



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и информационных технологий
Кафедра алгебраических и информационных систем



Рабочая программа дисциплины (модуля)

Б1.В.ДВ.02.01 Криптография

Направление подготовки	09.03.03 Прикладная информатика
Направленность (профиль) подготовки информационных систем	Проектирование и разработка информационных систем
Квалификация выпускника	бакалавр
Форма обучения	очная

Иркутск 2026 г.

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Цели: Ознакомление студентов с основами криптографии и основами обеспечения защиты информации, формирование практических умений и навыков при работе с криптографическими примитивами, формирование надпрофессиональных компетенций.

Задачи:

- достичь достаточного уровня знаний по криптографическим методам обеспечения информационной безопасности;
- сформировать у студентов практические навыки работы со средствами обеспечения криптографической безопасности.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

2.1. Учебная дисциплина (модуль) «Криптография» относится к части, формируемой участниками образовательных отношений «Блок 1. Дисциплины (модули)».

Дисциплина предназначена для формирования знаний и умений в сфере криптографической защиты информации.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

- Теория вероятностей и математическая статистика;
- Линейная алгебра;
- Программирование.

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

- Выполнение и защита выпускной квалификационной работы.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций (элементов следующих компетенций) в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-1 Способен разрабатывать и отлаживать программный код	ПК-1.1 Выполняет формализацию и алгоритмизацию поставленных задач для разработки программного кода	• Знает алгоритмы решения типичных задач, области и способы их применения • Знает методы и приемы алгоритмизации поставленных задач • Умеет использовать методы и приемы формализации и алгоритмизации поставленных задач • Умеет применять алгоритмы решения типовых задач в соответствующих областях

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-6 Способен применять универсальные компетенции профессиональной деятельности	ПК-6.3 Демонстрирует системное мышление при решении задач профессиональной деятельности	• Умеет анализировать задачи, учитывая взаимосвязи между их компонентами • Умеет выявлять причины и следствия в рамках сложных системных процессов • Способен структурировать информацию и видеть общую картину ситуации • Знает основные принципы и методы анализа и синтеза систем
	ПК-6.6 Планирует и осуществляет самообучение	• Умеет самостоятельно определять области для профессионального развития и формулировать цели обучения • Способен оценивать эффективность проведенного обучения и корректировать план при необходимости
	ПК-6.7 Демонстрирует владение профессиональной культурой	• Знает основные принципы профессиональной этики и культуры поведения • Знает стандарты и нормативы, регулирующие профессиональную деятельность в своей сфере

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, в том числе 54 часа на контроль, из них 54 часа на экзамен.

Из них реализуется с использованием электронного обучения и дистанционных образовательных технологий 58 часов самостоятельной работы.

Форма промежуточной аттестации: экзамен.

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

п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)				Формы текущего контроля успеваемости; Форма промежуточной аттестации (по семестрам)
			Контактная работа преподавателя с обучающимися			Самостоятельная работа	
			Лекции	Семинарские (практические) занятия	Консультации		
1	Симметричные алгоритмы шифрования	7	16	16	0	20	
2	Обеспечение целостности сообщений	7	8	8	0	16	
3	Алгоритмы с открытым ключом	7	10	10	0	22	
Итого за 7 семестр			34	34	0	58	Экз (54)
Итого часов			34	34	0	58	

4.2 План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Затраты времени, час. (из них с применением ДОТ)		
7	Симметричные алгоритмы шифрования	Для овладения знаниями: чтение учебной литературы, чтение дополнительной литературы Для закрепления и систематизации знаний: работа с конспектом лекций Для формирования умений: решение задач, работа с тренажером Подготовка к экзамену	В течение семестра	20 (20)	Тест, Пз	ИОС Domic

7	Обеспечение целостности сообщений	Для овладения знаниями: чтение учебной литературы Для закрепления и систематизации знаний: работа с конспектом лекций Для формирования умений: решение задач Подготовка к экзамену	В течение семестра	16 (16)	Тест, Пз	ИОС Domic
7	Алгоритмы с открытым ключом	Для овладения знаниями: чтение учебной литературы Для закрепления и систематизации знаний: работа с конспектом лекций Подготовка к экзамену	В течение семестра	22 (22)	Тест, Пз	ИОС Domic
Общая трудоемкость самостоятельной работы по дисциплине (час)				58		
Из них объем самостоятельной работы с использованием электронного обучения и дистанционных образовательных технологий (час)				58		
Бюджет времени самостоятельной работы, предусмотренный учебным планом для данной дисциплины (час)				58		

4.3 Содержание учебного материала

Трудоемкость дисциплины (з.е.)	5
Наименование основных разделов (модулей)	Симметричные алгоритмы шифрования Обеспечение целостности сообщений Алгоритмы с открытым ключом
Формы текущего контроля	Тест, лабораторная работа, практическое задание, устный опрос
Форма промежуточной аттестации	Экзамен

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость, час. (из них электронные часы)	Оценочные средства	Формируемые компетенции
1	1	Многоразовый блокнот	16 (0)	Тест, ЛР	ПК-6.3, ПК-6.6
2	2	Атака подменой сообщения	8 (0)	Тест, ЛР	ПК-6.6, ПК-1.1, ПК-6.3
3	3	Задача дискретного логарифмирования	10 (0)	Тест, ЛР	ПК-6.3, ПК-6.6, ПК-6.7, ПК-1.1

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение самостоятельной работы студентов

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	Симметричные алгоритмы шифрования	Симметричные криптосистемы. Шифрование AES	ПК-6	ПК-6.3 ПК-6.6 ПК-6.7
2	Обеспечение целостности сообщений	Вычисление кодов аутентификации сообщений	ПК-1, ПК-6	ПК-1.1 ПК-6.7
3	Алгоритмы с открытым ключом	Шифрование RSA	ПК-6	ПК-6.6 ПК-6.7

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 профессионального 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 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 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.

Формы внеаудиторной самостоятельной работы

Составление глоссария Цель самостоятельной работы: повысить уровень информационный культуры; приобрести новые знания; отработать необходимые навыки в предметной области учебного курса. Глоссарий — словарь специализированных терминов и их определений. Статья глоссария — определение термина. Содержание задания: сбор и систематизация понятий или терминов, объединенных общей специфической тематикой, по одному либо нескольким источникам. Выполнение задания: 1) внимательно прочитать работу; 2) определить наиболее часто встречающиеся термины; 3) составить список терминов, объединенных общей тематикой; 4) расположить термины в алфавитном порядке;

5) составить статьи глоссария: — дать точную формулировку термина в именительном падеже; — объемно раскрыть смысл данного термина Планируемые результаты самостоятельной работы: способность студентов решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Разработка проекта (индивидуального, группового) Цель самостоятельной работы: развитие способности прогнозировать, проектировать, моделировать. Проект — «ограниченное во времени целенаправленное изменение отдельной системы с установленными требованиями к качеству результатов, возможными рамками расхода средств и ресурсов и специфической организацией». Выполнение задания: 1) диагностика ситуации (проблематизация, целеполагание, конкретизация цели, форматирование проекта); 2) проектирование (уточнение цели, функций, задач и плана работы; теоретическое моделирование методов и средств решения задач; детальная проработка этапов решения конкретных задач; пошаговое выполнение запланированных проектных действий; систематизация и обобщение полученных результатов, конструирование предполагаемого результата, пошаговое выполнение проектных действий); 3) рефлексия (выяснение соответствия полученного результата замыслу; определение качества полученного продукта; перспективы его развития и использования). Предполагаемые результаты самостоятельной работы: готовность студентов использовать знание современных проблем науки и образования при решении образовательных и профессиональных задач; готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач; — способность прогнозировать, проектировать, моделировать.

Информационный поиск Цель самостоятельной работы: развитие способности к проектированию и преобразованию учебных действий на основе различных видов информационного поиска. Информационный поиск — поиск неструктурированной документальной информации. Список современных задач информационного поиска: решение вопросов моделирования; классификация документов; фильтрация, классификация документов; проектирование архитектур поисковых систем и пользовательских интерфейсов; извлечение информации (аннотирование и реферирование документов); выбор информационно-поискового языка запроса в поисковых системах. Содержание задания по видам поиска: поиск библиографический — поиск необходимых сведений об источнике и установление его наличия в системе других источников. Ведется путем разыскания библиографической информации и библиографических пособий (информационных изданий); поиск самих информационных источников (документов и изданий), в которых есть или может содержаться нужная информация; — поиск фактических сведений, содержащихся в литературе, книге (например, об исторических фактах и событиях, о биографических данных из жизни и деятельности писателя, ученого и т. п.). Выполнение задания:

- 1) определение области знаний;
- 2) выбор типа и источников данных;
- 3) сбор материалов, необходимых для наполнения информационной модели;
- 4) отбор наиболее полезной информации;
- 5) выбор метода обработки информации (классификация, кластеризация, регрессионный анализ и т.д.);
- 6) выбор алгоритма поиска закономерностей;
- 7) поиск закономерностей, формальных правил и структурных связей в собранной

информации;

8) творческая интерпретация полученных результатов.

Планируемые результаты самостоятельной работы: — способность студентов решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; готовность использовать знание современных проблем науки и образования при решении образовательных и профессиональных задач.

Разработка мультимедийной презентации Цели самостоятельной работы (варианты): — освоение (закрепление, обобщение, систематизация) учебного материала; — обеспечение контроля качества знаний; — формирование специальных компетенций, обеспечивающих возможность работы с информационными технологиями; — становление общекультурных компетенций. Мультимедийная презентация — представление содержания учебного материала, учебной задачи с использованием мультимедийных технологий.

Выполнение задания:

1. Этап проектирования: — определение целей использования презентации; — сбор необходимого материала (тексты, рисунки, схемы и др.); — формирование структуры и логики подачи материала; — создание папки, в которую помещен собранный материал.

2. Этап конструирования: — выбор программы MS PowerPoint в меню компьютера; — определение дизайна слайдов; — наполнение слайдов собранной текстовой и наглядной информацией; — включение эффектов анимации и музыкального сопровождения (при необходимости); — установка режима показа слайдов (титольный слайд, включающий наименование кафедры, где выполнена работа, название презентации, город и год; содержательный — список слайдов презентации, сгруппированных по темам сообщения; заключительный слайд содержит выводы, пожелания, список литературы и пр.).

3. Этап моделирования — проверка и коррекция подготовленного материала, определение продолжительности его демонстрации.

Планируемые результаты самостоятельной работы: — повышение информационной культуры студентов и обеспечение их готовности к интеграции в современное информационное пространство; — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; — способность к критическому восприятию, обобщению, анализу профессиональной информации, постановке цели и выбору путей ее достижения; — способность применять современные методики и технологии организации и реализации образовательного процесса на различных образовательных ступенях в различных образовательных учреждениях; — готовность использовать индивидуальные креативные способности для оригинального решения исследовательских задач.

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

4.5. Примерная тематика курсовых работ (проектов)

По данной дисциплине выполнение курсовых проектов (работ) не предусматривается.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература

1. Рябец, Леонид Владимирович. Задачник-практикум по криптографии [Текст] : учеб. пособие / Л. В. Рябец ; Вост.-Сиб. гос. акад. образования. - Иркутск : Изд-во ВСГАО, 2013. - 75 с. ; 21 см. - Библиогр.: с. 73-75. - ISBN 978-5-85827-864-1 : 90.00 р.

2. Лось, Алексей Борисович. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ [Электронный ресурс] : учебник / Лось А.Б., Нестеренко А.Ю., Рожков М.И. - Электрон. текстовые дан. - М. : Издательство Юрайт, 2016. - 473 с. - (Бакалавр. Академический курс). - ЭБС "Юрайт". - Неогранич. доступ. - ISBN 978-5-9916-6378-6 : 1065.00 р.

3. Введение в криптографию [Текст] : научное издание / ред. В. В. Ященко. - 4-е изд., доп. - М. : Изд-во МЦНМО, 2012. - 347 с. ; 22 см. - Алф. указ.: с. 341-347. - ISBN 978-5-4439-0026-1 : 490.56 р., 405.99 р.

б) дополнительная литература

1. Шаньгин, Владимир Федорович. Защита компьютерной информации. Эффективные методы и средства [Текст] : учеб. пособие / В. Ф. Шаньгин. - М. : ДМК Пресс, 2010. - 542 с. ; 24 см. - Библиогр.: с. 524-529. - Предм. указ.: с. 530-542. - ISBN 978-5-94074-518-1 : 447.20 р.

в) периодическая литература

Нет.

г) базы данных, информационно-справочные и поисковые системы

1. Java Cryptography Architecture (JCA) Reference Guide. URL: <https://docs.oracle.com/en/java/javase/11/security/java-cryptography-architecture-jca-reference-guide.html>

В соответствии с п. 4.3.4. ФГОС ВО, обучающимся в течение всего периода обучения обеспечен неограниченный доступ (удаленный доступ) к электронно-библиотечным системам:

— Открытая электронная база ресурсов и исследований «Университетская информационная система РОССИЯ» [Электронный ресурс] : сайт. – Режим доступа: <http://uisrussia.msu.ru> бессрочный

— Государственная информационная система «Национальная электронная библиотека» [Электронный ресурс] : сайт. – Режим доступа: <http://нэб.рф>. бессрочный

— Научная электронная библиотека «ELIBRARY.RU» [Электронный ресурс] : сайт. - Контракт № 148 от 23.12.2020 г. Акт от 24.12.2020 г. Срок действия по 31.12.2022 г. – Режим доступа: <http://elibrary.ru/>

— ЭБС «Издательство Лань». Контракт № 04-Е-0346 от 12.11.2021 г. № 976 от 14.11.2021 г. Срок действия по 13.11.2022 г. – Режим доступа: <https://www.e.lanbook.com>

— ЭБС ЭЧЗ «Библиотех». Государственный контракт № 019 от 22.02.2011 г. ООО «Библиотех». Лицензионное соглашение к Государственному контракту № 019 от 22.02.2011. Срок действия: бессрочный. – Режим доступа: <https://isu.bibliotech.ru/>

— ЭБС «Рукопт» ЦКБ «Бибком». № 04-Е-0343 от 12.11.2021 г. Акт № 6К-5195 от 14.11.2021 г. Срок действия по 13.11.2022г. – Режим доступа: <http://rucont.ru>

— ЭБС «Айбукс.ру/ibooks.ru» ООО «Айбукс». Контракт № 04-Е-0344 от 12.11.2021

г.; Акт от 14.11.2021 г. Срок действия по 13.11.2022 г. – Режим доступа: <http://ibooks.ru>

— Электронно-библиотечная система «ЭБС Юрайт». ООО «Электронное издательство Юрайт». Контракт № 04-Е-0258 от 20.09.2021г. Контракт № 04-Е-0258 от 20.09.2021 г. Срок действия по 17.10. 2022 г. – Режим доступа: <https://urait.ru>

— УБД ИВИС. Контракт № 04-Е-0347 от 12.11.2021 г. Акт от 15.11.2021 г. Срок действия с 01.01.2022 по 31.12.2022 г. – Режим доступа: <http://dlib.eastview.com>

— Электронная библиотека ИД Гребенников. Контракт № 04-Е-0348 от 12.11.2021г.; Акт № 348 от 15.11.2021 г. Срок действия с 01.01.2022 по 31.12.2022 – Режим доступа: <http://grebennikon.ru>

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
---	---	--

Специальные помещения: Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля, промежуточной аттестации.	Аудитория оборудована специализированной учебной мебелью, техническими средствами обучения, служащими для представления информации большой аудитории: Ноутбук(AserAspirev3-5516 (AMDA10-4600M 2300 МГц)) (1 штука) с неограниченным доступом к сети Интернет; Проектор Vivitek, экран ScreenVtdiaEcot- 3200*200MW 1:1, колонки, наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочей программе дисциплины «Архитектурный подход к развитию предприятий и информационных систем». Учебная лаборатория: компьютеры для проведения практических работ (Системный блок AMDAthlon-64 X3 445 3100 МГц), Монитор LG F1742S (2 штуки), Монитор ViewSonic VA703b(24 штуки) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации; проектор Sony XGA VPLSX535, экран ScreenVtdiaEcot- 3200*200MW 1:1	ОС Windows: DreamSpark Premium, Договор № 03-016-14 от 30.10.2014 Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcadmsStdnt w/Faculty (15000 лицензий) Kaspersky Endpoint Security длябизнеса- стандартный Russian Edition. 15002499 Node 1 year Educational License № 1B08-170221-054045-730-177 BusinessStudio Лицензия № 7464 (бессрочно)
--	---	---

Специальные помещения: компьютерный класс (учебная аудитория) для групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), организации самостоятельной работы, в том числе, научно-исследовательской	Аудитория оборудована специализированной учебной мебелью, техническими средствами обучения: компьютеры (системный блок AMD Athlon 64 X2 DualCore 3600+ 1900 МГц (15 штук), Монитор LGFlatron L1742SE (14 штук), Монитор ViewSonic VG720) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.	ОС Windows: DreamSpark Premium, Договор № 03-016-14 от 30.10.2014 Microsoft Office: 0365ProPiusOpenStudents ShrdSvr ALNG subs VL NL I MthAcadmsStdnt w/Faculty (15000 лицензий) Kaspersky Endpoint Security для бизнеса- стандартный Russian Edition. 15002499 Node 1 year Educational License № 1B08-170221-054045-730-177
--	---	---

6.2. Программное обеспечение

№	Наименование Программного продукта	Кол-во	Обоснование для пользования ПО	Дата выдачи лицензии	Срок действия права пользования
1	Комплект разработчика приложений Java Platform (JDK) 21, Standard Edition	50	Условия правообладателя	Условия правообладателя	Условия правообладателя

6.3. Технические и электронные средства

Методической системой преподавания предусмотрено использование технических и электронных средств обучения и контроля знаний студентов: мультимедийные презентации, фрагменты фильмов.

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации программы данной дисциплины используются различные образовательные технологии, в том числе электронное обучение и дистанционные образовательные технологии.

Проблемное обучение	Создание в учебной деятельности проблемных ситуаций и организация активной самостоятельной деятельности учащихся по их разрешению, в результате чего происходит творческое овладение знаниями, умениями, навыками, развиваются мыслительные способности
---------------------	---

Разноуровневое обучение	У преподавателя появляется возможность помогать слабому, уделять внимание сильному, реализуется желание сильных учащихся быстрее и глубже продвигаться в образовании. Сильные учащиеся утверждают в своих способностях, слабые получают возможность испытывать учебный успех, повышается уровень мотивации ученья.
Проектные методы обучения	Работа по данной методике дает возможность развивать индивидуальные творческие способности учащихся, более осознанно подходить к профессиональному и социальному самоопределению
Исследовательские методы в обучении	Дает возможность учащимся самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося
Лекционно-семинарско-зачетная система	Данная система дает возможность сконцентрировать материал в блоки и преподносить его как единое целое, а контроль проводить по предварительной подготовке обучающихся
Информационно-коммуникационные технологии	Изменение и неограниченное обогащение содержания образования, использование интегрированных курсов, доступ в ИНТЕРНЕТ.

Наименование тем занятий с использованием активных форм обучения:

№	Тема занятия	Вид занятия	Форма / Методы интерактивного обучения	Кол-во часов (из них электронные часы)
1				
2				
3				
4				
5				
6				

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные средства текущего контроля

№ п/п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
-------	--------------	-------------------------------	--

1	Тест	Симметричные алгоритмы шифрования. Обеспечение целостности сообщений. Алгоритмы с открытым ключом.	ПК-6.3, ПК-6.6, ПК-6.7
2	Лабораторная работа	Симметричные алгоритмы шифрования. Обеспечение целостности сообщений. Алгоритмы с открытым ключом.	ПК-6.3, ПК-1.1
3	Практическое задание	Симметричные алгоритмы шифрования. Обеспечение целостности сообщений. Алгоритмы с открытым ключом.	ПК-6.3, ПК-6.6, ПК-6.7, ПК-1.1
4	Устный опрос	Симметричные алгоритмы шифрования. Обеспечение целостности сообщений.	ПК-6.3, ПК-6.6

Примеры оценочных средств для текущего контроля

Демонстрационный вариант теста

1. Задание с единичным выбором. Выберите один правильный ответ.

Пусть функция $F: K \times \{0,1\}^n \rightarrow \{0,1\}^n$ является безопасной PRP. Предположим, что $n=128$. Пусть t --- одноразовый идентификатор и пользователь шифрует сообщение m с использованием вектора $IV=F(k,t)$. Этот вектор инициализации используется в для режима шифрования CBC с использованием функции F . Для шифрования сообщения m и одноразового идентификатора t используется один и тот же ключ k . Можно показать, что такая схема не является безопасной для атаки на основе выборочного открытого текста. Атакующий отправляет на шифрование сообщение, состоящее из двух блоков: $m=(0_n, 0_n)$ с одноразовым идентификатором $t=0_n$. В результате он получает шифр-текст, состоящий из двух блоков (c_0, c_1) . Далее атакующий отправляет на шифрование один блок открытого текста $m_1=c_0 \oplus c_1$ с одноразовым идентификатором $t=c_0$. В ответ атакующий получает шифр-текст c_2 . Определите, какое отношение связывает (c_0, c_1, c_2) .

- a. $c_0=c_2$
- b. $c_1=c_2$
- c. $c_1=c_0$
- d. $c_1=0^n$

2. Задание с единичным выбором. Выберите один правильный ответ.

Рассмотрим схему CBC-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 готового тега сообщения m и ключа MAC получить тег нового сообщения m' .

- a. 4

- b. 3
- c. n-1
- d. 2

3. Задание с единичным выбором. Выберите один правильный ответ.

Тип доверенной третьей стороны, которая выдает цифровые сертификаты, используемые для создания цифровых подписей и пары ключей называется

- a. PKI
- b. CA
- c. CSP

4. Задание с единичным выбором. Выберите один правильный ответ.

Укажите механизм безопасности, который позволяет HTTPS веб-сайтам противостоять выдаче себя за другое лицо со стороны злоумышленников, использующих мошеннические сертификаты

- a. Data Execution Prevention
- b. Public Key Pinning
- c. Unified Threat Management

8.2. Оценочные средства для промежуточной аттестации

Вопросы к экзамену:

1. Общие принципы криптографии. Защита от несанкционированного доступа. Основные способы криптоанализа простых шифров. Идеальный шифр. Шифр Вернама. Лемма о теоретически стойком шифре. Поточковые шифры. Атаки на поточковые шифры. Двухразовый блокнот.

2. Примеры поточковых шифров. RC4 и его уязвимости. Безопасность поточковых генераторов. Статистический тест для генератора. Криптографическое определение псевдослучайного генератора.

3. Принцип итерирования. Понятие псевдослучайной функции и псевдослучайной перестановки. Шифр ГОСТ 28147. Описание структуры. Теорема о трехраундовой сети Фейстеля. Шифр AES. Описание структуры и принципы работы. Переборные атаки на блочные шифры.

4. 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.

5. Коды аутентификации сообщений. Построение кодов аутентификации больших сообщений. Конструкции CBC-MAC и NMAC. Их эффективность. Схема атаки с использованием коллизий.

6. Конструкция HMAC. Построение кодов аутентификации больших сообщений. Механизмы набивки сообщений.

7. Построение кодов аутентификации сообщений из стойких к коллизиям функций. Атака на основе парадокса дней рождений.

8. Необходимость применения аутентичного шифрования. Понятие целостности шифр-текста. Атака на основе выборочного шифр-текста. Аутентичное шифрование на примере протокола TLS.

9. Стандарт PKCS1. Атаки на RSA. Атака при малом значении закрытого ключа.

10. Задача дискретного логарифмирования. Метод ключевого обмена Диффи-Хеллмана.

11. Схема Шамира разделения секрета.

12. Алгоритм Шнорра доказательства знания

Примеры заданий к экзамену:

1. Практическое задание. Расшифрование данных по варианту

Выполнить расшифрование данных по предложенному варианту.

2. Устный опрос. Подготовка по определениям

Подготовка по определениям. Например, определение семантически-стойкого шифра, безопасного потокового генератора, безопасной псевдослучайной функции.

3. Устный опрос. Опрос по определениям

Опрос по определениями. Например определение безопасной схемы построения кодов аутентификации, определение криптографически стойкой хеш-функции и т.п.

4. Практическое задание. Создание самоподписанного сертификата

В данном задании вы выступаете в роли некоторого удостоверяющего центра. Вам известны [закрытый ключ](#) и [сертификат открытого ключа](#) этого удостоверяющего центра. Такая пара ключей используется только для работы с подчиненными сертификатами и не используется для работы непосредственно с сообщениями.

Требуется сгенерировать для некоторого абонента, обратившегося в УЦ, пару ключей для формирования подписи сообщений, сформировать сертификат открытого ключа, подписать некоторое сообщение на ключе абонента и передать сообщение, подпись сообщения и сертификат открытого ключа для проверки целостности сообщения.

Часть 1. Создание собственной пары ключей абонента

С помощью OpenSSL создайте собственную пару ключей абонента по следующей схеме:

a. Сгенерируйте с помощью команды `openssl genrsa` закрытый ключ обратившегося абонента.

b. Сгенерируйте с помощью команды `openssl req` запрос на создание сертификата открытого ключа. По параметрам сертификата должно быть понятно, что он принадлежит "этому абоненту" (ваши ФИО). Для использования команды потребуется [файл конфигурации](#) OpenSSL

c. С помощью команды `openssl X509` создайте сертификат открытого ключа и подпишите его с помощью закрытого ключа удостоверяющего центра.

Часть 2. Подпись сообщения

Работать можно по следующей схеме:

— Создайте некоторое текстовое сообщение.

a. С помощью команды `openssl dgst` подпишите это сообщение с хеш-функцией SHA512 на **закрытом ключе** абонента.

b. Отправьте на проверку файл с текстовым сообщением, файл с подписью сообщения и сертификатом абонента.

Проверка электронной подписи будет проводиться следующими командами:

```
openssl x509 -pubkey -noout -in student.cer > pubkey.pem
```

```
openssl dgst -sha512 -verify pubkey.pem -signature sign.file msg.file
```

Другие оценочные средства:

Не предусмотрены

Разработчики:

_____	_____	_____
(подпись)	доцент (занимаемая должность)	Л.В. Рябец (инициалы, фамилия)

Программа составлена в соответствии с требованиями ФГОС ВО и учетом рекомендаций ПООП по направлению подготовки 09.03.03 «Прикладная информатика».

Программа рассмотрена на заседании кафедры алгебраических и информационных систем

Протокол № __ от «__» _____ 20__ г.

Зав. кафедрой

В.И. Пантелеев

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.