

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Рукович Александр Владимирович

Должность: Директор

Дата подписания: 05.03.2025 11:55:32

Уникальный программный ключ:

f45eb7c44954caac05ea7d4f32eb8d7d6b3cb96ae6d9b4bda094afddaffb705f

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Технический институт (филиал) ФГАОУ ВО «СВФУ» в г. Нерюнгри

Кафедра Математики и информатики

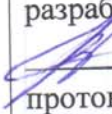
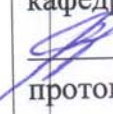
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.08.02 Методы и средства защиты компьютерной информации

для программы бакалавриата
по направлению подготовки 01.03.02 «Прикладная математика и информатика»
Направленность (профиль) программы: Системное программирование и компьютерные технологии

Форма обучения: очная

Автор(ы): Похорукова М.Ю., к.т.н., доцент кафедры МиИ, maria.pokhorukova@gmail.com

РЕКОМЕНДОВАНО	ОДОБРЕНО	ПРОВЕРЕНО
Заведующий кафедрой разработчика МиИ  / Самохина В.М. протокол № <u>10</u> от « <u>05</u> » <u>05</u> 20 <u>23</u> г.	Заведующий выпускающей кафедрой МиИ  / Самохина В.М. протокол № <u>10</u> от « <u>05</u> » <u>05</u> 20 <u>23</u> г.	Нормоконтроль в составе ОПОП пройден / Специалист УМО <u>В.Тулба</u> / Кравчук К.А. « <u>15</u> » <u>05</u> 20 <u>23</u> г.
Рекомендовано к утверждению в составе ОПОП Председатель УМС  Ядреева Л.Д. протокол УМС № <u>10</u> от « <u>19</u> » <u>05</u> 20 <u>23</u> г.		Зав. библиотекой  Т. Болшова « <u>15</u> » <u>05</u> 20 <u>23</u> г.

Нерюнгри 2023

1. АННОТАЦИЯ
к рабочей программе дисциплины
Б1.В.ДВ.08.02 Методы и средства защиты компьютерной информации
Трудоемкость 3 з.е.

1.1. Цель освоения и краткое содержание дисциплины

Цель освоения дисциплины: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартам шифрования;
- изучение математических основ защиты информации; а также методов, средств и инструментов шифрования, применяемых в сфере информационных технологий;
- привитие навыков работы с методами шифрования и криптоанализа.

Краткое содержание дисциплины: Основные понятия информационной безопасности и защиты информации. Криптография и криптосистемы. Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Планируемые результаты освоения программы (код и содержание компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине	Оценочные средства
Профессиональные компетенции	ПК-3: способен осуществлять алгоритмизацию поставленных задач и применять выбранные языки программирования для написания программного кода.	ПК-3.1: Способен выполнять формализацию и алгоритмизацию поставленных задач в соответствии с требованиями технического задания ПК-3.2: Способен написать программный код с использованием языков программирования, использовать выбранную среду программирования и средства системы управления базами данных, стандартные библиотеки языка программирования ПК-3.3: Способен применять методы и приемы отладки	знать: основные понятия информационной безопасности; методы криптографии и средства защиты от удаленных атак через сеть; особенности биометрических методов защиты информации. уметь: написать программный код для решения задач профессиональной деятельности с учетом основных требований защиты компьютерной информации. владеть: навыками выбора методов и приемов отладки программного кода на основе теоретических	Лабораторные работы, СРС, контрольная работа

		программного кода, интерпретировать сообщения об ошибках, применять современные компиляторы, отладчики программного кода	знаний в области информационной безопасности.	
--	--	--	---	--

1.3. Место дисциплины в структуре образовательной программы

Индекс	Наименование дисциплины (модуля), практики	Семестр изучения	Индексы и наименования учебных дисциплин (модулей), практик	
			на которые опирается содержание данной дисциплины (модуля)	для которых содержание данной дисциплины (модуля) выступает опорой
Б1.В.ДВ.08.02	Методы и средства защиты компьютерной информации	8	Б1.О.22 Проектирование информационных систем Б1.О.07 Основы права Б1.В.02 Разработка и сопровождение программного обеспечения Б2.В.01(П) Производственная II технологическая практика	Б2.В.02(П) Проектно-технологическая практика Б3.01(Д) Выполнение и защита выпускной квалификационной работы

1.4. Язык преподавания: русский.

2. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Выписка из учебного плана (гр. Б-ПМ-23):

Код и название дисциплины по учебному плану	Б1.В.ДВ.08.02 Методы и средства защиты компьютерной информации	
Курс изучения	4	
Семестр(ы) изучения	8	
Форма промежуточной аттестации (зачет/экзамен)	зачет	
Контрольная работа, семестр выполнения	8	
Трудоемкость (в ЗЕТ)	3 ЗЕТ	
Трудоемкость (в часах) (сумма строк №1,2,3), в т.ч.:	108	
№1. Контактная работа обучающихся с преподавателем (КР), в часах:	Объем аудиторной работы, в часах	В т.ч. с применением ДОТ или ЭО ¹ , в часах
Объем работы (в часах) (1.1.+1.2.+1.3.):	38	-
1.1. Занятия лекционного типа (лекции)	12	-
1.2. Занятия семинарского типа, всего, в т.ч.:	-	-
- семинары (практические занятия, коллоквиумы и т.п.)	-	-
- лабораторные работы	24	-
- практикумы	-	-
1.3. КСР (контроль самостоятельной работы, консультации)	2	-
№2. Самостоятельная работа обучающихся (СРС) (в часах)	70	
№3. Количество часов на экзамен (при наличии экзамена в учебном плане)	-	

¹Указывается, если в аннотации образовательной программы по позиции «Сведения о применении дистанционных технологий и электронного обучения» указан ответ «да».

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

3.1. Распределение часов по разделам и видам учебных занятий

Раздел	Всего часов	Контактная работа, в часах									Часы СРС
		Лекции	из них с применением ЭО и ДОТ	Лабораторные занятия	из них с применением ЭО и ДОТ	Лабораторные работы	из них с применением ЭО и ДОТ	Практикумы	из них с применением ЭО и ДОТ	КСР (консультации)	
8 семестр											
Основные понятия информационной безопасности и защиты информации	25	4	-	8	-	-	-	-	-	-	8 (ЛР) 5 (Т)
Криптография и криптосистемы.	26	4	-	8	-	-	-	-	-	1	8 (ЛР) 10 (СРС) 5 (Т)
Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.	47	4	-	8	-	-	-	-	-	1	8 (ЛР) 10 (СРС) 16 (К)
Итого:	108	12	-	24	-	-	-	-	-	2	70

Примечание: ЛБ - подготовка к лабораторным занятиям, СРС – выполнение самостоятельных работ, К – написание контрольной работы.

3.2. Содержание тем программы дисциплины

Тема 1. Основные понятия информационной безопасности и защиты информации.

Информация. Основные понятия и определения информационной безопасности и защиты информации. Закон о защите информации. Защита информации от утечки. Защита информации от несанкционированного доступа.

Тема 2. Криптография и криптосистемы.

Криптография и криптосистемы. Хеш-функции. Шифры. Аутентификация. Понятие стойкости криптографических алгоритмов. Схема шифрованной связи. Шифрование. Симметричное и несимметричное шифрование. Способы шифрования. Шифры гаммирования и генераторы псевдослучайной последовательности.

Тема 3. Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.

Система биометрической аутентификации пользователя. Дактилоскопические системы аутентификации. Система аутентификации по форме ладони. Электронные идентификаторы.

Идентификаторы на базе контактных смарткарт. Бесконтактные идентификаторы RFID. Методы обнаружения сетевых атак. Электронная цифровая подпись

3.3. Формы и методы проведения занятий, применяемые учебные технологии

В процессе преподавания дисциплины используются традиционные технологии наряду с активными и интерактивными технологиями.

Учебные технологии, используемые в образовательном процессе

Раздел дисциплины	Семестр	Используемые активные/интерактивные образовательные технологии	Количество часов
Основные понятия информационной безопасности и защиты информации	8	Лекция-визуализация, презентация, проблемное обучение	4
Криптография и криптосистемы.		Лекция-визуализация, презентация, проблемное обучение	4
Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.		Дискуссионные методы, case-study (анализ конкретных, практических ситуаций).	6
Итого:			14

При *проблемном обучении* под руководством преподавателя формулируется проблемный вопрос, создаются проблемные ситуации, в результате чего активизируется самостоятельная деятельность студентов, происходит овладение профессиональными компетенциями.

Дискуссионные методы могут быть реализованы в виде диалога участников или групп участников, групповой дискуссии, анализа конкретной ситуации или других.

4. Перечень учебно-методического обеспечения для самостоятельной работы² обучающихся по дисциплине

Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудоемкость (в часах)	Формы и методы контроля
8 семестр				
1	Основные понятия информационной безопасности и защиты информации	Подготовка к лабораторным занятиям Тестирование	8 (ЛР) 5 (Т)	Анализ теоретического материала, выполнение практических заданий. Выполнение теста
2	Криптография и криптосистемы.	Подготовка к лабораторным занятиям СРС Тестирование	8 (ЛР) 10 (СРС) 5 (Т)	Анализ теоретического материала, выполнение практических заданий. Выполнение задания СРС (ауд. СРС) Выполнение теста
3	Электронная цифровая подпись. Методы и	Подготовка к лабораторным	8 (ЛР) 10	Анализ теоретического материала, выполнение

² Самостоятельная работа студента может быть внеаудиторной (выполняется студентом самостоятельно без участия преподавателя – например, подготовка конспектов, выполнение письменных работ и др.) и аудиторной (выполняется студентом в аудитории самостоятельно под руководством преподавателя – например, лабораторная или практическая работа).

средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.	занятиям Выполнение контрольной работы	(СРС) 16 (К)	практических заданий. Выполнение контрольной работы
Итого:		70	

Лабораторная работа

В период освоения дисциплины студенты посещают лекционные занятия, самостоятельно изучают дополнительный теоретический материал к лабораторным занятиям. Критериями оценки работы на лабораторных занятиях является: полнота и правильность выполненного задания; степень осознанности, понимания изученного; оформление задания.

Темы лабораторных работ

Тема 1. Основные понятия информационной безопасности и защиты информации.

Тема 2. Криптография и криптосистемы.

Тема 3. Электронная цифровая подпись. Методы и средства защиты от удаленных атак через сеть. Биометрические методы защиты информации.

Максимальный балл, который студент может набрать на лабораторном занятии – 3 балла.

Критерии оценки:

0 баллов - ставится, если студент не выполнил лабораторную работу.

1 балл - ставится, если студент обнаруживает знание и понимание основных положений лабораторной работы, но при выполнении заданий допущены ошибки или задание выполнено на 50%; оформление работы выполнено недостаточно последовательно (отсутствуют цель/листинг/результаты/выводы).

2 балла - ставится, если студентом при выполнении заданий допущены неточности или задание выполнено на 70%; оформление работы выполнено с ошибками (отсутствуют цель/выводы).

3 балла - ставится, если студент полностью выполнил задание, правильно ответил на теоретические вопросы преподавателя, оформление работы выполнено последовательно и полно (присутствуют цели работы, задания, листинг программ, результаты и выводы).

Самостоятельная работа студента

Включает проработку конспектов лекций, обязательной и дополнительной учебной литературы в соответствии с планом занятия; выполнение заданий. Основной формой проверки СРС является устный фронтальный опрос на занятии и письменные ответы на вопросы для проверки знаний по теме.

Темы заданий для самостоятельной работы студентов

Тема 1. Принципы засекречивания сведений и отнесения их к государственной тайне

Тема 2. Порядок отнесения информации к коммерческой тайне и способы ее получения

Критерии оценивания:

0 баллов – самостоятельная работа не выполнена.

1 балл – демонстрирует, лишь поверхностный уровень выполнения работы, в содержании выполнения задания допущены принципиальные ошибки.

2 балла – ставится тогда, когда студент выполнил самостоятельную работу, но дает не точные ответы на заданные вопросы.

3 балла – ставится тогда, когда студент выполнил самостоятельную работу, показан высокий уровень освоения студентом учебного материала, содержание выполнения задания не содержит ошибок.

Тестирование

Образцы тестовых заданий:

1. Что такое несанкционированный доступ?

а) доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

- b) удаление не нужной информации
 - c) вход в систему без согласования с руководителем организации
2. Какой алгоритм шифрования используется в платёжных системах Яндекс.Деньги, Web-money и Cyberplat ?
- a) RSA
 - b) ECDSA
 - c) DSA
3. Что НЕ относится к угрозам информационной безопасности?
- a) преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)
 - b) классификация информации
 - c) сбой и отказы оборудования (технических средств)
4. Шифрование с симметричным ключом предполагает, что ... ?
- a) используются два разных ключа
 - b) оба ключа одинаковы
 - c) используется один ключ
5. Что такое электронная цифровая подпись?
- a) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе
 - b) электронный документ, достоверность которого подтверждена удостоверяющим центром
 - c) набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями

Критерии оценки:

Процент выполненных тестовых заданий	Количество набранных баллов
91% - 100%	10
81% - 90%	9
71% - 80%	8
61% - 70%	7
51% - 60%	6
<50%	0

Контрольная работа

Контрольная работа предполагает выполнение письменной работы с обязательными практическими примерами по одной из тем.

Тематика контрольных работ

1. Угрозы и обеспечение безопасности автоматизированных ИС.
2. Криптография и криптосистемы.
3. Стандарт шифрования данных DES.
4. Алгоритм шифрования данных IDEA.
5. Электронная цифровая подпись.
6. Управление криптографическими ключами.
7. Резервное хранение информации RAID.
8. Биометрические методы защиты информации.
9. Программы с потенциально опасными последствиями.
10. Правовые аспекты информационной безопасности.
11. Методы защиты от копирования данных.

Критерии оценки:

№	Критерий		
---	----------	--	--

1.	Соответствие содержания заявленной теме	16	26
2.	Логичность и последовательность в изложении материала	16	26
3.	Способность к работе с литературными источниками, Интернет-ресурсами, справочной и энциклопедической литературой	16	26
4.	Способность к выполнению практических заданий по заданной тематике	16	26
5.	Использование соответствующих компьютерных программ при выполнении практических заданий	16	26
6.	Анализ полученных результатов, наличие вывода о проделанной работе	16	26
7.	Правильность оформления (наличие всех структурных частей, структурная упорядоченность, ссылки на литературу, цитаты, таблицы, рисунки и т.д.);	16	26
8.	Соответствие оформления правилам компьютерного набора текста (соблюдение объема, шрифтов, интервалов, выравнивания текста на страницах, нумерация страниц и т.д.);	16	26
9.	Наличие презентационного материала	16	26
10.	Правильность ответов на заданные вопросы по заявленной теме	16	26
	Итого	10	20

Соответствие критерию: полностью соответствует – 2 балла; частично – 1 балл; не соответствует – 0 баллов.

5. Методические указания для обучающихся по освоению дисциплины

Методические указания для помощи обучающимся в успешном освоении дисциплины в соответствии с запланированными видами учебной и самостоятельной работы обучающихся размещены в СДО Moodle: <http://moodle.nfygu.ru/course/view.php?id=13347>

Рейтинговый регламент по дисциплине:

№	Вид выполняемой учебной работы (контролирующие материалы)		Количество баллов (min)	Количество баллов (max)	Примечание
	Испытания / Формы СРС	Время, час			
	Подготовка к лабораторным заданиям	12ЛР*26=246	12ЛР*26=246	12ЛР*36=366	Теоретическое изучение материала, решение задач
2	Выполнение контрольной работы	16	10	20	в письменном виде, по вариантам
3	Выполнение самостоятельной работы	10СРС*2=20	8СРС*2=16	8СРС*3=24	в письменном виде, по вариантам
4	Тестирование	2Т*5=10	2Т*5=10	2Т*10=20	
	Итого:	70	606	1006	

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Показатели, критерии и шкала оценивания

Коды оцениваемых компетенций	Показатель оценивания (по п.1.2.РПД)	Уровни освоения	Критерии оценивания (дескрипторы)	Оценка
ПК-3: способен осуществлять алгоритмизацию поставленных задач и применять	знать: основные понятия информационной безопасности; методы криптографии и	Освоено	Обучаемый показал полное знание учебно-программного материала, успешно выполнил предусмотренные	Зачтено

выбранные языки программирования для написания программного кода	<p>средства защиты от удаленных атак через сеть; особенности биометрических методов защиты информации.</p> <p>уметь: написать программный код для решения задач профессиональной деятельности с учетом основных требований защиты компьютерной информации.</p> <p>владеть: навыками выбора методов и приемов отладки программного кода на основе теоретических знаний в области информационной безопасности.</p>		рабочей программой задания, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе профессиональной деятельности.	
		Не освоено	Обучаемый не знает большей части основного содержания дисциплины, допускает грубые ошибки в формулировках основных понятий и не умеет использовать полученные знания при решении типовых практических задач в области профессиональной деятельности.	Не зачтено

6.2. Методические материалы, определяющие процедуры оценивания

Характеристики процедуры	
Вид процедуры	зачет
Цель процедуры	выявить степень сформированности компетенций ПК-3
Локальные акты вуза, регламентирующие проведение процедуры	Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся СВФУ, версия 3.0, утверждено ректором СВФУ 19.02.2019 г. Положение о балльно-рейтинговой системе в СВФУ, версия 4.0, утверждено 21.02.2018 г.
Субъекты, на которых направлена процедура	студенты 4 курса бакалавриата
Период проведения процедуры	Летняя экзаменационная сессия
Требования к помещениям и материально-техническим средствам	10 компьютеров
Требования к банку оценочных средств	-
Описание проведения процедуры	В соответствии с п. 5.13 Положения о балльно-рейтинговой системе в СВФУ, зачет «ставится при наборе 60 баллов». Таким образом, процедура зачета не предусмотрена.
Шкалы оценивания результатов	-
Результаты процедуры	В результате сдачи всех заданий студенту необходимо набрать не менее 60 баллов, чтобы получить зачет.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины³

№	Автор, название, место издания, издательство, год издания учебной литературы, вид и характеристика иных информационных ресурсов	Наличие грифа, вид грифа	Библиотека ТИ (ф) СВФУ, кол-во экземпляров	Электронные издания: точка доступа к ресурсу (наименование ЭБС, ЭБ СВФУ)	Количество студентов
Основная литература⁴					
1	Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для студ. вузов / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 2-е изд., стер. – Москва: Академия, 2007. – 331 с.: ил. – (Высшее профессиональное образование). – Библиогр.: с. 327-328. – ISBN 978-5-7695-4148-3 : 208?67	Гриф МО РФ	20		18
2	Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ;			http://biblioclub.ru/index.php?page=book&id=428605	18
Дополнительная литература					
3	Ковалев, Д. В. Информационная безопасность : учебное пособие : [16+] / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.			https://biblioclub.ru/index.php?page=book&id=493175	18
4	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.			https://biblioclub.ru/index.php?page=book&id=576726	18

³ Для удобства проведения ежегодного обновления перечня основной и дополнительной учебной литературы рекомендуется размещать раздел 7 на отдельном листе, с обязательной отметкой в Учебной библиотеке.

⁴ Рекомендуется указывать не более 3-5 источников (с грифами).

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сеть-Интернет), необходимых для освоения дисциплины

Университетская библиотека ONLINE - <http://biblioclub.ru/>

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Виды учебных занятий*	Наименование аудиторий, кабинетов, лабораторий и пр.	Перечень оборудования
1.	Лекционные занятия	Мультимедийный кабинет	интерактивная доска, ноутбук, мультимедийный проектор
2.	Подготовка к СРС	Кабинет для СРС № 402	Компьютер, доступ к интернет
3.	Лабораторные занятия	Кабинет № 201, 207	Компьютеры, доступ к интернет

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

10.1. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине⁵

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

- использование на занятиях электронных изданий (чтение лекций с использованием слайд-презентаций, электронного учебного пособия), видео- и аудиоматериалов (через Интернет);
- организация взаимодействия с обучающимися посредством электронной почты и СДО Moodle.

10.2. Перечень программного обеспечения

- MS Office, MS Visual Studio.

10.3. Перечень информационных справочных систем

Не используются.

⁵В перечне могут быть указаны такие информационные технологии, как использование на занятиях электронных изданий (чтение лекций с использованием слайд-презентаций, электронного курса лекций, графических объектов, видео- аудио- материалов (через Интернет), виртуальных лабораторий, практикумов), специализированных и офисных программ, информационных (справочных) систем, баз данных, организация взаимодействия с обучающимися посредством электронной почты, форумов, Интернет-групп, скайп, чаты, видеоконференцсвязь, компьютерное тестирование, дистанционные занятия (олимпиады, конференции), вебинар (семинар, организованный через Интернет), подготовка проектов с использованием электронного офиса или оболочки) и т.п.

