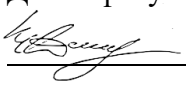
МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерных сетей

УТВЕРЖДАЮ
Декан факультета ИВТ
 Д.Ю. Чалый
«23»_____мая_____2023 г.

Рабочая программа дисциплины
«Информационная безопасность»

Направление подготовки
01.03.02 Прикладная математика и информатика

Направленность (профиль)
«Искусственный интеллект»

Квалификация выпускника
Бакалавр

Форма обучения
очная

Программа рассмотрена на
заседании кафедры
от 17 апреля 2023 г.,
протокол № 8

Программа одобрена НМК
факультета ИВТ
протокол № 6 от
28 апреля 2023 г.

Ярославль

1. Цели освоения дисциплины

Результаты изучения дисциплины «Информационная безопасность» востребованы на преддипломной практике и выпускной квалификационной работе.

2. Место дисциплины в структуре образовательной программы бакалавриата *(магистратуры, специалитета)*

Дисциплина «Информационная безопасность» согласно учебному плану входит в модуль «Технологии передачи и обработки данных» и реализуется в 7 семестре. Изучается на основе знаний, полученных при изучении дисциплин модулей «Современные цифровые технологии» и «Аппаратное и программное обеспечение компьютера».

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы бакалавриата *(магистратуры, специалитета)*

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-4. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ИОПК4.1Знает структуру базовых и специализированных информационных технологий, принципы их работы. ИОПК4.2Умеет выбирать информационные технологии для решения задач профессиональной деятельности и обосновывать свой выбор. ИОПК4.3Владеет навыками применения базовых и специализированных информационных технологий для решения задач профессиональной деятельности.	Демонстрирует глубокое знание и понимание структуры базовых и специализированных информационных технологий, принципов их работы.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)*
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1.	Общие принципы проектирования систем защиты информации.		6		12			24	
	в том числе с ЭО и ДОТ							*2*	
2.	Криптографические методы защиты информации.		6		6			24	
	в том числе с ЭО и ДОТ							2	
3.	Компьютерные сети. Защита информации.		6		6			24	
	в том числе с ЭО и ДОТ							2	
4.	Политики и стандарты безопасности.		6		12			18	
	в том числе с ЭО и ДОТ							2	
	ИТОГО		24		36			84	Экзамен
	в том числе с ЭО и ДОТ							8	

Содержание разделов дисциплины:

Раздел 1.
Понятие информации и информационной безопасности. Угрозы безопасности в информационных системах. Категории информационной безопасности. Источники, риски, формы атак на информационные системы. Построение систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации. Понятия идентификации и аутоинтефикации, протоколирование и аудит. Разграничение доступа. Формальные модели защиты информации. Надежность и безопасность программного обеспечения.

Раздел 2. Криптографические методы защиты информации.
Основные понятия и определения. Классические шифры. Понятие криптографической системы. Симметричное и асимметричное шифрование. Криптостойкость алгоритмов. Современные алгоритмы шифрования. Стандарты шифрования данных. Методы генерации криптографически качественных псевдослучайных последовательностей. Хеш-функции. Электронно-цифровая подпись. Системы управления ключами. Понятия однонаправленной функции.

Раздел 3. Компьютерные сети. Защита информации.
Общая характеристика и классификация компьютерных сетей. Сетевые сервисы и стандарты. Локальные и глобальные компьютерные сети. Интернет. Защита информации в локальных и глобальных компьютерных сетях.

Раздел 4. Политики и стандарты безопасности.
Правовые и организационные методы. Особенности законодательства РФ в области информационной безопасности. Политики информационной безопасности предприятий. Стандарты в области управления информационной безопасностью.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

1. MozillaFirefox

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

1. ОС семейства MicrosoftWindows
2. Microsoft Office

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

1. Microsoft Office 365
2. Movavi Video Stuite

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», рекомендуемых для освоения дисциплины

а) основная литература

1. Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490
2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279

б) дополнительная литература

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227
2. Федин, Ф. О. Информационная безопасность баз данных : учебное пособие / Ф.О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020

— Часть 1 — 2020. — 133 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167605

в) ресурсы сети «Интернет»

1. Электронная библиотека «Университетская библиотека online». URL: http://biblioclub.ru/
2. Информационная система «Единое окно доступа к образовательным ресурсам». URL: http://window.edu.ru/
3. Образовательный портал Череповецкого государственного университета. URL: https://edu.chsu.ru/
4. Аналитические и учебные материалы лаборатории Касперского http://www.securelist.com/ru/
5. Защита от Microsoft http://windows.microsoft.com/ru-RU/windows/products/security-essentials
6. Национальный институт стандартов и технологии. http://csrc.nist.gov/publications/PubsFIPS.htmlNIST-FIPS-201-2.pdf
7. Официальный сайт FIPShttp://www.itl.nist.gov/fipspubs/
8. Сайт материалов по информационной безопасности http://www.iso27000.ru/
9. ISO 27001 оригинал от Британского института стандартов
10. Электронный учебник Б. Шнайера "Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си" http://www.ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm
11. Электронный курс Ю. Лифшица "Современные задачи криптографии"http://yury.name/cryptography/-

Приложение № 1 к рабочей программе дисциплины
«Информационная безопасность»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы,
используемые в процессе текущего контроля успеваемости

Перечень оценочных средств

Компетенции	Индикаторы достижения компетенций	Оценочные средства
ОПК-4. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ИОПК4.1Знает структуру базовых и специализированных информационных технологий, принципы их работы. ИОПК4.2Умеет выбирать информационные технологии для решения задач профессиональной деятельности и обосновывать свой выбор. ИОПК4.3Владеет навыками применения базовых и специализированных информационных технологий для решения задач профессиональной деятельности.	Задания для выполнения лабораторных работ. Задания для самостоятельной работы. Вопросы к экзамену.

Образцы заданий для самостоятельной работы:

По итогам самостоятельной работы студент готовит отчет, включающий в себя ответы на вопросы и решение заданий, предполагавшихся к выполнению в ходе самостоятельной работы. Отчет сдается преподавателю в электронной форме.

Раздел 1. Общие принципы проектирования систем защиты информации.

1. Каковы цели защиты информации?
2. В чем состоит целостность данных?
3. В чем состоит конфиденциальность данных?
4. В чем состоит доступность данных?

5. Приведите примеры технических угроз информационной безопасности.
6. Какие проблемы для информационной безопасности порождает человеческий фактор?
7. Приведите примеры технических средств обеспечения информационной безопасности и защиты информации.
8. Назовите организационные меры обеспечения информационной безопасности и защиты информации. Обоснуйте целесообразность этих мер.
9. Назовите правовые меры обеспечения информационной безопасности и защиты информации.
10. Перечислите основные угрозы надежности и безопасности программного обеспечения.

Раздел 2. Криптографические методы защиты информации.

1. Криптография, криптоанализ и криптология – каково соотношение между этими науками?
2. Каково соотношение между шифрованием и кодированием?
3. Каково соотношение между стеганографией и криптографией?
4. Что такое ключ шифрования?
5. В чем принципиальное различие между симметричными и ассимитричными шифрами?
6. Почему шифр Цезаря очень неустойчив к взлому?
7. На чем основан взлом шифра Виженера по Казинскому?
8. В чем состоит различие между принципом устройства шифров подстановой и шифров перестановок?
9. В чем заключаются преимущества и недостатки гаммирования по сравнению с другими симметричными шифрами?
10. В сем состоит различие между блочными и потоковыми шифрами?
11. В чем состоит принцип Керкхоффса?
12. В чем заключаются принципы рассеивания и перемешивания? В чем из целесообразность?
13. Почему алгоритм DES не удовлетворяет современным требованиям к секретности?
14. В чем заключается атака методом грубой силы?
15. Что такое «проблема распределения ключей» в криптографии с закрытым ключом?
16. В чем состоит проблема доверия между пользователями в криптографии с закрытым ключом?
17. Что такое однонаправленная функция?
18. Какая однонаправленная функция лежит в основе алгоритма RSA ассиметричного шифрования?
19. Для каких действий используется открытый ключ в ассиметричной криптографии?

20. Для каких действий используется закрытый ключ в ассиметричной криптографии?

Раздел 3. Компьютерные сети. Защита информации.

1. Опишите, как осуществляется защита информации в локальных и глобальных компьютерных сетях.
2. Как осуществляется использование программ шифрования в компьютерной сети?
3. Для чего осуществляется резервное копирование и архивация данных?
4. Какие протоколы локальной сети используются для обеспечения безопасности работы?
5. Какие протоколы глобальной сети используются для обеспечения безопасности работы?

Раздел 4. Политики и стандарты безопасности.

6. Что запрещено пропагандировать согласно Конституции РФ?
7. Если международным договором РФ установлены иные правила, чем предусмотрено законом РФ, то правила какого нормативного акта должны применяться, согласно Конституции?
8. На какие виды подразделяется информация в зависимости от порядка ее предоставления (распространения) согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»?
9. К каким видам информации не может быть ограничен доступ согласно Федеральному закону ««Об информации, информационных технологиях и о защите информации»?
10. Распространение каких видов информации запрещается Федеральным законом «Об информации, информационных технологиях и о защите информации»?
11. Каковы национальные интересы РФ согласно Доктрине информационной безопасности Российской Федерации?

Образцы заданий для лабораторных работ

По итогам выполнения лабораторной работы студент демонстрирует результаты работы преподавателю, а также сдает в электронном виде отчет, содержащий порядок выполнения работы.

Раздел 1. Общие принципы проектирования систем защиты информации

Решите кейс, предложенный преподавателем.

Раздел 2. Криптографические методы защиты информации.

Лабораторная работа «Шифрование»

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2. Расшифруйте сообщения, зашифрованные с помощью
   шифра №1 ○ И.РЮУ.ЪФОБГНО ○
   СЛХГ.ЪЛХО.ФОО.ЩВ
2. Пусть исходный алфавит содержит следующие символы:
   АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
   Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО
   сообщения: ○ КРИПТОСТОЙКОСТЬ

- ГАММИРОВАНИЕ

3. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):
   АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
   Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:
   - ШВМБУЖНЯ
   - ЯБХЪШЮМХ
4. Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?
5. Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9А. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?
6. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:
   - ЖЕЛТЫЙ_ОГОНЬ
   - МЫ_НАСТУПАЕМ

Лабораторная работа «Шифр Цезаря»
На любом языке программирования напишите программу, реализующую алгоритм Цезаря.
Техническое задание:

1. Зашифрование и расшифрование текстов, записанных кириллицей и латиницей.
2. Взлом зашифрованного русскоязычного текста методом наименьших квадратов.
3. Замена во вводимом тексте буквы ё на е.
4. Очистка вводимого текста от всех небуквенных символов, знаков препинания, пробелов, приведение всех букв к строчному регистру.
5. Приведение введенного значения ключа к диапазону [0; 32] для кириллицы, [0; 26] для латиницы.
6. Выдача обратного текста группами по пять слов.
7. Защита от неправильных действий пользователя.
8. Дружественный интерфейс.

Лабораторная работа «Шифр Виженера»
На любом языке программирования напишите программу, реализующую алгоритм Виженера.
Техническое задание:

1. Зашифрование и расшифрование текстов, записанных кириллицей.
2. Взлом зашифрованного русскоязычного текста методом наименьших квадратов на основе идей Казинского (в случае использования идей Фридмана необходимо уметь внятно объяснить эти идеи).
3. Замена во вводимом тексте буквы ё на е.

4. Очистка вводимого текста от всех небуквенных символов, знаков препинания, пробелов, приведение всех букв к строчному регистру.
5. Выдача обратного текста группами по пять символов.
6. Защита от неправильных действий пользователя.
7. Дружественный интерфейс. *Раздел 3. Компьютерные сети. Защита информации.*

Лабораторная работа «Шифрование и цифровая подпись сообщений»
Используя программу PGP (англ. Pretty Good Privacy), выполните следующие задания: 1. Создайте пару ключей шифрования (открытый и закрытый)

2. Подпишите сообщение электронной цифровой подписью.
3. Зашифруйте сообщение для напарника по лабораторной работе. Отправьте сообщение напарнику.
4. Расшифруйте сообщение, полученное от напарника.
5. Проверьте подлинность электронной цифровой подписи в полученном сообщении.
6. Объясните смысл выполненных операций. *Раздел 4. Политики и стандарты безопасности.* Решите кейс, предложенный преподавателем.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к экзамену:

1. Понятие информации и информационной безопасности.
2. Угрозы надежности и безопасности программного обеспечения.
3. Категории информационной безопасности.
4. Источники, риски, формы атак на информацию.
5. Построение систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации.
6. Понятия идентификации и аутоинтефикации, протоколирование и аудит.
   Разграничение доступа.
7. Формальные модели защиты информации.
8. Криптография. Основные понятия и определения.
9. Классические шифры.
10. Понятие криптографической системы.
11. Симметричное и асимметричное шифрование.
12. Криптостойкость алгоритмов.
13. Современные алгоритмы шифрования.
14. Стандарты шифрования данных.
15. Методы генерации криптографически качественных псевдослучайных последовательностей.
16. Хеш-функции.
17. Электронно-цифровая подпись.
18. Системы управления ключами.

19. Понятия однонаправленной функции.
20. Общая характеристика и классификация компьютерных сетей. Сетевые сервисы и стандарты.
21. Защита информации в локальных и глобальных компьютерных сетях.
22. Правовые и организационные методы обеспечения информационной безопасности.
23. Особенности законодательства РФ в области информационной безопасности.
24. Политики информационной безопасности предприятий.
25. Стандарты в области управления информационной безопасностью.

Уровни оценки компетенций следующие: базовый – 55-69 баллов, повышенный – 70-100 баллов.

Преподаватель в течение лабораторных работ проводит систематический контроль знаний студентов, ориентируясь на перечень вопросов для проведения зачета. Поэтому, если текущий рейтинг по дисциплине будет равен или превысит 55 баллов, студент может получить зачет по дисциплине без прохождения промежуточной аттестации или экзамен с оценкой «удовлетворительно».

Критерии оценки лабораторных работ и практических занятий (от 0 до 10 баллов):

- ***9-10 баллов*** выставляется студенту, если работа выполнена самостоятельно и полностью верно; представлен отчет, содержащий результаты выполнения заданий лабораторной работы и ответы на контрольные вопросы; студент анализирует результаты, полученные в ходе выполнения лабораторной работы, делает выводы.

- ***7-8 баллов*** выставляется студенту, если работа выполнена самостоятельно, в целом правильно, но имеются некоторые неточности в выполнении заданий или ответах на контрольные вопросы; представлен отчет, содержащий результаты выполнения заданий лабораторной работы и ответы на контрольные вопросы; студент анализирует результаты, полученные в ходе выполнения лабораторной работы, делает выводы.

- ***5-6 баллов*** выставляется студенту, если работа выполнена самостоятельно, в целом правильно, но имеются некоторые неточности в выполнении заданий или ответах на контрольные вопросы; представлен отчет, содержащий результаты выполнения заданий лабораторной работы и ответы на контрольные вопросы; студент испытывает затруднения при проведении анализа результатов, полученных в ходе выполнения лабораторной работы, и формулировке выводов.
- ***3-4 балла*** выставляется студенту, если студент не до конца справился с заданием, не совсем верно ответил на контрольные вопросы, однако оформил отчет по результатам работы.

- ***1-2 балла*** выставляется студенту, если студент не до конца справился с заданием, не совсем верно ответил на контрольные вопросы, не оформил отчет по результатам работы.

- ***0 баллов*** выставляется студенту, если студент не справился с заданием, неверно ответил на представленные вопросы.

Ответ на зачете/экзамене оценивается исходя из 40 баллов (максимум). Билет содержит теоретический вопрос и практическое задание, преподаватель может задавать дополнительные вопросы. Полный ответ на основной вопрос оценивается максимум в 20 баллов, предполагает свободное изложение (не чтение) всего необходимого материала,

ответы студента на уточняющие вопросы, если они есть. Правильный ответ на дополнительный вопрос оценивается максимум в 5 баллов. Правильное выполнение практического задания оценивается в 20 баллов.

Критерии оценивания компетенций:

Индикаторы достижения компетенций	**Критерии оценивания компетенций**		
	Недостаточный уровень	**Базовый уровень**	**Повышенный уровень**
ИОПК4.1 Знает структуру базовых и специализированных информационных технологий, принципы их работы.	Не знает структуру базовых и специализированных информационных технологий, принципы их работы.	Демонстрирует знание структуры базовых и специализированных информационных технологий, принципов их работы.	Демонстрирует глубокое знание и понимание структуры базовых и специализированных информационных технологий, принципов их работы.
ИОПК4.2 Умеет выбирать информационные технологии для решения задач профессиональной деятельности и обосновывать свой выбор.	Испытывает серьезные затруднения при выборе информационных технологий для решения задач профессиональной деятельности и обосновании своего выбора.	Демонстрирует умение выбирать информационные технологии для решения задач профессиональной деятельности и обосновывать свой выбор.	Самостоятельно и грамотно выбирает информационные технологии для решения задач профессиональной деятельности и обосновывает свой выбор.
ИОПК4.3 Владеет навыками применения базовых и специализированных информационных технологий для решения задач профессиональной деятельности.	Не владеет навыками применения базовых и специализированных информационных технологий для решения задач профессиональной деятельности.	Демонстрирует владение навыками применения базовых и специализированных информационных технологий для решения задач профессиональной деятельности.	Демонстрирует свободное владение навыками применения базовых и специализированных информационных технологий для решения задач профессиональной деятельности.

Приложение № 2 к рабочей программе дисциплины
«Информационная безопасность»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Информационная безопасность» являются лекции, причем в достаточно большом объеме. Это связано с тем, что в основе дисциплины лежит особый математический аппарат, с помощью которого решаются довольно сложные и громоздкие задачи. По большинству тем предусмотрены практические занятия, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы с математическим аппаратом дифференциальных уравнений.
Для успешного освоения дисциплины очень важно решение достаточно большого количества задач, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия и основы дифференциальных уравнений. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.
Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.
Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с аппаратом дифференциальных уравнений, в течение обучения проводятся мероприятия текущей аттестации в виде контрольных работ в обоих семестрах изучения дисциплины. Также проводятся консультации (при необходимости) по разбору заданий, которые вызвали затруднения.
Освоить вопросы, излагаемые в процессе изучения дисциплины «Информационная безопасность» самостоятельно студенту крайне сложно. Это связано со сложностью изучаемого материала и большим объемом курса. Поэтому посещение всех аудиторных занятий является совершенно необходимым.

Для самостоятельного подбора литературы в библиотеке ЯрГУ рекомендуется использовать:

1. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.
2. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.
3. Электронная картотека «Книгообеспеченность»

(http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.