МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт математики и механики им. Н.И. Лобачевского

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Введение в криптографию

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Наука о данных
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018

Содержание

Программу дисциплины разработал(а)(и): профессор, д.н. (доцент) Тронин С.Н. (Кафедра Интеллектуальные технологии поиска, Институт информационных технологий и интеллектуальных систем), Serge.Tronin@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-2	Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Основные идеи, на которых основана современная криптография. Классические примеры шифров, цифровых подписей, и некоторых других криптографических протоколов. Основные идеи, на которых основана эллиптическая криптография. Примеры затемненных цифровых подписей. Первичные сведения о постквантовой криптографии.

Должен уметь:

Строить новые примеры шифров и цифровых подписей, исходя из общих конструкций, изложенных в лекционном курсе. Самостоятельно изучать новые сведения по криптографии, используя специальную литературу.

Должен владеть:

Методикой анализа корректности построения шифров и цифровых подписей, а также оценки их криптостойкости.

Должен демонстрировать способность и готовность:

Расширять область своих знаний в криптографии и криптоанализе.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.04.02 Дисциплины (модули)" основной профессиональной образовательной программы 02.03.01 "Математика и компьютерные науки (Наука о данных)" и относится к дисциплинам по выбору.

Осваивается на 4 курсе в 7 семестре.

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

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 68 часа(ов), в том числе лекции - 32 часа(ов), практические занятия - 36 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 22 часа(ов).

Контроль (зачёт / экзамен) - 18 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 7 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)						Самостоятельная работа
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
1.	Тема 1. Общая характеристика криптографии и криптоанализа. Шифры и								

секретные ключи. Атаки на шифры. Примеры шифров. Одноключевая криптография и криптография с открытым ключом.

N	Разделы дисциплины / модуля	Се-местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само-стоя-тель-ная ра-бота
			Лекции, всего	Лекции в эл. форме	Практи-ческие занятия, всего	Практи-ческие в эл. форме	Лабора-торные работы, всего	Лабора-торные в эл. форме	
2.	Тема 2. Потоковые и блочные шифры. DES и AES.	7	3	0	2	0	0	0	2
3.	Тема 3. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана. Проблема доскретного логарифма.	7	3	0	4	0	0	0	2
4.	Тема 4. Криптосистема RSA, и ее криптостойкость.	7	3	0	2	0	0	0	2
5.	Тема 5. Общее определение цифровых подписей. Цифровая подпись RSA. Криптографические хэш-функции.	7	2	0	2	0	0	0	2
6.	Тема 6. Криптосистема Эль-Гамаля, и постренные по тому же принципу цифровые подписи.	7	3	0	6	0	0	0	4
7.	Тема 7. Цифровые подписи DSA и Шнорра.	7	2	0	4	0	0	0	2
8.	Тема 8. Затемненные цифровые подписи. Финансовая криптография и электронное голосование.	7	3	0	2	0	0	0	1
9.	Тема 9. Эллиптическая криптография	7	4	0	5	0	0	0	4
10.	Тема 10. Постквантовая криптогафия. Криптосистема NTRU	7	5	0	5	0	0	0	1
	Итого		32	0	36	0	0	0	22

4.2 Содержание дисциплины (модуля)

Тема 1. Общая характеристика криптографии и криптоанализа. Шифры и секретные ключи. Атаки на шифры. Примеры шифров. Одноключевая криптография и криптография с открытым ключом.

Общая характеристика криптографии и криптоанализа. Шифры и секретные ключи. Атаки на шифры. Исторические шифры. Шифр Цезаря, шифр Вижинера, аппаратное шифрование (Энигма и т.п.). Другие примеры шифров. Клод Шеннон и его вклад в криптографию. Одноключевая криптография и криптография с открытым ключом.

Тема 2. Потоковые и блочные шифры. DES и AES.

Потоковые и блочные шифры. Схема Фейстеля. DES и его модификации. Четыре режима шифрования. Советский аналог DES. Шифр Rijndael, и американский государственный стандарт шифрования AES. Использование конечных полей. Потоковые шифры, гаммирование. Генераторы псевдослучайных чисел. Современный российский государственный стандарт блочного шифрования (шифр "Кузнечик").

Тема 3. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана. Проблема доскретного логарифма.

Криптография с открытым ключом. Односторонние функции. Гипотетические примеры односторонних функций: разложение на множители и дискретный логарифм. Открытый ключ как

односторонняя функция секретного, Алгоритм Шора и проблема "квантового апокалипсиса". Протокол Диффи-Хеллмана. Задача о дискретном логарифме и некоторые методы ее решения..

Тема 4. Криптосистема RSA, и ее криптостойкость.

Криптосистема RSA. Задача о разложении натурального числа на простые множители и ее сложность. Функция Эйлера и способ ее вычисления. Китайская теорема об остатках. Теорема, дающая обоснование возможности однозначного дешифрования. Слабости RSA, и возможные атаки. Состояние проблемы о разложимости на множители.

Тема 5. Общее определение цифровых подписей. Цифровая подпись RSA. Криптографические хэш-функции.

Общее определение цифровой (элктронной) подписи. Генерация подписи, и проверка подписи. Критерий надежности подписи: возможность вывести формулу подписи, исходя из условий проверки. Цифровые подписи и односторонние функции. Требования, предъявляемые к цифровым подписям. Цифровая подпись RSA. Криптографические хэш-функции. Требования, предъявляемые к криптографическим хэш-функциям. Использование хэш-функций в цифровых подписях.

Тема 6. Криптосистема Эль-Гамаля, и постренные по тому же принципу цифровые подписи.

Криптосистема Эль-Гамаля: шифрование и цифровая подпись. Особенность цифровой подписи Эль-Гамаля - сеансовый (эфемерный) ключ. Методы практического вычисления: расширенный алгоритм Евклида (деление в кольцах вычетов), и примитивные элементы конечных полей (в частности, первообразные корни по простому модулю). Некоторые другие подписи, построенные по тому же принципу цифровые подписи. Решение задач.

Тема 7. Цифровые подписи DSA и Шнорра.

Бывший государственный стандарт цифровой подписи США - подпись DSA. Обоснование подписи в обе стороны (в частности, вывод формулы подписи из условий проверки). Цифровая подпись Шнорра, и ее достоинства (это одна из немногих подписей, криптостойкость которой строго обоснована). Задача аутентификации. Аутентификация на основе подписи Шнорра.

Тема 8. Затемненные цифровые подписи. Финансовая криптография и электронное голосование.

Затемненные (слепы, подпси вслепую, blind) цифровые подписи. Примеры затемненных подписе: подпись на основе RSA, и затемненная подпись Эль-Гамаля. Электронные деньги (e-cash). Простейшая схема использования электронных денег, в которой участвует банк (подписывающий), покупатель, и продавец. Требования, предъявляемые к электронным деньгам. Частично затемненные цифровые подписи. Финансовая криптография и электронное голосование.

Тема 9. Эллиптическая криптография

Эллиптическая криптография. Группы точек эллиптических кривых над конечными полями. Примеры вычислений таких групп. Решение задач. Строение групп точек эллиптических кривых. Задача о дискретном логарифме в группах точек эллиптических кривых. Подпись ECDSA. ПРотокол Менезеса -Вэнстона. Аналог подписи Эль-Гамаля. Российский государственный стандарт цифровых подписей.

Тема 10. Постквантовая криптогафия. Криптосистема NTRU

Перспективы развития криптографии в связи с возможным появлением программируемых квантовых компьютеров. Алгоритм Шора и теорема Ожигова. Постквантовая криптография. Решетки. Сложные задачи на решетках. Кратчайший вектор решетки и ближайший к данному вектору вектор решетки. Криптосистема NTRU (Nth TRUncated polynomial ring).

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Лекториум - https://www.lektorium.tv

Математическая криптография - http://cryptography.ru

Национальный Открытый Университет "ИНТУИТ" - http://www.intuit.ru

Энциклопедия теоретической и прикладной криптографии - http://cryptowiki.net/index.php?title=Main_Page

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Данный курс является вводным. Он предназначен для первого знакомства с современной криптографией. Ввиду ограниченности времени на лекциях будут рассказаны самые в основном простые идеи и методы, относящиеся к шифрованию, цифровым (электронным) подписям, и немного сверх того. НО будут рассказаны также некоторые и практически важные вещи, например, современный российский ГОСТ цифровой подписи. В заключительном разделе курса дается общая характеристика ситуации, которая может возникнуть после появления квантовых компьютеров, и излагается общая схема одного из перспективных шифров (NTRU), который, предположительно, не может быть взломан квантовым компьютером.
практические занятия	Имеется большое количество материала, который следует освоить в форме решения задач. Так как упор делается на математическую сторону криптографии, то эти задачи в основном имеют математический характер. Но придется также повторить (или впервые освоить) ряд тем из теории чисел и алгебры. В частности, вычисления в кольцах вычетов и конечных полях. Завершающая тема практических занятий - вычисления в группах точек эллиптических кривых над конечными полями.

Вид работ	Методические рекомендации
самостоя-тельная работа	Самостоятельная работа состоит из повторения лекционного материала, решения домашних заданий, и (что всячески приветствуется) самостоятельного изучения тем, которые на лекциях были изложены кратко или только упомянуты. Студенты получат электронную базу данных, содержащую несколько сотен книг на русском и английском языках, где можно найти исчерпывающую информацию по широкому кругу вопросов.
экзамен	Вопросы билетов: 1. Потоковые шифры. Абсолютно надежные шифры. 2. Блочные шифры. Примеры. Схема Фейстеля. DES. 3. Режимы шифрования. 4. Криптография с открытым ключом. Цифровые подписи. . 5. Алгоритм RSA и его обоснование. 6. Цифровая подпись RSA. Криптографические хэш-функции. 7. Шифрование по методу Эль-Гамаля. 8. Цифровая подпись Эль-Гамаля. 9. Цифровая подпись DSA (DSS). 10. Цифровая подпись Шнорра. 11. Цифровые платежные системы. Электронные деньги. Затемненные (слепые) цифровые подписи. 12. Группы точек эллиптических кривых. 13. Криптография на эллиптических кривых: алгоритм шифрования Менезеса-Вэнстона. 14. Криптография на эллиптических кривых: ECDSA. 15. Цифровая подпись ГОСТ Р 34.10-2012.

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

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 02.03.01 "Математика и компьютерные науки" и профилю подготовки "Наука о данных".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.04.02 Введение в криптографию

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Наука о данных
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018

Основная литература:

1. Введение в криптографию / под общей редакцией В. В. Ященко. - Москва: МЦНМО, 2012. - 348 с. - ISBN 978-5-4439-0026-1. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/71813 (дата обращения: 10.03.2020). - Режим доступа: для авториз. пользователей.

2. Музыкантский, А. И. Лекции по криптографии: учебное пособие / А. И. Музыкантский, В. В. Фурин. - 2-е изд. - Москва: МЦНМО, 2013. - 68 с. - ISBN 978-5-4439-2075-7. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/56408 (дата обращения: 10.03.2020). - Режим доступа: для авториз. пользователей.

3. Масленников, М. Е. Практическая криптография: пособие / Масленников М.Е. - Санкт-Петербург: БХВ-Петербург, 2015. - 465 с. ISBN 978-5-9775-1884-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/944503

(дата обращения: 10.03.2020). - Режим доступа: по подписке.

Дополнительная литература:

1. Смолин, Ю.Н. Алгебра и теория чисел : учебное пособие / Ю.Н. Смолин. - 5-е изд., стер.-Москва : ФЛИНТА, 2017. - 464 с. - ISBN 978-5-9765-0050-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1034573 (дата обращения: 10.03.2020). - Режим доступа: по подписке.

2. Торстейнсон, П. Криптография и безопасность в технологии. NET / П. Торстейнсон, Г. А. Ганеш ; под редакцией С. М. Молявко ; перевод с английского В. Д. Хорева. - 3-е изд. (эл.). - Москва : Лаборатория знаний, 2015. - 428 с. - ISBN 978-5-9963-2952-6. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/70724 (дата обращения: 10.03.2020). - Режим доступа: для авториз. пользователей.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.04.02 Введение в криптографию

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Наука о данных
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.