Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский университет Государственной противопожарной службы МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Магистратура по направлению подготовки 27.04.03 «Системный анализ и управление» направленность (профиль) «Системный анализ и управление в организационно-технических системах»

Санкт-Петербург

1. Цель и задачи дисциплины «Криптографические методы защиты информации»

Цели освоения дисциплины «Криптографические методы защиты информации»:

- формирование у обучающихся целостной системы знаний в области информационной безопасности в части защиты информации с помощью криптографических методов защиты информации и примеров реализации на практике;
- приобретение обучающимися практических навыков по защите информации, необходимых для формирования и развития ряда профессионально важных качеств;

В процессе освоения дисциплины «**Криптографические методы защиты информации**» обучающийся формирует и демонстрирует нормативно заданные компетенции (таблица 1).

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ПК-5	способен применять методы математического и системного анализа и теории принятия решений для исследования функциональных задач управления организационно-техническими системами на основе отечественных и мировых тенденций развития методов, управления, информационных и интеллектуальных технологий

Задачи дисциплины

- знать криптографические методы и средства защиты конфиденциальной информации;
- уметь ориентироваться в нормативно-правовой базе и стандартах в области криптографической защиты информации;
- уметь идентифицировать актуальные угрозы безопасности современных информационных систем;
- знать принципы разработки шифров, основы математических методов, используемых в криптографии;
- овладеть профессиональной терминологией в сфере криптографической защиты конфиденциальной информации.

2. Перечень планируемых результатов обучения дисциплины, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	**Планируемые результаты обучения по дисциплине**
Тип задачи профессиональной деятельности: организационно-управленческий	
Владеет умением инновационного видения развития и модификации привычных образцов деятельности.	Знает
	Терминологию, ключевые положения нормативно-правовых актов и стандартов в сфере совершенствовании деятельности по защите информации криптографическими методами ПК-5.1
	Умеет
	Организовывать системы защиты конфиденциальной информации с использованием криптографических методов. Применять терминологию, лексику и основные категории в сфере криптографической защиты информации ПК-5.1
Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности.	Знает
	Правовые, организационные и технические меры защиты информации при ее передаче и хранении в информационных системах, возможные пути применения современных методов криптографической защиты информации для решения служебных задач. ПК 5.2
	Умеет
	Системно анализировать и толковать действующие нормативные правовые акты и стандарты в области совершенствования защиты служебной информации криптографическими методами. ПК 5.2.

3. Место дисциплины в структуре ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений дисциплин магистратуры по направлению подготовки 27.04.03 «Системный анализ и управление», направленность (профиль) «Системный анализ и управление в организационно-технических системах»

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины обучения составляет 2 зачетные единицы (72 часа).

4.1 Распределение трудоемкости учебной дисциплины по заочной форме обучения и видам работ

Вид учебной работы	Трудоемкость			
	з.е.	час.	по курсам	
			2	3
Общая трудоемкость дисциплины по учебному плану	**2**	**72**	**36**	**36**
Контактная работа, в том числе:		**10**	**2**	**8**
Аудиторные занятия		**10**	**2**	**8**
Лекции (Л)		4	2	2
Практические занятия (ПЗ)		6		6
Самостоятельная работа (СРС)		**62**	**34**	**28**
Зачет с оценкой		+		+

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

№ п/п	Наименование разделов и тем	Всего часов	Количество часов по видам занятий, в том числе практическая подготовка*			Самостоятельная работа	Контроль	Примечание
			Лекции	Практические занятия	Лабораторные работы			
1	2	3	4	5	6	7	8	9

Раздел 1. История криптографии								
1.	Тема 1. История развития криптографии	10				10		
Раздел 2. Основные понятия и определения криптографии. Нормативная база и стандарты								
2.	Тема 2. Криптографическая терминология	14				14		
3.	Тема 3. Нормативная база и стандарты в области криптографической защиты информации	12	2			10		
4.	**Итого за 1 курс**	**36**	**2**			**34**		
Раздел 3. Методы и средства криптографической защиты информации								
5.	Тема 4. Методы криптографической защиты информации. Криптографические алгоритмы	8	2			6		
6.	Тема 5. Средства криптографической защиты информации	8				8		
Раздел 4. Криптографические протоколы. Цифровая подпись								
7.	Тема 6. Основы криптографических протоколов	6				6		
8.	Тема 7. Электронная (цифровая)подпись	6		2/2**		4		
Раздел 5. Управление ключами								
9.	Тема 8. Ключевая подсистема криптосистемы. Протоколы обмена ключами	8		4		4		
10.	Зачет с оценкой	+					+	
11.	**Итого за 2 курс**	**36**	**2**	**6/2****		**28**		
Итого по дисциплине		**72**	**4**	**6/2****		**62**		

** практическая подготовка при реализации дисциплин организуется путем проведения практических и семинарских занятий, лабораторных работ, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью*

*** где 2 часа – практическая подготовка*

4.3 Содержание дисциплины «Криптографические методы защиты информации»

РАЗДЕЛ 1. ИСТОРИЯ КРИПТОГРАФИИ

Тема 1. История развития криптографии

Самостоятельная работа. Сведения из истории криптографии. Основные этапы развития криптографии. Шифр Цезаря. Криптоанализ шифра Вижинера. Появление криптографии в России. Советская криптография. Принципы Шеннона. Требования к криптографическим системам защиты информации.

Рекомендуемая литература

основная: [1,2,3]

дополнительная: [1,2,3]

РАЗДЕЛ 2. ОСНОВЫ КРИПТОГРАФИИ

Тема 2. Криптографическая терминология.

Самостоятельная работа. Политика в сфере обеспечения информационной безопасности России. Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Цели защиты информации. Основное отличие криптографических и стеганографических методов защиты информации. Носители защищаемой информации. Понятие информации. Криптография. Криптоанализ. Атаки на криптографические системы. Криптографическое преобразование. Зашифрование. Криптографическая защита информации (данных). Криптографическая функция. Криптографическое средство защиты информации. Криптографический алгоритм. Шифр. Криптографический ключ. Классическая схема секретной системы.

Конфиденциальность информации. Понятие конфиденциальной информации. Способы реализации криптографических методов. Понятие и виды криптографических атак. Криптографический протокол. Криптографические методы защиты информации. Методы стеганографии. Общие принципы построения СКЗИ. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам.

Рекомендуемая литература

основная: [1,2,3]

дополнительная: [1,2,3]

Тема 3. Нормативная база и стандарты в области криптографической защиты информации

Практические занятия. Организационно-правовое обеспечение криптографической защиты информации. Нормативные документы федерального органа исполнительной власти в сфере безопасности по криптографической защите информации, не содержащей сведения, составляющие государственную тайну.

Нормативное регулирование криптографической защиты информации. Национальные стандарты ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Стандарт ГОСТ Р 34.10-2012. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». Стандарт ГОСТ Р 34.11-2012. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Р 1323565.1.012-2017 «Принципы разработки и модернизации шифровальных (криптографических) средств

защиты информации». Порядок эксплуатации СКЗИ. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Рекомендации по стандартизации Р 1323565.1.025-2019 «Форматы сообщений, защищенных криптографическими методами». Вопросы нормативно-правовом регулирование в сфере интеллектуальной собственности. "Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 , «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66, а также «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утвержденных приказом ФСБ от 10.07.2014 № 378.

Самостоятельная работа. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. Федеральные законы Российской Федерации в области защиты информации, национальные стандарты Российской Федерации в области криптографической защиты информации. Классификация средств криптографической защиты информации. Принципы применения криптографических механизмов защиты. Вопросы правового регулирования и стандартизации в области криптографической защиты информации.

Рекомендуемая литература
основная: [1,2,3]
дополнительная: [1,2,3]

РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 4. Методы криптографической защиты информации. Криптографические алгоритмы

Лекция. Криптографические методы защиты конфиденциальной информации. Предпосылки использования криптографических средств защиты информации в МЧС России. Виды шифров. Алгоритмы симметричного и ассиметричного (шифрование с открытым ключом) шифрования. Основные понятия и классификация средств ассиметричной

криптографической защиты информации. Основные свойства асимметричных криптосистем. Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции.

Самостоятельная работа. Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Режимы работы блочных алгоритмов. ГОСТ Р 34. 12 - 2015, ГОСТ 34.13 - 2018. ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров». Алгоритм криптографического преобразования данных ГОСТ. Основные свойства хэш-функций. Использование блочных алгоритмов шифрования для формирования хеш-функции. Обзор алгоритмов формирования хеш-функций.

Рекомендуемая литература

основная: [1,2,3]

дополнительная: [1,2,3]

Тема 5. Средства криптографической защиты информации

Самостоятельная работа. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей.

РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ. ЦИФРОВАЯ ПОДПИСЬ

Тема 6. Основы криптографических протоколов

Лекция. Криптографические протоколы.

Классификация криптографических протоколов. Основные свойства и уязвимости криптографических протоколов. Понятия цикла, шага, роли и сеанса. Протокол обеспечения безопасности (security protocol). Перечень наиболее широко известных атак на криптографические протоколы

Самостоятельная работа. Понятие и виды криптографического криптографических протоколов. Свойства безопасности. Протокол конфиденциального обмена. Классификация методов анализа уязвимостей. Атаки на криптографические протоколы. Р 1323565.1.025-2019 «Информационная технология (ИТ). Криптографическая защита информации. Форматы сообщений, защищенных криптографическими

методами». ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Национальный стандарт РФ ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст).

Рекомендуемая литература
основная: [1,2,3]
дополнительная: [1,2,3]

Тема 7. Электронная (цифровая)подпись

Практические занятия. Цифровая подпись на основе алгоритмов с открытым ключом. Использование электронной подписи и признание ее действительности. Свойства цифровой подписи. Протоколы цифровой подписи, реализуемые с использованием ассиметричных криптосистем. Нормативная правовая база, регламентирующая электронную (цифровую) подпись. Использование электронной подписи в МЧС России. Признание действительности электронной подписи.

Самостоятельная работа. Электронная подпись. Сертификат ключа проверки электронной подписи. Квалифицированный сертификат. Квалифицированный сертификат ключа проверки электронной подписи. Владелец сертификата ключа проверки электронной подписи. Ключ электронной подписи. Ключ проверки электронной подписи. Удостоверяющий центр. Средства электронной подписи. Средства удостоверяющего центра. Подтверждение владения ключом электронной подписи. Метка доверенного времени. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей. Признание квалифицированной электронной подписи.

Рекомендуемая литература
основная: [1,2,3]
дополнительная: [1,2,3]

РАЗДЕЛ 5. УПРАВЛЕНИЕ КЛЮЧАМИ

Тема 8. Ключевая подсистема криптосистемы. Протоколы обмена ключами.

Практические занятия. Управление ключами в системах с открытым ключом. Алгоритм распределение ключей по схеме Диффи-Хелмана.

Самостоятельная работа. Управление ключами в системах с открытым ключом. Организационные и технические меры обеспечения секретности ключей. Разделение секрета. Рассылка ключей. Хранение ключей. Смена ключей. Протоколы обмена ключами. Особенности

ключевых систем для защиты данных, хранящихся в информационных системах.

Рекомендуемая литература
основная: [1,2,3]
дополнительная: [1,2,3]

5. Методические рекомендации по организации изучения дисциплины

При реализации программы дисциплины используются такие виды занятий: лекция и практическое занятие.

1. Лекция: составляет основу теоретического обучения и должна давать 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.

Ведущим методом в лекции выступает устное изложение учебного материала, сопровождающееся демонстрацией видео- и кинофильмов, слайдов, схем, использованием компьютерной техники.

На лекционных занятиях используется мультимедийный проектор с комплектом презентаций.

2. Практическое занятие: практическое занятие проводится в целях: выработки практических умений и приобретения навыков, закрепления пройденного материала по соответствующей теме дисциплины. Главным их содержанием является практическая работа каждого слушателя (обучающегося).

3. Консультации проводятся преподавателем, ведущим занятия в учебной группе и носят групповой характер.

4. Самостоятельная работа: направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим учебным занятиям, зачету с оценкой.

Самостоятельная работа обучающихся проводится в часы самостоятельной подготовки.

6. Оценочные материалы по дисциплине «Криптографические методы защиты информации»

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

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме зачета с оценкой.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса

1. Назовите основные стандарты в области информационной безопасности и защиты информации
2. Перечислите и дайте определение основным моделям доступа
3. Перечислите элементы структуры системы защиты государственной тайны
4. Назовите регуляторов в сфере защиты государственной тайны и зоны их ответственности
5. Перечислите порядок допуска должностных лиц и граждан к государственной тайне
6. Назовите типы каналов силового деструктивного воздействия на информационную систему;
7. Перечислите пути проникновения всплеска энергии для каждого из типов каналов силового деструктивного воздействия
8. Приведите классификацию технических каналов утечки информации
9. Дайте определение нетрадиционного информационного канала
10. Приведите классификацию компьютерных преступлений

Типовые задания для тестирования

1. Угроза информационной безопасности – это...
2. Уязвимость – это...
3. Какой степени секретности НЕ существует?
4. Основанием для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться...
5. К органам защиты государственной тайны относятся...
6. Государственную тайну составляют сведения...
7. Условием прекращения допуска к государственной тайне является...
8. Резонирующий емкостной накопитель подключили ко вторичной обмотке трансформаторной подстанции. Определите КСДВ.
9. Мощный разряд молнии в непосредственной близости. Определите КСДВ.

10. Внедрение программной закладки в источник бесперебойного питания. Определите КСДВ.

11. Наводки информационных сигналов в посторонних проводниках (фидерах). Выберите тип ТКУИ.

12. Перехват речевых сигналов направленными микрофонами. Выберите тип ТКУИ.

13. Приём информации, передаваемой закладными устройствами по электросети 220 В. Выберите тип ТКУИ.

14. Беспроводной прием информации, передаваемой закладными устройствами. Выберите тип ТКУИ.

15. Сколько страниц текстовой информации (2000 символов/страница) может быть сокрыто методами стеганографии в мегапиксельной фотографии формата bmp?

16. Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 30 секундах монозвучания файла формата wav?

17. Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 30 секундах стереозвучания файла формата wav?

18. Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 1 странице текстового файла?

19. Как размер криптограммы влияет на успешность и время дешифровки?

20. Сообщение какого объема можно зашифровать, используя «Решетку Кардано» с 15 прорезями для букв?

21. Сообщение какого максимального объема можно зашифровать, используя «Решетку Кардано» 10х10?

22. Компьютерная программа, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на компьютерную систему – это...

23. Дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом – это...

24. Ситуация, в которой один человек или программа успешно маскируется под другую путём фальсификации данных, что позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом – это...

6.1.2. Промежуточной аттестации

Примерный перечень вопросов к зачету с оценкой

1. Приведите примеры шифров, применявшихся еще до нашей эры?

2. Приведите пример шифра, для которого сам открытый текст является ключом?

3. Какие шифры являются омофонами, в чем их преимущество перед шифрами простой замены?

4. Какими шифрами пользовались Цезарь, Галилей, Наполеон? Что является ключом шифра Виженера?

5. Приведите пример шифра, допускающего неоднозначное зашифрование?

6. Дайте общую характеристику Федеральному закону «Об электронной подписи»?

7 .В чем состоит правило Керхгоффса, почему это правило является общепризнанным в криптографии?

8. Назовите действующие нормативные правовые документы ФСБ России в криптографической сфере?

9 . Дайте общую характеристику алгоритмов шифрования из действующих стандартов?

10. Чем отличаются симметричные от асимметричных шифрсистем?

11.Какие средства относятся к СКЗИ согласно законодательству Российской Федерации?

12.Раскройте, в чем заключается обеспечение режима защиты информации путем использования СКЗИ?

13. Назовите особенности обеспечения криптографической защиты информации в автоматизированной (информационной) системе федерального органа исполнительной власти?

14.Когда родилась криптография с открытыми ключами и первая реальная система шифрования?

15. Каких выдающихся криптографов XX в. Вы знаете?

16. Чем отличаются подходы к обеспечению безопасности информации в криптографии и в методах сокрытия информации?

17. Какие средства используются для обеспечения невозможности отказа от авторства ключей?

18. Какими методами обеспечивается конфиденциальность информации?

19. В чем разница между обычным и открытым распределением ключей

20 .Для чего нужны схемы разделения секрета?

21. Что такое сертификат открытого распределения ключей?

22. Каковы функции центра сертификации ключей?

23. Чем отличаются алгебраическая и вероятностная модели шифра?

24. С какими целями в криптографии вводятся модели открытых текстов?

25. С какими примерами шифров замены и перестановки вы познакомились в историческом обзоре?

26. Существуют ли шифры, не являющиеся ни шифрами замены, ни шифрами перестановки?

27. Приведите пример шифра многозначной замены?

28. Может ли блочный шифр быть шифром разнозначной замены?

29. Приведите пример шифра перестановки, который может рассматриваться и как блочный шифр замены?

30. Как определить по криптограмме, полученной с помощью шифра вертикальной перестановки, число коротких столбцов заполненного открытым текстом основного прямоугольника?

31. Какие свойства открытого текста используются при вскрытии шифра вертикальной перестановки?

32. Какие шифры называются шифрами простой замены?

33. Что является ключом шифра простой замены, каково максимально возможное число ключей шифра простой замены?

34 Что более целесообразно для надежной защиты информации: архивация открытого текста с последующим зашифрованием или шифрование открытого текста с последующей архивацией?

35. Является ли надежным шифрование литературного текста с помощью модульного гаммирования, использующего гамму, два знака которой имеют суммарную вероятность, совпадающую с суммарной вероятностью остальных знаков?

36. Почему наложение на открытый текст гаммы, представляющей собой периодическую последовательность небольшого периода, не дает надежной защиты?

37. Почему недопустимо использовать дважды одну и ту же гамму для зашифрования разных открытых текстов?

41. Почему в качестве гаммы нецелесообразно использовать текст художественного произведения?

42. Как можно качественно охарактеризовать избыточность языка?

43. Почему неопределенность шифра по открытому тексту (или по ключу)

можно рассматривать как меру теоретической стойкости шифра?

44. Как зависит расстояние единственности для шифра от энтропии языка?

45. Найдите расстояние единственности для шифра Виженера, который используется для шифрования технических текстов на русском языке с избыточностью 0,8?

46. Какие атаки используются в криптоанализе?

47.Какой шифр называется совершенным (для атаки на основе шифртекста) ?

48.В каком случае шифр модульного гаммирования является совершенным (для атаки на основе шифртекста) ?

49.Чем отличаются понятия теоретической и практической стойкости шифра?

50.Что такое имитостойкость шифра, что может служить мерой имитостойкости шифра, является ли шифр гаммирования имитостойким?

51.Что такое совершенная имитостойкость шифра?

52. Является ли шифр гаммирования шифром, не размножающим искажения типа «замена знаков», искажения типа «пропуск знаков»?

53. Каковы с точки зрения криптографии преимущества и недостатки перехода к шифрованию сообщений в алфавитах большой мощности?

54.Как реализуется предложенный К. Шенноном принцип «перемешивания» при практической реализации алгоритмов блочного шифрования?

55.Каковы основные недостатки алгоритма DES, и каковы пути их устранения?

56. Как связан «парадокс дней рождения» с криптографическими качествами блочных шифров в режиме простой замены?

57.В каких случаях можно рекомендовать использование блочного шифра в режиме простой замены?

58.От каких потенциальных слабостей позволяет избавиться использование блочных шифров в режимах шифрования с обратной связью?

59.Почему возникает проблема синхронизации поточных шифров?

60.Какой необходимый минимум функциональных возможностей должен быть заложен в шифрующем блоке?

61.За счет чего можно обеспечить стойкость алгоритма шифрования при повторном использовании ключей?

62. Какие причины обусловили широкое использование линейных регистров сдвига в качестве управляющих блоков поточных шифрсистем?

63. В чем состоят преимущества систем с открытыми ключами перед симметричными шифрсистемами?

64. К какому типу принадлежит схема шифрования, используемая в системе Эль-Гамаля, в чем ее преимущества?

65. На какие группы могут быть разбиты алгоритмы идентификации?

66. За счет чего повышается надежность идентификации при использовании пластиковой карты и личного идентификационного номера?

67. Каковы возможные схемы использования одноразовых паролей?

68. Какая идея лежит в основе протоколов с нулевым разглашением?

69. Для каких целей применяются хеш-функции?

70. Перечислите основные требования, предъявляемые к хеш-функциям?

71. Почему нельзя использовать в качестве хеш-функций линейные отображения?

72. Сравните требования, предъявляемые к ключевым и бесключевым хеш-функциям?

73. Можно ли использовать в качестве бесключевой хеш-функции ключевую хеш-функцию с фиксированным ключом?

74. Что общего между обычной и электронной подписями, чем они различаются?

75. Какие задачи позволяет решить электронная подпись?

76. В чем заключается принципиальная сложность в практическом применении систем электронной подписи?

77.Для чего необходим удостоверяющий центр?

78. Почему в криптографических системах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и цифровой подписи?

79. Каковы преимущества централизованного распределения ключей?

80.Каким образом распространяются сертификаты открытых систем в криптосистемах?

81.Что понимается под термином «управление криптографическими ключами»?

82. Какова основная цель и основные задачи управления ключами?

83. Что такое целостность информации?

84 . Для каких аспектов информационного взаимодействия необходима аутентификация?

85. В чем суть предварительного распределения ключей?

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
зачет с оценкой	правильность и полнота ответа	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
		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
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	удовлетворительно
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность	неудовлетворительно

		изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	

7. Ресурсное обеспечение дисциплины

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

Microsoft Windows 7 Professional – ПО-BE8-834 [Лицензионное]

Microsoft Office Standard 2010 – ПО-413-406 [Лицензионное]

7-Zip – ПО-F33-948 [Свободно распространяемое]

Adobe Acrobat Reader – ПО-F63-948 [Свободно распространяемое]

Google Chrome – ПО-F2C-926 [Свободно распространяемое]

МойОфис Образование – ПО-41B-124 [Свободно распространяемое - Отечественное]

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. Электронная библиотека Санкт-Петербургского университета ГПС МЧС России: http://elib.igps.ru

4. Электронно-библиотечная система IPRBOOK: http://www.iprbookshop.ru/

5. Электронно-библиотечная система ЛАНЬ: https://e.lanbook.com/

7.3. Литература

Основная:

1. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89455.html

2. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. —

Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102017.html

3. Майстренко, Н. В. Основы теории информации и криптографии : учебное пособие / Н. В. Майстренко, А. В. Майстренко. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2018. — 81 с. — ISBN 978-5-8265-1950-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/94362.html

Дополнительная:

1. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. –300 с. Режим доступа: http://elib.igps.ru/?4&type=card&cid=ALSFR-6d86bbe6-aeac-49db-bc2e-068c7a55cb8d&remote=false

2. Бахаров, Л. Е. Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л. Е. Бахаров. — Москва : Издательский Дом МИСиС, 2019. — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98171.html

3. Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 95 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/17925.html

7.4. Материально-техническое обеспечение

Для материально-технического обеспечения дисциплины используются аудитории для проведения лекционных, практических занятий, промежуточной аттестации, самостоятельной работы обучающихся.

Материально-техническими средствами обучения дисциплины являются:

- мультимедийный проектор;
- экран;
- магнитная доска;
- наглядные пособия;
- интерактивная доска;
- компьютеры с выходом в интернет.

Автор: к.ю.н. Метельков А.Н.