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

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)
Организация и технология защиты информации
(по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 31.03.2022

Оглавление

1. Пояснительная записка

1.1. Цель и задачи дисциплины

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

Задачи дисциплины: овладение студентами основными понятиями, математическими моделями и методами современной криптографии, умение студентами: решать типовые криптографические задачи; работать со специальной математической литературой, использовать математический аппарат для решения прикладных криптографических задач защиты информации в различных сферах человеческой деятельности.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Способен применять соответствующий математический аппарат для решения профессиональных задач	Уметь: решать типовые криптографические задачи защиты информации;
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Владеть: навыками использования положений стандартов в области СКЗИ при разработке, настройке и эксплуатации
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знать: математические модели кодирования систем информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
	ОПК-9.2 Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	Уметь: применять теоретические знания при разработке ОРД; применять информационные технологии для поиска и обработки информации; применять математические модели для оценки стойкости СКЗИ
	ОПК-9.3 Владеет методами и средствами криптографической и технической защиты информации	Владеть: навыками поиска нужной информации в нормативных базах и источниках; навыками эксплуатации криптографиче-

		ских протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем электронного документооборота

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Теория информации».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практик: «Практика по получению профессиональных умений и опыта профессиональной деятельности по технической защите информации, «Преддипломная практика».

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов

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
6	Лекции	**24**
6	Практические занятия	**36**
	Всего:	**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 48 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Введение в дисциплину**	Общие положения криптологии. Базовые криптографические термины, понятия и определения. Классическая и математическая криптография. Стойкость криптографических схем (неформальное введение).
2	**История криптографии**	Эра донаучной криптографии. Шифр «Сциталь», шифры Цезаря, Полибия, Тритемия, Кардано, Порты, Виженера, большой и малый шифр Наполеона. Формы византийской тайнописи. Древнерусские шифры «Пермская азбука», «Простая и мудрая литорея», «Фиоть и Хвиоть», «Уголки», «Тарабарщина». Шифр Вернама.

		Шифровальные машины «Lorenz» и «Enigma».
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 затемненной 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.
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 защищенных каналов

		передачи данных. Основные используемые на практике методы организации защищенных каналов передачи данных. Гибридные схемы шифрования. Протоколы, одновременно обеспечивающие конфиденциальность и аутентичность информации. Банковские криптографические протоколы. Электронные монеты и переводимые электронные монеты. Электронный бумажник. Электронные платежи. Протоколы конфиденциальных вычислений и конфиденциального вычисления функции.
5	**Нормативные акты, регламентирующие деятельность в области криптографической защиты информации**	Федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «О техническом регулировании». Постановление Правительства Российской Федерации от 23 сентября 2002 года №691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами». Положение о разработке, производ-стве, реализации и эксплуатации шифровальных (криптографических) средств защиты ин-формации (Положение ПКЗ-2005), утв. Приказом Директора ФСБ России от 09 февраля 2005 года №66. Отечественные (криптографические) ГОСТЫ: ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.
6	**Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке**	Организации, осуществляющие деятельность в области криптографической защиты информации. Линейка продуктов «КриптоПро». Линейка продуктов «Secret Disk». Защищенный абонентский пункт системы «Атлас» (изделие М-468Р). Решения ФГУП «НТЦ «Атлас» по созданию защищенных (до класса АК3) автоматизированных систем на платформе Майкрософт. СКЗИ «Крипто БД». Другие продукты и услуги в области криптографической защиты информации.

4. Образовательные технологии

При реализации рабочей программы дисциплины «Криптографические методы защиты информации» используются следующие образовательные технологии:

Образовательные технологии

№ п/п	Наименование темы	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1	Введение в дисциплину	Лекция 1.1 Лекция 1.2 Самостоятельная работа	Традиционная с использованием презентаций Подготовка к занятиям с использованием ЭБС
2	История криптографии	Лекция 2.1 Лекция 2.2 Практическое занятие 1. Самостоятельная работа	Лекция-дискуссия Тестирование Занятия с использованием специализированного ПО – S-Tools Подготовка к занятиям с использованием ЭБС
3	Базовые криптографические методы и схемы криптографической защиты информации	Лекция 3.1 Лекция 3.2 Практическое занятие 2. Самостоятельная работа	Лекция-дискуссия Тестирование Занятия с использованием специализированного ПО – Masker Подготовка к занятиям с использованием ЭБС
4	Криптографические протоколы	Лекция 4.1 Лекция 4.2 Лекция 4.3 Практические занятия 3. Самостоятельная работа	Проблемная лекция Традиционная с использованием презентаций Тестирование Занятия с использованием специализированного ПО – VeraCrypt Подготовка к занятиям с использованием ЭБС
5	Нормативные акты, регламентирующие деятельность в области криптографической защиты информации	Лекция 5.1 Лекция 5.2 Лекция 5.3 Практическое занятие 4. Самостоятельная работа	Лекция с разбором конкретных ситуаций Тестирование Занятия с использованием специализированного ПО – Крипто-Про Подготовка к занятиям с использованием ЭБС
6	Средства и услуги в области криптографической защиты информации,	Лекция 6.1 Лекция 6.2	Лекция-дискуссия Тестирование

№ п/п	Наименование темы	Виды учебных занятий	Образовательные технологии
	представленные на отечественном рынке	Практическое занятие 5. Самостоятельная работа	Занятия с использованием специализированного ПО – Крипто-Про Подготовка к занятиям с использованием ЭБС

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль: *- тестирование (темы 2-6)* *- практические задания (темы 2-3)* *- практические задания (темы 4-6)*	 *2 баллов* *10 баллов* *10 баллов*	 *10 баллов* *20 баллов* *30 баллов*
Промежуточная аттестация - зачет *(Ответы на вопросы)*		*40 баллов*
Итого за семестр		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	*Контролируемые разделы дисциплины*	*Код контролируемой компетенции*	*Наименование оценочного средства*
1.	Темы 1 – 6	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2.1; УК-2.2;	Опрос
2.	Практические занятия 1 – 5	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2.1; УК-2.2	План практического занятия

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	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	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 выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	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 выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	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. 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	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

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности - проверка сформированности компетенций УК-2, ОПК-9

Контрольные задания	**Проверяемые компетенции**
1.Каковы основные свойства криптографической системы и	ОПК-9.1,

криптографического протокола? Приведите примеры процедур обмена сообщениями, которые являются раундами и шагами криптографических протоколов.	ОПК-9.2
2. В чем заключаются свойства полноты и корректности интерактивного доказательства?	УК-2.1,УК-2.2
3. В чем отличие интерактивных систем доказательства с нулевым разглашением знания от интерактивных систем доказательства? Сохраняется ли свойство нулевого разглашения при последовательном и параллельном выполнении протоколов?	УК-2.1, ОПК-9.2, УК-2.2
4. Что понимается под компрометацией криптографического протокола? Приведите примеры: атаки по известным ключам; словарной атаки.	ОПК-9.2, ОПК-9.3
5. 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. 6. 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>.	ОПК-9.2, УК-2.1.УК-2.2 ОПК-9.2, УК-2.1, УК-2.2
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.)	ОПК-9.2, ОПК-9.3
8. Как преобразовать протокол аутентификации Шнорра в схему электронной подписи?	ОПК-9.2, УК-2.1

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?	ОПК-9.2, УК-2.1
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?	ОПК-9.2, ОПК-9.3
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.	ОПК-9.1, ОПК-9.2

Промежуточная аттестация (контрольные вопросы) - проверка сформированности компетенций УК-2, ОПК-9

Контрольные вопросы	**Проверяемые компетенции**
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?	ОПК-9.2, УК-2.1,УК-2.2
2. Назовите известные Вам режимы работы блочных шифров, позволяющие обеспечить: только секретность сообщений; только подлинность сообщений; одновременно секретность и подлинность сообщений.	ОПК-9.1, ОПК-9.2

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?	ОПК-9.1, ОПК-9.2
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?	ОПК-9.2, ОПК-9.3
5. Какие функции может выполнять центр доверия в протоколах распределения ключей? Приведите примеры.	ОПК-9.2, ОПК-9.3
6. В чем разница между понятиями: способы распространения ключей и протоколы распределения ключей?	ОПК-9.1, ОПК-9.2
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.	ОПК-9.1, ОПК-9.2, УК-2.1, УК-2.2
8. Приведите протокол конфиденциально реализуемой операции умножения переменной на константу с использованием (t,n)-пороговой схемы Шамира.	ОПК-9.2, ОПК-9.3
9. Приведите примеры реализации систем защищенного электронного документооборота и защищенной электронной почты.	ОПК-9.2, ОПК-9.3
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.	ОПК-9.1, ОПК-9.2

Примерные задания для тестирования - проверка сформированности компетенций УК-2,ОПК-9

1. Длина ключа алгоритма DES:
а) 56 бит.
б) 48 бит.
в) 512 бит.

2. Криптостойкость — это:
а) устойчивость к внешним излучениям..
б). способность криптографического алгоритма противостоять криптоанализу
в) устойчивость к деформациям.

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). [Электрон-

ный 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 28.11.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_40241/, свободный. – Загл. с экрана.

Литература
основная

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — Москва: Издательство Юрайт, 2020. — 220 с. — (Высшее образование). — ISBN 978-5-9916-9244-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452871
2. Криптографические методы защиты информации: учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433133
3. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 Информационная безопасность : по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О. В. ; отв. ред. А. А. Тарасов]. - Электрон. дан. - Москва: РГГУ, 2013. - 30 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009341. - Загл. с экрана. - ISBN 978-5-7281-1789-6.
4. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
5. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

6.2. **Перечень ресурсов информационно-телекоммуникационной сети «Интернет».**

1. Анохин М. И. Конспект лекций курса. Введение в математическую криптографию / Математическая криптография [Электронный ресурс] // Режим доступа: http://cryptography.ru/wp-content/uploads/2016/04/math_crypto_lecture_ notes.pdf (дата обращения: август 2017).

2. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf (дата обращения: август 2017).

3. 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 (дата обращения: август 2017).

4. Goldreich O. Foundations of cryptography. [Электронный ресурс]. – Режим доступа: http://www.twirpx.com/file/493751/ (дата обращения: август 2017).

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

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

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. Microsoft Share Point 2010
6. Vmware Player 15.5
7. Process Monitor
8. Masker
9. VeraCrypt
10. S-Tools
11. Демо-дистрибутивы СКЗИ «Крипто-Про»

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

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 CE;

– 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, регулируемыми эргономическими партами СИ-1;

– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий.

- проверка сформированности компетенций УК-2,ОПК-9

Практическое занятие 1 (4 часа). История криптографии. Основные положения криптографии - *проверка сформированности компетенций УК-2*

Вопросы для изучения и обсуждения:

Криптосинтез и криптоанализ. Криптографическая система (подсистемы шифрования, идентификации, имитозащиты, электронной подписи). Криптографический протокол. Криптографический примитив.

Криптоаналитик (противник). Криптоаналитик активный и пассивный.

Теоретико-информационная стойкость (совершенная криптографическая стойкость, безусловная стойкость, шенноновская стойкость). Теоретико-сложностная стойкость.

Электронная подпись. Шифр, ключ, Шифрование/дешифрование. Шифртекст (криптограмма). Криптографическая система с секретным ключом. Блочная криптосистема. Поточная криптосистема. Криптографическая система с открытым ключом. Имитозащита. Стеганография.

Роль и место криптографических методов в защите современных информационных систем.

Контрольные вопросы:

1. Опишите взаимосвязь криптографии и криптологии и их основных составляющих дисциплин.

2. Приведите примеры криптографических систем с секретным ключом и криптографических систем с открытым ключом.

3. Опишите требования, которые должны быть предъявлены к криптографическим системам.

4. Выполните классификацию основных видов атак криптоаналитика (противника) на криптографические системы.

5. Дайте определения теоретической и практической стойкости криптографических систем и поясните их различия.

6. В чем отличие криптографии от стеганографии? Приведите примеры.

Практическое занятие 2 (8 часов). Базовые криптографические методы и схемы криптографической защиты информации - *проверка сформированности компетенций УК-2,ОПК-9*

Вопросы для изучения и обсуждения:

1. 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. Формальное определение теоретической и практической стойкости криптографических систем.

2. Схемы электронной подписи. Атаки и угрозы для схем электронной подписи. Примеры схем электронной подписи: RSA, Эль-Гамаля, Фиата-Шамира, Шнорра, ГОСТ Р 34.10-2012.

3. Криптографически стойкие хэш-функции. Методы поиска коллизий. Методы защиты от поиска коллизий. Хэш-функции Р.Ривеста и МККТТ Х.509.

4. 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.

5. Схемы вероятностного шифрования. Схема Голдвассер-Микали.

6. Разновидности схем электронной подписи. Схемы конфиденциальной подписи. Схемы групповой подписи. Схемы мультиподписи. Схемы затемненной подписи. Схемы подписи для интеллектуальных карточек. Схемы подписи вида «офф-лайн/он-лайн». (n,t)-пороговые схемы подписи. Процедуры арбитража в схемах электронной подписи.

7. Прикладные схемы интерактивной аутентификации. Схемы Шнорра, Фиата-Шамира, Гийю-Кискатера.

Контрольные вопросы:

1. Математически опишите криптографические системы с секретным и открытым ключами, схемы электронной подписи.

2. Дайте формальные определения односторонней функции и функции с секретом.

3. Дайте формальное определение псевдослучайному генератору.

4. Опишите свойства полноты, корректности и нулевого разглашения для интерактивных систем доказательств с нулевым разглашением.

5. Почему схема интерактивной аутентификации Шнорра является схемой с сокрытием свидетельства, а не системой доказательства с нулевым разглашением?

Практическое занятие 3 (8 часов). Криптографические протоколы - *проверка сформированности компетенций УК-2, ОПК-9*

Вопросы для изучения и обсуждения:

1. Основы теории криптографических протоколов. Свойства и основные параметры криптографических протоколов.

2. Классификация основных видов атак на криптографические протоколы.

3. 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.

4. 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.

5. Банковские криптографические протоколы. Электронные монеты и переводимые электронные монеты. Электронный бумажник. Электронные платежи.

Контрольные вопросы:

1. Каковы основные свойства криптографической системы и криптографического протокола? Что такое шаг, раунд и сеанс в криптографическом протоколе?

2. В чем заключаются свойства полноты и корректности интерактивного доказательства?

3. В чем отличие интерактивных систем доказательства с нулевым разглашением знания от интерактивных систем доказательства? Сохраняется ли свойство нулевого разглашения при последовательном и параллельном выполнении протоколов?

4. Что понимается под компрометацией криптографического протокола? Приведите примеры:

атаки по известным ключам;

словарной атаки.

5. 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.)

6. Как преобразовать протокол аутентификации Шнорра в схему цифровой подписи?

Практическое занятие 4 (8 часов). Нормативные акты, регламентирующие деятельность в области криптографической защиты информации - *проверка сформированности компетенций УК-2*

Вопросы для изучения и обсуждения:

1. Федеральные законы РФ «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «О техническом регулировании».

2. Постановление Правительства Российской Федерации от 23 сентября 2002 года №691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

3. 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.

4. Отечественные (криптографические) ГОСТы: ГОСТ 28147-89, ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

Выполнение задания:

В ходе практической работы имитируется процесс сертификации и эксплуатации средств криптографической защиты информации (СКЗИ), реализованных в соответствии с ГОСТ ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 и рассматривается пакет документов, необходимый для сертификации и эксплуатации СКЗИ и собственно сертификат соответствия СКЗИ нормативным документам и/или ТУ.

Контрольные вопросы:

1. Приведите основные положения Федеральных законов РФ «Об информации, информационных технологиях и о защите информации», «О персональных данных», «Об электронной подписи», «О техническом регулировании» в части криптографической защиты информации.

2. Опишите структуру и основные функции Удостоверяющего центра в соответствии положениями Федерального закона «Об электронной подписи».

3. Расскажите об основных типах электронной подписи, назначении, структуре и полях сертификатов открытых ключей в соответствии положениями Федерального закона «Об электронной подписи».

4. Опишите основные этапы сертификации и эксплуатации СКЗИ в соответствии с положением ПКЗ-2005.

5. Опишите основные поля сертификата соответствия на СКЗИ, реализованные в соответствии ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015.

Практическое занятие 5 (8 часов). Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке - *проверка сформированности компетенций УК-2, ОПК-9*

Вопросы для изучения и обсуждения:

1. Российские организации, осуществляющие деятельность в области криптографической защиты информации.

2. Линейка продуктов «КриптоПро», линейка продуктов «Secret Disk», «TrueCrypt»

3. Защищенный абонентский пункт системы «Атлас» (изделие М-468Р). Решения ФГУП «НТЦ «Атлас» по созданию защищенных (до класса АК3) автоматизированных систем на платформе Майкрософт.

4. СКЗИ «Крипто БД».

5. Другие продукты и услуги в области криптографической защиты информации.

Выполнение задания:

В ходе практической работы осуществляется получение демо-дистрибутива СКЗИ с сайта компаний «КриптоПро», выполнение установки и реализация основных функций СКЗИ.

Контрольные вопросы:

1. Назовите основные функции существующих СКЗИ, представленных на отечественном рынке продукции и услуг в области криптографической защиты информации.

2. Какие функции безопасности реализуются существующими СКЗИ:

- обеспечение конфиденциальности;
- обеспечение целостности;
- аутентификация информации;
- аутентификация пользователей.

3. Найти в сети Интернет СКЗИ, не представленные в вышеуказанном списке СКЗИ, описать его назначение и основные функции.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина « Методы и средства криптографической защиты информации» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

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

Задачи: овладение студентами основными криптографическими понятиями, умение студентами: решать типовые криптографические задачи, востребованные практикой; работать со специальной криптографической литературой и нормативными документами; использовать полученные знания для решения прикладных задач современной криптографии.

Дисциплина направлена на формирование следующих компетенций:

- УК-2 – Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- ОПК-9 – Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Знать:

математические модели кодирования систем информации; нормативно-правовые требования в области разработки и применения СКЗИ; основные модели, методы и средства криптографической защиты информации;

Уметь:

решать типовые криптографические задачи защиты информации; применять информационные технологии для поиска и обработки информации.

Владеть:

навыками поиска нужной информации в нормативных базах и источниках; навыками использования положений стандартов в области СКЗИ при разработке, настройке и эксплуатации

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.