

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

_____ 13 мая _____ 20 24 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04.ДВ.01.01 Основы информационной безопасности

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план б010302_24_ИПОиЗИ.plx

Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:

Зачет 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Неделя	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	64	64	64	64
В том числе инт.	12	12	12	12
В том числе в форме практ.подготовки	64	64	64	64
Итого ауд.	96	96	96	96
Контактная работа	96	96	96	96
Сам. работа	48	48	48	48
Итого	144	144	144	144

Программу составил(и):
к.т.н., доц., Фигура К.Н. _____

Рабочая программа дисциплины

Основы информационной безопасности

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:

Направление: 01.03.02 Прикладная математика и информатика
утвержденного приказом ректора от 30.01.2024 № 32.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 21.03.2024 г. № 9

Срок действия программы: 2024 - 2028 уч.г.

Зав. кафедрой Горохов Д.Б.

Председатель МКФ Латушкина С.В.

Протокол от 26.04.2024 г. № 8

Ответственный за реализацию ОПОП _____ Горохов Д.Б.

Директор библиотеки _____ Сотник Т.Ф.

№ регистрации _____ 43
(методический 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
Информатики, математики и физики

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
Информатики, математики и физики

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
Информатики, математики и физики

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
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2028 г. № ____

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Получение устойчивых практических навыков по нормативно-правовому обеспечению информационной безопасности и защите информации с применением технических средств.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:		Б1.В.04.ДВ.01.01
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Системное программирование	
2.1.2	Языки и методы программирования	
2.1.3	Компьютерные сети	
2.1.4	Сценарные языки программирования	
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Выполнение и защита выпускной квалификационной работы	
2.2.2	Комплексное обеспечение безопасности объекта информатизации	
2.2.3	Программно-аппаратные средства защиты информации	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**ПК-3: Способен администрировать системы защиты информации автоматизированных систем**

Индикатор 1	ПК-3.1. Выполняет работы по администрированию системы защиты информации автоматизированных систем.
Индикатор 1	ПК-3.2. Выполняет установленные процедуры обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы.

В результате освоения дисциплины обучающийся должен

3.1	Знать:	
3.1.1	основы безопасности операционных систем; основные программно-аппаратные средства обеспечения информационной	
3.1.2	безопасности.	
3.2	Уметь:	
3.2.1	выполнять основные этапы решения задач информационной безопасности; применять на практике основные общеметодологические принципы теории информационной безопасности.	
3.3	Владеть:	
3.3.1	основными программно-аппаратными средствами обеспечения информационной безопасности; навыками управления деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетенции	Литература	Инте ракт.	Примечание
	Раздел	Раздел 1. Организационно-правовое обеспечение информационной безопасности						
1.1	Лек	Введение в правовое обеспечение информационной безопасности	6	2	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
1.2	Лек	Государственная система защиты информации в Российской Федерации, ее организационная структура и функции	6	2	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2

1.3	Лек	Информация как объект правового регулирования	6	2	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
1.4	Лек	Правовой режим защиты государственной тайны	6	4	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-3.1, ПК-3.2
1.5	Лек	Нормативное правовое регулирование в области коммерческой тайны	6	2	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-3.1, ПК-3.2
1.6	Лек	Нормативное обеспечение криптографической защиты информации	6	2	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
1.7	Лек	Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных	6	4	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-3.1, ПК-3.2
1.8	Лаб	Организационно-правовое обеспечение информационной безопасности	6	20	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	4	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-3.1, ПК-3.2
1.9	Ср	Подготовка к выполнению ЛР	6	12	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
1.10	Зачёт	Подготовка к зачёту	6	10	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
	Раздел	Раздел 2. Техническая защита информации						
2.1	Лек	Операционная система специального назначения Astra Linux Special Edition	6	8	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
2.2	Лаб	Операционная система специального назначения Astra Linux Special Edition	6	14	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2

2.3	Лек	Инженерно-техническое обеспечение защиты информации	6	2	ПК-3		0	ПК-3.1, ПК-3.2
2.4	Лаб	Инженерно-техническое обеспечение защиты информации	6	10	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
2.5	Лек	Технические каналы утечки информации	6	4	ПК-3		0	ПК-3.1, ПК-3.2
2.6	Лаб	Технические каналы утечки информации	6	20	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-3.1, ПК-3.2
2.7	Ср	Подготовка к выполнению ЛР	6	12	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2
2.8	Зачёт	Подготовка к зачёту	6	14	ПК-3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-3.1, ПК-3.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностях (электронные библиотеки))

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

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

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

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

ЛЕКЦИЯ-ДИСКУССИЯ.

Лекция-дискуссия №1(2 час.).

Тема: Правовой режим защиты государственной тайны.

Лекция-дискуссия №2(2 час.).

Тема: Нормативное правовое регулирование в области коммерческой тайны.

Лекция-дискуссия №3(2 час.).

Тема: Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных.

CASE-STUDY (АНАЛИЗ КОНКРЕТНЫХ СИТУАЦИЙ, СИТУАЦИОННЫЙ АНАЛИЗ).

case-study (анализ конкретных ситуаций, ситуационный анализ) №1 (4 час.).

Тема: Организационно-правовое обеспечение информационной безопасности.

case-study (анализ конкретных ситуаций, ситуационный анализ) №2 (2 час.).

Тема: Технические каналы утечки информации.

ЛАБОРАТОРНЫЕ РАБОТЫ.

Лабораторная работа №1.

Тема: Организационно-правовое обеспечение информационной безопасности.

Вопросы:

1) Государственная система защиты информации в Российской Федерации, ее организационная структура и функции;

- 2) Информация как объект правового регулирования;
- 3) Правовой режим защиты государственной тайны;
- 4) Нормативное правовое регулирование в области коммерческой тайны;
- 5) Нормативное обеспечение криптографической защиты информации;
- 6) Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных.

Лабораторная работа №2.

Тема: Операционная система специального назначения Astra Linux Special Edition

Вопросы:

- 1) Работа с учётными записями пользователей и группами;
- 2) Настройка параметров мандатного управления доступом и мандатного контроля целостности;
- 3) Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности;
- 4) Администрирование ОССН в рамках реализации мандатного контроля целостности;
- 5) Настройка механизмов организации замкнутой программной среды;
- 6) Настройка сетевого взаимодействия;

Лабораторная работа №3.

Тема: Инженерно-техническое обеспечение защиты информации.

Вопросы:

- 1) Концепция инженерно-технической защиты информации;
- 2) Цели, задачи, ресурсы системы защиты информации;
- 3) Угрозы безопасности информации и меры по их предотвращению;
- 4) Принципы инженерно-технической защиты информации;
- 5) Принципы построения системы инженерно-технической защиты информации;

Лабораторная работа №4.

Тема: Технические каналы утечки информации.

Вопросы:

- 1) Типовые структура и виды технических каналов утечки информации;
- 2) Основные показатели технических каналов утечки информации;
- 3) Комплексное использование технических каналов утечки информации;
- 4) Акустические и оптические каналы утечки информации;
- 5) Радиоэлектронные каналы утечки информации;
- 6) Вещественные каналы утечки информации.

6.2. Темы письменных работ

Учебным планом не предусмотрено.

6.3. Фонд оценочных средств

Вопросы к зачёту:

Раздел 1. Организационно-правовое обеспечение информационной безопасности.

- 1.1. Информационная безопасность государства;
- 1.2. Нормативные правовые акты Российской Федерации в области информации, информационных технологий и защиты информации;
- 1.3. Конституционные права граждан на информацию и возможности их ограничения;
- 1.4. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции;
- 1.5. Информация как объект правовых отношений;
- 1.6. Субъекты и объекты правовых отношений в информационной сфере;
- 1.7. Виды информации по законодательству Российской Федерации;
- 1.8. Государственная тайна как особый вид защищаемой информации;
- 1.9. Законодательство Российской Федерации в области защиты государственной тайны;
- 1.10. Отнесение сведений к государственной тайне;
- 1.11. Засекречивание и рассекречивание;
- 1.12. Допуск к государственной тайне и доступ к сведениям, составляющим государственную тайну;
- 1.13. Особенности информационных правоотношений, возникающих при производстве, передаче и потреблении информации, составляющей коммерческую тайну;
- 1.14. Правовой режим коммерческой тайны;
- 1.15. Охрана коммерческой тайны в трудовых отношениях;
- 1.16. Защита прав на коммерческую тайну;
- 1.17. Федеральные законы в области криптографической защиты информации;
- 1.18. Положение о лицензировании в области криптографической защиты информации;
- 1.19. Электронная подпись;
- 1.20. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных;
- 1.21. Правовая основа системы лицензирования и сертификации;
- 1.22. Аттестация объектов информатизации по требованиям безопасности информации.

Раздел 2. Техническая защита информации.

- 2.1. Концепция инженерно-технической защиты информации;
- 2.2. Цели, задачи, ресурсы системы защиты информации;
- 2.3. Угрозы безопасности информации и меры по их предотвращению;
- 2.4. Принципы инженерно-технической защиты информации;

- 2.5. Принципы построения системы инженерно-технической защиты информации;
 2.6. Типовые структура и виды технических каналов утечки информации;
 2.7. Основные показатели технических каналов утечки информации;
 2.8. Комплексное использование технических каналов утечки информации;
 2.9. Акустические и оптические каналы утечки информации;
 2.10. Радиоэлектронные каналы утечки информации;
 2.11. Вещественные каналы утечки информации.

6.4. Перечень видов оценочных средств

Отчеты по лабораторным работам, вопросы к зачёту.

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

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛП. 1	Ярочкин В.И.	Информационная безопасность: Учебник для вузов	Москва: Академический Проект, 2003	25	
ЛП. 2	Ишейнов 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
ЛП. 3	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
ЛП. 4	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
ЛП. 1	Торокин А.А.	Инженерно-техническая защита информации: учебное пособие	Москва: Гелиос АРВ, 2005	10	
ЛП. 2	Гребеншико в Ю. Б., Низамов А. Ж., Евсеев В. Л.	Физические явления и процессы в области информационной безопасности: учебное пособие	Москва: Прометей, 2019	1	http://biblioclub.ru/index.php?page=book&id=576045
ЛП. 3	Титов А. А.	Инженерно-техническая защита информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	1	http://biblioclub.ru/index.php?page=book&id=208567

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
ЛЗ. 1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
ЛЗ. 2	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

7.3.1 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	Adobe Acrobat Reader DC
7.3.1.4	doPDF
7.3.1.5	LibreOffice

7.3.2 Перечень информационных справочных систем

7.3.2.1	Справочно-правовая система «Консультант Плюс»
7.3.2.2	«Университетская библиотека online»
7.3.2.3	Электронный каталог библиотеки БрГУ
7.3.2.4	Электронная библиотека БрГУ

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение аудитории	Вид занятия
1346	Учебная аудитория (дисплейный класс)	Основное оборудование: - доска интерактивная Smart Board SB680; Системный блок Prime Box S302, 5-135000, 16GB DOR5, Gigabyte 4060, 1TBs5 D – 15 шт.; - Монитор Asus VA24E 23,8 - 15 шт.; - принтер HP LaserJet 1000 Series; - проектор Unifri35 (Vixuiti) SmartTechnologies; - коммутатор D-Link DES-1050G. Дополнительно: - маркерная доска - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 32/15 шт. - комплект мебели (посадочных мест) для преподавателя - 1 шт.	Лек
1346	Учебная аудитория (дисплейный класс)	Основное оборудование: - доска интерактивная Smart Board SB680; Системный блок Prime Box S302, 5-135000, 16GB DOR5, Gigabyte 4060, 1TBs5 D – 15 шт.; - Монитор Asus VA24E 23,8 - 15 шт.; - принтер HP LaserJet 1000 Series; - проектор Unifri35 (Vixuiti) SmartTechnologies; - коммутатор D-Link DES-1050G. Дополнительно: - маркерная доска - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 32/15 шт. - комплект мебели (посадочных мест) для преподавателя - 1 шт.	Лаб
1001	читальный зал №3	Учебная мебель. Оборудование 15- CPU 5000/RAM 2Gb/HDD (Монитор TFT 19 LG 1953S-SF); принтер HP LaserJet P3005	Ср
1346	Учебная аудитория (дисплейный класс)	Основное оборудование: - доска интерактивная Smart Board SB680; Системный блок Prime Box S302, 5-135000, 16GB DOR5, Gigabyte 4060, 1TBs5 D – 15 шт.; - Монитор Asus VA24E 23,8 - 15 шт.; - принтер HP LaserJet 1000 Series; - проектор Unifri35 (Vixuiti) SmartTechnologies; - коммутатор D-Link DES-1050G. Дополнительно: - маркерная доска - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 32/15 шт. - комплект мебели (посадочных мест) для преподавателя - 1 шт.	Зачёт

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

Дисциплина "Основы информационной безопасности" направлена на получение и совершенствование знаний и устойчивых практических навыков по нормативно-правовому обеспечению информационной безопасности и защите информации с применением технических средств.

Работа на лекциях.

Написание конспекта лекций: краткое, последовательное изложение основных положений, формулировок, выводов, обобщений; техническое оформление записей (подчеркивание, выделение ключевых слов и терминов). Активная работа на лекции.

Лабораторные работы.

Выполнение заданий с использованием методических рекомендаций по выполнению лабораторных работ, оформление отчётов, защита лабораторных работ.

Самостоятельная работа обучающихся.

Подготовка к лабораторным работам: проработка материалов по темам лабораторных работ с использованием рекомендуемой литературы, конспекта лекций, ресурсов информационно-телекоммуникационной сети Интернет; выполнение заданий; оформление отчётов по лабораторным работам; подготовка к защите лабораторных работ.

Подготовка к зачету: систематическая работа с конспектом лекций: чтение записей; проверка терминов с помощью списка рекомендуемой литературы; обозначение вопросов, материал, которых вызывает трудности; попытка найти ответ в рекомендуемых источниках; подготовка вопросов преподавателю, если не удастся самостоятельно разобраться в материале.