптосистемы. Примеры потоковых криптосистем: RC2/RC4, A5, Salsa20.

Тема 1.4. Вопросы практической реализации симметричных криптосистем

Управление криптографическими ключами. Генераторы случайных и псевдослучайных чисел. Равномерные и неравномерные ключевые пространства. Централизованное и децентрализованное распределение ключей. Защита ключей при хранении.

Имитостойкость и помехоустойчивость шифров.

Программные и аппаратные шифраторы. Примеры программных реализаций средств криптографической защиты информации: шифрующая файловая система EFS, полнодисковое шифрование BitLocker. Полнодисковое шифрования LUKS.

Раздел 2. Криптосистемы с открытым ключом

Тема 2.1. Асимметричная криптография

Основные концепции криптографии с открытым ключом. Система Диффи-Хеллмана.

Математические основы асимметричной криптографии. Теорема Ферма, теорема Эйлера, расширенный алгоритм Евклида, алгоритм быстрого возведения в степень по модулю. Алгоритм проверки чисел на простоту. Генерация простых чисел.

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.

Криптосистема Рабина. Семантическая стойкость. Вероятностное шифрование (система Блюма-Гольдвассер).

Тема 2.2. Цифровая подпись

Бесключевые функции хэширования. Функция хэширования ГОСТ Р 34.11-2012. 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.

Тема 2.3. 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 Р 34.10-2012. Выбор параметров цифровой подписи.

Тема 2.4. Квантовая криптография

Основные концепции и вопросы практической реализации квантовой криптографии.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	*2*	*3*
1.1	Задача 1. Криптоанализ шифров табличной перестановки	ПЗ/ Решение практических задач, отчет. Индивидуальное контрольное задание №1
	Задача 2. Криптоанализ шифра простой замены	
	Задача 3. Криптоанализ многоалфавитного шифра (шифр Виженера)	
1.2	Задача 4. Изучение шифра AES	ПЗ/ Решение практических задач, отчет
	Задача 5. Криптоанализ блочного шифра. Слайдовая атака	
1.3	Задача 6. Изучение потокового шифра на LSFR	ПЗ/ Решение практических задач, отчет
1.4	Задача 7. Изучение средств шифрования ОС Windows	ПЗ/ Решение практических задач, отчет
2.1	Задача 8. Изучение шифра RSA	ПЗ/ Решение практических задач, отчет. Индивидуальное контрольное задание №2
	Задача 9. Атака на алгоритм RSA методом Ферма	
	Задача 10. Атака на алгоритм RSA методом повторного шифрования	
	Задача 11. Атака на алгоритм RSA методом бесключевого чтения	
	Задача 12. Атака на алгоритм RSA на основе Китайской теоремы об остатках	
	Задача 13. Изучение криптосистемы Блюма – Гольдвассер	
2.2	Задача 14. Изучение электронной цифровой подписи Эль-Гамаля	ПЗ/ Решение практических задач, отчет
	Задача 15. Создание скрытого канала в цифровой подписи Эль-Гамаля	
2.3	Задача 16. Вычисление точек эллиптической кривой над конечным полем	ПЗ/ Решение практических задач, отчет
	Задача 17. Шифрование с использованием эллиптических кривых	
	Задача 18. Цифровая подпись на эллиптических кривых	

* ПЗ – практические занятия, СЗ – семинарские занятия, ЛР – лабораторные работы

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1. Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

– рабочей программой дисциплины: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся,

– порядком проведения текущего контроля успеваемости и промежуточной аттестации;

– графиком консультаций преподавателей кафедры.

Систематическое выполнение учебной работы на занятиях лекционных и семинарских типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины обучающимся следует:

– слушать, конспектировать излагаемый преподавателем материал;

– ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;

– задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;

– выполнять задания практических занятий полностью и установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратится к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 - недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2. Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к ограничениям их здоровья.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ темы	Вид самостоятельной работы
1	*2*
1.1	Изучение литературных источников, подготовка к ПЗ, подготовка к экзамену.
1.2	Изучение литературных источников, подготовка к ПЗ, подготовка к экзамену.
1.3	Изучение литературных источников, подготовка к ПЗ, подготовка к экзамену.
1.4	Изучение литературных источников, подготовка к ПЗ, подготовка к экзамену.
2.1	Изучение литературных источников, подготовка к ПЗ, подготовка к экзамену.
2.2	Изучение литературных источников, подготовка к ПЗ, подготовка к экзамену.

№ темы	Вид самостоятельной работы
2.3	Изучение литературных источников, подготовка ПЗ, подготовка к экзамену.
2.4	Изучение литературных источников, подготовка по контрольным вопросам, подготовка к экзамену.
1.1	Подготовка к контрольной точке №1
2.1	Подготовка к контрольной точке №2

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Криптографические методы защиты информации*» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 1.1, 1.2, 1.3, 1.4, 2.1, 2.2, 2.3.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по изучению приемов и методов реализации алгоритмов шифрования, расшифрования и цифровой подписи, а также использованию и настройке средств криптографической защиты информации.

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1 Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое обеспечение дисциплины

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Основная/ дополнительная литература**	**Книгообеспеченность**	
		Кол-во экз. в библ. СПбГЭУ	**Электронные ресурсы**
Васильева И. Н. Криптографические методы защиты информации : учебник и практикум . — Электрон. дан. — Москва : Издательство Юрайт, 2017 .— 349 с.	основная	–	ЭБС Юрайт
Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Электрон. дан. — Москва : Издательство Юрайт, 2016. — 473 с.	основная	–	ЭБС Юрайт
Бабаш А.В. Криптографические методы защиты информации: учебно-методическое пособие: Том 1. — Электрон. дан. - Москва : Издательский Центр РИОР, 2018 - 413 с.	дополнительная	–	ЭБС ZNANIUM
Фомичёв В. М., Мельников Д. А. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: Учебник / под ред. Фомичёва В.М. - Электрон. дан. - Москва : Юрайт, 2017 - 209 с.	дополнительная	–	ЭБС Юрайт

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
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

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
2	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
3	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
4	Электронная библиотечная система BOOK.ru - www.book.ru
5	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
6	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
7	Электронная библиотека СПбГЭУ– opac.unecon.ru

9.2. Материально-техническое обеспечение учебного процесса

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

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№ п/п	Наименование ПО
1	Microsoft Windows Professional (КОНТРАКТ № 244/20 «26» июня 2020 г
2	Microsoft Office Professional (КОНТРАКТ № 244/20 «26» июня 2020 г)
3	7-Zip (freeware)

10. 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.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).