

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«**Российский государственный гуманитарный университет**»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра комплексной защиты информации

**КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ В СОЦИОТЕХНИЧЕСКИХ
СИСТЕМАХ**
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

01.04.04 Прикладная математика

Код и наименование направления подготовки/специальности

Математические методы и модели обработки
и защиты информации в социотехнических системах

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *магистратура*

Форма обучения: *очная, заочная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ
Рабочая программа дисциплины

Составитель(и):

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор

Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО

Протокол заседания кафедры

Комплексной защиты информации

№ 8 от 14.03.2024

Оглавление

1. Пояснительная записка.....	4
1.1. Цель и задачи дисциплины.....	4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций.....	4
1.3. Место дисциплины в структуре образовательной программы.....	4
2. Структура дисциплины.....	4
3. Содержание дисциплины.....	5
4. Образовательные технологии.....	7
5. Оценка планируемых результатов обучения.....	8
5.1 Система оценивания.....	8
5.2 Критерии выставления оценки по дисциплине.....	8
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине.....	9
6. Учебно-методическое и информационное обеспечение дисциплины.....	11
6.1 Список источников и литературы.....	11
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».....	13
6.3 Профессиональные базы данных и информационно-справочные системы.....	13
7. Материально-техническое обеспечение дисциплины.....	13
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов.....	14
9. Методические материалы.....	15
9.1 Планы практических занятий.....	15
Приложение 1. Аннотация рабочей программы дисциплины.....	17

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – получение основных представлений об использовании криптографических методов для защиты информации при её хранении, обработке и дистанционной передаче электронных данных.

Задачи дисциплины:

- овладение студентами основными криптографическими понятиями;
- научить студентов решать типовые криптографические задачи, востребованные практикой;
- научить студентов работать со специальной криптографической литературой и нормативными документами;
- использование полученных знаний для решения прикладных задач современной криптографии.

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

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-2. Способен осуществлять поиск, изучение и разработку новых теоретических или практических проблем, сведений, относящихся к решению текущих научных исследований, производственных задач; в информационных средах находить, создавать основные элементы будущих математических структур или конструктивных математических моделей	ПК-2.2– Рассматривает социотехнические системы как совокупность информационных систем ПК-2.3 -Выделяет информационные потоки, определяет точки бифуркаций ПК-2.4- Строит математические модели различных типов, исследует их ПК-2.5 -В совершенстве владеет методами передачи информации и применения пакетов прикладных программ	Знать: основные модели, методы и средства криптографической защиты информации Уметь: решать типовые криптографические задачи защиты информации; Владеть: методами проведения экспериментов в области синтеза и анализа криптографических систем и протоколов и оценки их результатов.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические приложения в социотехнических системах» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Криптография в социотехнических системах», «Основы современных технологий коммуникации в социотехнических системах».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения практик: Производственная практика (Научно-исследовательская работа).

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 5 з.е., 180 академических часа(ов).

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	16
3	Практические занятия	34
Всего:		50

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 130 академических часа(ов).

Структура дисциплины для заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	-
3	Лабораторные	12
Всего:		12

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 96 академических часа(ов).

3. Содержание дисциплины

Тема 1. Введение в дисциплину

Общие положения криптологии. Базовые криптографические термины, понятия и определения. Классическая и математическая криптография. Стойкость криптографических схем (неформальное введение).

Тема 2. Роль и место криптографических методов в защите современных информационных систем

Базовая эталонная модель Взаимосвязи открытых систем (ISO/OSI). Архитектура защиты ISO/OSI, криптографические услуги и механизмы. Основные положения ГОСТ Р ИСО 7498-2-99. Криптографические услуги и механизмы в стеке протоколов TCP/IP.

Тема 3. Базовые криптографические методы и схемы криптографической защиты информации

Криптосистемы с секретным ключом, атаки на криптосистемы с секретным ключом. Криптосистемы с открытым ключом, открытое распределение ключей Диффи-Хеллмана, атаки на криптосистемы с открытым ключом. Теоретическая и практическая стойкость криптосистем. Схемы электронной подписи. Криптографически стойкие хэш-функции. Методы поиска коллизий.

Элементы теории вычислительной сложности. Односторонние функции и функции с секретом. Псевдослучайные генераторы. Интерактивные системы доказательств и интерактивные системы доказательств с нулевым разглашением. Схемы с сокрытием свидетельства и с неразличимыми свидетельствами. Схемы вероятностного шифрования.

Разновидности схем электронной подписи. Схемы конфиденциальной подписи. Схемы групповой подписи. Схемы мультиподписи. Схемы затемнённой подписи. Схемы подписи для интеллектуальных карточек. Схемы подписи вида «офф-лайн/он-лайн». (n, t) -пороговые схемы

подписи. Процедуры арбитража в схемах электронной подписи. Практические схемы интерактивной аутентификации.

Тема 4. Криптографические протоколы

Основы теории криптографических протоколов. Свойства и основные параметры криптографических протоколов. Классификация основных видов атак на криптографические протоколы.

Протоколы аутентификации. Требования к протоколам аутентификации. Парольная аутентификация (протоколы с фиксированными паролями, протоколы с одноразовыми паролями). Протоколы типа «запрос – ответ» (односторонняя аутентификация, основанная на метке времени, односторонняя аутентификация с использованием случайных чисел, протоколы с использованием асимметричных криптосистем, протоколы с использованием электронной подписи). Протоколы аутентификации, основанные на использовании интерактивных систем доказательств с нулевым разглашением знания.

Протоколы распределения ключей. Сферы применения протоколов распределения ключей. Классификация протоколов распределения ключей. Протоколы, основанные на криптосистемах с секретным ключом. Протоколы распределения ключей, основанных на криптосистемах с открытым ключом.

Протоколы образования защищённых каналов передачи данных. Основные используемые на практике методы организации защищённых каналов передачи данных. Гибридные схемы шифрования. Протоколы, одновременно обеспечивающие конфиденциальность и аутентичность информации.

Тема 5. Криптографические приложения в современных информационных системах

Протоколы образования защищённых каналов передачи данных: PPTP, TLS, SSH, SSL, HTTPS, IPSec, другие протоколы.

Основные положения Федерального закона «Об электронной подписи», ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Принципы использования, виды и средства электронных подписей. Удостоверяющие центры. Сертификаты ключей проверки электронной подписи.

Электронный документооборот, электронная почта и их криптографическая защита. Обеспечение конфиденциальности, целостности, аутентификации электронных сообщений, невозможности отказа от их авторства. Примеры реализации систем защищённого электронного документооборота и защищённой электронной почты.

Системы электронных платежей (СЭП). Криптографические аспекты функционирования СЭП. Анонимные и неанонимные СЭП. СЭП реального времени.

Банковские информационные технологии и криптографические сервисы. Технологии Банка России, технологии SWIFT. Системы дистанционного банковского обслуживания. Системы платежей по банковским картам. Интеллектуальные карты и криптографические особенности их применения в банковском деле. Стандарт Банка России СТО БР ИББС 1.0.

Другие криптографические приложения и криптографические сетевые сервисы. Анонимные сети. Беспроводные сети. Криптографические протоколы для облачных вычислений. Защищённые NFC-соединения. Защищённая трансляция контента.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение в дисциплину	Лекция 1 Самостоятельная работа	Лекция-визуализация с применением слайд-проектора Изучение материалов. Консультация посредством

			электронной почты (ЭП)
2	Роль и место криптографических методов в защите современных информационных систем	Лекция 2 Самостоятельная работа	Лекция-визуализация с применением слайд-проектора Изучение материалов. Консультация посредством (ЭП)
3	Базовые криптографические методы и схемы криптографической защиты информации	Лекция 3. Самостоятельная работа	Лекция-визуализация с применением слайд-проектора Изучение материалов. Консультация посредством (ЭП)
4	Криптографические протоколы	Лекция 4. Самостоятельная работа	Лекция-визуализация с применением слайд-проектора Изучение материалов. Консультация посредством (ЭП)
5	Криптографические приложения в современных информационных системах	Лекция 5. Самостоятельная работа	Лекция-визуализация с применением слайд-проектора Изучение материалов. Консультация посредством (ЭП)
6	Практическое занятие № 1. Исследование криптографических протоколов при помощи Wireshark	Практическое занятие. Самостоятельная работа	Выполнение практической работы. Составление и защита отчёта. Изучение материалов. Консультация посредством (ЭП)
7	Практическое занятие № 2. Исследование криптографических протоколов RADIUS и TACASC+ в симуляторе Cisco Packet Tracer	Практическое занятие Самостоятельная работа	Выполнение практической работы. Составление и защита отчёта. Консультация посредством электронной почты (ЭП)
8	Практическое занятие № 3. Создание VPN-канала в симуляторе Cisco Packet Tracer	Практическое занятие Самостоятельная работа	Выполнение практической работы. Составление и защита отчёта. Консультация посредством электронной почты (ЭП)

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего

Текущий контроль: – <i>опрос</i> – <i>выполнение практических работ</i>	5 баллов 10 баллов	30 баллов 30 баллов
Промежуточная аттестация – зачет с оценкой (Зачёт по билетам)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно		не зачтено
0 – 19		F	

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетворительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет- ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль

Примерные вопросы для устного опроса

- Каковы основные свойства криптографической системы и криптографического протокола? Приведите примеры процедур обмена сообщениями, которые являются раундами и шагами криптографических протоколов.
- В чём заключаются свойства полноты и корректности интерактивного доказательства?
- В чём отличие интерактивных систем доказательства с нулевым разглашением знания от интерактивных систем доказательства? Сохраняется ли свойство нулевого разглашения при последовательном и параллельном выполнении протоколов?
- Что понимается под компрометацией криптографического протокола? Приведите примеры: атаки по известным ключам; словарной атаки.
- Имеется схема открытого шифрования RSA. d – секретный ключ участника P , e – открытый ключ, соответствующий этому секретному ключу, n – модуль схемы шифрования. P имеет шифртекст C . P хочет доказать V знание секретного ключа d , но так, чтобы V не узнал этот ключ, и чтобы он не смог расшифровать какой-либо шифртекст (в том числе и C). Как это можно сделать? (Предложите протокол доказательства с нулевым разглашением знания.) Вычислительные возможности P и V в процессе обмена полиномиально ограничены.
- Известна формула Андерсена определения длины пароля:

$$S_t = \frac{1}{2} N^x \cdot \frac{L}{T},$$

где S_t – время безопасности (раскрытия) пароля (в течение этого времени пароль сохраняет тайну);

T – скорость ввода пароля, симв./мин.;

x – длина пароля, симв.;

N – мощность алфавита;

L – число вводимых символов и др. знаков, необходимых для инициализации опознания (может быть больше длины пароля).

Постройте графики зависимости времени безопасности:

а) PIN-кода;

б) цифро-алфавитного пароля (русский алфавит)

от длины пароля при условии:

ручного ввода символов на клавиатуре ($T=120$);

автоматизированного подбора паролей ($T=1200$),

считая, что число попыток ввода пароля не ограничено, а для ввода пароля необходимо набрать его на клавиатуре и нажать клавишу <Enter>.

7. Проведите сравнение протоколов аутентификации, основанных на доказательствах с нулевым разглашением знания (Фиата – Шамира, Гийю-Кискатера, Шнорра), по следующим параметрам: вычислительной сложности протокола для доказывающего и проверяющего, количеству передаваемых байтов данных, дополнительной памяти, необходимой P и V . Сделайте вывод о сравнительной эффективности протоколов. (Необходимые параметры выберите самостоятельно.)

8. Как преобразовать протокол аутентификации Шнорра в схему электронной подписи?

9. Предположим, что к данным, предназначенным для передачи в канал связи, согласно техническим условиям, отправителю необходимо применить: алгоритм блочного шифрования (шифр считать идеальным), алгоритм помехоустойчивого кодирования, алгоритм сжатия. В каком порядке следует применять эти алгоритмы и почему? На каком этапе в случае необходимости нужно сгенерировать электронную подпись отправителя? Имеет ли эта задача однозначное решение?

10. Поясните, в каких случаях для обеспечения подлинности сообщений необходимо применять электронную подпись, а в каких – хэш-функции с ключом? В чем преимущества и недостатки каждого метода?

11. Приведите основные положения Федерального закона «Об электронной подписи», ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012. Расскажите об принципах использования, видах и средствах электронных подписей, об удостоверяющих центрах и сертификатах ключей проверки электронной подписи.

Промежуточная аттестация

Примерные контрольные вопросы к зачёту с оценкой

1. Пусть (E, D) – схема симметричного шифрования, MAC – криптографическая хэш-функция с ключом. Пусть A и B имеют общие ключи: K_1 – для шифрования, K_2 – для хэш-функции. Они хотят передать сообщение m таким образом, чтобы была обеспечена секретность, целостность и подлинность сообщения. Им предложены следующие способы выполнения протокола:

а) $M, MAC_{K_2}(E_{K_1}(M))$;

б) $E_{K_1}(M, MAC_{K_2}(M))$;

в) $E_{K_1}(M), MAC_{K_2}(M)$;

г) $E_{K_1}(M), E_{K_1}(MAC_{K_2}(M))$;

д) $E_{K_1}(M), MAC_{K_2}(E_{K_1}(M))$;

е) $E_{K_1}(MAC_{K_2}(M)), MAC_{K_2}(E_{K_1}(M))$;

ж) $E_{K_1}(M, MAC_{K_2}(M)), MAC_{K_2}(M)$;

и) $E_{K_1}(M, A)$, где A – идентификатор отправителя (B расшифровывает шифртекст и проверяет, что вторая часть открытого текста совпадает с идентификатором отправителя).

Для каждого способа объясните, обеспечивает ли он требуемые свойства (секретности, целостности, подлинности)? Какие из этих способов предпочтительнее? Какие не пригодны для использования? Почему?

2. Назовите известные Вам режимы работы блочных шифров, позволяющие обеспечить:

только секретность сообщений;
только подлинность сообщений;
одновременно секретность и подлинность сообщений.

Какие из этих режимов считаются лучшими по соотношению «стойкость/скорость»?

3. Какие режимы алгоритмов шифрования ГОСТ 28147-89 и DES предпочтительнее использовать для шифрования полей базы данных автоматизированной банковской системы с интеллектуальной карточкой, содержащей сведения о клиентах (идентификаторы, открытые ключи, номера интеллектуальных карточек, состояние счета, отметка о включении интеллектуальных карточек в стоп-лист и т.д.), доступ к которой осуществляется в режиме реального времени, и почему?

4. Рассматривается схема электронной подписи с восстановлением сообщения из стандарта ISO/IEC 9796. Какой максимальной длины (в байтах) может быть сообщение, если требуется, чтобы подпись имела длину 512 битов?

5. Какие функции может выполнять центр доверия в протоколах распределения ключей? Приведите примеры.

6. В чем разница между понятиями: способы распространения ключей и протоколы распределения ключей?

7. Опишите схему Д. Чома со следующими параметрами: банкноты имеют разное достоинство, сумма, оплачиваемая продавцу, составляет 7 рублей, максимальная сумма, оплачиваемая покупателем, составляет 21 рубль.

8. Приведите протокол конфиденциально реализуемой операции умножения переменной на константу с использованием (t, n) -пороговой схемы Шамира.

9. Приведите примеры реализации систем защищённого электронного документооборота и защищённой электронной почты.

10. Приведите примеры реализации систем дистанционного банковского обслуживания и системы платежей по банковским картам. Расскажите об основных положениях Стандарта Банка России СТО БР ИББС 1.0.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. *Федеральный закон* от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., посл. от 01.05.2019). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* от 27 июля 2006 г. №152-ФЗ «О персональных данных» (с изм. и доп., посл. от 31.12.2017). [Электронный ресурс]: Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *Федеральный закон* от 6 апреля 2011 г. №63-ФЗ «Об электронной подписи» (с изм. и доп., посл. от 23.06.2016). [Электронный ресурс]: Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_112701/, свободный. – Загл. с экрана.
4. *Федеральный закон* от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании» (с изм. и доп., посл. от 29.07.2017). [Электронный ресурс]: Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.
5. *Постановление Правительства Российской Федерации* от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных(криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных

- (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)». (с изм. и доп., посл. от 18.05.2017). [Электронный ресурс]: Режим доступа : <http://www.consultant.ru/cons/cgi/online.cgi?rnd=8BEAE327715772BF511477DA184EFA2&req=doc&base=LAW&n=217125&dst=100007&fld=134&stat=refcode%3D16876%3Bdstident%3D100007%3Bindex%3D0#rnlenft0qj>, свободный. – Загл. с экрана.
6. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утв. Приказом Директора ФСБ России от 09 февраля 2005 года № 66. (с изм. и доп., посл. от 12.04.2010) [Электронный ресурс] : Режим доступа : <https://base.garant.ru/187947/>, свободный. – Загл. с экрана.
7. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». [Электронный ресурс]: Режим доступа : <http://docs.cntd.ru/document/1200007350>, свободный. – Загл. с экрана.
8. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». – Взамен ГОСТ Р 34.10-2001. [Электронный ресурс]: Режим доступа : <http://docs.cntd.ru/document/1200095034>, свободный. – Загл. с экрана.
9. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». [Электронный ресурс]: Режим доступа : <http://docs.cntd.ru/document/1200095035>, свободный. – Загл. с экрана.
10. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». [Электронный ресурс]: Режим доступа : <http://docs.cntd.ru/document/1200121983>, свободный. – Загл. с экрана.
11. ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров». [Электронный ресурс]: Режим доступа : <http://docs.cntd.ru/document/1200121984>, свободный. – Загл. с экрана.

Литература

Основная

- Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог: Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст: электронный. - URL: <https://znanium.com/catalog/product/991903> – Режим доступа: по подписке.
- Рябко, Б. Я. Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н., 2-е изд. - Москва : Гор. линия-Телеком, 2013. - 232 с. ISBN 978-5-9912-0350-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/427831>. – Режим доступа: по подписке.
- Цифровой бизнес: учебник / под науч. ред. О.В. Китовой. – Москва : ИНФРА-М, 2019. – 418 с. – (Высшее образование: Магистратура). – www.dx.doi.org/10.12737/textbook_5a0a8c777462e8.90172645. – ISBN 978-5-16-106396-5. – Текст : электронный. – URL: <https://new.znanium.com/catalog/product/989795>
- Криптографические методы защиты информации: Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. – 2-е изд., стереотип. - М.: Гор. линия-Телеком, 2012. – 229 с.: ил.; 60x90 1/16.

– (Специальность). (обложка) ISBN 978-5-9912-0286-2, 500 экз. – Режим доступа: <http://znanium.com/catalog/product/370317>.

Дополнительная

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/437163>.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf
2. Введение в криптографию/ Под общ. ред. В.В. Ященко. [Электронный ресурс]. – Режим доступа: <http://nature.web.ru/db/msg.html?mid=1157083&uri=book.html>

Национальная электронная библиотека (НЭБ) www.rusneb.ru
 ELibrary.ru Научная электронная библиотека www.elibrary.ru
 Электронная библиотека Grebennikon.ru www.grebennikon.ru
 Cambridge University Press
 ProQuest Dissertation & Theses Global
 SAGE Journals
 Taylor and Francis
 JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

- 1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Cisco Packet Tracer v.7.2
6. WireShark v.2.16 и выше

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA SE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Практическое занятие № 1. Исследование криптографических протоколов при помощи Wireshark

Задания:

1. Установка (при необходимости) анализатора трафика (сниффера) *Wireshark*.
2. Изучение интерфейса и правил работы с *Wireshark*.
3. Выполнить соответствующую настройку сниффера.
4. Создать пользовательские переменные среды для работы с защищёнными протоколами.
5. При необходимости создать временные учётные записи в соц. сетях Одноклассники, ВКонтакте и *Facebook*. Закрыть указанные страницы.
6. Очистить кэш браузера.
7. Включить захват трафика.
8. Войти в одну из соцсетей. Осуществить обмен сообщениями по выданному списку с другими пользователями сети (студентами группы). Выйти из соцсети.
9. Выделить пакеты данной соцсети и попытаться расшифровать сообщения, которыми обменивались в соцсети. Сделать скриншоты для отчёта.
10. Шаги 6...9 проделать для двух оставшихся соцсетей.
11. Включить захват трафика.
12. Открыть онлайн-банкинг. Проверить свой счёт. Выйти из банкинга. Остановить захват трафика. Попытаться расшифровать содержимое пакетов, переданных или полученных от банка.
13. Составить отчёт о практическом занятии.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изучить интерфейса и правил работы с *Wireshark*.
3. Ответить на теоритические вопросы при защите отчёта

Практическое занятие № 2. Исследование криптографических протоколов RADIUS и TACASC+ в симуляторе Cisco Packet Tracer

Задания:

1. Установка (при необходимости) ППП *Cisco Packet Tracer (CPT)*.
2. Изучение интерфейса *CPT*, режимов *CLI* настроек сетевых устройств в *CPT*.
3. При помощи преподавателя разработать схему сети гипотетической организации.
4. Составить топологию сети в *CPT*. Обязательно добавить сниффер на компьютер «нарушителя».

5. Продемонстрировать работу сети и перехват трафика нарушителем при открытом обмене и при использовании протоколов *RADIUS* и *TACASC+*.
6. Изучить структуру пакетов, в т.ч. и перехваченные «злоумышленником».
7. Составить отчёт о практическом занятии.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Изучить интерфейс *CPT*, режимы реального времени и симуляции, режимов *CLI* настроек сетевых устройств в *CPT*.
3. Преподаватель выдаёт каждому студенту пространство IP-адресов для работы.
4. Ответить на теоритические вопросы при защите отчёта

Практическое занятие № 3. Создание VPN-канала в симуляторе Cisco Packet Tracer

Задания:

1. Разработать схему сети между центральным офисом и филиалом.
2. Создать VPN-канал между филиалом и центральным офисом.
3. Настроить центр авторизации AAA.
4. Оформить отчёт о занятии.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому студенту адресное пространство частных сетей и адресов «провайдера».
2. Ответить на теоритические вопросы при защите отчёта

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Криптографические приложения в социотехнических системах» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: получение основных представлений об использовании криптографических методов для защиты информации при её хранении, обработке и дистанционной передаче электронных данных.

Задачи: овладеть студентами основными криптографическими понятиями; научить студентов решать типовые криптографические задачи, востребованные практикой; научить студентов работать со специальной криптографической литературой и нормативными документами; использование полученных знаний для решения прикладных задач современной криптографии.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен осуществлять поиск, изучение и разработку новых теоретических или практических проблем, сведений, относящихся к решению текущих научных исследований, производственных задач; в информационных средах находить, создавать основные элементы будущих математических структур или конструктивных математических моделей.

В результате освоения дисциплины обучающийся должен:

Знать: основные положения криптологии и практики криптографической защиты информации в социотехнических системах и требования к такой защите; основные модели, методы и средства криптографической защиты информации; классификацию математических моделей криптографических систем и криптографических протоколов.

Уметь: проводить экономический анализ работ по криптографической защите информации в современных социотехнических системах; применять существующие криптографические системы и криптографические протоколы в области социотехнических систем; решать типовые криптографические задачи защиты информации.

Владеть: способами защиты информационных систем от атак; методами обоснования оптимальности принятых криптографических решений с учётом различных требований регуляторов в этой области; методами проведения экспериментов в области синтеза и анализа криптографических систем и протоколов и оценки их результатов; навыками проверки адекватности математических моделей и соответствующих криптографических протоколов и схем, получивших применение в современных социотехнических системах.

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.

Общая трудоёмкость освоения дисциплины составляет 5 зачётных единиц.