МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 025493C4E0B34808564BE6735EBB2702
Владелец: Ситов Илья Сергеевич
Действителен: с 16.01.2023 до 10.04.2024

УТВЕРЖДАЮ

Проректор по учебной работе

_____Е.И.Луковникова

_____16 июня_____2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.07.ДВ.03.01 Защита в операционных системах

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

Учебный план b010302_23_ИПОиЗИ.plx
Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
Зачет 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	11			
Вид занятий	УП	РП	УП	РП
Лекции	22	22	22	22
Лабораторные	44	44	44	44
В том числе инт.	12	12	12	12
В том числе в форме практ.подготовки	44	44	44	44
Итого ауд.	66	66	66	66
Контактная работа	66	66	66	66
Сам. работа	78	78	78	78
Итого	144	144	144	144

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

Защита в операционных системах

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 17.02.2023 № 9.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 21 апреля 2023г. № 9

Срок действия программы: 2023-2027 уч.г.

Зав. кафедрой Горохов Д.Б.

Председатель МКФ

старший преподаватель Латушкина С.В. 24 апреля 2023г. №9

Ответственный за реализацию ОПОП _____ Горохов Д.Б.

Директор библиотеки _____ Сотник Т.Ф.
(подпись)

№ регистрации 46
(методический отдел)

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2024 г. № __
Зав. кафедрой _____

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Освоение комплекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.07.ДВ.03.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Операционные системы
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	Программно-аппаратные средства защиты информации
2.2.3	Производственная (преддипломная) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
Индикатор 1	УК-1.1 Выполняет поиск необходимой информации, её критический анализ и синтез информации, полученной из разных источников
Индикатор 2	УК-1.2 Использует системный подход для решения поставленных задач
УК-9: Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	
Индикатор 1	УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели и формы участия государства в экономике
ПК-4: Способен администрировать системы защиты информации автоматизированных систем	
Индикатор 1	ПК-4.1. Выполняет работы по администрированию системы защиты информации автоматизированных систем.
Индикатор 1	ПК-4.2. 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	основные принципы критического анализа и синтеза информации; методы критического анализа и оценки современных научных достижений; основные принципы и методы системного подхода; критерии оценки эффективности и надежности средств защиты операционных систем, основные средства и способы обеспечения информационной безопасности с учетом принципов экономического развития; программно-аппаратные средства защиты информации автоматизированных систем; принципы организации и структуру систем защиты программного обеспечения автоматизированных систем; основные меры по защите информации в автоматизированных системах
3.2	**Уметь:**
3.2.1	осуществлять поиск информации в разных источниках; получать новые знаний на основе критического анализа и синтеза информации; получать новые знаний на основе критического анализа и синтеза информации; применять методы системного подхода для решения поставленных задач; использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем, в том числе, в экономике, с учетом принципов ее функционирования; планировать политику безопасности операционных систем; проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; создавать, удалять и изменять учетные записи пользователей автоматизированной системы, устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации; формировать политику безопасности программных компонентов автоматизированных систем.
3.3	**Владеть:**
3.3.1	навыками исследования проблем предметной деятельности с применением критического анализа и синтеза; навыками выявления научных проблем предметной области и использования адекватных методов для их решения; навыками работы с современными операционными системами, восстановления операционных систем после сбоев; навыками установки и настройки современных операционных систем с учетом требований по обеспечению информационной безопасности и принципами экономического развития; навыками администрирования систем защиты информации автоматизированных систем; навыками 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**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Примечание**
	Раздел	**Раздел 1. Методы обеспечения безопасности операционных систем**						
1.1	Лек	Структура подсистем безопасности операционных систем	8	4	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	2	Лекция-беседа УК-1.1
1.2	Лек	Криптографические методы информационной безопасности	8	4	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	4	Лекция-беседа УК-1.1
1.3	Лек	Вредоносные программы	8	4	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	УК-1.1
1.4	Лаб	Локальная безопасность windows и анализ уязвимостей операционной системы	8	11	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	1	Работа в малых группах УК-1.1 ПК-3.1 УК-9.1
1.5	Лаб	Локальная безопасность linux и анализ уязвимостей операционной системы	8	11	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	1	Работа в малых группах УК-1.1 ПК-3.1 УК-9.1
1.6	Лаб	централизованная настройка информационной безопасности	8	10	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	1	Работа в малых группах УК-1.1 ПК-3.1 УК-9.1
1.7	Ср	Методы обеспечения безопасности операционных систем	8	22	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	УК-1.1 ПК-3.1 УК-9.1
1.8	Зачёт	Методы обеспечения безопасности операционных систем	8	16	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	УК-1.1 ПК-3.1 УК-9.1
	Раздел	**Раздел 2. Принципы разработки защищенного программного обеспечения**						
2.1	Лек	Безопасность опреционных систем	8	4	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	УК-1.1
2.2	Лек	Разработка защищенных приложений	8	6	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	УК-1.1
2.3	Лаб	Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная политика безопасности windows и linux	8	12	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	3	Работа в малых группах УК-1.1 ПК-3.1 УК-9.1
2.4	Ср	Методы обеспечения безопасности операционных систем	8	22	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	

2.5	Зачёт	Принципы разработки защищенного программного обеспечения	8	18	УК-1 УК-9 ПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2	0	УК-1.1 ПК-3.1 УК-9.1

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)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

Лекция-беседа №1 (4 часа)
Тема: Структура подсистем безопасности операционных систем

Лабораторная работа № 1 (11 часов)
Тема: Локальная безопасность windows и анализ уязвимостей операционной системы
Задание:
1. Настройка политики паролей
2. Настройка и проверка дополнительных параметров политики учетных записей
3. Настройка Политики блокировки учетной записи (Account Lockout Policy)

Лабораторная работа №2 (11 часов)
Тема: Локальная безопасность linux и анализ уязвимостей операционной системы
Задание:
1. Настройка политики паролей
2. Настройка и проверка дополнительных параметров политики учетных записей
3. Настройка Политики блокировки учетной записи

Лабораторная работа №3 (10 часов)
Тема: Централизованная настройка информационной безопасности
Задание:
1. Настройка параметров управления квотами
2. Запрещение дисковых квот

Лабораторная работа №4 (12 часов)
Тема: Понятие и сущность программной защиты информации. Управление правами пользователей. Локальная политика безопасности windows и linux
Задание:
1. Запустить ОС в минимальном окружении: ядро и командный интерпретатор. Выполнить задание в соответствии с индивидуальным вариантом:
Вопросы для защиты:
1 Найти файлы: passwd, group, shadow и gshadow; показать, пояснить.
2 Описать алгоритм взлома через CD-диск.
3 Описать алгоритм взлома через загрузчик.

6.2. Темы письменных работ

Не предусмотрено учебным планом

6.3. Фонд оценочных средств

Вопросы к зачету
Раздел 1. Методы обеспечения безопасности операционных систем.
1. Основные механизмы обеспечения безопасности операционных систем
2. Средства и методы аутентификации в ОС
3. Разграничение доступа к ресурсам ОС
4. Контроль работы подсистемы защиты ОС
5. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.
6. Какие параметры входят в политику блокировки учётной записи? Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
7. Что такое и для чего применяется MMC?
8. Что такое оснастка?
9. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?
10. Каким образом можно включить автозапуск программ через групповую политику?

11. При помощи какой команды можно получить список пользователей операционной системы? При помощи какой команды можно получить список групп пользователей операционной системы? При помощи какой команды можно создать нового пользователя?
12. Чем отличается процесс от потока? Как с помощью Process Explorer определить, каким процессом открыто определенное окно?
13. Для чего нужны квоты? Каким образом можно назначить квоту конкретному пользователю? Фиксируются ли попытки превышения квоты пользователем? Если «да», то где? Если «нет», то почему?
14. Какие основные причины сбоев операционной системы? На какие две группы делятся средства восстановления ОС? Какие средства восстановления в Windows XP вам известны?
15. Что такое MBR? С помощью какой программы можно исправить ошибки MBR?
Раздел 2. Принципы разработки защищенного программного обеспечения.
1. При помощи какого приложения возможно использование eToken для аутентификации в различных прикладных программах на рабочих станциях пользователей? Что такое «шаблоны приложений», применяемые eToken SSO? Что включает в себя профиль, сохраняемый на eToken?
2. Охарактеризуйте дискреционную модель управления доступом.
3. Раскройте понятие наследования разрешений. Как отключить наследование разрешений? Как реализовать принудительное наследование вложенными объектами установленных разрешений?
4. На чём основан принцип действия мандатного механизма разграничения доступа?
5. Разрешается ли пользователю доступ к файлу, если уровень допуска пользователя выше категории конфиденциальности файла? Перечислите категории конфиденциальности по умолчанию. Какой параметр предоставляет возможность управлять категориями конфиденциальности? Можно ли присвоить категорию конфиденциальности ресурсу, расположенному на диске с файловой системой FAT32?
6. Для чего нужен контроль потоков данных?
7. При каком уровне сеанса пользователь может изменять настройки операционной системы и приложений?
8. Какие права предоставляются пользователю при доступе к конфиденциальной информации, уровень которой ниже уровня сеанса?
9. Для чего используются белые списки? К каким классам устройств могут быть созданы белые списки? Какие варианты идентификации устройства применяются в белом списке?
10. Для чего используется теневое копирование файлов?
11. Для чего служит правило для сертификата? Как можно получить сертификат из файла?
12. Какие существуют настройки политики безопасности, связанные с аудитом?
13. Каким образом при помощи встроенных средств операционной системы Windows можно осуществлять контроль целостности настроек, связанных с информационной безопасностью?
14. Каким образом при помощи встроенных средств Windows можно автоматизировать настройку операционной системы в соответствии с требуемыми параметрами безопасности?
15. Что такое «Шаблон безопасности»? Для чего предназначена оснастка «Шаблоны безопасности»? Какие группы настроек входят в шаблон безопасности?
16. Для чего предназначена оснастка «Анализ и настройка безопасности»? Опишите последовательность действий администратора при проведении анализа настроек безопасности операционной системы. Опишите последовательность действий администратора при настройке безопасности операционной системы. Приведите возможные типы результатов анализа параметров безопасности операционной системы. Каким образом можно внести в шаблон текущие настройки безопасности операционной системы?

6.4. Перечень видов оценочных средств

Лекция - беседа, лабораторные работы, 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	Кобылянский В. Г.	Операционные системы, среды и оболочки: учебное пособие	Новосибирск: Новосибирский государственный технический университет, 2018	1	http://biblioclub.ru/index.php?page=book&id=576354
Л1.2	Власенко А. Ю., Карабцев С. Н., Рейн Т. С.	Операционные системы: учебное пособие	Кемерово: Кемеровский государственный университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=574269
Л1.3	Ложников П. С., Провоторский А. О.	Средства безопасности операционной системы ROSA Linux: учебное пособие	Омск: Омский государственный технический университет (ОмГТУ), 2017	1	http://biblioclub.ru/index.php?page=book&id=493349

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.4	Пахмурин Д. О.	Операционные системы ЭВМ: учебное пособие	Томск: ТУСУР, 2013	1	http://biblioclub.ru/index.php?page=book&id=480573

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Куль Т. П.	Операционные системы: учебное пособие	Минск: РИПО, 2015	1	http://biblioclub.ru/index.php?page=book&id=463629
Л2.2	Карпов В., Коньков К.	Основы операционных систем: практикум	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	1	http://biblioclub.ru/index.php?page=book&id=429022

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	LibreOffice

7.3.2 Перечень информационных справочных систем

7.3.2.1	Издательство "Лань" электронно-библиотечная система
7.3.2.2	«Университетская библиотека online»
7.3.2.3	Электронный каталог библиотеки БрГУ
7.3.2.4	Электронная библиотека БрГУ
7.3.2.5	Информационная система "Единое окно доступа к образовательным ресурсам"
7.3.2.6	Научная электронная библиотека eLIBRARY.RU
7.3.2.7	Национальная электронная библиотека НЭБ

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение аудитории	Вид занятия
А1207	Учебная аудитория (мультимедийный/дисплейный класс)	Основное оборудование: - интерактивная доска SMART Board X885ix со встроенным проектором UX – 1 шт.; - системный блок CPU 5000/RAM 2Gb/HDD - 14 шт.; - монитор TFT 19 LG1953S-SF – 14шт.; - принтер HP Laser jet P3015d – 1 шт.; - сканер CANOSCAN LIDE220 – 1 шт.; Дополнительно: - маркерная доска – 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) – 24/14 шт.; - комплект мебели (посадочных мест/АРМ) для преподавателя – 1/1 шт.: персональный компьютер i5-2500/H67/4Gb/500Gb – 1 шт. монитор TFT19 Samsung E1920NR – 1 шт.;	Лек
А1203	Лаборатория параллельных вычислений	Основное оборудование: - ПК i5-2500/H67/4Gb/500Gb- 15 шт.; - монитор TFT19 Samsung E1920NR - 15 шт.; Дополнительно: - доска магнитно-маркерная - 1 шт. - интерактивная доска SMART Board X885ix со встроенным проектором UX 60 - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 15/15 шт. - комплект мебели (посадочных мест/АРМ) - для преподавателя - 1/ 1 шт. ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR .	Лаб
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
А1203	Лаборатория параллельных вычислений	Основное оборудование: - ПК i5-2500/H67/4Gb/500Gb- 15 шт.; - монитор TFT19 Samsung E1920NR - 15 шт.; Дополнительно:	Зачёт

		- доска магнитно-маркерная - 1 шт. - интерактивная доска SMART Board X885ix со встроенным проектором UX 60 - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 15/15 шт. - комплект мебели (посадочных мест/АРМ) - для преподавателя - 1/ 1 шт. ПК i5-2500/H67/4Gb/500Gb; монитор TFT19 Samsung E1920NR .	

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

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 практических заданий преподавателя;знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе. Успешность выполнения лабораторных работ и практических заданий определяется подготовкой к ним. Подготовка к лабораторным работам и пркактическим занятиям содержит: - изучение теоретического материала, содержащегося в учебной литературе, изучение лекционного материала,- знакомство с заданиями; - составление плана выполнения; - реализация;- написание отчета.
В процессе изучения дисциплины студент должен выполнить курсовую работу, основной целью которых является проверкак его знаний, умений и навыков, полученных при изучении дисциплины.
Наиболее продуктивной является самостоятельная работа. Она складывается из чтения учебников и методических пособий, решения задач, выполнения контрольных заданий.
Студент должен помнить, что только при систематической и упорной самостоятельной работе можно качественно освоить учебный материал.
Завершающим этапом изучения данной дисциплины в соответствии с учебным планом является сдача экзамена. На экзамене студент должен: проявить умение применять теоретические сведения к решению задач построение и анализ алгоритмов; знание теоретических основ курса на уровне определений, теорем, формул; умение выбирать методы анализа и оценки выбранных решений.