МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ИГУ»)

Институт математики и информационных технологий

Кафедра информационных технологий

«УТВЕРЖДАЮ»
Директор ИМИТ ИГУ
_____ М. В. Фалалеев
«17» мая 2023 г.

Рабочая программа дисциплины (модуля)

Б1.О.26 Информационная безопасность

Направление подготовки 02.03.02 Математическое обеспечение и администрирование информационных систем

Направленность (профиль) подготовки Математическое обеспечение и администрирование информационных систем

Квалификация выпускника бакалавр

Форма обучения очная

Иркутск 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели: ознакомление студентов с теоретическими основами информационной безопасности, основами криптографии и основами обеспечения защиты информации, формирование практических умений и навыков, необходимых для приобретения квалификации бакалавра информационных технологий, формирование ключевых профильных компетенций.
Задачи: дать специальные знания по дисциплине, 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.26 Информационная безопасность относится к обязательной части Блока 1 образовательной программы.
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Б1.О.17 Защита информации.

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: Б1.В.11 Администрирование информационных систем.

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 02.03.03 Математическое обеспечение и администрирование информационных систем:
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-2 Способен применять современный математический аппарат, связанный с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности;
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение для информационных систем и баз данных, в том числе отечественного производства.

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; формальные модели безопасности.;
уметь: соблюдать основные требования по противодействию наиболее распространенным угрозам информационной безопасности. составлять политики безопасности уровня методов предприятия; анализировать и выбирать средства обеспечения информационной безопасности; 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 4 зачетных ед., 144 час.

Форма промежуточной аттестации: экзамен.

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		
Раздел 1. Криптографические основы информационной безопасности						
Тема 1.1. Основы криптографии		4	4		3	Опрос, защита отчета о лабораторной работе
Тема 1.2. Блочное шифрование		4	4		3	Опрос, защита отчета о лабораторной работе
Тема 1.3. Целостность сообщений		4	4		3	Опрос, защита отчета о лабораторной работе
Тема 1.4. Цифровая подпись		4	6		4	Опрос, защита отчета о лабораторной работе
Раздел 2. Организационные основы информационной безопасности						
Тема 2.1. Нормативные основы информационной безопасности		6	4		3	Опрос, защита отчета о лабораторной работе
Тема 2.2. Виды и классификация возможных нарушений информационной безопасности		4	6		3	Опрос, защита отчета о лабораторной работе
Тема 2.3. Политика безопасности		4	4		3	Опрос, защита отчета о лабораторной работе
Тема 2.4. Безопасность беспроводных сетей		6	4		3	Опрос, защита отчета о лабораторной работе

Итого (6 семестр):		36	36		27	экз.

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		
Тема 1.1. Основы криптографии	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	2 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Тема 1.2. Блочное шифрование	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	4 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Тема 1.3. Целостность сообщений	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	6 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Тема 1.4. Цифровая подпись	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	8 неделя	4	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru

Тема 2.1. Нормативные основы информационной безопасности	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	10 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Тема 2.2. Виды и классификация возможных нарушений информационной безопасности	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	12 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Тема 2.3. Политика безопасности	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	14 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Тема 2.4. Безопасность беспроводных сетей	Изучение учебной и научной литературы, подготовка к текущей и промежуточной аттестации, оформление отчета к лабораторным работам	16 неделя	3	Опрос, защита отчета о лабораторной работе	Основная и дополнительная литература в соответствии с разделом 5 РПД, методические материалы в ресурсе дисциплины на educa.isu.ru
Общая трудоемкость самостоятельной работы (час.)			27		
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 «Об информации, информационных технологиях и о защите информации». Закон «О персональных данных». Закон «Об электронной подписи».
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 компьютерных 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
Тема 1.1. Основы криптографии	4	ЛР «Основы криптографии»	УК-2, ОПК-2
Тема 1.2. Блочное шифрование	4	ЛР «Блочное шифрование»	УК-2, ОПК-2
Тема 1.3. Целостность сообщений	4	ЛР «Простое хэширование»	УК-2, ОПК-2
Тема 1.4. Цифровая подпись	4	ЛР «Формирование электронной подписи в VipNet»	УК-2, ОПК-2, ОПК-5

Тема 2.1. Нормативные основы информационной безопасности	4	ЛР «Изучение государственной системы защиты информации»	УК-2, ОПК-2
Тема 2.2. Виды и классификация возможных нарушений информационной безопасности	4	ЛР «Определение факторов, воздействующих на информацию», ЛР «Метод экспертных оценок»	УК-2, ОПК-2
Тема 2.3. Политика безопасности	4	ЛР «Анализ политики безопасности с помощью MSAT»	УК-2, ОПК-2, ОПК-5
Тема 2.4. Безопасность комптютерных сетей	4	ЛР «Проектирование системы защиты информации»	УК-2, ОПК-2, ОПК-5

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

Тема	Задание	Формируемые компетенции
Тема 2.1 Нормативные основы информационной безопасности	Состав документов на объект информатизации и ИСКИИ. Требования к защите сетей связи общего пользования.	УК-2, ОПК-2, ОПК-5
Тема 2.2. Виды и классификация возможных нарушений информационной безопасности	Методика определения угроз безопасности	УК-2, ОПК-2
Тема 2.3. Политика безопасности	Рекомендованные приемы разработки правил информационной безопасности	УК-2, ОПК-2
Тема 2.4. Безопасность компьютерных сетей	Инженерно-техническая укрепленность объекта.	УК-2, ОПК-2, ОПК-5

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

а) основная литература:

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. Некоммерческая Интернет-версия «Консультант Плюс» www.consultant.ru
2. Банк данных угроз ИБ bdu.fstec.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование

ЭТОТ РАЗДЕЛ НЕ ЗАПОЛНЯТЬ

6.2. Программное обеспечение

1. Java
2. Visual C++
3. Lasarus
4. Python
5. VipNet
6. LibreOffice

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Оценочные средства текущего контроля

Вид контроля	Контролируемые темы	Контролируемые компетенции
Защита отчета о лабораторной работе	1.1 - 2.4	УК-2, ОПК-2, ОПК-5

Примеры оценочных средств текущего контроля

Контрольные вопросы к лабораторной работе «Создание ЭП в ViPNet»

1.Что является единицей разграничения доступа в защищенной сети?
2.Зачем нужны списки рассылки копий?
3.Что нужно сделать в ЦУС, чтобы заново начать генерацию DST файлов?
4.Что должен сделать администратор при смене мастер-ключа?
5.Что содержится в DST файле?
6.Где задаются полномочия (права доступа пользователя)?
7.Для какой программы задаются полномочия?
8.Что происходит при нажатии кнопки «Сформировать все справочники» в «ЦУС»?
9.Что такое сетевой узел?
10.Что такое Главные абоненты?
11.Где хранится мастер-ключ?
12.Что находится на ключевой дискете?
13.Для чего служит ключевой набор?

7.2. Оценочные средства для промежуточной аттестации

Список вопросов для промежуточной аттестации:

1. Почему компьютерные вирусы причисляют к особому классу разрушающих программных воздействий. Раскройте основные каналы распространения компьютерных вирусов и других вредоносных программ.
2. На какие группы подразделяются методы и средства нейтрализации угроз информационной безопасности в компьютерных системах, представьте классификацию методов и средств борьбы с компьютерными вирусами. В чем заключаются методы использования резидентных сторожей и аппаратно-программной защиты от вирусов.
3. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Приведите правила мандатного (полномочного) разграничения доступа и поясните их.
4. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте смысл функционирования схемы шифрования в алгоритме DES. Основные режимы работы блочного симметричного алгоритма.
5. Перечислите и поясните возможные типы сетевых атак на компьютерные (информационные) системы, какие существуют технологии построения систем обнаружения атак.
6. Перечислите защитные механизмы, реализуемые программно-аппаратными комплексами (средствами) защиты информации в компьютерных системах (ПЭВМ). Дайте определение понятию - «субъект доступа», какие процедуры реализуются при его обращении к компьютерной системе.
7. Перечислите атрибутивные идентификаторы, используемые для идентификации субъекта доступа в КС, и коротко дайте им определение. Перечислите рекомендации для организации парольной защиты.
8. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.
9. Как осуществляемся управление криптоключами, требования к распределению ключей, методы распределения ключей, поясните схему открытого распределения ключей Диффи-Хеллмана

10. Раскройте процедуры алгоритмов цифровой подписи на основе отечественных стандартов ГОСТ Р 34.10.
11. Основные подходы к защите данных от НСД: какие действия выполняются при

организации доступа к оборудованию и ПО компьютерных систем (ПЭВМ); оценка эффективности наращивания средств контроля доступа по кривой роста относительного уровня обеспечения безопасности компьютерных систем (ПЭВМ).
12. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте смысл функционирования схемы шифрования в алгоритме ГОСТ 28147-89. Основные режимы работы блочного симметричного алгоритма.
13. Какие основные функции выполняет подсистема защиты операционных систем (ОС), дайте коротко им определение. В чем заключается процедура аудита применительно к ОС, чем она обусловлена, каким требованиям она должна удовлетворять?
14. Перечислите базовые технологии (механизмы) безопасности информации в компьютерных системах. Дайте определение процессам идентификации, аутентификации и авторизации для обеспечения защиты информации. Приведите и раскройте типы процессов аутентификации, какие атаки проводятся на протоколы аутентификаций и какие механизмы применяются для их отражения.
15. Дайте определение и поясните технологии построения систем обнаружения сетевых вторжений и выявления признаков атак на информационные системы.
16. Перечислите и раскройте способы строгой аутентификации. Поясните на структурной схеме применение односторонней хэш-функции к сообщению, дополненному секретным ключом.
17. Поясните на структурных схемах простую аутентификацию пользователя ресурсов компьютерной системы с использованием пароля и аутентификацию, основанную на использовании односторонней хэш-функции для проверки пароля.
18. Дайте определение основным понятиям процесса разграничения доступа к объектам операционной системы (ОС): «объект доступа»; «метод доступа»; «субъект доступа»; «право доступа». Приведите правила избирательного разграничения доступа и поясните их реализацию на примере матрицы доступа, дайте определение понятиям: домен доступа; список прав доступа.
19. В чем заключается задача идентификации пользователя, дайте определение понятию протокола идентификации. В чем заключается локальная и удаленная идентификация, что такое идентифицирующая информация.
20. Перечислите и раскройте способы строгой аутентификации. Поясните на структурной схеме применение для аутентификации односторонней хэш-функции с параметром-ключом.
21. Какими способами блокируется угроза несанкционированного копирования информации ПЭВМ, в чем они заключаются, раскройте их содержание.
22. Какие существуют криптосистемы шифрования, раскройте их смысл функционирования.
23. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте процедуру хэширования по алгоритму ГОСТ Р 34.11.
24. Приведите классификацию криптографических алгоритмов и охарактеризуйте их.
25. В чем заключается биометрическая аутентификация пользователей, какие у нее достоинства и недостатки.
26. В чем заключается процедура простой аутентификации, какими способами она производится, поясните схематично ее реализацию с использованием пароля.
27. Раскройте основные процедуры формирования электронной цифровой подписи и функции хэширования.
28. Приведите классификацию криптографических алгоритмов и охарактеризуйте их. Раскройте алгоритм шифрования RSA.
29. Перечислите методы противодействия дизассемблированию программ для ЭВМ, охарактеризуйте их.

30. Перечислите методы ограничения доступа к компонентам ЭВМ, какие применяют средства для ограничения доступа к компонентам ЭВМ.
31. Раскройте основные методы аутентификации, использующие пароли и PIN-коды.

Примеры оценочных средств для промежуточной аттестации:

Примеры заданий экзаменационного теста:
№1
Политика безопасности - это
а) документ верхнего уровня, цель которого обеспечение решения вопросов информационной безопасности и вовлечение высшего руководства организации в данный процесс
б) совокупность документов, регламентирующих правила обращения с конфиденциальной информацией в зависимости от фазы ее обработки и категории конфиденциальности
в) совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации предприятия

№2
На федеральном уровне приоритеты обеспечения информационной безопасности определяются
а) Доктриной информационной безопасности РФ
б) Федеральными законами
в) Политикой безопасности

№3
Фактор, воздействующий на информацию - это...
а) явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней
б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
в) субъект, случайно или преднамеренно совершивший действие, следствием которого является возникновение и/или реализация угроз нарушения безопасности информации

№4
Обязательными к использованию при оценке угроз безопасности информации, обрабатываемой в информационных системах персональных данных и государственных информационных являются сведения из:

а) Банка данных угроз информационной безопасности ФСТЭК России
б) Государственного стандарта «Факторы, воздействующие на информацию»
в) Kaspersky Threat Landscape

№5
Если полномочия субъекта представляются списком ресурсов, доступных пользователю, и правами по доступу к каждому ресурсу из списка, то такой метод называется...

а) дискреционным
б) мандатным
в) ролевым

№6
Угрозу перехвата данных можно отнести к угрозам...
а) конфиденциальности
б) целостности
в) доступности

№7
Можно ли обеспечить 100% защиту от всех видов ущерба?
а) нет, и целью защиты информации становится уменьшение размеров ущерба до допустимых значений.
б) да, но сделать это невозможно экономически целесообразным способом
в) иногда, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба

№8
Дискреционное управление доступом - это...
а) разграничение доступа между поименованными субъектами и поименованными объектами
б) разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и допуска субъектов к информации соответствующего уровня конфиденциальности
в) организация прав доступа субъектов к объектам сгруппированных с учетом специфики их применения

№9
Метод защиты программы от исследования путем обфускации заключается в:
а) различной сложности преобразовании кода в процессе его выполнения
б) автоматической генерации участков исполняемого кода в процессе выполнения
в) создании избыточности указателей перехода, и внедрении взаимоувязанных нефункциональных участков кода, затрудняющих анализ декомпилированного текста

№10
Сертификация средств криптографической защиты информации осуществляется при участии:
а) ФСБ России
б) ФСТЭК России
в) Роскомнадзора

№11
Обычный способ идентификации - это...
а) ввод имени пользователя при входе в систему
б) пароль
в) изучение физиологических и поведенческих характеристик субъекта

№12
К достоинству моделей дискреционного доступа можно отнести...
а) их гибкость

б) возможность наложения ограничений на передачу информации от одного пользователя другому
в) контроль информационных потоков

Разработчик: Муценек В.Е., старший преподаватель кафедры Информационных технологий