ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК - 10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности
ОПК – 7.1	Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

Задачи дисциплины:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-10.1. Понимает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; основные методы и средства технической защиты информации; особенности применения криптографических и технических методов и средств защиты информации для решения задач профессиональной деятельности	**Знает** нормативные требования по административно-правовому регулированию в области криптографической защиты информации, основные задачи и понятия криптографии, этапы развития криптографии, виды информации, подлежащей шифрованию, классификацию шифров **Умеет** использовать типовые шифры замены и перестановки
ОПК-10.2. Анализирует программные модели средств криптографической защиты информации, осуществляет подбор средств технической защиты информации для решения задач профессиональной деятельности	**Знает** методы криптографического синтеза и анализа, постановки задач криптоанализа и подходы к их решению **Умеет** применять частотные характеристики языков и их использование в криптоанализе, формулировать требования к шифрам и основные характеристики шифров, реализовывать типовые поточные и блочные симметричные шифры

ОПК-10.3. Применяет различные криптографические средства защиты информации и средства технической защиты для решения задач профессиональной деятельности	**Знает** принципы построения современных шифрсистем, основные математические методы, используемые в анализе типовых криптографических алгоритмов **Умеет** реализовывать системы шифрования с открытыми ключами, использовать основных типов шифров и криптографических алгоритмов использовать различные криптографические средства защиты информации и средства технической защиты для решения задач профессиональной деятельности
ОПК-7.1.1. Использует программные и программно-аппаратные средства в качестве компонентов систем защиты информации автоматизированных систем, типовые архитектуры и принципы построения современных защищенных информационных систем	**Знает** государственные стандарты в области криптографии, методы криптозащиты компьютерных систем и сетей, принципы построения современных защищенных информационных систем **Умеет** применять криптографию в решении задач аутентификации, построения систем цифровой подписи

3. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части, образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация - **Анализ безопасности информационных систем**.

4. Структура и содержание

Дисциплина «Методы и средства криптографической защиты информации» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 180 академических часов (5 зачетных единиц).

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость			
	з.е.	час.	по семестрам	
			5	6
Общая трудоемкость дисциплины по учебному плану	**5**	**180**	**72**	**108**
Контактная работа, в том числе:		**74**	**36**	**38**

Вид учебной работы	Трудоемкость			
	з.е.	час.	по семестрам	
			5	6
Аудиторные занятия		**72**	**36**	**36**
Лекции (Л)		34	16	18
Практические занятия (ПЗ)		38	20	18
Консультация		**2**		**2**
Самостоятельная работа (СРС)		**70**	**36**	**34**
Зачет			+	
Экзамен		**36**		**36**

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов и тем	**Всего часов**	**Количество часов по видам занятий**				**Самостоятельная работа**
		Лекции	**Практические занятия**	**Консультации**	**Контроль**	
5 семестр						
Раздел 1. Общие сведения. Введение	36	8	10			18
Раздел 2. Симметричная криптография	36	8	10			18
Зачет	+					
итого за 5 семестр	**72**	**16**	**20**			**36**
6 семестр						
Раздел 3. Несимметричная криптография	24	6	6			12
Раздел 4. Электронно-цифровая подпись	24	6	6			12
Раздел 5. Криптографические протоколы	22	6	6			10
Консультации	2			2		
Экзамен	36				36	
итого за 6 семестр	**108**	**18**	**18**	**2**	**36**	**34**
Всего	**180**	**34**	**38**	**2**	**36**	**70**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Общие сведения. Введение

Лекции. Основные понятия и определения криптографии. Этапы развития криптографии. Роль математики в развитии методов защиты информации. Новые направления в криптографии. Криптографические примитивы и криптографические протоколы по защите информации. Двухсторонние и многосторонние протоколы. Типы предполагаемых противников. Формальные методы оценки качества криптографических протоколов

Практические занятия. Шифры. Примеры. Стойкость шифра. Классификация методов дешифрования

Самостоятельная работа. История криптографии: исторические шифры, история отечественной криптографии, средства защиты информации в период перехода от древности к современности, шифры Виженера, модели шифров по К. Шеннону, обобщенная модель шифра, понятие симметричной криптосистемы, системы шифрования с открытыми ключами, блочные и поточные шифры, простейшие шифры и их свойства, композиции шифров, стойкость шифра, однонаправленные функции, современная классификация известных шифров, простые методы криптоанализа известных шифров. Характер криптографической деятельности. Виды информации, подлежащие закрытию, их модели и свойства. Модели нарушителя и безопасных систем. Модель Долева-Яо. Принципы построения криптографических алгоритмов. Понятие криптографического протокола. Протокол Нидхема-Шредера. Понятия аутентификации сущности и аутентификации сообщений. Модели шифров. Основные требования к шифрам. Программные реализации шифров. Особенности использования вычислительной техники в криптографии. Понятие сложности алгоритма, сложность некоторых известных алгоритмов. Недетерминированное полиномиальное время. Гипотеза P=NP. Алгоритм быстрого возведения в степень, обобщенный алгоритм Евклида. Модулярная арифметика. Теоремы Эйлера, Лагранжа, Ферма. Китайская теорема об ос-татках. Квадратичные вычеты и невычеты. Вычисление квадратного корня в модулярной арифметике по простому и по составному модулям. Понятие о конечных полях по неприводимым многочленам. Методы получения случайных и псевдослучайных последовательностей.

Рекомендуемая литература:

основная [1, 2];

дополнительная [1,2,3]

Раздел 2. Симметричная криптография

Лекции. Блочные и поточные криптосистемы и их классификация. Описание DES - RC4 AES, ГОСТ 28147-89, Кузнечик и др. Режимы использования и их сравнение (ECB,CBC, OFB). Криптографические свойства функций.

Практические занятия. Хзш функции. Хэш цепочки. Дерево Меркле. Стандарты хэш функций. Шифры замены, перестановки, шифры гаммирования. композиционные шифры, сети Файстеля.

Самостоятельная работа. Блочные шифры: проблема выравнивания, требования к построению блочных шифров. Поточные шифры: синтез поточных шифров, требования к поточным шифрам, режимы использования поточных шифров, синхронизация поточных шифров, опознавание, контроль целостности данных, управление ключами. Криптосистемы DES и отечественного ГОСТа. Стандарт криптографической защиты AES-Rijndael. Криптографическая стойкость шифров. Основные атаки на симметричные шифры. Совершенные шифры. Теоретико-информационный подход к оценке криптостойкости шифров. Вопросы практической стойкости. Имитостойкость и помехоустойчивость шифров. Различие между программными и аппаратными реализациями. Криптографические параметры узлов и блоков шифраторов. Синтез шифров.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2,3]

Раздел 3. Несимметричная криптография

Лекции. Основные понятия криптографии с открытым ключом. Сравнение криптосистем с открытым и секретным ключом. Однонаправленные (односторонние) функции по Нидхэму. Однонаправленные функции, основанные на сложности задачи дискретного логарифмирования. Применения в современных технологиях. Однонаправленные (односторонние) функции с секретом и их применение для цели шифрования информации. Схемы RSA, Рабина, Эль Гамаля, МакЭлайса, Меркля – Хеллмана. Некоторые методы быстрой модульной арифметики и их применение для ускорения криптографических алгоритмов.

Практические занятия. Ассиметричные методы шифрования. Сравнение двух классов криптосистем, гибридные криптосистемы. Принципы криптоанализа, критерии распознавания открытого текста, универсальные методы криптоанализа: Дифференциальный криптоанализ, дифференциальный криптоанализ DES и трехраундового DES.

Самостоятельная работа. Вопросы организации сетей засекреченной связи. Ключевые системы. Схема открытого распределения ключей Диффи-Хеллмана. К5А. Криптосистема Рабина. криптосистема Эль Гамаль. Сравнение двух классов криптосистем, гиб-ридные криптосистемы.

Принципы криптоанализа, критерии распознавания от-крытого текста, универсальные методы криптоанализа: Дифференциальный криптоанализ, дифференциальный криптоанализ DES и трехраундового DES. Битовая стойкость алгоритма RSA. Понятие оракула четности. Битовая стойкость дискретного логарифма

Рекомендуемая литература:

основная [1, 2,];

дополнительная [1, 2, 3]

Раздел 4. Электронно-цифровая подпись.

Лекции. Понятия о цифровой подписи на основе однонаправленной функции с секретом. Классификация атак на схемы цифровой подписи. Сравнение стандартов цифровой подписи США (FIPS PUB 186) и России (ГОСТ Р 34.10-94). Стандарт цифровой подписи ГОСТ Р 34.10-2001, 2015 на основе эллиптических кривых. Схемы подписи, в которых подделка подписи может быть доказана. Схемы мультиподписи (multisignature scheme). Групповая подпись (group signature scheme). Подпись по доверенности (proxy signature).

Практические занятия. Схемы подписи Фиата-Шамира, Файге-Фиата-Шамира и др. Схема Шнорра. Подпись вслепую (blind signature) и ее применения. Схемы конфиденциальной подписи (undeniable signature) и их применение. Протоколы проверки и отвержения как примеры протоколов доказательств с нулевым разглашением. Схемы Шаума.

Самостоятельная работа. Симметричные средства. Криптографические хеш-функции. Электронная цифровая подпись, цифровая подпись на основе RSA, криптосистемы Рабина и Эль Гамаля. Существующие уязвимости системы Эль-Гамаля.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2,3]

Раздел 5. Криптографические протоколы.

Управление ключами. Доказуемо безопасные генераторы ключей. Некоторые способы сокращения объемов хранимых ключей. Протоколы распределения криптографических ключей. Криптографическая инфраструктура на основе механизма открытых ключей(PKI). Модели криптографической инфраструктуры. Протоколы, основанные на идентификационной информации (ID-based cryptosystems). Протоколы с разделением секрета. Пороговые схемы. Криптосистемы и протоколы на эллиптических кривых.

Лекции.

Практические занятия. Протоколы идентификации и аутентификации. Протоколы честного обмена секретами. Интерактивные схемы доказательств.

Самостоятельная работа. Протоколы электронного тайного голосования. Понятие о протоколах электронных платежей.

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2,3]

5. Методические рекомендации по организации изучения дисциплины «Методы и средства криптографической защиты информации»

При реализации программы дисциплины используются лекционные и практические занятия.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники;

– концентрировать внимание обучающихся на наиболее сложных и узловых вопросах;

– стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цели практического занятия: выработка практических умений и приобретение навыков, закрепление пройденного материала по соответствующей теме дисциплины.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине «Методы и средства криптографической защиты информации»

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме опроса и тестирования.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме зачета в 5 семестре и экзамена в 6 семестре.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса:

1. Основные понятия и определения криптографии.
2. Виды криптосистем.
3. Задачи, решаемые методами криптографии.
4. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений.
5. Критерии на открытый текст.
6. Особенности нетекстовых сообщений.
7. История криптографии.
8. Основные этапы становления науки криптографии.
9. Классификация шифров замены.
10. Шифр Цезаря.
11. Шифр простой замены.
12. Шифр Плейфера.
13. Полибианский квадрат.
14. Шифр Хилла.
15. Шифр Виженера.
16. Частотный анализ.
17. Тест Казиски.
18. Классификация шифров перестановки.
19. Примеры шифров перестановки и их криптоанализ.
20. Шифры гаммирования.
21. Шифр Вернама.
22. Подходы к его криптоанализу.
23. Композиции шифров.
24. Enigma.
25. Шифр Хейглина.
26. Математическая модель шифра.
27. Атаки и угрозы шифрам.
28. Блочные шифры и их ключевая система.
29. Замены и перестановки.
30. Сеть Файстеля.
31. Шифры DES, ГОСТ 28147-89.
32. Шифр AES.

Примерный перечень вопросов выносимых на зачет

1. Шифр IDEA.

2. Подходы к криптоанализу блочных шифров.
3. Дифференциальный криптоанализ.
4. Линейный криптоанализ.
5. Режимы шифрования.
6. Многократное шифрование.
7. Композиция блочных шифров.
8. Совершенные шифры.
9. Пример совершенного шифра.
10. Энтропийные характеристики шифров.
11. Идеальные шифры.
12. Избыточность языка.
13. Оценка числа ложных ключей и расстояние единственности.
14. Безусловно стойкие и вычислительно стойкие шифры.
15. Псевдослучайные последовательности (ПСП).
16. Характеристики генераторов ПСП (ПСГ).
17. Требования к криптографическим ПСП.
18. Примеры ПСГ и криптографических ПСГ.
19. Поточные шифры.
20. Общая схема поточного шифра.
21. Синхронные и самосинхронизирующиеся шифры.
22. Регистры сдвига с обратной линейной связью (РСЛОС).
23. ПСГ на основе РСЛОС.
24. Шифр A5.
25. Нелинейные регистры сдвига.
26. Шифр RC4.
27. Теория имитостойкости Симмонса.
28. Имитация и подмена сообщения.
29. Характеристики имитостойкости.
30. Совершенная имитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Ключевые хэш-функции.
37. Понятие односторонней функции и односторонней функции с "лазейкой".
38. Проблемы факторизации целых чисел и логарифмирования в конечных полях.

Примерный перечень вопросов выносимых на экзамен

1. Криптосистема Диффи-Хэллмана. Пример.
2. Криптосистема RSA. Пример.

3. Криптосистема Эль-Гамаля. Пример.
4. Криптосистема Рабина. Пример.
5. Криптосистема Гольдвассер-Микали. Пример.
6. Криптосистема Блюма-Гольдвассер. Пример.
7. Рюкзачные шифры.
8. Криптосистема Меркла-Хэллмана.
9. Понятие электронной цифровой подписи и требования к ней.
10. Атаки и угрозы схемам ЭЦП.
11. Подпись RSA, Эль-Гамаля.
12. Подпись Фиата-Шамира.
13. Подпись Онга-Шнорра-Шамира.
14. Неотрицаемая подпись Шаума-ван-Антверпена.
15. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
16. Эллиптическая кривая над конечным полем.
17. Операции на эллиптической кривой.
18. Сумма точек. Кратная точка.
19. Проблема дискретного логарифмирования на эллиптической кривой.
20. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой.
21. Шифр Эль-Гамаля на эллиптической кривой.
22. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10- 2001, ECDSA.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
Экзамен, зачёт	правильность и полнота ответа; выполнение контрольных нормативов	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	Отлично, зачтено
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя.	Хорошо, зачтено
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют	Удовлетворительно зачтено

		выводы.	
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	Неудовлетворительно, незачтено

7. Ресурсное обеспечение дисциплины «Методы и средства криптографической защиты информации»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- МойОфис Образование [ПО-41В-124] - Полный комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4557]

- Astra Linux Common Edition релиз Орел [ПО-25В-603] - Операционная система общего назначения "Astra Linux Common Edition" [Коммерческая (Full Package Product). Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4433]

7.2. Профессиональные базы данных и информационные справочные системы

1. Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс]. – Режим доступа: http://window.edu.ru/, доступ только после самостоятельной регистрации
2. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации
3. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ
4. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный доступ

7.3. Литература

Основная литература:

1. Фороузан Б.А. Криптография и безопасность сетей : учебное пособие / Фороузан Б.А.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-

0946-2. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html (дата обращения: 29.08.2023). — Режим доступа: для авторизир. пользователей

2. Овчинников, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Овчинников. — Санкт-Петербург : ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216491 (дата обращения: 29.08.2023). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111097 (дата обращения: 29.08.2023). — Режим доступа: для авториз. пользователей.

2. Бахаров Л.Е. Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Бахаров Л.Е.. — Москва : Издательский Дом МИСиС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98171.html (дата обращения: 29.08.2023). — Режим доступа: для авторизир. пользователей

3. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563 (дата обращения: 29.08.2023). — Режим доступа: для авториз. пользователей.

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Авторы: к.т.н., доцент Матвеев А.В., к.ю.н. Метельков А.Н.