МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

_____Е.И.Луковникова

06 мая _____20 24 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.14 Информационная безопасность

Закреплена за кафедрой **Базовая кафедра менеджмента и информационных технологий**

Учебный план bs090303_24_УПвЦЭ.plx
Направление: 09.03.03 Прикладная информатика

Квалификация **Бакалавр**

Форма обучения **заочная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля на курсах:
Зачет 3

Распределение часов дисциплины по курсам

Курс	3		Итого	
Вид занятий	УП	РП		
Лекции	2	2	2	2
Лабораторные	2	2	2	2
В том числе инт.	2	2	2	2
Итого ауд.	4	4	4	4
Контактная работа	4	4	4	4
Сам. работа	100	100	100	100
Часы на контроль	4	4	4	4
Итого	108	108	108	108

Программу составил(и):
к.т.н., доц., Иванов М.Ю. _____
Рабочая программа дисциплины

Информационная безопасность

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)
составлена на основании учебного плана:

Направление: 09.03.03 Прикладная информатика
утвержденного приказом ректора от 30.01.2024 № 32.

Рабочая программа одобрена на заседании кафедры

Базовая кафедра менеджмента и информационных технологий

Протокол от 20 марта 2024 г. № 11

Срок действия программы: 2024-2027 уч.г.

Зав. кафедрой Вахрушева М. Ю.

Председатель МКФ

доцент, к.э.н., Грудистова Е.Г. 05.04.2024 г. № 7 _____

Ответственный за реализацию ОПОП _____ Вахрушева М.Ю.
(подпись)

Директор библиотеки _____ Сотник Т.Ф.
(подпись)

№ регистрации 26
(учебный отдел)

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Базовая кафедра менеджмента и информационных технологий

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2025 г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Базовая кафедра менеджмента и информационных технологий

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2026 г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Базовая кафедра менеджмента и информационных технологий

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2027 г. № __
Зав. кафедрой

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Базовая кафедра менеджмента и информационных технологий

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2028 г. № __
Зав. кафедрой

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Изучение теоретических и практических основ в области методов и способов обеспечения сохранности, целостности и безопасности информационных ресурсов

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.14
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Информационные системы и технологии
2.1.2	Информатика и программирование
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Разработка программных приложений

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	
Индикатор 1	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Индикатор 2	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Индикатор 3	Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	
Индикатор 1	Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
Индикатор 2	Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
Индикатор 3	Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	принципы, методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;способы решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;основы подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе;основные стандарты оформления технической документации с учетом требований информационной безопасности;основные требования оформления технической документации с учетом требований информационной безопасности;основные виды технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности
3.2	**Уметь:**
3.2.1	находить решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности;решать стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности;составлять обзоры, аннотации, рефераты, научные доклады, публикации и библиографию по научно-исследовательской работе;применять техническую документацию с учетом требований информационной безопасности;применять стандарты оформления технической документации с учетом требований информационной безопасности;применять стандарты для составления технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности
3.3	**Владеть:**

3.3.1	навыками применения информационно-коммуникационных технологий с учетом основных требований информационной безопасности;методологией использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности;навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;навыками оформления технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности;навыками использования технической документации на различных стадиях жизненного цикла информационной системы с учетом требований информационной безопасности;навыками составления технической документации на различных этапах жизненного цикла информационной системы с учетом требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел	**Раздел 1. Понятие и основные положения информационной безопасности**						
1.1	Лек	Классификация угроз информационной безопасности	3	0,5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0,5	Лекция-дискуссия, ОПК-3.1
1.2	Лек	Анализ способов возможных нарушений информационной безопасности	3	0,5	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0,5	Лекция-дискуссия, ОПК-3.1
1.3	Зачёт	Подготовка к зачету	3	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1
	Раздел	**Раздел 2. Основные положения теории информационной безопасности**						
2.1	Лек	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	3	0,2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1
2.2	Лек	Модели безопасности и их применение	3	0,2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1
2.3	Зачёт	Подготовка к зачету	3	1	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1
	Раздел	**Раздел 3. Основные технологии построения защищенных экономических информационных систем**						
3.1	Лек	Концепция информационной безопасности	3	0,2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1
3.2	Лек	Методы криптографии	3	0,2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1
3.3	Лек	Защита и разработка защищенных экономических информационных систем	3	0,2	ОПК-3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1

3.4	Лаб	Шифрование текстовой информации случайной перестановкой символов	3	0,5	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1	0,5	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3.5	Лаб	Шифрование текстовой информации заменой символов	3	0,5	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1	0,5	Анализ конкретных ситуаций, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3.6	Лаб	Шифрование текстовой информации сдвигами по паролю символов	3	0,5	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1	0	Анализ конкретных ситуаций, ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3.7	Лаб	Шифрование текстовой информации заменой части символов	3	0,5	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3.8	Ср	Подготовка к лабораторным работам	3	100	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
3.9	Зачёт	Подготовка к зачету	3	2	ОПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.2 Л2.3 Л2.4 Л2.5	0	ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.2, ОПК-4.3

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии с использованием активных методов обучения (лекция – дискуссия)

Образовательные технологии с использованием интерактивных методов обучения (case-study (анализ конкретных ситуаций))

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Перечень тем для лекции-дискуссии:
Раздел 1. Понятие и основные положения информационной безопасности:
1. Понятие угрозы информационной безопасности
2. Классификация угроз информационной безопасности
3. Ранжирование угроз информационной безопасности по степени возможного ущерба
4. Несанкционированный доступ к информации
5. Способы несанкционированного доступа к информации
6. Ранжирование способов несанкционированного доступа к информации по степени возможного ущерба
Перечень тем для анализа конкретных ситуаций:
Раздел 3. Основные технологии построения защищенных экономических информационных систем:
1. Определение понятий «криптография», «криптоанализ», «шифрование», «шифр», «ключ»
2. Основные методы криптографии, их достоинства и недостатки
3. Основные способы криптографических преобразований

4. Характеристика базовых симметричных криптоалгоритмов
5. Блочный метод шифрования информации. Требования, которым должна удовлетворять функция криптопреобразования стойкого блочного шифра
6. Прикладные задачи экономики, решаемые с помощью шифрования
7. Гаммирование и его сущность
8. Базовые биективные математические функции, используемые в криптографии

6.2. Темы письменных работ

Не предусмотрено

6.3. Фонд оценочных средств

Вопросы к зачету:
Раздел 1. Понятие и основные положения информационной безопасности:
1.1 Понятие информационной безопасности
1.2 Основные составляющие информационной безопасности
1.3 Международные стандарты информационного обмена
1.4 Понятие угрозы и критерии классификации угроз
1.5 Виды возможных нарушений безопасности информационных систем
1.6 Типовые способы удаленных атак на информацию в сети
1.7 Методы сбора сведений для вторжения в компьютерную сеть
1.8 Модель нарушителя информационной безопасности
1.9 Несанкционированный доступ к информации. Способы НСД
1.10 Шпионские программные закладки
Раздел 2. Основные положения теории информационной безопасности:
2.1 Правовые основы защиты информации
2.2 Документы, регламентирующие деятельность по обеспечению защиты информации
2.3 Уровни информационной защиты
2.4 Модели информационной безопасности
2.5 Средства защиты информации от несанкционированного доступа
2.6 Классификация парольных средств защиты
Раздел 3. Основные технологии построения защищенных экономических информационных систем:
3.1 Криптография. Основные понятия и определения, задачи криптографии
3.2 Классификация способов криптографического преобразования информации
3.3 Симметричные методы криптографии
3.4 Блочные шифры
3.5 Асимметричные методы криптографии
3.6 Формальные модели атак и угроз в криптографии
3.7 Понятие стойкости криптографического алгоритма
3.8 Классические методы криптоанализа
3.9 Использование методов криптографии в экономике (банковском деле, электронных платежных системах и т.п.)
3.10 Угрозы безопасности информации в платежных системах
3.11 Проблемы криптографической защиты платежных систем
3.12 Требования к криптографическим средствам защиты банковской информации
3.13 Новые направления обеспечения безопасности информации в банковском деле
3.14 Концепция защиты информации
3.15 Политика информационной безопасности

6.4. Перечень видов оценочных средств

Перечень тем для лекции-дискуссии, перечень тем для анализа конкретных ситуаций, вопросы к зачету

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва|Берлин: Директ-Медиа, 2020	1	http://biblioclub.ru/index.php?page=book&id=571485
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=493175

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.3	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	1	http://biblioclub.ru/index.php?page=book&id=438331

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Иванов М.Ю.	Информационные технологии: методы криптографии: учебное пособие	Братск: БрГУ, 2010	30	
Л2.2	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л2.3	Трушин В. А., Котов Ю. А., Левин Л. С., Донской К. А.	Введение в информационную безопасность и защиту информации: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2017	1	http://biblioclub.ru/index.php?page=book&id=575113
Л2.4	Гультяева Т. А.	Основы информационной безопасности: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018	1	http://biblioclub.ru/index.php?page=book&id=574729
Л2.5	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=562246

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л3.1	Иванов М.Ю.	Информационная безопасность: методические указания к выполнению лабораторных работ	Братск: БрГУ, 2014	20	

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	PascalABC
7.3.1.4	Turbo Pascal

7.3.2 Перечень информационных справочных систем

7.3.2.1	ИСС "Кодекс". Информационно-справочная система
7.3.2.2	Справочно-правовая система «Консультант Плюс»
7.3.2.3	Издательство "Лань" электронно-библиотечная система
7.3.2.4	«Университетская библиотека online»
7.3.2.5	Электронный каталог библиотеки БрГУ
7.3.2.6	Электронная библиотека БрГУ
7.3.2.7	Научная электронная библиотека eLIBRARY.RU
7.3.2.8	Национальная электронная библиотека НЭБ
7.3.2.9	Университетская информационная система РОССИЯ (УИС РОССИЯ)

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение аудитории	Вид занятия

3217	Учебная аудитория (мультимедийный класс)	Основное оборудование: - интерактивная доска SMART Board 680i2/Unifl, - интерактивный планшет Wacom PL-720, - колонки Microlab Solo-7C, - ноутбук Samsung R610<NP-R610-FS08>, - телевизор плазменный Samsung 63 PS-63A756T1M. Дополнительно: - маркерная доска – 1 шт. Учебная мебель: - комплект мебели (посадочных мест) – 60 шт.; - комплект мебели (посадочных мест) для преподавателя – 1 шт	Лек
3234	Учебная аудитория (дисплейный класс)	Основное оборудование: - системный блок AMD Ryzen 5 7600X 4.70GHz 16 Gb (16 шт.); - монитор MSI PRO MP 242 Series (16 шт.). Дополнительно: - маркерная доска – 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) – 24/16 шт.; - комплект мебели (посадочных мест) для преподавателя – 1 шт.	Ср
3236	Учебная аудитория (дисплейный класс)	Основное оборудование: - системный блок AMD A10-7800 Radeon R7 (12 шт.), - системный блок для слабовидящих пользователей AMD A10-7850K (1 шт.), - монитор Philips233 V5QHABP (13 шт.). Дополнительно: - маркерная доска – 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) – 26/12 шт.; - комплект мебели (посадочных мест) для преподавателя – 1 шт.; - комплект мебели (посадочных мест/АРМ) для оператора – 1/1 шт.	Лаб
3101	Учебная аудитория (дисплейный класс)	Основное оборудование: - ПК AMD 3.9 GHz 4GbDVD 19 KbMs (11 шт.). Дополнительно: - маркерная доска – 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) – 20/11 шт.; - комплект мебели (посадочных мест) для преподавателя – 1 шт.;	Зачёт
2201	читальный зал №1	Комплект мебели (посадочных мест) Стеллажи Комплект мебели (посадочных мест) для библиотекаря Выставочные шкафы ПК i5-2500/H67/4Gb (монитор TFT19 Samsung) (10шт.); принтер HP Laser Jet P2055D (1шт.)	Ср

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина «Информационная безопасность» направлена на овладение основами теоретических и практических знаний в области выявления угроз информационной безопасности, организационно-технических мероприятий по защите информации в информационных системах, обеспечения сохранности, целостности и безопасности информационных ресурсов.

Изучение дисциплины «Информационная безопасность» предусматривает: лекции; лабораторные работы; самостоятельную работу обучающихся; зачет.

Помимо освоения основных разделов дисциплины необходимо овладеть навыками и умениями применения изученных методов для управления информационной безопасностью, применения и реализации тех или иных методов в конкретных ситуациях.

В процессе изучения дисциплины на первом этапе рекомендуется обратить внимание на понятийно-категориальный аппарат дисциплины. Овладение ключевыми понятиями является важным этапом в освоении содержания современных методов обеспечения информационной безопасности.

При подготовке к сдаче зачета рекомендуется особое внимание уделить вопросам, связанным с современными методами криптографического преобразования информации.

В процессе выполнения лабораторных работ происходит закрепление знаний, формирование умений и навыков шифрования и дешифрования текстовой информации с использованием возможностей распространенных языков программирования и блочных шифров.

Самостоятельную работу по изучению дисциплины необходимо начинать с проработки конспекта лекций, обобщения, систематизации, углубления и конкретизации полученных теоретических знаний с использованием основной и дополнительной литературы, а также рекомендуемых ресурсов информационно-телекоммуникационной сети «Интернет».

В процессе консультации с преподавателем необходимо уточнять вопросы, термины, материал, вызвавший трудности при самостоятельной работе.

Работа с литературой является важнейшим элементом в получении знаний по дисциплине. Прежде всего, необходимо воспользоваться списком рекомендуемой по данной дисциплине литературой. Дополнительные сведения по изучаемым темам можно найти в периодической печати и информационно-телекоммуникационной сети «Интернет».

Предусмотрено проведение аудиторных занятий (в виде лекций и лабораторных работ) в сочетании с внеаудиторной

работой.