МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
ИНСТИТУТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра математического анализа и дифференциальных уравнений

Рабочая программа дисциплины (модуля)

Б1.О.35 Основы информационной безопасности

Направление подготовки 01.03.02 Прикладная математика и информатика

Направленность (профиль) подготовки Математическое и компьютерное моделирование

Квалификация выпускника БАКАЛАВР

Форма обучения очная

Иркутск 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели: ознакомление студентов с теоретическими основами информационной безопасности, основами криптографии и основами обеспечения защиты информации.

Задачи: достичь достаточного уровня знаний по криптографическим и организационным методам обеспечения информационной безопасности и сформировать у студентов практические навыки работы со средствами обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Учебная дисциплина Б1.О.35 Основы информационной безопасности относится к обязательной части Блока 1 образовательной программы.
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Информатика и программирование.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Производственная практика.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки 01.03.02 Прикладная математика и информатика:
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен
знать: международные и национальные стандарты в области информационной безопасности; основные виды угроз информационной безопасности и способы противодействия этим угрозам; основные нормативные правовые документы в сфере информационной безопасности; основные прикладные алгоритмы криптографии; основные средства обеспечения информационной безопасности; инфраструктуру открытых ключей;
уметь: соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности; составлять политики безопасности уровня методов предприятия; анализировать и выбирать средства обеспечения информационной безопасности; использовать криптографические преобразования для решения задач профессиональной деятельности; анализировать алгоритмы взаимодействия на наличие уязвимостей;
владеть: основными навыками защиты информации; приемами анализа и классификации угроз информационной безопасности; основными навыками использования нормативных документов при организации обеспечения информационной безопасности на предприятии; навыками реализации прикладных алгоритмов криптографии в языках программирования, работы с криптопровайдерами, использования криптографических примитивов в языках программирования.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных ед., 108 час.

Форма промежуточной аттестации: зачет.

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

Раздел дисциплины / тема	Сем.	Виды учебной работы				Формы текущего контроля; Формы промежут. аттестации
		Контактная работа преподавателя с обучающимися			Самост. работа	
		Лекции	Лаб. занятия	Практ. занятия		
Основы криптографии						
Блочное шифрование						
Целостность сообщений						
Цифровая подпись						
Нормативные основы информационной безопасности						
Виды и классификация возможных нарушений информационной безопасности						
Политика безопасности						
Безопасность беспроводных сетей						
Итого (7 семестр):		30	30		40	зач.

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Раздел дисциплины / тема	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самост. работы
	Вид самост. работы	Сроки выполнения	Затраты времени		
Основы криптографии					
Блочное шифрование					
Целостность сообщений					
Цифровая подпись					
Нормативные основы информационной безопасности					
Виды и классификация возможных нарушений информационной безопасности					
Политика безопасности					
Безопасность беспроводных сетей					
Общая трудоемкость самостоятельной работы (час.)			40		
Из них с использованием электронного обучения и дистанционных образовательных технологий (час.)					

4.3. Содержание учебного материала

РАЗДЕЛ 1. КРИПТОГРАФИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ

БЕЗОПАСНОСТИ
ТЕМА 1.1. Основы криптографии
Общие принципы и модели. Защита от несанкционированного доступа. Понятие ключа. Шифрование и кодирование. Криптосистемы. Шифр Вернама. Лемма о теоретически стойком шифре. Потоковые шифры.
ТЕМА 1.2. Блочное шифрование
Принцип итерирования. Понятие псевдослучайной функции и псевдослучайной перестановки. Шифр DES. Описание структуры. Шифр AES. Описание структуры и принципы работы. Переборные атаки на блочные шифры. Переборные атаки на блочные шифры. Проблема Случайное шифрование. Одноразовое шифрование. Режим CBC. Набивка блоков. Режим CTR.
ТЕМА 1.3. Целостность сообщений
Коды аутентификации сообщений. Построение кодов аутентификации больших сообщений. Конструкции CBC-MAC и NMAC. Хеш-функции. Конструкция Меркла-Дамгарда для построения хеш-функций. Понятие целостности шифр-текста. Аутентичное шифрования на примере протокола TLS.
ТЕМА 1.4. Цифровая подпись
Понятие цифровой подписи. Основные принципы и отличия от реальной подписи. Алгоритмы цифровой подписи. DSS. ГОСТ. Закон об ЭЦП в России. Различные виды подписи. Удостоверяющие центры. Понятие ключа подписи. Инфраструктура открытых ключей (PKI).
РАЗДЕЛ 2. ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕМА 2.1. Нормативные основы информационной безопасности
Направления ИБ. Механизмы. Инструментарий. Методы защиты информации. Виды противников и нарушителей информационной безопасности. Международные стандарты информационного обмена. Категории прав на информацию. Служебная, коммерческая и государственная тайны. Сведения, не составляющие коммерческую и государственную тайну. Закон «Информации, информатизации и защите информации». Закон о персональных данных. Закон об ЭЦП.
ТЕМА 2.2. Виды и классификация возможных нарушений информационной безопасности
Понятие угрозы и уязвимости. Классификации угроз. Три вида нарушений безопасности. Меры по противодействию угрозам нарушения конфиденциальности, целостности, доступности. Построение модели угроз и методики оценки рисков. Качественные и количественные методики оценки рисков. Классификация компьютерных вирусов. Меры по их профилактике. Методология защиты информационных систем.
ТЕМА 2.3. Политика безопасности
Цели и задачи организации. Взаимодействие между субъектами. Правила безопасности. Уровни формирования политик безопасности.
ТЕМА 2.4. Безопасность беспроводных сетей
Беспроводные сети стандартов 802.11. Особенности защиты информации в беспроводных сетях. Основные угрозы и уязвимости. Режимы функционирования и шифрования данных в беспроводных сетях.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

Тема занятия	Всего часов	Оценочные средства	Формируемые компетенции
Основы криптографии			
Блочное шифрование			
Целостность сообщений			
Цифровая подпись			

Нормативные основы информационной безопасности			
Виды и классификация возможных нарушений информационной безопасности			
Политика безопасности			
Безопасность беспроводных сетей			

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы

Тема	Задание	Формируемые компетенции
Основы криптографии		
Блочное шифрование		
Целостность сообщений		
Цифровая подпись		
Нормативные основы информационной безопасности		
Виды и классификация возможных нарушений информационной безопасности		
Политика безопасности		
Безопасность беспроводных сетей		

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов всех форм и видов обучения является одним из обязательных видов образовательной деятельности, обеспечивающей реализацию требований Федеральных государственных стандартов высшего образования. Согласно требованиям нормативных документов самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов. Самостоятельная работа студентов представляет собой совокупность аудиторных и внеаудиторных занятий и работ. Самостоятельная работа в рамках образовательного процесса в вузе решает следующие задачи:
– закрепление и расширение знаний, умений, полученных студентами во время аудиторных и внеаудиторных занятий, превращение их в стереотипы умственной и физической деятельности;
– приобретение дополнительных знаний и навыков по дисциплинам учебного плана;
– формирование и развитие знаний и навыков, связанных с научно-исследовательской деятельностью;
– развитие ориентации и установки на качественное освоение образовательной программы;
– развитие навыков самоорганизации;
– формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;
– выработка навыков эффективной самостоятельной профессиональной теоретической, практической и учебно-исследовательской деятельности.

Подготовка к лекции. Качество освоения содержания конкретной дисциплины прямо зависит от того, насколько студент сам, без внешнего принуждения формирует у себя установку на получение на лекциях новых знаний, дополняющих уже имеющиеся по данной дисциплине. Время на подготовку студентов к двухчасовой лекции по нормативам составляет не менее 0,2 часа.

Подготовка к практическому занятию. Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической, научной деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии. Подготовка к практическому занятию нередко требует подбора материала, данных и специальных источников, с которыми предстоит учебная работа. Студенты должны дома подготовить к занятию 3–4 примера формулировки темы исследования, представленного в монографиях, научных статьях, отчетах. Затем они самостоятельно осуществляют поиск соответствующих источников, определяют актуальность конкретного исследования процессов и явлений, выделяют основные способы доказательства авторами научных работ ценности того, чем они занимаются. В ходе самого практического занятия студенты сначала представляют найденные ими варианты формулировки актуальности исследования, обсуждают их и обосновывают свое мнение о наилучшем варианте. Время на подготовку к практическому занятию по нормативам составляет не менее 0,2 часа.

Подготовка к семинарскому занятию. Самостоятельная подготовка к семинару направлена: на развитие способности к чтению научной и иной литературы; на поиск дополнительной информации, позволяющей глубже разобраться в некоторых вопросах; на выделение при работе с разными источниками необходимой информации, которая требуется для полного ответа на вопросы плана семинарского занятия; на выработку умения правильно выписывать высказывания авторов из имеющихся источников информации, оформлять их по библиографическим нормам; на развитие умения осуществлять анализ выбранных источников информации; на подготовку собственного выступления по обсуждаемым вопросам; на формирование навыка оперативного реагирования на разные мнения, которые могут возникать при обсуждении тех или иных научных проблем. Время на подготовку к семинару по нормативам составляет не менее 0,2 часа.

Подготовка к коллоквиуму. Коллоквиум представляет собой коллективное обсуждение раздела дисциплины на основе самостоятельного изучения этого раздела студентами. Подготовка к данному виду учебных занятий осуществляется в следующем порядке. Преподаватель дает список вопросов, ответы на которые следует получить при изучении определенного перечня научных источников. Студентам во внеаудиторное время необходимо прочитать специальную литературу, выписать из нее ответы на вопросы, которые будут обсуждаться на коллоквиуме, мысленно сформулировать свое мнение по каждому из вопросов, которое они выскажут на занятии. Время на подготовку к коллоквиуму по нормативам составляет не менее 0,2 часа.

Подготовка к контрольной работе. Контрольная работа назначается после изучения определенного раздела (разделов) дисциплины и представляет собой совокупность развернутых письменных ответов студентов на вопросы, которые они заранее получают от преподавателя. Самостоятельная подготовка к контрольной работе включает в себя: — изучение конспектов лекций, раскрывающих материал, знание которого проверяется контрольной работой; повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения; изучение дополнительной литературы, в которой конкретизируется содержание

проверяемых знаний; составление в мысленной форме ответов на поставленные в контрольной работе вопросы; формирование психологической установки на успешное выполнение всех заданий. Время на подготовку к контрольной работе по нормативам составляет 2 часа.

Подготовка к зачету. Самостоятельная подготовка к зачету должна осуществляться в течение всего семестра. Подготовка включает следующие действия: перечитать все лекции, а также материалы, которые готовились к семинарским и практическим занятиям в течение семестра, соотнести эту информацию с вопросами, которые даны к зачету, если информации недостаточно, ответы находят в предложенной преподавателем литературе. Рекомендуется делать краткие записи. Время на подготовку к зачету по нормативам составляет не менее 4 часов.

Подготовка к экзамену. Самостоятельная подготовка к экзамену схожа с подготовкой к зачету, особенно если он дифференцированный. Но объем учебного материала, который нужно восстановить в памяти к экзамену, вновь осмыслить и понять, значительно больше, поэтому требуется больше времени и умственных усилий. Важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. Необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к экзамену. Время на подготовку к экзамену по нормативам составляет 36 часов для бакалавров.

В ФБГОУ ВО «ИГУ» организация самостоятельной работы студентов регламентируется Положением о самостоятельной работе студентов, принятым Ученым советом ИГУ 22 июня 2012 г.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Введение в криптографию / ред. В. В. Ященко. – М.: Изд-во МЦНМО, 2012. – 347 с. – ISBN: 978-5-4439-0026-1 (26 экз.)
2. Рябец Л.В. Задачник-практикум по криптографии: учеб. пособие / Л.В. Рябец. – Иркутск : Изд-во Вост-Сиб. гос. акад. образ., 2013. – 76 с. – ISBN: 978-5-85827-864-1 (30 экз.)
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК-Пресс. – 2010. – 542 с. – ISBN: 978-5-94074-518-1 (25 экз.)
4. Келлеров А. С., Корольков Ю. Д. Основы информационной безопасности : учеб. пособие. – Иркутск: Изд-во ИГУ, 2013. – 113 с. . – ISBN: 978-5-9624-0791-3 (30 экз.)

б) дополнительная литература:

5. Герман О.Н. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования / О.Н. Герман. – М.: Академия. – 2012. – 257 с. – ISBN: 978-5-7695-6786-5. Режим доступа: ЭЧЗ «Библиотех». – Неогранич. доступ.
6. Конеев И. Р. Информационная безопасность предприятия: научное издание / И. Р. Конеев, А. В. Беляев. – СПб.: БХВ-Петербург, 2003. – 733 с. – ISBN 5-94157-280-8 (99 экз).

7. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учеб. пособие / А. В. Бабаш. – М.: КноРус, 2013. – 131 с. – ISBN 978-5-406-02760-8 (50 экз.).
8. Смарт Н. Криптография: учебное пособие / Н. Смарт – М.: Техносфера, 2005. – 525 с. – ISBN 5-94836-043-1 (5 экз.)
9. Нечаев, В.И. Элементы криптографии: основы теории защиты информации: Учеб.пособие для ун-тов и пед.вузов / В.И. Нечаев. – М.: Высш. шк., 1999. – 109 с. – ISBN 5060036448 (17 экз.).
10. Чмора А. Л. Современная прикладная криптография: учеб.пособие / А.Л. Чмора – М.: Гелиос АРВ, 2001. – 244 с. – ISBN 5854380374 (51экз.)
11. Глухов М.М. Введение в теоретико-числовые методы криптографии / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. – СПб.: Лань. – 2011. – 400 с. – ISBN: 978-5-8114-1116-0. Режим доступа: ЭБС «Лань». – Неогранич. доступ.

в) базы данных, информационно-справочные и поисковые системы:

1.
2.
3.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование

ЭТОТ РАЗДЕЛ НЕ ЗАПОЛНЯТЬ

6.2. Программное обеспечение

ПЕРЕЧИСЛИТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ТРЕБУЕМОЕ ДЛЯ ДИСЦИПЛИНЫ

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Оценочные средства текущего контроля

Вид контроля	Контролируемые темы	Контролируемые компетенции

Примеры оценочных средств текущего контроля

Тест к разделу Аутентичное шифрование
Вопрос 1 Предположим, что система MAC (S,V) используется для защиты файлов в файловой системе компьютера. К каждому файлу добавляется специальный tag. Алгоритм S в своей работе использует только содержимое файла. Для каких атак подобная система MAC является уязвимой?
Варианты ответов
Выполнить конкатенацию двух файлов в системе и создать третий.
Удалить последний байт в файле.

Изменить время модификации файла.
Поменять местами два файла в файловой системе.
Добавить новые данные в файл.
Вопрос 2 Пусть система MAC (S,V) является безопасной. Система определена над пространством (K,M,T), где M={0,1}n и T={0,1}128. Какие из предложенных ниже конструкций являются безопасными MAC?
Варианты ответов
S′(k,m)=S(k,m) и V′(k,m,t)={V(k,m,t),1,m≠0n;otherwise
S′(k,m)=S(k,m ∥ m) и V′(k,m,t)=V(k,m ∥ m,t)
S′(k,m)=S(k,m)[0,...,126] и V′(k,m,t)=[V(k,m,t ∥ 0)orV(k,m,t ∥ 1)]
S′(k,m)={S(k,1n),S(k,m),m=0n;otherwise и
V′(k,m,t)={V(k,1n,t),V(k,m,t),m=0n;otherwise
S′(k,m)=[S(k,m),S(k,0n)] и V′(k,m,(t1,t2))=[V(k,m,t1)andV(k,m,t2)]
S′(k,m)=[t=S(k,m),output(t,t)] и V′(k,m,(t1,t2))={V(k,m,t1),0,t1=t2;otherwise
Вопрос 3 Схема вычисления кодов аутентификации сообщений ECBC-MAC использует фиксированный вектор инициализации (в лекции использовался нулевой вектор). Предположим, что вместо фиксированного, для каждого сообщения используется случайный вектор IV и этот вектор добавляется к tag. Другими словами, S(k,m)=(r,ECBCr(k,m)), где r это случайный IV. Алгоритм проверки по ключу k, сообщению m и тегу (r,t) выдает 1 ("yes"), если t=ECBCr(k,m).
Такая схема построения MAC является небезопасной. Атакующий может получить тег (r,t) для сообщения m, состоящего из одного блока. Теперь он способен сконструировать новый тег для нового сообщения. Укажите пару тег, сообщение, которую может сконструировать атакующий.
Варианты ответов
Тег (m⊕t,t) является правильным для сообщения m⊕1n.
Тег (r⊕t,r) является правильным для сообщения m.
Тег (r⊕t,m) является правильным для сообщения 0n.
Тег (r⊕1n,t) является правильным для сообщения m⊕1n.
Вопрос 4 Алиса намеревается организовать широковещательную отправку сообщений для 6 получателей B1,…,B6. Секретность сообщений не важна, важна целостность и аутентичность. Каждый из получателей должен быть уверен, что сообщение получено от Алисы.
Для своей задачи Алиса решила использовать MAC. Предположим, что Алиса и 6 пользователей работают с одним общим ключом k. Тогда каждый из B1,…,B6 при получении сообщения может проверить правильность тега. Но эта схема небезопасна, т.к., например, пользователь B1 может создать сообщение, прикрепить к нему тег, полученный на ключе k и отправить в сеть. При этом, пользователи B2,…,B6 будут уверены, что сообщение получено от Алисы.
Вместо этого, Алиса сгенерировала 4 секретных ключа S={k1,…,k4}. Каждому пользователю Bi она передала подмножество ключей Si⊆S. Теперь Алиса при передаче сообщения прикладывает к нему четыре тега, каждый из которых получен на одном из четырех ключей. Когда пользователь Bi получает сообщение он проверяет только те теги сообщения, для которых у него есть ключи.
Выберите правильный способ, которым Алиса может распределить случайные ключи так, чтобы никто из пользователей не смог бы создавать сообщения для других пользователей правильные сообщения от имени Алисы
Варианты ответов
S1={k1,k2}, S2={k1}, S3={k1,k4}, S4={k2,k3}, S5={k2,k4}, S6={k3,k4}
S1={k2}, S2={k2,k3}, S3={k3,k4}, S4={k1,k3}, S5={k1,k2}, S6={k1,k4}
S1={k1,k2}, S2={k2,k3}, S3={k3,k4}, S4={k1,k3}, S5={k1,k2}, S6={k1,k4}

S1={k1k2}, S2={k1,k3}, S3={k1,k4}, S4={k2,k3}, S5={k2,k4}, S6={k3,k4}
Вопрос 5 Рассмотрим схему ECBC-MAC на основе шифра AES. Предположим, что мы вычислили тег для длинного сообщения m, состоящего из n блоков. Длина сообщения кратна длине блока AES и набивка сообщения не использовалась. Пусть сообщение m′ получено из сообщения m заменой последнего бита на противоположный. Сколько операций AES необходимо выполнить для того, чтобы из тега сообщения m и ключа MAC получить тег нового сообщения m′.
Варианты ответов
2
n−1
3
4
Вопрос 6 Пусть H:M→T стойкая к коллизиям хеш функция. Какая из следующий функций также будет стойкой к коллизиям.
Варианты ответов
H′(m)=H(m[0,…,|m|−2])
H′(m)=H(m) // H(m)
H′(m)=H(H(m))
H′(m)=H(m)⊕H(m⊕1|m|)
H′(m)=H(m)[0,…,31]
H′(m)=H(|m|), где |m| есть длина сообщения m
H′(m)=H(m // m)
H′(m)=H(m // 0)
H′(m)=H(m)⊕H(m)

Например:
Демонстрационный вариант контрольной работы №1 (№2, №3)
Демонстрационный вариант теста №1 (№2, №3)
Вопросы для собеседования №1 (№2, №3)
Вопросы для коллоквиума №1 (№2, №3)
Темы рефератов и др.

7.2. Оценочные средства для промежуточной аттестации

Список вопросов для промежуточной аттестации:

1. Основное определение информационной безопасности. Направления ИБ. Механизмы. Инструментарий.
2. Методы защиты информации. Виды противников и нарушителей информационной безопасности.
3. Понятие угрозы и уязвимости. Классификации угроз. Три вида нарушений безопасности. Меры по противодействию угрозам нарушения конфиденциальности, целостности, доступности.
4. Цели и задачи организации в области обеспечения информационной безопасности. Взаимодействие между субъектами. Правила безопасности. Уровни формирования политик безопасности.
5. Классификация компьютерных вирусов. Меры по их профилактике. Методология защиты информационных систем.
6. Беспроводные сети стандартов 802.11. Особенности защиты информации в беспроводных сетях. Основные угрозы и уязвимости. Режимы

функционирования и шифрования данных в беспроводных сетях.
7. Общие принципы криптографии. Защита от несанкционированного доступа. Основные способы криптоанализа простых шифров. Идеальный шифр.
8. Шифр Вернама. Лемма о теоретически стойком шифре. Потоковые шифры. Атаки на потоковые шифры. Двухразовый блокнот.
9. Шифр AES. Описание структуры и принципы работы. Переборные атаки на блочные шифры.
10. Случайное шифрование. Одноразовое шифрование. Режим CBC. Шифрование с предсказанным значением вектора инициализации. CBC для одноразового шифрования. Набивка блоков. Режим CTR. Сравнение режимов CBC и CTR.
11. Коды аутентификации сообщений. Построение кодов аутентификации больших сообщений. Конструкции CBC-MAC и NMAC. Их эффективность. Схема атаки с использованием коллизий.
12. Конструкция Меркла-Дамгарда для построения хеш-функций. Построение безопасных сжимающих функций.
13. Необходимость применения аутентичного шифрования. Понятие целостности шифр-текста. Атака на основе выборочного шифр-текста. Аутентичное шифрования на примере протокола TLS.
14. Понятие цифровой подписи. Основные принципы и отличия от реальной подписи. Алгоритмы цифровой подписи.
15. Инфраструктура открытых ключей. Закон об ЭЦП в России. Различные виды подписи. Удостоверяющие центры.

Примеры оценочных средств для промежуточной аттестации:

1.
2.
3.

Разработчик: Рябец Л. В., кандидат физ.-мат. наук, доцент