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

Кафедра интеллектуальных информационных радиофизических систем

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Техническая защита информации

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

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

Программа одобрена НМК
физического факультета
протокол № 5 от 25 апреля 2023 г.

Ярославль

1. Цели освоения дисциплины

Целями освоения дисциплины «Техническая защита информации» являются физические основы образования технических каналов утечки информации и принципы работы технических средств защиты информации.

Основная задача курса заключается в выработке у студентов навыков и умения оценки возможности возникновения утечки информации по техническим каналам, а также эффективности средств и методов защиты информации.

2. Место дисциплины в структуре ОП магистратуры

Дисциплина «Техническая защита информации» относится к обязательной части Блока 1.

Для освоения данной дисциплины студенты должны обладать аппаратом векторного анализа, знать основы электродинамики, электроники и схемотехники, технического противодействия компьютерной разведке, иметь представление об основных понятиях акустики, механики и электричества.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП магистратуры

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП 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-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	**ИД_ОПК-1_4.** Предлагает решения по защите объектов информатизации от утечки информации по техническим каналам	**Знать:** – физические основы утечки информации по техническим каналам в объектах информатизации; **Уметь:** – рассчитывать параметры защищенности объектов информатизации от утечки по техническим каналам; – анализировать и осуществлять обоснованный выбор технических средств защиты информации; – пользоваться базовыми методами прикладного искусственного интеллекта в задачах анализа утечки информации по техническим каналам в информационных сетях и на других объектах информатизации. **Владеть навыками:** – использования пакетов прикладных программ для расчёта характеристик антенных

		элементов: MMANA-GAL. – использования пакетов прикладных программ для расчета акустических параметров материалов OpenFoam. – проектирования объектов информатизации.
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	**ИД_ОПК-2_5.** Предлагает реализацию новых идей в задачах своей профессиональной деятельности на основе проведённого источникового поиска	**Знать:** – основные этапы подготовки научного отчёта и конструкторско-технологической документации. **Уметь:** – использовать электронные профессиональные базы данных и знаний для подготовки научных отчётов. **Владеть навыками:** коллективной работы над проектами и оформления научных отчётов и проектной документации с использованием GitHub и Google –документов.
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**ИД_УК-1.6** владеет навыками поиска информации с использованием современных средств и технологий;	**Знать:** – основные этапы подготовки научного отчёта и конструкторско-технологической документации. **Уметь:** – использовать электронные профессиональные базы данных и знаний для подготовки научных отчётов. **Владеть навыками:** – поиска подходящей информации с использованием баз цитирования elibrary, google.scholar и др., интернет-сообществ stackexchange и др. компиляции информации с использованием GitHub и Google –документов.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 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						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Введение		2					5	
2	Технические каналы утечки речевой информации		15	8	16			10	отчет по лабораторной работе №1;
3	Технические каналы утечки информации, обрабатываемой техническими средствами обработки и передачи информации (ТСПИ)		15	8	16			10	отчет по лабораторной работе №2;
							0,3	2,7	Зачет
	Всего		32	16	32		0,3	27,7	
4	Технические каналы утечки информации при передаче ее по каналам связи		4	4	4			8	отчет по лабораторной работе №3;
5	Мероприятия по выявлению каналов утечки информации		4	4	4			8	отчет по лабораторной работе №4;
6	Организация инженерно-технической защиты информации		8	8	8			8	защита коллективного проекта
							0,5	33,5	Экзамен
	Всего		16	16	16	2	0,5	57,5	
	Всего		**48**	**32**	**48**	**2**	**0,8**	**85,2**	

Содержание разделов дисциплины

1. Введение

1.1 Введение. Виды, источники и носители защищаемой информации.

1.2 Технические каналы утечки информации. Структура, классификация и основные характеристики.

2. Технические каналы утечки речевой информации.

2.1. Краткие сведения по акустике. Звуковое поле. Линейные характеристики звукового поля. Энергетические характеристики звукового поля. Плоская волна. Сферическая волна. Акустические и электрические уровни. Звуковые сигналы. Маскировка звуковых сигналов.

2.2. Понятность и разборчивость речи. Частотный диапазон и спектры. Звуковое поле в помещении. Звуковой фон в помещении. Характеристики помещения. Звукопоглощающие материалы и конструкции. Звукоизоляция помещений.

2.3. Акустические каналы утечки речевой информации.

2.4. Виброакустические технические каналы утечки речевой информации.

2.5. Оптико-электронный канал утечки речевой информации.

2.6. Параметрические каналы утечки речевой информации.

3.Технические каналы утечки информации, обрабатываемой ТСПИ

3.1. Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля. Элементарный электрический излучатель. Элементарный магнитный излучатель.

3.2. Электромагнитные каналы утечки информации ТСПИ

3.3. Электрические каналы утечки информации. Наводки электромагнитных излучений ТСПИ

3.4. Параметрический канал утечки информации.

4. Технические каналы утечки информации при передаче ее по каналам связи

4.1. Электрические линии связи. Средства передачи электрических сигналов.

4.2. Каналы утечки информации за счет паразитных связей.

4.3. Электрические каналы утечки информации. Контроль и прослушивание телефонных каналов связи.

4.4. Электромагнитные каналы утечки информации.

4.5. Индукционный канал утечки информации.

4.6. Безопасность оптоволоконных кабельных систем.

5. Мероприятия по выявлению каналов утечки информации

5.1. Общие принципы выявления. Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы спектра, радиочастотомеры. Нелинейные локаторы. Металлодетекторы. Подавители диктофонов.

5.2. Технические средства защиты информации. Защита информации в сетях связи. Аппаратура контроля линий связи. Аппаратура защиты линий связи. Средства создания акустических маскирующих помех. Средства создания электромагнитных маскирующих помех.

5.3. Безэховые камеры (БЭК). Экранированные помещения.

6. Организация инженерно-технической защиты информации.

6.1. Задачи инженерно-технической защиты информации. Принципы инженерно технической защиты информации. Основные методы защиты информации техническими средствами.

6.2. Способы и средства инженерной и технической охраны объектов.

6.3. Способы и средства противодействия подслушиванию.

6.4. Способы и средства предотвращения утечки информации с помощью закладных устройств. Демаскирующие признаки закладных устройств.

6.5. Основы методологии инженерно-технической защиты информации.

6.6. Моделирование и расчет технических каналов утечки информации. Моделирование звукоизолирующих и экранирующих материалов. Обзор коммерческих и открытых программных продуктов для моделирования и расчёта характеристик антенных устройств/систем. Знакомство с открытыми программными продуктами: MMANA-GAL, OpenFoam. Элементы численных методов.

6.7. Проектирование защиты информации на объекте информатизации. Обзор пакета FreeCAD для подготовки проектной документации.

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Лабораторное занятие – дает возможность получить навыки практической работы с лабораторными макетами электронных устройств, а также с современной измерительной аппаратурой и системами компьютерного моделирования.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся по темам дисциплины;
- представлены примерные темы для коллективных заданий обучающихся;
- представлен список учебной литературы, рекомендуемой для освоения дисциплины;
- представлена информация о форме и времени проведения консультаций по дисциплине в режиме онлайн;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

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

В процессе осуществления образовательного процесса по дисциплине используются:

- программы Microsoft Office и издательская система LaTex;
- Adobe Acrobat Reader;

- MMANA-GAL;
- OpenFoam;
- FreeCAD.

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

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

– База данных патентов (https://rospatent.gov.ru/ru)

База данных ГОСТов Федерального агентства по техническому регулированию и метрологии (https://www.gost.ru/portal/gost/)

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

а) основная литература

1) Мельников В. П. Информационная безопасность и защита информации: учеб. пособие для вузов. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова; УМО по университет. политехн. образованию - 4-е изд., стереотип. - М.: Академия, 2009. - 331 с.

2) Скрипник, Д. А. Общие вопросы технической защиты информации / Скрипник Д. А. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/intuit_163.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.

3) Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002 (дата обращения: 26.01.2022).

4) Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 26.01.2022). — Режим доступа: для авториз. пользователей.

б) дополнительная литература

1) Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Рагозин Ю. Н. - Санкт-петербург : ИЦ Интермедия, 2019. - 216 с. - ISBN 978-5-4383-0182-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785438301820.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.

2) Торокин, Анатолий Алексеевич Инженерно-техническая защита информации: учеб. пособие для вузов / А. А. Торокин; Учеб.-метод. совет по образованию в области информационной безопасности. - М.: Гелиос АРВ, 2005. - 959 с.

3) Ярочкин, В. И. Информационная безопасность : учебник для вузов / Ярочкин В. И. - Москва : Академический Проект, 2020. - 544 с. (Gaudeamus) - ISBN 978-5-8291-3031-2. -

Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785829130312.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.

4) Шаньгин, В. Ф. Информационная безопасность и защита информации / Шаньгин В. Ф. - Москва : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785940747680.html (дата обращения: 26.01.2022). - Режим доступа : по подписке.

5) Завгородний Виктор Иванович Комплексная защита информации в компьютерных системах: Учеб.пособие для вузов / В. И. Завгородний; Учеб.-метод.объединение по образованию в обл.статистики,прикладной информатики и мат.методов в экономике. - М: Логос, 2001. - 263с.

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).

2.Информационная система "Единое окно доступа к образовательным ресурсам" (http://www.edu.ru (раздел Учебно-методическая библиотека) или по прямой ссылке http://window.edu.ru/library).

3. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru).

4. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации в открытом доступе: (http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty)

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);

-учебные аудитории для проведения занятий лабораторных работ;

- учебные аудитории для проведения групповых и индивидуальных консультаций,

- учебные аудитории для проведения текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;

-помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор:

доцент кафедры

инфокоммуникаций и радиофизики _____ Очиров А.А.

Приложение №1 к рабочей программе дисциплины
«Техническая защита информации»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Лабораторный практикум

1. **Лабораторная работа №1.** Исследование технических каналов утечки акустической информации. Исследование эффективности средств защиты акустической информации.
2. **Лабораторная работа №2**. Исследование технических каналов утечки информации, обрабатываемой техническими средствами приема, обработки и передачи информации. Исследование эффективности средств защиты информации от утечки по каналу ПЭМИ.
3. **Лабораторная работа №3** Исследование эффективности средств защиты информации от утечки за счет побочных электромагнитных наводок. Исследование технического канала утечки информации при передаче ее по каналам связи.
4. **Лабораторная работа №4** Исследование способов обнаружения закладочных технических устройств, предназначенных для беспроводной передачи информации.

Контрольные вопросы по результатам выполнения лабораторной работы № 1

1. Как реализуется метод «высокочастотного навязывания»?
2. На чем основана реализация лазерного канала утечки информации?
3. Как реализуется метод «высокочастотного облучения»?
4. Каковы основные акустические параметры речевых сигналов?
5. От чего зависит звукоизоляция основных строительных конструкций?
6. Что является наиболее распространенными причинами снижения звукоизоляции строительных конструкций?
7. Какие элементы строительных конструкций наиболее опасны с точки зрения несанкционированного съема информации?
8. Какие основные каналы утечки акустической информации?
9. Виды разборчивости речи.
10. Опишите экспериментально-расчетную методику оценки речевой разборчивости.
11. Принципы построения генераторов акустического и вибрационного шумов. Основные разновидности.

12. Укажите основные характеристики виброакустического канала утечки информации.
13. Основные характеристики звуковых волн.
14. Поясните принцип выбора контрольных точек для проведения виброакустических измерений.
15. Пассивные методы защиты информации.
16. Активные методы защиты информации.

Контрольные вопросы по результатам выполнения лабораторной работы №№ 2, 3

1. Дайте определение технического канала утечки информации.
2. В чем отличие основных технических средств (ТСПИ) от вспомогательных технических средств и систем (ВТСС)?
3. Дайте определение контролируемой зоны (КЗ).
4. Назовите основные виды каналов утечки информации, обрабатываемой ТСПИ.
5. Объясните физическую сущность возникновения побочных электромагнитных излучений.
6. Какие причины приводят к возникновению электрических каналов утечки информации?
7. Что представляют собой закладные устройства (ЗУ)?
8. Назовите основные виды каналов утечки речевой информации.
9. Назовите основные виды каналов утечки информации, передаваемой по каналам связи.
10. Какие каналы утечки информации могут возникать при работе средств вычислительной техники?
11. Какие излучения относятся к электромагнитным каналам утечки информации?
12. За счет чего возникают электрические каналы утечки информации?
13. Каким параметром определяется зона возможного перехвата информации?
14. Первичные и вторичные параметры линий связи
15. Назовите возможные каналы утечки информации при передаче ее по каналам связи.
16. Взаимная индуктивность электромонтажных линий связи
17. Паразитные связи.
18. Микрофонный эффект
19. Прослушивание через микрофон телефонного аппарата.
20. Индукционный канал утечки информации.
21. Назовите возможные средства контроля линий связи.
22. Назовите возможные средства защиты линий связи.

Контрольные вопросы по результатам выполнения лабораторной работы № 4

1. Опишите общие принципы выявления закладочных технических устройств.
2. Принципы работы индикаторов электромагнитного поля.
3. Принципы работы нелинейных локаторов.
4. Принципы работы металлодетекторов.
5. Принципы работы подавителей микрофонов.
6. Высокочастотное навязываение.

7. Параметрический канал утечки информации.
8. Особенности реализации разных типов закладочных устройств и принципы их обнаружения.

Примерные темы заданий для коллективной работы обучающихся

1. Собрать индикатор электромагнитного поля.
2. Провести моделирование распространения звуковой волны в различных материалах и оценить звукоизоляцию исследуемого материала
3. Провести моделирование электрической сети как антенного элемента и оценить технические параметры побочного электромагнитного сигнала от такого рода антенны.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену

1. Технические каналы утечки информации. Общие понятия. Структура. Классификация. Основные характеристики.
2. Технические каналы утечки информации, обрабатываемой ТСПИ.
3. Физическая природа побочных электромагнитных излучений.
4. Электромагнитные каналы утечки информации ТСПИ.
5. Электрические каналы утечки информации. Параметрический канал утечки информации.
6. Технические каналы утечки информации при передаче ее по каналам связи. Электрические линии связи.
7. Технические каналы утечки информации при передаче ее по каналам связи. Каналы утечки за счет паразитных связей.
8. Технические каналы утечки речевой информации. Звуковое поле.
9. Технические каналы утечки речевой информации. Звуковые сигналы. Маскировка звуковых сигналов.
10. Технические каналы утечки речевой информации. Виды шумов. Понятность и разборчивость речи.
11. Частотный диапазон и спектры. Звуковое поле в помещении.
12. Звуковой фон в помещении. Характеристики помещения. Звукопоглощающие материалы и конструкции.
13. Звукоизоляция помещений.
14. Акустические каналы утечки речевой информации. Микрофоны.
15. Гидроакустические датчики. СВЧ- и ИК- передатчики. Виброакустические технические каналы утечки речевой информации.
16. Акустоэлектрические каналы утечки речевой информации. Оптико-электронный технический канал утечки информации. Параметрические технические каналы утечки информации.
17. Концепция и методы инженерно-технической защиты информации.
18. Экранирование электромагнитных волн.
19. Экранированные помещения. БЭК
20. Безопасность оптоволоконных кабельных систем.
21. Методы и принципы инженерно-технической защиты информации.
22. Общие принципы выявления технических каналов утечки информации.

23. Индикаторы электромагнитного поля. Сканирующие радиоприемники.
24. Анализаторы спектра, радиочастотомеры. Нелинейные локаторы.
25. Металлодетекторы. Подавители диктофонов

Приложение №2 к рабочей программе дисциплины
«Техническая защита информации»

Методические указания для студентов по освоению дисциплины

Основной формой занятий по дисциплине «Техническая защита информации» являются лабораторные занятия. На лабораторных занятиях излагается необходимый минимум теоретических сведений, ставятся вопросы, на которые надо найти ответ самостоятельно, даются рекомендации по побору литературы, даются отсылки к нормативной базе. Теоретический материал представляет собой компиляцию из огромного количества источников, поэтому материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и дополнять информацией, полученной из учебной и научной литературы.

Для успешного освоения дисциплины обязательно выполнение всех лабораторных работ, они являются формой текущей аттестации.

Изучение дисциплины заканчивается экзаменом. Билет состоит из одного теоретического вопроса по материалам курса.

- Теоретический вопрос в билете на зачете оценивается в 4 балла:
  - 2 балл, если вопрос раскрыт более чем на 50%, но менее чем на 70% от требуемого объёма.
  - 3 балла, если вопрос раскрыт более чем на 70%, но менее, чем на 90% от требуемого объёма.
  - 4 балла, если вопрос раскрыт более чем на 90% от требуемого объёма.

Оценка за экзамен складывается из оценки за лабораторные задания, оценки за коллективный проект, оценки за ответ на вопрос на экзамене и оценки на зачете.

Баллы / Вид деятельности	«1»	«2»	«3»
Лабораторные задания	Лабораторные работы суммарно выполнены и сданы не менее, чем на 70%.	Полностью выполнены и сданы все лабораторные работы	Все лабораторные работы выполнены и сданы целиком и качественно.
Коллективный проект	Коллективный проект выполнен с оценкой «удовлетворительно».	Коллективный проект выполнен с оценкой «хорошо.	Коллективный проект выполнен с оценкой «отлично».

Итоговая оценка высчитывается исходя из суммарного балла по всем видам работ, определяемого по следующему правилу: к оценкам за теоретический вопрос в билете на экзамене и зачете суммируются баллы за лабораторные задания и коллективный проект.

В результате для получения оценки «зачтено» необходимо, чтобы суммарный балл был не ниже 3, Для получения оценки «удовлетворительно» необходимо, чтобы суммарный балл был не ниже 5 оценки «хорошо» - не ниже 7, оценки «отлично» - не ниже 9.

Учебно-методическое обеспечение
самостоятельной работы студентов по дисциплине

1. Для самостоятельной работы рекомендуется использовать учебную литературу, указанную в разделе № 8 данной рабочей программы.

2. Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru) - электронная библиотека, обеспечивающая доступ к наиболее востребованным материалам-первоисточникам, учебной, научной и художественной литературе ведущих издательств (*регистрация в электронной библиотеке – только в сети университета. После регистрации работа с системой возможна с любой точки доступа в Internet.).

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.