МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Институт прикладной математики и компьютерных наук
Кафедра «Прикладная математика и информатика»

Утверждено на заседании кафедры
«Прикладная математика и информатика»
« 21 » января 2021 г., протокол № 6

Заведующий кафедрой
_____ В.И. Иванов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Методы защиты информации»

основной профессиональной образовательной программы
высшего образования – программы бакалавриата

по направлению подготовки
01.03.02 Прикладная математика и информатика

с направленностью (профилем)
Прикладная математика и информатика

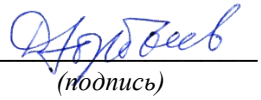
Форма обучения: очная

Идентификационный номер образовательной программы: 010302-01-21

Тула 2021 год

ЛИСТ СОГЛАСОВАНИЯ
рабочей программы дисциплины (модуля)

Разработчик:

Горбачев Д.В., профессор каф. ПМиИ, д.ф.-м.н.	
(ФИО, должность, ученая степень, ученое звание)	*(подпись)*

1 Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины (модуля) является изучение современных математических методов и программных средств защиты цифровой информации, включая элементы теории кодирования и криптографии.

Задачами освоения дисциплины (модуля) являются:

- изучение теории и методов защиты информации;
- освоение программных средств защиты информации;
- знакомство с современными проблемами в области информационной безопасности.

2 Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Дисциплина (модуль) относится к части основной профессиональной образовательной программы, формируемой участниками образовательных отношений.

Дисциплина (модуль) изучается в восьмом семестре.

3 Перечень планируемых результатов обучения по дисциплине (модулю)

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы (формируемыми компетенциями) и индикаторами их достижения, установленными в общей характеристике основной профессиональной образовательной программы, приведён ниже.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

1) архитектуру систем хранения и обработки информации и возможности их взаимодействия, модели и структуры данных; физические модели БД, языки и системы программирования БД, угрозы безопасности БД, способы их предотвращения и инструменты обеспечения безопасности БД (код компетенции – ПК-2, код индикатора – ПК-2.1);
2) архитектуру, устройство и принцип функционирования вычислительных систем, сетевые протоколы и основы web-технологий, программные средства и платформы для разработки web-ресурсов, системы хранения и анализа баз данных, современные принципы построения интерфейсов пользователя, содержание и методы решения задач по созданию и редактированию контента (код компетенции – ПК-4, код индикатора – ПК-4.1).

Уметь:

1) применять языки и системы программирования БД для оптимизации выполнения запросов профессиональных задач по управлению БД; выявлять угрозы безопасности на уровне БД; применять на практике базовые средства резервного копирования и восстановления для установленной БД (код компетенции – ПК-2, код индикатора – ПК-2.2);
2) вырабатывать варианты реализации требований, оценивать их содержание и трудоемкость выполнения в зависимости от квалификации, применять методы и приемы формализации задач; производить оценку и обоснование рекомендуемых решений; осуществлять создание и реструктуризацию сайтов и web-страниц, информационных блоков базы данных; эффективно работать с системой управления контентом (код компетенции – ПК-4, код индикатора – ПК-4.2).

Владеть:

1) навыками анализа возможностей по управлению вычислительными ресурсами, взаимодействующими с БД, возможных угроз для безопасности данных, формирования выводов об эффективности работы БД; методиками выбора основных средств поддержки информационной безопасности на уровне БД и выполнения резервного копирования (код компетенции – ПК-2, код индикатора – ПК-2.3);
2) навыками выработки решения по наполнению сайта контентом, координации работ по созданию и редактированию контента, изменения структуры сайта с помощью системы управления контентом, мониторинга и оценки результатов выполнения работ и формулированию замечаний и рекомендаций (код компетенции – ПК-4, код индикатора – ПК-4.3).

Полные наименования компетенций и индикаторов их достижения представлены в общей характеристике основной профессиональной образовательной программы.

4 Объем и содержание дисциплины (модуля)

4.1 Объем дисциплины (модуля), объем контактной и самостоятельной работы обучающегося при освоении дисциплины (модуля), формы промежуточной аттестации по дисциплине (модулю)

Номер семестра	Формы промежуточной аттестации	Общий объем в зачетных единицах	Общий объем в академических часах	Объем контактной работы в академических часах						Объем самостоятельной работы в академических часах
				Лекционные занятия	Практические (семинарские) занятия	Лабораторные работы	Клинические практические занятия	Консультации	Промежуточная аттестация	
Очная форма обучения										
8	ЗЧ	3	108	24	–	24	–	–	0,1	59,9
Итого	–	3	108	24	–	24	–	–	0,1	59,9

Условные сокращения: Э – экзамен, ЗЧ – зачет, ДЗ – дифференцированный зачет (зачет с оценкой), КП – защита курсового проекта, КР – защита курсовой работы.

4.2 Содержание лекционных занятий

Очная форма обучения

№ п/п	Темы лекционных занятий
	8 семестр
1	Проблемы защиты информации. Введение. Защита от потерь. Защита от несанкционированного доступа. Стандарты информационной безопасности. Приложения к базам данных и Web
2	Работа с нечетко заданной информацией. Регулярные выражения, поиск и замена текста. Синтаксис PERL-совместимых регулярных выражений. Примеры. Сжатие информации при помощи префиксных кодов. Двоичная арифметика, префиксные коды. Код Шэнона–Фэно, пример. Код Хаффмана, пример

№ п/п	Темы лекционных занятий
3	Словарные методы сжатия. Общие сведения. Алгоритм Лемпеля–Зива (LZ). Алгоритм Лемпеля–Зива–Велча (LZW). Алгоритм сжатия BZIP. Преобразование Барроуза–Уиллера. Описание алгоритма. Пример
4	Поле вычетов по простому модулю. Кольцо вычетов, быстрое вычисление остатка. Расширенный алгоритм Евклида. Малая теорема Ферма, теорема Эйлера. Поле вычетов
5	Поле Галуа. Кольцо многочленов над полем вычетом. Пример поля из 8 элементов. Конструкция поля Галуа, дискретный логарифм
6	Контрольные суммы. Назначение контрольных сумм. Хеш-функции. CRC-код
7	Коды, исправляющие ошибки. Постановка задачи, код Хемминга. Необходимые утверждения, линейные коды. БЧХ-коды
8	Введение в криптографию. Терминология, исторические примеры шифрования. Симметричные и ассиметричные шифры. Криптоанализ. Симметрические криптоалгоритмы. Введение, шифр Вернама, оценка стойкости шифра. Нарушение условий стойкости, примеры атак на шифр. Блочные шифры, условия стойкости, примеры. Сеть Фейштеля, шифр TEA
9	Криптографические хэш-функции. Введение, свойства криптографических хеш-функций. Использование блочных шифров для построения хэш-функций. Примеры криптографических хэш-функций. Приложения хэш-функций, генерация ключей, аутентификация. Криптоанализ хэш-функций, радужные таблицы, использование «соли»
10	Асимметричные криптоалгоритмы с открытым ключом. Введение, односторонние функции. Алгоритм Диффи–Хеллмана. Практическое применение
11	Алгоритм RSA. Исторический экскурс. Описание алгоритма RSA, пример. Практическое применение
12	Криптографические протоколы. Введение. Основные криптопротоколы, цифровая подпись. Протоколы SSH, SSL, примеры

4.3 Содержание практических (семинарских) занятий

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.4 Содержание лабораторных работ

Очная форма обучения

№ п/п	Темы лабораторных работ
	8 семестр
1	Консоли Windows и Linux, системные команды
2	Использование командных файлов
3	Поиск и замена при помощи регулярных выражений
4	Архивация, синхронизация, контрольные суммы
5	Восстановление информации. Надежная очистка данных
6	Шифрование файлов, прозрачное шифрование
7	Криптографические хеш-функции
8	Доступ к удаленной консоли через Telnet и защищенное соединение в Putty
9	Защита при помощи Firewall и антивирусов

№ п/п	Темы лабораторных работ
10	Система контроля версий Git. Использование GitHub

4.5 Содержание клинических практических занятий

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.6 Содержание самостоятельной работы обучающегося

Очная форма обучения

№ п/п	Виды и формы самостоятельной работы
	8 семестр
1	Подготовка к лабораторным работам
2	Подготовка к промежуточной аттестации и ее прохождение

5 Система формирования оценки результатов обучения по дисциплине (модулю) в рамках текущего контроля успеваемости и промежуточной аттестации обучающегося

Очная форма обучения

Мероприятия текущего контроля успеваемости и промежуточной аттестации обучающегося			Максимальное количество баллов
		8 семестр	
Текущий контроль успеваемости	Первый рубежный контроль	**Оцениваемая учебная деятельность обучающегося:**	
		Посещение лекционных занятий	4
		Выполнение лабораторных работ	26
		Итого	30
	Второй рубежный контроль	**Оцениваемая учебная деятельность обучающегося:**	
		Посещение лекционных занятий	4
		Выполнение лабораторных работ	26
		Итого	30
Промежуточная аттестация	Зачет		40 (100*)

* В случае отказа обучающегося от результатов текущего контроля успеваемости

Шкала соответствия оценок в стобалльной и академической системах оценивания результатов обучения по дисциплине (модулю)

Система оценивания результатов обучения	Оценки			
Стобалльная система оценивания	0 – 39	40 – 60	61 – 80	81 – 100

Система оценивания результатов обучения	Оценки			
Академическая система оценивания (экзамен, дифференцированный зачет, защита курсового проекта, защита курсовой работы)	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Академическая система оценивания (зачет)	Не зачтено	Зачтено		

6 Описание материально-технической базы (включая оборудование и технические средства обучения), необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для осуществления образовательного процесса по дисциплине (модулю) требуется учебная аудитория, оборудованная доской для написания мелом. Для проведения лабораторных работ требуется аудитория, оснащенная компьютерами с подключением к сети «Интернет» и обеспечением доступа в электронную-образовательную среду».

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература

1. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. — Режим доступа: для авториз. пользователей.
2. Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 95 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/17925.html. — Режим доступа: для авторизир. пользователей.
3. Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации: учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010. — 104 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/17926.html. — Режим доступа: для авторизир. пользователей.
4. Нерсесянц, А. А. Защита информации: учебное пособие / А. А. Нерсесянц. — Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010. — 61 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/61295.html. — Режим доступа: для авторизир. пользователей.

7.2 Дополнительная литература

1. Глаголев, В.В. Алгебраическая теория кодирования : учебн. пособие / В.В. Глаголев. — Тула : Издательство ТулГУ, 2004. — 116 с. — ISBN 5-7679-0564-9. — Текст: электронный // Библиотех: электронно-библиотечная система. — URL:

https://tsutula.bibliotech.ru/Reader/Book/2015111311155332343400008693. — Режим доступа: для авториз. пользователей.
2. Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. — Ростов-на-Дону : Феникс, 2016. — 349 с. — ISBN 978-5-222-26911-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/59350.html. — Режим доступа: для авторизир. пользователей.
3. Сэломон, Д. Сжатие данных, изображений и звука : учеб. пособие для вузов / Д. Сэломон; пер. с англ. В.В. Чепыжова. — М. : Техносфера, 2004. — 368с. : ил. — (Мир программирования). — Библиогр. в конце кн. — ISBN 5-94836-027-X : 202.50.
4. Галатенко, В.А. Стандарты информационной безопасности : Курс лекций / В.А. Галатенко; Под ред. В.Б. Бетелина; Интернет ун-т информ. технологий. — М., 2004. — 328с. — (Основы информационных технологий). — Библиогр. в конце кн. — ISBN 5-9556-0007-8 /в пер./ : 200.00.
5. Ященко, В.В. Введение в криптографию: Новые математические дисциплины : Учебник / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др.; Под общ. ред. В.В. Ященко. — СПб. и др. : МЦНМО: Питер, 2001. — 288с. : ил. — Библиогр. в конце гл. — ISBN 5-318-00443-1 /в пер./ : 81.00.
6. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко; Ин-т проблем информационной безопасности МГУ. — М. : МЦНМО, 2003. — 328с. : ил. — (Информационная безопасность: криптография). — Библиогр. в конце кн. — ISBN 5-94057-103-4 /в пер./ : 73.00.
7. Шнайер, Б. Секреты и ложь : Безопасность данных в цифровом мире: Пер.с англ. / Б. Шнайер. — М.и др. : Питер, 2003. — 368с. — (Классика Computer Science). — Библиогр. в конце кн. — ISBN 5-318-00193-9 /в пер./ : 235.00. — ISBN 0-471-25311-1 (англ.).

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

1. http://window.edu.ru – Единое окно доступа к образовательным ресурсам.
2. http://elibrary.ru/ – Научная Электронная Библиотека eLibrary.
3. http://cyberleninka.ru/ – КиберЛенинка — научная электронная библиотека.
4. http://www.intuit.ru – Национальный открытый университет «ИНТУИТ».

9 Перечень информационных технологий, необходимых для осуществления образовательного процесса по дисциплине (модулю)

9.1 Перечень необходимого ежегодно обновляемого лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. Пакет офисных приложений «МойОфис».

9.2 Перечень необходимых современных профессиональных баз данных и информационных справочных систем

Современные профессиональные базы данных и информационные справочные системы не требуются.