Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тульский государственный педагогический университет им. Л.Н. Толстого»
ФГБОУ ВО «ТГПУ им. Л.Н. Толстого»

УТВЕРЖДЕНА

на заседании Ученого совета университета

протокол № 8 от 31 августа 2017 г.

Рабочая программа дисциплины «История криптографии»

Трудоемкость: 2 зачетные единицы

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2013

Заведующий кафедрой алгебры, математического анализа и геометрии

Н.М. Добровольский

Декан факультета истории и права

Н.В.Лебединец

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Достижение планируемых результатов обучения, соотнесенных с общими целями и задачами ОПОП, является целью освоения дисциплины.

Планируемые результаты освоения образовательной программы (код и название компетенции)	Планируемые результаты обучения	Этапы формирования компетенции в процессе освоения образовательной программы
способность организовывать сотрудничество обучающихся, поддерживать их активность, инициативность и самостоятельность, развивать творческие способности (ПК -7)	**Выпускник знает:** возможности использования содержания дисциплины в реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов. **Умеет**: отбирать учебный материал дисциплины, необходимый для реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов. **Владеет:** навыками конструирования содержания учебного материала по дисциплине, необходимого для реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.	В соответствии с учебным планом и планируемыми результатами освоения ОПОП

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина относится к дисциплинам по выбору вариативной части образовательной программы и изучается в 4 семестре.

К началу изучения дисциплины студенты должны владеть:

- знаниями основных методов хранения и переработки информации в устройствах персонального компьютера, иметь представление об устройстве современного общества;
- умениями отображения информации в виде функциональной зависимости;
- навыками и (или) опытом деятельности работы на компьютере, оперирования десятичными числами.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Объем зачетных единиц / часов по формам обучения
	Очная
Максимальная учебная нагрузка (всего)	2/72

Контактная работа обучающихся с преподавателем (всего)	**30**
в том числе:	
Лекции в т.ч. в интерактивной форме	12
лабораторные занятия (включая защиту отчета по лабораторным работам) в т.ч. в интерактивной форме	16
контрольные работы	2
Самостоятельная работа студента (всего)	**42**
в том числе:	
внеаудиторная самостоятельная работа по подготовке к лекционным занятиям	10
внеаудиторная самостоятельная работа по подготовке к лабораторным занятиям и защите отчета	12
выполнение заданий для самостоятельной работы в системе управления обучением MOODLE	10
подготовка к зачету	10
Промежуточная аттестация в форме зачета	

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ, СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ИЛИ АСТРОНОМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Наименование тем (разделов).	Количество академических или астрономических часов по видам учебных занятий			
	Занятия лекционного типа	Практические занятия	Другие виды учебных занятий	Самостоятельная работа обучающихся
Тема 1. Криптография в Древнем мире	2	2		5
Тема 2. Криптография от Средних веков до Нового времени	2	2		5
Тема 3. Криптография в литературе	2	2		5
Тема 4. Криптография первой мировой войны	2	4		5
Тема 5. Криптография второй мировой войны	2	2		5
Тема 6. Математическая криптография	2	2		5
Тема 7. Современная криптография		2		2
Контроль самостоятельной работы студентов			2	
Подготовка к зачету				10
ИТОГО	12	16	2	42

Тема 1.
Криптография в Древнем мире

Криптография в Древнем мире. Атбаш. Сцитала. Диск Энея, линейка Энея, книжный шифр. Квадрат Полибия. Шифр Цезаря. Тайнопись.

Тема 2.

Криптография от Средних веков до Нового времени

Криптография от Средних веков до Нового времени. Развитие криптографии в арабских странах. Криптография эпохи Возрождения

Испанская империя и колонии в Америке. «Индейская криптография». Чёрные кабинеты

Криптография в британских колониях и США.

На пути к математической криптографии.

Тема 3.
Криптография в литературе

Криптография в литературе

А.Конан Дойль «Пляшущие человечки»

Э. По «Золотой жук»

Ж.Верн «Путешествие к центру Земли»

В.Каверин «Исполнение желаний»

Тема 4.
Криптография первой мировой войны

Криптография первой мировой войны.

Тема 5.
Криптография второй мировой войны

Криптография второй мировой войны. Германия: «Энигма», «Fish»

Тема 6.
Математическая криптография

Математическая криптография

Тема 7.
Современная криптография

Современная криптография

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Преподавание дисциплины предполагает использование следующего учебно-методического обеспечения.

Комплекта мультимедийных презентаций для лекционных занятий.

Теоретического курса и информационных приложений, размещенных в электронной образовательной среде MOODLe.

Комплекса тестовых заданий и заданий для практических занятий, размещенных в электронной образовательной среде MOODLe.

Самостоятельная работа обучающихся, направленная на углубление и закрепление знаний, а также развитие практических умений, повышение творческого потенциала студентов и заключается в:

- самостоятельном изучении теоретического материала дисциплины с использованием лекционного материала, модульной объектно-ориентированной динамической учебной среды Moodle, информационных баз, методических разработок, специальной учебной и научной литературы;
- выполнении домашних заданий;
- изучении теоретического материала к практическим занятиям;

– подготовке проектов;
– подготовке к зачету.

Комплект учебно-методического сопровождения дисциплины (опорные конспекты лекций, методические рекомендации по выполнению практических заданий, электронный вариант РПД), доступен студентам в ЭБС, в системе управления обучением MOODLE, из локальной сети ФГБОУ ВО «ТГПУ им. Л. Н. Толстого», Интернет-сайта университета из раздела «Электронное обучение» и может использоваться в процессе выполнения самостоятельной работы.

При подготовке к практическим и лабораторным занятиям студентам доступны следующие учебно-методические ресурсы:

1. Технические средства автоматизации и управления : учебник для академического бакалавриата / О. С. Колосов [и др.] ; под общ. ред. О. С. Колосова. — М. : Издательство Юрайт, 2017. — 291 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-8208-4.Год: 2017 / Гриф УМО ВО URL:https://www.biblio-online.ru/book/981B166D-BA5A-4F4E-AF15-D2E181A9C257
2. Рогов, В. А. Технические средства автоматизации и управления : учебник для СПО / В. А. Рогов, А. Д. Чудаков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 404 с. — (Профессиональное образование). — ISBN 978-5-534-50000-4. URL: https://www.biblio-online.ru/book/61D221D7-6E70-451C-824B-236D5FAEAA45
3. Смирнов, Ю.А. Технические средства автоматизации и управления. [Электронный ресурс] — Электрон. дан. — СПб. : Лань, 2017. — 456 с. — Режим доступа: URL:http://e.lanbook.com/book/91063

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Формирование компетенции «способность организовывать сотрудничество обучающихся, поддерживать их активность, инициативность и самостоятельность, развивать творческие способности (ПК -7)» осуществляется в несколько этапов в соответствии с учебным планом и планируемыми результатами освоения ОПОП.

6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
Знания	возможностей использования содержания дисциплины в реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.	Отметка «зачтено» выставляется, если студент в целом за семестр набрал от 41 до 100 баллов (с учетом баллов, набранных на промежуточной аттестации (зачете)). Отметка «не зачтено» вы-
Умения	отбирать учебный материал дисциплины, необходимый для реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.	

Навыки	конструирования содержания учебного материала по дисциплине, необходимого для реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.	ставляется, если студент в целом за семестр набрал менее 41 балла (с учетом баллов, набранных на промежуточной аттестации (зачете)).

Составляющие итоговой оценки за дисциплину:

1) Текущий контроль (общий вес 70 баллов):

до 8 баллов - посещение лекций;

до 12 баллов - межсессионная аттестация студентов (контрольная работа, коллоквиум, тестирование и другие формы проведения аттестации);

до 50 баллов – выполнение практических работ (из них 40 баллов – выполнение и оформление отчета по практическим занятиям, 10 баллов – выполнение студентами индивидуальных проектов и заданий, размещенных в LMS MOODLE).

2) Итоговый контроль заключается в проведении зачета (общий вес - 30 баллов).

Перевод процентов в академические оценки производится после суммирования процентов текущего и итогового контроля. При этом, для получения положительной итоговой оценки на экзамене необходимо получить не менее 50% по каждой составляющей и выполнить все лабораторные работы. Если лабораторная работа выполняется не в **определенные сроки**, то студент получает вдвое меньше баллов за каждую работу.

Шкала перевода баллов в оценку:

До 40 - «не зачтено»; 41 - 100 - «зачтено».

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных проектных заданий.

6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Контрольные вопросы для подготовки к тесту

1. Какой период истории криптографии характеризуется развитием нового направления - криптографии с открытым ключом?
2. Назовите способы защиты текста в Древнем мире.
3. Как называется полная замена одного алфавита на другой с целью шифрования информации?
4. Какой арабский филолог первым обратил внимание на возможность использования стандартных фраз открытого текста для дешифрования?
5. Какого учёного эпохи Возрождения называют отцом западной криптографии?
6. Какой термин применяется для обозначения зашифрованных документов в испанских колониях Америки?
7. Как называлась служба, занимающаяся дешифрованием корреспонденции при правительстве Франции?
8. Какого учителя и государственного деятеля называют отцом криптографии США?
9. Назовите литературные произведения, в которых встречаются упоминания о криптографии.
10. Как называется самая известная электрическая роторная шифровальная машина?
11. Какой метод шифрования использовался в новом устройстве «Lorenz SZ 40»?
12. Назовите области применения криптографии в современном мире.

Вопросы к зачету

1. Криптография в Древнем мире. Атбаш. Сцитала. Диск Энея, линейка Энея, книжный шифр.
2. Квадрат Полибия. Шифр Цезаря. Тайнопись.
3. Криптография от Средних веков до Нового времени. Развитие криптографии в арабских странах. Криптография эпохи Возрождения
4. Испанская империя и колонии в Америке. «Индейская криптография». Чёрные кабинеты
5. Криптография в британских колониях и США.
6. На пути к математической криптографии.
7. Криптография в литературе
8. А.Конан Дойль «Пляшущие человечки»
9. Э. По «Золотой жук»
10. Ж.Верн «Путешествие к центру Земли»
11. В.Каверин «Исполнение желаний»
12. Криптография первой мировой войны.
13. Криптография второй мировой войны. Германия: «Энигма», «Fish»
14. Математическая криптография
15. Современная криптография

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Описание балльно-рейтинговой системы по дисциплине.

Итоговая рейтинговая оценка по дисциплине складывается из следующих составляющих:

1) За каждый укрупненный блок тем студент может максимально получить 1-32 баллов, которые включают в себя: посещение лекционных занятий, выполнение заданий лабораторной работы и заданий для самостоятельного выполнения.

2) Обязательной формой текущей аттестации знаний является выполнение заданий в среде электронного обучения LMS Moodle. Максимальная оценка данного вида деятельности 10 баллов.

3) Студентам, желающим повысить свой рейтинг, предлагаются задания повышенной сложности (творческие задания), которые максимально могут быть оценены в 10 баллов.

4) На зачете ответ студента может быть максимально оценен в 30 баллов.

Место контроля в структуре дисциплины	Форма контроля	Используемый критерий оценивания	Максимальный балл
Тема 1. Криптография в Древнем мире	Краткий опрос по теме лекции	Знать понятия технических средствха управления, основные понятия. Понятие организационной техники.	0,5
	Защита лабораторных работ	Знать принципы классификации технических средств управления	10
	КСРС	Выполнение заданий самостоятельной работы	0,5
Тема 2. Криптография от Средних веков до Нового времени	Краткий опрос по теме лекции	Знать понятия копирование и тиражирование.	1
	КСРС	Выполнение заданий само-	1

		стоятельной работы	
Тема 3. Криптография в литературе	Краткий опрос по теме лекции	Знать основные понятия раздела передача информации, системы передачи информации.	0,5
	КСРС	Выполнение заданий самостоятельной работы	0,5
Тема 4. Криптография первой мировой войны. Криптография второй мировой войны	Краткий опрос по теме лекции	Знать требования, предъявляемые к средствам и системам поиска документов и информации.	0,5
	Защита лабораторных работ	Знать что такое картотеки, виды и разновидности, принципы организации Уметь использовать средства обозримого хранения информации	30
	КСРС	Выполнение заданий самостоятельной работы	0,5
Тема **5**. Математическая криптография	Краткий опрос по теме лекции	Знать основные рекомендации по выбору технических средств для оснащения современного офиса.	0,5
	КСРС	Выполнение заданий самостоятельной работы	0,5
Тема **6**. Современная криптография	Краткий опрос по теме лекции	Знать основные возможности компьютерных технологий в делопроизводстве	1
	КСРС	Выполнение заданий самостоятельной работы	1
Выполнение заданий в среде электронного обучения LMS Moodle			10
Выполнение теста			12
Промежуточная аттестация	Зачет	Наличие знаний учебного материала дисциплины; умений, выработанных в процессе изучения дисциплины.	30
Итого:			100

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

7.1. Основная литература

1. *Нестеров, С. А.* Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. https://biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. https://biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847

7.2. Дополнительная литература

1. Богатырева Ю.И. Информационная безопасность. Учебно–методическое пособие для студентов, обучающихся по направлению 050100 «Педагогическое образование» /Ю.И. Богатырева. – Тула: ТГПУ им. Л.Н. Толстого, 2014. – Электрон. изд. – 1 электрон. оптич. диск (CD–ROM). – № гос. регистрации 0321400675 – № рег. свид. ФГУП НТЦ «Информрегистр» 35205 от 12.03.2014.
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-00843-2. https://biblio-online.ru/book/054509D0-1E35-4080-9E86-19742B336897

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. ИКТ [Электронный ресурс] : федеральный образовательный портал / ФГАУ ГНИИ ИТТ "Информика". - М. : [б. и.], 2003. - Загл. с титул. экрана. - Б. ц.
   URL: http://www.ict.edu.ru
2. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.
   URL: http://www.mathnet.ru
3. Университетская библиотека Online [Электронный ресурс]: электронная библиотечная система / ООО «Директ-Медиа». – Загл. с титул. экрана. – Б. ц. URL: www.biblioclub.ru.
4. Электронная библиотека ЮРАЙТ [Электронный ресурс]: электронная библиотечная система / ООО «Электронное издательство ЮРАЙТ». – Загл. с титул. экрана. – Б. ц. URL : https://www.biblio-online.ru/.
5. Электронно-библиотечная система «Лань» [Электронный ресурс]: электронная биб- лиотечная система. – Загл. с титул. экрана. – Б. ц. URL: (http://e.lanbook.com).
6. Среда электронного обучения ТГПУ им. Л.Н. Толстого [Электронный ресурс]. – http://moodle.tsput.ru.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

К началу изучения дисциплины обучающимся необходимо:

– ознакомиться с нормативной правовой базой, устанавливающей требования к реализации ОПОП направления, используя современные профессиональные базы данных и/или информационные справочные системы и/или внутривузовское сетевое окружение;

– получить индивидуальные логин и пароль для доступа в электронную информационно-образовательную среду ТГПУ им. Л.Н. Толстого (доступ в систему Moodle и личный

кабинет обучающегося ТГПУ им. Л.Н. Толстого в информационно-телекоммуникационной сети «Интернет»);

– ознакомиться с настоящими методическими указаниями для обучающихся по освоению дисциплины; перечнем основной и дополнительной учебной литературы, необходимой для освоения дисциплины; перечнем ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины; перечнем учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине; методическими материалами, определяющими процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

На лекциях важно сосредоточить внимание на ее содержании. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине. Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы. Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

Прочное усвоение и долговременное закрепление учебного материала невозможно без продуманной самостоятельной работы. Такая работа требует от студента значительных усилий, творчества и высокой организованности. В ходе самостоятельной работы студенты выполняют следующие задачи: дорабатывают лекции, изучают рекомендованную литературу, готовятся к практическим занятиям, к коллоквиуму, контрольным работам по отдельным темам дисциплины. При этом эффективность учебной деятельности студента во многом зависит от того, как он распорядился выделенным для самостоятельной работы бюджетом времени.

Результатом самостоятельной работы является прочное усвоение материалов по предмету согласно программы дисциплины. В итоге этой работы формируются профессиональные умения и компетенции, развивается творческий подход к решению возникших в ходе учебной деятельности проблемных задач, появляется самостоятельности мышления.

Целью практических занятий по данной дисциплине является закрепление теоретических знаний, полученных при изучении дисциплины и формирование и развитие умений и навыков.

Подготовка студентов к практическому занятию направлена на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальных умений у обучающихся: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

В процессе освоения дисциплины обучающимся необходимо посещать учебные занятия, выполнять задания, предусмотренные настоящей рабочей программой; самостоятельно использовать основную, при необходимости дополнительную учебную литературу, необхо-

димую для освоения дисциплины; ресурсы информационно-телекоммуникационной сети «Интернет», необходимые для освоения дисциплины; учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине. Также в процессе освоения дисциплины обучающимся не реже чем раз в неделю отслеживать текущую информацию, при необходимости размещаемую в системе Moodle.

При выполнении заданий к практическим занятиям основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной практической работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению. После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Преподавание дисциплины должно включать в себя следующие образовательные технологии:

1) Проведение лекций с использованием презентаций на основе мультимедийных технологий;
2) Обеспечение студентов сопутствующими материалами, размещенными среде Moodle;
3) Применение эвристических и проблемно-поисковых технологий по изучаемому курсу;
4) Использование активных и диалоговых технологий;

Тематика практических занятий по дисциплине

Практическое занятие 1. Криптография в Древнем мире. Атбаш. Скитала. Диск Энея, линейка Энея, книжный шифр. Квадрат Полибия. Шифр Цезаря. Тайнописи.

Задание 1. Зашифровать свою фамилию с помощью шифра атбаш.

Задание 2. Дешифровать сообщение, зашифрованное с помощью шифра атбаш.

Задание 3. Зашифровать свою фамилию с помощью шифра Цезаря.

Задание 4. Дешифровать сообщение, зашифрованное шифром Цезаря.

Задание 5. Зашифровать свою фамилию с помощью квадрата Полибия 6х6.

Задание 6. Дешифровать сообщение, зашифрованное с помощью квадрата Полибия 6х6.

Практическое занятие 2. Криптография от Средних веков до Нового времени. Развитие криптографии в арабских странах. Криптография эпохи Возрождения. Испанская империя и колонии в Америке. «Индейская криптография». Чёрные кабинеты. Криптография в британских колониях и США.

Задание 1. Зашифровать свою фамилию с помощью таблицы Виженера. В качестве ключа использовать свое имя.

Задание 2. Дешифровать сообщение, зашифрованное с помощью таблицы Виженера.

Задание 3. Дешифровать сообщение, зашифрованное с помощью прямоугольника Плейфейра.

Задание 4. Зашифровать сообщение «Hide the gold in the tree stump». Ключ «playfair example».

Практическое занятие 3-4. Криптография в литературе.

Задание 1. Расшифровать послание Шерлока Холмса.

Задание 2. Придумать свой шифр из символов.

Задание 3. Подготовить сообщение (реферат) по одной из следующих тем:

1. А.Конан Дойль «Пляшущие человечки»
2. Э. По «Золотой жук»
3. Ж.Верн «Путешествие к центру Земли»
4. В.Каверин «Исполнение желаний»
5. Упоминание о криптографии в произведении, прочитанном вами.

Практическое занятие 5. Криптография Первой мировой войны.

Задание. Подготовить сообщение (реферат) по одной из следующих тем:

1. Французская криптография времен Первой мировой войны.
2. Криптография Первой мировой войны. Россия.

3. Развитие криптографии в Англии в период Первой мировой войны.
4. Криптография в Германии в период Первой мировой войны.

Практическое занятие 6. Криптография Второй мировой войны. Германия: «Энигма», «Fish».

Задание. Подготовить сообщение (реферат) по одной из следующих тем:

1. История возникновения электрической роторной шифровальной машины «Энигма».
2. Машина Лоренца: возникновение, назначение, принцип работы.
3. Советские шифры и коды времен Второй мировой войны.
4. Американская шифровальная машина М-209 (CSP-1500).
5. Проект «Венона».

Практическое занятие 7. Математическая криптография.

Задание. Подготовьте сообщение о людях, внесших вклад в развитие математической криптографии.

Темы для индивидуальных сообщений и рефератов:

1. Клод Шеннон.
2. Дэвид Кан. «Взломщики кодов».
3. Хорст Фейстель.
4. Уитфилд Диффи и Мартин Хеллман. «Новые направления в криптографии».

Практическое занятие 8. Современная криптография.

Задание. Подготовьте небольшое сообщение о развитии криптографии в XXI веке.

Темы для индивидуальных сообщений и рефератов:

1. Электронная цифровая подпись.
2. Защита электронной почты от спама.
3. Криптография и сотовая связь.
4. Криптография и цифровое телевидение.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

При осуществлении образовательного процесса по дисциплине используются информационные технологии, охватывающие ресурсы (компьютеры, программное обеспечение и сети), необходимые для управления информацией (создание, хранение, управление, передача и поиск информации):

- технические средства: компьютерная техника и средства связи (ноутбук, проектор, экран, USB-накопители и т.п.);
- коммуникационные средства (проверка домашних заданий и консультирование посредством электронной почты, личного кабинета студента и преподавателя, видеотрансляций);
- организационно-методическое обеспечение (электронные учебные и учебно-методические материалы, компьютерное тестирование, использование электронных мультимедийных презентаций при проведении лекционных и практических занятий); - программное обеспечение (Microsoft Office (Excel, Power Point, Word и т.д.), Skype, по- исковые системы, электронная почта и т.п.);
- среда электронного обучения ТГПУ им. Л.Н. Толстого http://moodle.tsput.ru.

Дисциплина обеспечена комплектом лицензионного программного обеспечения:

1. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.
2. Программное обеспечение Microsoft Office XP Professional Win32 Russian– Лицензия № 16698685 от 08.08.2003 г.
3. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия

№46138962 от 16.11.2009 г.

4. Операционная система Microsoft Windows Professional 7 Russian – Лицензия №48497058 от 13.05.2011 г.

5. Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.

6. Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.

7. Комплексная Система Антивирусной Защиты Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License – Лицензия № 1894-150512-101810 от 12-05-2015 г.

У обучающихся имеется доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых ежегодно обновляется:

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.

2. Официальный интернет-портал правовой информации http://pravo.gov.ru.

3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.

4. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Дисциплина обеспечена специальными помещениями для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещениями для самостоятельной работы. Аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Учебные помещения для проведения занятий лекционного и семинарского типа оборудованы мультимедийным демонстрационным оборудованием, для демонстрации учебно-наглядных пособий, обеспечивающих тематические иллюстрации, соответствующие рабочей учебной программе дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ТГПУ им. Л.Н. Толстого, внутривузовское сетевое окружение.

12. АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ.

1. Планируемые результаты обучения при освоении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины у студента должны быть сформированы следующие компетенции: способность организовывать сотрудничество обучающихся, поддерживать их активность, инициативность и самостоятельность, развивать творческие способности (ПК -7)

В результате освоения дисциплины студент должен приобрести:

знание возможностей использования содержания дисциплины в реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.

умения отбирать учебный материал дисциплины, необходимый для реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.

навыки конструирования содержания учебного материала по дисциплине, необходимого для реализации образовательных программ по учебным предметам в соответствии с требованиями образовательных стандартов.

2. Место дисциплины в структуре ОПОП.

Дисциплина относится к дисциплинам по выбору вариативной части образовательной программы и изучается в 4 семестре.

К началу изучения дисциплины студенты должны владеть:

- знаниями основных методов хранения и переработки информации в устройствах персонального компьютера, иметь представление об устройстве современного общества;
- умениями отображения информации в виде функциональной зависимости;
- навыками и (или) опытом деятельности работы на компьютере, оперирования десятичными числами.

3. Объем дисциплины 2 зачетные единицы.
4. Образовательный процесс осуществляется на русском языке.
5. Разработчики: Реброва И.Ю., к.ф.-м.н., доцент кафедры АМАиГ

13. Лист регистрации изменений к рабочей программе дисциплины

В рабочую программу внесены изменения в части обновления состава лицензионного программного обеспечения, профессиональных баз данных и информационно-справочных систем, к которым должен быть обеспечен доступ обучающимся, и перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

Внесены изменения в п.7 «Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».

Решение ученого совета университета, протокол № 2 от 16 февраля 2017 года.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

2017-2018 учебный год

Обновлен состав необходимого комплекта лицензионного программного обеспечения.

1. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.
2. Операционная система Microsoft Windows Professional 7 Russian – Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 года.
3. Операционная система Microsoft Windows 10 Professional Russian - контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 года.
4. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия №46138962 от 16.11.2009 г.
5. Программное обеспечение Microsoft Office 2013 Professional - контракт № 405535 от 2 ноября 2015 года, контракт № ПР/ФЕН/15/18 от 23.10.2015 г.
6. Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
7. Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
8. Комплексная Система Антивирусной Защиты Kaspersky Endpoint Security для бизнеса –

Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License – Лицензия № 17E0-170518-102844-823-690 от 18-05-2017 г.

Обновлен состав современных профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ обучающимся.

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.
2. Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.
3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
4. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.
5. Web of Science Core Collection – политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных http://webofscience.com.
6. Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН) http://neicon.ru.
7. Базы данных издательства Springer https://link.springer.com.

Изменения к рабочей программе дисциплины утверждены на заседании Ученого совета университета, протокол № 8 от 31 августа 2017 г.

Программа составлена в соответствии с требованиями ФГОС ВО.

Разработчик (и):

Фамилия, имя, отчество	**Учёная степень**	**Учёное звание**	**Должность**
Реброва Ирина Юрьевна	Кандидат физ.-мат. наук	Доцент	Декан ФМФИ