МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6FC632A3C216B9FFDA0F5EADC52C05FE
Владелец: Ситов Илья Сергеевич
Действителен: с 25.03.2024 до 18.06.2025

УТВЕРЖДАЮ

Проректор по учебной работе

_____Е.И.Луковникова

14 мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.05 Информационная безопасность

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

Учебный план b090302_24_ИСиТ.plx
Направление: 09.03.02 Информационные системы и технологии

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
Экзамен 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	34	34	34	34
Лабораторные	34	34	34	34
В том числе инт.	8	8	8	8
В том числе в форме практ.подготовки	34	34	34	34
Итого ауд.	68	68	68	68
Контактная работа	68	68	68	68
Сам. работа	22	22	22	22
Часы на контроль	54	54	54	54
Итого	144	144	144	144

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

Информационная безопасность

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)
составлена на основании учебного плана:

Направление: 09.03.02 Информационные системы и технологии
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 42
(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
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.05
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Системное администрирование
2.1.2	Информационные и автоматизированные системы
2.1.3	Сетевое администрирование
2.1.4	Инфокоммуникационные системы и сети
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Основы процессов внедрения информационных систем
2.2.2	Производственная (преддипломная) практика
2.2.3	Выполнение и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-6: Способность управлять безопасностью сетевых устройств и программного обеспечения, проводить контроль производительности сетевой инфраструктуры инфокоммуникационной системы	
Индикатор 1	ПК-6.1. Выполняет работы по управлению безопасностью сетевых устройств и программного обеспечения администрируемой сети.
Индикатор 1	ПК-6.2. Осуществляет контроль производительности сетевой инфраструктуры инфокоммуникационной системы с использованием штатных и внешних программно-аппаратных средств контроля.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	базовые направления обеспечения информационной безопасности предприятия; современные программные средства, в том числе отечественного производства, при решении задач обеспечения необходимого уровня информационной безопасности; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.
3.2	**Уметь:**
3.2.1	разрабатывать способы защиты информации и меры противодействия несанкционированному доступу к источникам конфиденциальной информации; использовать современные ИТ и программные средства при анализе защищенности ИС предприятия; применять информационно-коммуникационные технологии к решению задач профессиональной деятельности с учетом требований информационной безопасности.
3.3	**Владеть:**
3.3.1	методологией построения средств противодействия угрозам; методами и приёмами разработки концептуальных моделей информационной безопасности предприятия; современными IT – технологиями, используемыми для обмена информацией в рамках профессиональной деятельности с учётом 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. Организационно-правовое обеспечение информационной безопасности**						
1.1	Лек	Введение в правовое обеспечение информационной безопасности	7	2	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2

1.2	Лек	Государственная система защиты информации в Российской Федерации, ее организационная структура и функции	7	4	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
1.3	Лек	Информация как объект правового регулирования	7	4	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
1.4	Лек	Правовой режим защиты государственной тайны	7	4	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
1.5	Лек	Нормативное правовое регулирование в области коммерческой тайны	7	4	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-6.1, ПК-6.2
1.6	Лек	Нормативное обеспечение криптографической защиты информации	7	4	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
1.7	Лек	Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных	7	4	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
1.8	Лаб	Организационно-правовое обеспечение информационной безопасности	7	10	ПК-6	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-6.1, ПК-6.2
1.9	Ср	Подготовка к выполнению ЛР	7	8	ПК-6	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-6.1, ПК-6.2
1.10	Экзамен	Подготовка к экзамену	7	27	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
	Раздел	**Раздел 2. Техническая защита информации**						
2.1	Лек	Операционная система специального назначения Astra Linux Special Edition	7	8	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2

2.2	Лаб	Операционная система специального назначения Astra Linux Special Edition	7	12	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
2.3	Лаб	Инженерно-техническое обеспечение защиты информации	7	5	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
2.4	Лаб	Технические каналы утечки информации	7	7	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
2.5	Ср	Подготовка к выполнению ЛР	7	14	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2
2.6	Экзамен	Подготовка к экзамену	7	27	ПК-6	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-6.1, ПК-6.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

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 активных методов обучения (лекция – дискуссия)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

ЛЕКЦИЯ-ДИСКУССИЯ.
Лекция-дискуссия №1(2 час.).
Тема: Нормативное правовое регулирование в области коммерческой тайны.

CASE-STUDY (АНАЛИЗ КОНКРЕТНЫХ СИТУАЦИЙ, СИТУАЦИОННЫЙ АНАЛИЗ).
case-study (анализ конкретных ситуаций, ситуационный анализ) №1 (6 час.)
Тема: Организационно-правовое обеспечение информационной безопасности.

ЛАБОРАТОРНЫЕ РАБОТЫ.
Лабораторная работа №1.
Тема: Организационно-правовое обеспечение информационной безопасности.
Вопросы для рассмотрения:
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 для рассмотрения:
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 для рассмотрения:
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 для рассмотрения:
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

Экзаменнационные вопросы:
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

Лабораторные работы (отчеты по лабораторным работам), экзаменационные вопросы (перечень вопросов по разделам дисциплины).

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	Ярочкин В.И.	Информационная безопасность: Учебник для вузов	Москва: Академический Проект, 2003	25	
Л1.2	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
Л1.3	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
Л1.4	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
Л2.1	Торокин А.А.	Инженерно-техническая защита информации: учебное пособие	Москва: Гелиос АРВ, 2005	10	
Л2.2	Гребенщиков 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
Л2.3	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
Л3.1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л3.2	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	Электронная библиотека БрГУ
7.3.2.2	Электронный каталог библиотеки БрГУ
7.3.2.3	«Университетская библиотека online»
7.3.2.4	Справочно-правовая система «Консультант Плюс»

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.	Экзамен

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

Дисциплина "Информационная безопасность" нацелена на получение устойчивых практических навыков по нормативно-правовому обеспечению информационной безопасности и защите информации с применением технических средств.

Лекции.

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 теме лабораторной работы с использованием рекомендуемой литературы, конспекта лекций, ресурсов информационно-телекоммуникационной сети Интернет; выполнение заданий; оформление отчетов по лабораторным работам; подготовка к защите лабораторных работ.

Подготовка к экзамену: систематическая работа с конспектом лекций: чтение записей; проверка терминов с помощью энциклопедий, словарей и справочников; обозначение вопросов, материал, которых вызывает трудности; попытка найти ответ в рекомендуемых источниках; подготовка вопросов преподавателю, если не удается самостоятельно разобраться в материале.