МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 20F5B82B6FCD3E163457DD0BEA039495
Владелец: Патрусова Алена Михайловна
Действителен: с 02.06.2025 до 26.08.2026

УТВЕРЖДАЮ

Проректор по образовательной деятельности

_____А.М. Патрусова

13 мая _____2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04.02 Программно-аппаратные средства защиты информации

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

Учебный план b010302_25_ИИиЗИ.plx
Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Виды контроля в семестрах:
Зачет 7, Зачет с оценкой 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	17		11			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	17	17	11	11	28	28
Лабораторные	17	17	22	22	39	39
В том числе инт.	12	12	12	12	24	24
В том числе в форме практ.подготовки	17	17	22	22	39	39
Итого ауд.	34	34	33	33	67	67
Контактная работа	34	34	33	33	67	67
Сам. работа	74	74	75	75	149	149
Итого	108	108	108	108	216	216

Программу составил(и):
б.с., ст.пр., Федорович Д.О. _____
Рабочая программа дисциплины

Программно-аппаратные средства защиты информации

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 31.01.2025 № 61.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 16.04.2025 г. № 11

Срок действия программы: 4 года

Зав. кафедрой Горохов Денис Борисович

Председатель МКФ

старший преподаватель Латушкина С.В. 28.04.2025г. протокол №8

Ответственный за реализацию ОПОП _____ Горохов Д.Б.

Директор библиотеки _____ Сотник Т.Ф.

№ регистрации 49

Визирование РПД для исполнения в учебном году

Председатель МКФ

_____ _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 20 -20 учебном году на заседании кафедры

Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 20__ г. № ____

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	формирование у студентов знаний по основам инженерно-технической защиты информации, а также выработка навыков и умений в применении полученных знаний в условиях работы на конкретных объектах информационной безопасности; знаний по основам защиты информации в компьютерных системах, при помощи программных средств, а также навыков и умения в применении знаний для конкретных условий; развитие системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.04.02
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Криптографические методы защиты информации
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная (преддипломная) практика
2.2.2	Комплексное обеспечение безопасности объекта информатизации
2.2.3	Защита в операционных системах

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-4: Способен администрировать системы защиты информации автоматизированных систем
ПК-4.1: Выполняет работы по администрированию системы защиты информации автоматизированных систем
Знать: принципы формирования политики информационной безопасности в автоматизированных системах
Уметь: формировать политику безопасности программных компонентов автоматизированных систем; устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации
Владеть: навыками администрирования систем защиты информации автоматизированных систем
ПК-4.2: Выполняет установленные процедуры обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы
Знать: методы контроля эффективности защиты информации от утечки по техническим каналам
Уметь: использовать криптографические методы и средства защиты информации в автоматизированных системах; регистрировать события, связанные с защитой информации в автоматизированных системах
Владеть: выполнения установленных процедур обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Индикаторы	Литература	Интеракт.	Примечание
	Раздел	**Раздел 1. Основы технических средств и методов защиты информации**						
1.1	Лек	Концепции инженерно-технической защиты информации	7	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	лекция - беседа
1.2	Лаб	Концепции инженерно-технической защиты информации	7	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.3	Ср	Концепции инженерно-технической защиты информации	7	10	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.4	Зачёт	Концепции инженерно-технической защиты информации	7	5	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	

1.5	Лек	Теоретические основы инженерно-технической защиты информации	7	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.6	Лаб	Теоретические основы инженерно-технической защиты информации	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	2	работа в малых группах
1.7	Ср	Теоретические основы инженерно-технической защиты информации	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.8	Зачёт	Теоретические основы инженерно-технической защиты информации	7	5	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.9	Лек	Физические основы защиты информации	7	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.10	Лаб	Физические основы защиты информации	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	4	работа в малых группах
1.11	Ср	Физические основы защиты информации	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.12	Зачёт	Физические основы защиты информации	7	10	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.13	Лек	Технические средства добывания и инженерно-технической защиты	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	4	лекция - беседа
1.14	Лаб	Технические средства добывания и инженерно-технической защиты	7	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.15	Ср	Технические средства добывания и инженерно-технической защиты	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.16	Зачёт	Технические средства добывания и инженерно-технической защиты	7	10	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.17	Лек	Организационные основы инженерно-технической защиты информации	7	3	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	

1.18	Лаб	Организационные основы инженерно-технической защиты информации	7	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.19	Ср	Организационные основы инженерно-технической защиты информации	7	3	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.20	Зачёт	Организационные основы инженерно-технической защиты информации	7	6	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.21	Лек	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	2	лекция - беседа
1.22	Лаб	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	3	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.23	Ср	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	5	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
1.24	Зачёт	Методическое обеспечение инженерно технической защиты автоматизированных систем от вредоносных программных воздействий	7	8	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
	Раздел	**Раздел 2. Программно-аппаратные средства обеспечения информационной безопасности.**						
2.1	Лек	Методы и средства защиты программного обеспечения.	8	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
2.2	Лаб	Методы и средства защиты программного обеспечения.	8	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
2.3	Ср	Методы и средства защиты программного обеспечения.	8	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
2.4	ЗачётСОц	Методы и средства защиты программного обеспечения.	8	6	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
2.5	Лек	Построение изолированной программной среды.	8	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	

2.6	Лаб	Построение изолированной программной среды.	8	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	работа в малых группах
2.7	Ср	Построение изолированной программной среды.	8	14	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
2.8	ЗачётСОц	Построение изолированной программной среды.	8	12	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
	Раздел	**Раздел 3. Обеспечение информационной безопасности компьютерных сетей.**						
3.1	Лек	Стандарты информационной безопасности.	8	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	2	лекция - беседа
3.2	Лаб	Стандарты информационной безопасности.	8	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	2	работа в малых группах
3.3	Ср	Стандарты информационной безопасности.	8	12	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
3.4	ЗачётСОц	Стандарты информационной безопасности.	8	6	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1	0	
	Раздел	**Раздел 4. Использование программно-аппаратных средств защиты с учетом развитя технологии ИИ**						
4.1	Лек	Аппаратные средства безопасности: TPM и HSM в контексте ИИ	8	2	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
4.2	Лаб	Анализ инцидентов безопасности: Реакция на атаки на системы с использованием ИИ	8	4	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	4	Работа в малых группах
4.3	Лек	Будущее программно-аппаратных средств защиты с учетом развития технологий ИИ	8	3	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	
4.4	Лаб	Кейс-стадии успешного применения средств защиты в проектах на основе ИИ	8	6	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	4	Работа в малых группах
4.5	Ср	Использование программно-аппаратных средств защиты с учетом развития технологии ИИ	8	10	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	

4.6	ЗачётСОц	Использование программно-аппаратных средств защиты с учетом развития технологии ИИ	8	13	ПК-4.1 ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5	0	

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

Технология коллективного взаимодействия (работа в малых группах) (самостоятельное изучение обучающимися нового материала посредством сотрудничества в малых группах, дает возможность всем участникам участвовать в работе, практиковать навыки сотрудничества, межличностного общения)

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))

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Текущий контроль

Текущим контролем успеваемости обучающихся является межсессионная аттестация – единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам/практикам.
Порядок проведения, содержание и особенности текущего контроля успеваемости представлены в разработанном Фонде оценочных средств для данной дисциплины.

6.2. Темы письменных работ

не предусмотрено учебным планом

6.3. Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета, дифференцированного зачета.
Порядок проведения, содержание и критерии оценивания итоговой промежуточной аттестации представлены в Фонде оценочных средств для данной дисциплины.

6.4. Перечень видов оценочных средств

ЛР, вопросы к зачету, вопросы к зачету с оценкой

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	Долозов Н. Л., Гультяева Т. А.	Программные средства защиты информации: конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2015	1	http://biblioclub.ru/index.php?page=book&id=438307
Л1.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник для вузов	Санкт-Петербург: Лань, 2023	1	https://e.lanbook.com/book/293009

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л2.2	Басыня Е. А.	Системное администрирование и информационная безопасность: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018	1	http://biblioclub.ru/index.php?page=book&id=575325

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.3	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
Л2.4	Лохов В. И., Петренко В. И., Мандрица И. В., Максименко Ю. К.	Технические средства защиты информации. Лабораторный практикум. Technical means of information protection. Laboratory practicals: учебное пособие для вузов	Санкт-Петербург: Лань, 2024	1	https://e.lanbook.com/book/434159
Л2.5	Краковский Ю. М.	Методы и средства защиты информации: учебное пособие для вузов	Санкт-Петербург: Лань, 2025	1	https://e.lanbook.com/book/463013

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронный каталог библиотеки БрГУ	http://ecat.brstu.ru/catalog

7.3.1 Перечень программного обеспечения

7.3.1.1	Chrome
7.3.1.2	Visual Studio Community
7.3.1.3	Python IDLE
7.3.1.4	LibreOffice
7.3.1.5	ОС Linux

7.3.2 Перечень информационных справочных систем

7.3.2.1	ЭОС "Образовательная платформа ЮРАЙТ"
7.3.2.2	Издательство "Лань" электронно-библиотечная система
7.3.2.3	«Университетская библиотека online»
7.3.2.4	Электронный каталог библиотеки БрГУ
7.3.2.5	Электронная библиотека БрГУ
7.3.2.6	Научная электронная библиотека eLIBRARY.RU

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение аудитории	Вид занятия
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
1345	Учебная аудитория (дисплейный класс)	Основное оборудование: - 15 Персональных компьютеров i5-13500/DDR5 16 GB/SSD 1TB/GeForce RTX4060 (Монитор Asus VA24EHF); - интерактивная доска SMART Board SB680, проектор Unifri35 (Vixuiti) SmartTechnologies, Дополнительно: - коммутатор D-Link DES-1050G Учебная мебель: - комплект мебели (посадочных мест/АРМ) – 32/15 шт.; - комплект мебели (посадочных мест/АРМ) для преподавателя – 1 шт.;	Лек
1345	Учебная аудитория (дисплейный класс)	Основное оборудование: - 15 Персональных компьютеров i5-13500/DDR5 16 GB/SSD 1TB/GeForce RTX4060 (Монитор Asus VA24EHF); - интерактивная доска SMART Board SB680, проектор Unifri35 (Vixuiti) SmartTechnologies, Дополнительно: - коммутатор D-Link DES-1050G Учебная мебель: - комплект мебели (посадочных мест/АРМ) – 32/15 шт.; - комплект мебели (посадочных мест/АРМ) для преподавателя – 1	Лаб

		шт.;	

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

Лабораторная работы реализуются в форме практической подготовки при освоении образовательной программы в условиях выполнения обучающимися определенных видов заданий, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю образовательной программы.
Обучающийся должен разработать собственный режим равномерного освоения дисциплины. Подготовка студента к предстоящей лекции включает в себя ряд важных познавательно-практических этапов:

- чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником;

- техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств);

- выполнение заданий преподавателя;
- знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Успешность выполнения лабораторных работ определяется подготовкой к ним.
Подготовка к лабораторным работами содержит:

- изучение теоретического материала, содержащегося в учебной литературе, изучение лекционного материала;

- знакомство с заданиями на лабораторную работу;

- составление плана выполнения лабораторной работы и практического задания.

Наиболее продуктивной является самостоятельная работа в библиотеке, где доступны основные и дополнительные печатные и электронные источники.

При выполнении приведенных выше рекомендаций подготовка к экзамену сведется к повторению изученного и совершенствованию навыков применения теоретических положений и различных методов решения к стандартным и нестандартным заданиям.