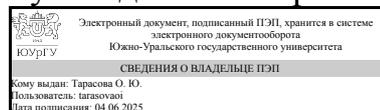


УТВЕРЖДАЮ:  
Руководитель направления



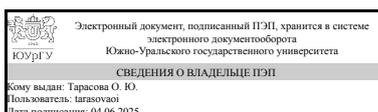
О. Ю. Тарасова

## РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.10.06 Программирование защищенных интеллектуальных систем  
для направления 09.03.04 Программная инженерия  
уровень Бакалавриат  
форма обучения очная  
кафедра-разработчик Математика и вычислительная техника

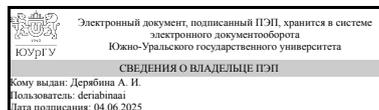
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 920

Зав.кафедрой разработчика,  
к.физ.-мат.н., доц.



О. Ю. Тарасова

Разработчик программы,  
к.техн.н., доцент



А. И. Дерябина

## 1. Цели и задачи дисциплины

Формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ) и защиты информации (ЗИ), умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в системах защиты информации (СЗИ) в вычислительных системах и сетях (ВСС). Цель изучения дисциплины достигается путем решения следующих задач: изучение теоретических положений ИБ, ее средств и методов, особенностей их использования в ВСС, перспектив развития в информационных технологиях (ИТ), предметной и смежных с ней областях; повышения уровня профессиональной культуры и исполнительской дисциплины бакалавров, понимание необходимости использования СЗИ в ВСС, в профессиональной деятельности по специальности; освоения основных средств и методов обеспечения ИБ, методик их результативного использования; изучения технических и программно-аппаратных средств ЗИ, их основных характеристик; приобретения умений и навыков работы с СЗИ

## Краткое содержание дисциплины

Дисциплина посвящена изучению существующих технологий и программно-аппаратных средств защиты компьютерных сетей. В содержание дисциплины входят четыре основные направления: Комплексный подход к обеспечению информационной безопасности. Методы и средства обеспечения безопасности информации. Компьютерные вирусы и средства антивирусной защиты. Стандарты защищенности информации в компьютерных системах. В ходе изучения дисциплины студенты получают знания о современных технологиях защиты информации. Также студенты учатся разбираться с многообразием законодательных актов Российской Федерации и международных стандартах в области защиты информации.

## 2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
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	Знает: методы обнаружения вторжений в информационные системы (ИС); методы безопасного использования коммуникационных сетей общего доступа при построении защищенных ИС; основные принципы применения аппаратных и программных средств обеспечения информационной безопасности Умеет: применять современные программные и аппаратные средства защиты информации; классифицировать и оценивать угрозы информационной безопасности для ИС Имеет практический опыт: работы с ведущими программными и аппаратными комплексными средствами защиты информации
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной	Знает: основные стандарты в области информационной безопасности и искусственного интеллекта

деятельностью	<p>Умеет: разрабатывать подходы, согласно действующих норм, для систем искусственного интеллекта в задачах информационной безопасности</p> <p>Имеет практический опыт: решения задач информационной безопасности систем искусственного интеллекта</p>
ОПК-6 Способен разрабатывать алгоритмы и программы, пригодные для практического использования, применять основы информатики и программирования к проектированию, конструированию и тестированию программных продуктов	<p>Знает: основы разработки систем информационной безопасности</p> <p>Умеет: разрабатывать алгоритмы для задач информационной безопасности</p> <p>Имеет практический опыт: тестирования алгоритмов в задачах информационной безопасности</p>

### 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
<p>1.О.10.03 Программирование на языке С++,</p> <p>1.О.15 Структуры и алгоритмы обработки данных,</p> <p>1.О.10.05 Веб-программирование для систем искусственного интеллекта,</p> <p>1.О.10.02 Основы программирования,</p> <p>1.О.10.04 Объектно-ориентированное программирование</p>	<p>1.О.23 Информационные системы,</p> <p>1.О.19 Компьютерная графика,</p> <p>1.О.14 Тестирование программного обеспечения</p>

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
1.О.15 Структуры и алгоритмы обработки данных	<p>Знает: основные типы структур данных, используемые в мировой практике программирования; способы отображения структур данных на структуры хранения; основные операции и алгоритмы над структурами</p> <p>Умеет: применять изученные типы данных и алгоритмы работы с ними при решении конкретных задач; оценивать затраты времени и ресурсов при использовании тех или иных структур и алгоритмов в существующих и вновь разрабатываемых программных средствах</p> <p>Имеет практический опыт: программирования операций над основными базовыми структурами данных при программировании конкретных задач</p>
1.О.10.04 Объектно-ориентированное программирование	<p>Знает: концепцию объектно-ориентированного программирования и соответствующие требования к программному обеспечению, составные части объектно-ориентированной парадигмы программирования; основы объектно-ориентированного языка программирования</p>

	<p>Умеет: применять объектно-ориентированный язык программирования, современную среду разработки для решения задач профессиональной деятельности и обосновывать принимаемые проектные решения, применять объектно-ориентированную декомпозицию задач; разрабатывать объектно-ориентированные библиотеки Имеет практический опыт: разработки программных решений в соответствии с требованиями применения объектно-ориентированного подхода, разработки программ в объектно-ориентированной парадигме</p>
<p>1.О.10.03 Программирование на языке С++</p>	<p>Знает: основы языка программирования С++, методы отладки программ Умеет: проводить структурную декомпозицию задач, применять конструкции языка С++ для решения задач по заданному или разработанному алгоритму Имеет практический опыт: программирования на языке С++, а так же навыки отладки и тестирования программ</p>
<p>1.О.10.05 Веб-программирование для систем искусственного интеллекта</p>	<p>Знает: основы проектирования сайтов и применяемые технологии, основы программирования Internet-страниц различными программными средствами., основы проектирования сайтов и применяемые технологии, основы программирования Internet-страниц различными программными средствами Умеет: создавать статические HTML-страницы и применять таблицы стилей; писать клиентские скрипты на языке javascript; писать серверные приложения на языке php; осуществлять доступ к базам данных при проектировании web-сайта; настраивать конфигурацию web-сервера, создавать статические HTML-страницы и применять таблицы стилей; писать клиентские скрипты на языке javascript; писать серверные приложения на языке php; осуществлять доступ к базам данных при проектировании web-сайта; настраивать конфигурацию web-сервера Имеет практический опыт: разработки web-приложений с применением современных языков программирования и технологий, разработки web-приложений с применением современных языков программирования и технологий</p>
<p>1.О.10.02 Основы программирования</p>	<p>Знает: основы алгоритмического языка программирования, методы отладки структурных программ; подходы к решению алгоритмических задач, современные программные средства разработки и тестирования программных продуктов Умеет: разрабатывать алгоритмы с использованием базовых алгоритмических конструкций, проводить структурную декомпозицию задач, составлять программный код, отвечающий заданному или разработанному алгоритму, применять язык программирования в</p>

	современной среде разработки для решения задач профессиональной деятельности Имеет практический опыт: программирования на алгоритмическом языке в разрезе процедурного подхода, а так же навыки отладки и тестирования программ, создания и отладки программ в современной среде разработки, оформления отчетов, используя информационные технологии и программные средства
--	---

#### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		5	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	48	48	
Лекции (Л)	16	16	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	53,5	53,5	
Подготовка к практическим занятиям	16	16	
Подготовка к диф. зач.	21	21	
Изучение тем, вынесенных на самостоятельную проработку	16,5	16,5	
Консультации и промежуточная аттестация	6,5	6,5	
Вид контроля (зачет, диф.зачет, экзамен)	-	диф.зачет	

#### 5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Комплексный подход к обеспечению информационной безопасности	16	4	12	0
2	Методы и средства обеспечения безопасности информации	12	4	8	0
3	Компьютерные вирусы и средства антивирусной защиты	10	4	6	0
4	Стандарты защищенности информации в компьютерных системах	10	4	6	0

##### 5.1. Лекции

№	№	Наименование или краткое содержание лекционного занятия	Кол-
---	---	---	------

лекции	раздела		во часов
1	1	Введение в проблему информационной безопасности, ее актуальности. Основные объекты информационных систем, подлежащие защите. Цели и задачи обеспечения информационной безопасности для различных объектов	1
2	1	Основные понятия информационной безопасности. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический. Требования к комплексным системам защиты информации.	1
3	1	Компьютерная система как объект защиты информации. Понятие угрозы информационной безопасности в компьютерных системах. Классификация и общий анализ угроз информационной безопасности в компьютерных системах. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Административный, процедурный и программно-технический уровни информационной безопасности. Административный, процедурный и программно-технический уровни информационной безопасности	2
4	2	Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Противодействие наблюдению. Противодействие прослушиванию. Методы и средства защиты от побочных электромагнитных излучений и наводок. Способы несанкционированного доступа к информации в компьютерных системах. Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа. Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация. Управление доступом: основные понятия, виды разграничения доступа, особенности дискреционного, мандатного и ролевого управления доступом.	2
5	2	Защита программных средств от несанкционированного копирования и исследования. Протоколирование и аудит: основные понятия, активный аудит. Методы аутентификации, использующие пароли. Построение системы разграничения доступа в базе данных на основе ролевой модели. Развитие криптографических систем. Основные понятия криптологии. Классификация криптографических средств. Симметричные криптосистемы: DES и ее модификации, ГОСТ 28147 – 89, принципы их построения. Ассиметричные криптосистемы: однонаправленные функции, RSA, принципы построения. Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные. Функция хэширования. Электронная подпись и ее применение для контроля целостности программ и данных. Компьютерная стеганография и ее применение.	2
5	3	Основные каналы распространения вирусов. Вредоносные программы и их классификация. Программные закладки и методы защиты от них. Антивирусные программные комплексы.	4
6	4	Характеристика систем стандартизации в области защиты информации. Европейские критерии безопасности информационных технологий. Документы Гостехкомиссии России по защите информации.	2
7	4	Оценочные стандарты и технические спецификации: «Оранжевая книга». Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».	2

## 5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1,2,3	1	Практическая работа № 1 «Хеш-функция (MD5)»	6
4,5,6	1	Практическая работа № 2 «Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира)»	6
7,8	2	Практическая работа № 3 «Контроль целостности (биты четности, контрольные цифры, CRC и ECC)»	4
9,10	2	Практическая работа № 4 «Электронная цифровая подпись (RSA, ГОСТы 34.10-94 и 34.10-2001)»	4
11,12,13	3	Практическая работа № 5 «Контроль целостности (MAC-код DES-CBC)»	6
14,15,16	4	Практическая работа № 6 «Гайные многосторонние вычисления и разделение секрета	6

### 5.3. Лабораторные работы

Не предусмотрены

### 5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Подготовка к практическим занятиям	ЭУМД Осн лит: №1 (с.155-180), ЭУМД №2 (с.280-298) Метод.указан.: №1, 2, 3	5	16
Подготовка к диф. зач.	ЭУМД Осн лит: №1 (с.155-180), ЭУМД №2 (с.280-298), ЭУМД №3 (Главы 9,11,15). Доп.лит.: ЭУМД №1 (Урок 5,6,7,8), Метод.указан.: №1,	5	21
Изучение тем, вынесенных на самостоятельную проработку	ЭУМД Осн лит: №1 (с.155-180, с. 211-227, с. 232-240), №2 (с. 76-86, с. 148-178), №3 (Главы 5-9, 11,12,15,16,18). ЭУМД Доп.лит.: №2 (Главы 4,5,6,7,10,12,13) №3 (Главы 6,7,8,9).	5	16,5

### 6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

#### 6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учитывается в ПА
1	5	Текущий контроль	Практическая работа № 1 «Хеш-функция (MD5)»	1	15	13-15 баллов - практические навыки работы с освоенным материалом	дифференцированный зачет

						полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	
2	5	Текущий контроль	Практическая работа № 2 «Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира)»	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	дифференцированный зачет
3	5	Текущий контроль	Практическая работа № 3 «Контроль целостности (биты четности, контрольные цифры, CRC и ECC)»	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	дифференцированный зачет
4	5	Текущий контроль	Практическая работа № 4 «Электронная цифровая подпись (RSA, ГОСТы 34.10-94 и 34.10-2001)»	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13	дифференцированный зачет

						баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	
5	5	Текущий контроль	Практическая работа № 5 «Контроль целостности (MAC-код DES-CBC)»	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	дифференцированный зачет
6	5	Текущий контроль	Практическая работа № 6 «Тайные многосторонние вычисления и разделение секрета	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	дифференцированный зачет
7	5	Промежуточная аттестация	дифференцированный зачет	-	130	Оценка за дифференцированный зачет складывается из теоретической части (в виде ответа на 20 заданий в тестовой форме, за каждый правильный ответ 2	дифференцированный зачет

					балла). Общая оценка за дифференцированный зачет: Отлично: не менее 85% правильно выполненных заданий Хорошо: от 75 до 84% правильно выполненных заданий Удовлетворительно: от 60 до 74% правильно выполненных заданий Неудовлетворительно: менее 60% правильно выполненных заданий  При выставлении Итоговой оценки по дисциплине учитываются накопленные баллы за текущие контрольные мероприятия и оценка на экзамене.	
--	--	--	--	--	---	--

## 6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
дифференцированный зачет	Дифференцированный зачет включает в себя теоретическую часть в виде ответа на 20 заданий в тестовой форме. При выставлении Итоговой оценки по дисциплине учитываются накопленные баллы за текущие контрольные мероприятия и оценка на диф. зач. Для расчета итоговой оценки баллы за ответы на тестовые вопросы и практические работы представляются в виде доли от максимального балла конкретного задания и ответа на вопрос, выраженной в процентах.	В соответствии с пп. 2.5, 2.6 Положения

## 6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ОПК-3	Знает: методы обнаружения вторжений в информационные системы (ИС); методы безопасного использования коммуникационных сетей общего доступа при построении защищенных ИС; основные принципы применения аппаратных и программных средств обеспечения информационной безопасности	+						
ОПК-3	Умеет: применять современные программные и аппаратные средства защиты информации; классифицировать и оценивать угрозы информационной безопасности для ИС	+			+			
ОПК-3	Имеет практический опыт: работы с ведущими программными и аппаратными комплексными средствами защиты информации				+			

ОПК-4	Знает: основные стандарты в области информационной безопасности и искусственного интеллекта		+					+
ОПК-4	Умеет: разрабатывать подходы, согласно действующих норм, для систем искусственного интеллекта в задачах информационной безопасности		+					+
ОПК-4	Имеет практический опыт: решения задач информационной безопасности систем искусственного интеллекта						+	+
ОПК-6	Знает: основы разработки систем информационной безопасности			+				+
ОПК-6	Умеет: разрабатывать алгоритмы для задач информационной безопасности			+				+
ОПК-6	Имеет практический опыт: тестирования алгоритмов в задачах информационной безопасности							++

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

#### а) основная литература:

1. Заскалина, Е. Н. Программирование в 1С [Текст] : метод. указания к лабораторным работам для бакалавров направления 09.03.04 "Программ. инженерия" / Е. Н. Заскалина ; под ред. Е. В. Соколовой ; Юж.-Урал. гос. ун-т, Златоуст. фил., Каф. Математика и вычисл. техника ; ЮУрГУ. – Челябинск : Издат. центр ЮУрГУ, 2019. – 79 с. : ил.

#### б) дополнительная литература:

Не предусмотрена

#### в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Вестник Южно-Уральского государственного университета. Серия: Математика. Механика. Физика [Электронный ресурс] / Юж.-Урал. гос. ун-т. – Электрон. дан. – Челябинск : Изд-во ЮУрГУ. – 2003 – Режим доступа: [https://e.lanbook.com/journal/2547#journal\\_name](https://e.lanbook.com/journal/2547#journal_name). – Загл. с экрана.
2. Вестник Южно-Уральского государственного университета. Серия: Математическое моделирование и программирование [Электронный ресурс] / Юж. - Урал.гос.ун-т. -Электрон.дан. - Челябинск: Изд-во ЮУрГУ. - 2008-2016 - Режим доступа: [https://e.lanbook.com/journal/2548#journal\\_name](https://e.lanbook.com/journal/2548#journal_name) - Загл. с экрана

#### г) методические указания для студентов по освоению дисциплины:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие/ П.Н.Девянин. - М: "Горячая линия-Телеком", 2012. - 320с.

#### из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие/ П.Н.Девянин. - М: "Горячая линия-Телеком", 2012. - 320с.

### Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	ЭБС издательства Лань	Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. <a href="https://e.lanbook.com/book/163844">https://e.lanbook.com/book/163844</a>
2	Методические пособия для самостоятельной работы студента	ЭБС издательства Лань	Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. <a href="https://e.lanbook.com/book/157086">https://e.lanbook.com/book/157086</a>

Перечень используемого программного обеспечения:

1. Microsoft-Microsoft Imagine Premium (Windows Client, Windows Server, Visual Studio Professional, Visual Studio Premium, Windows Embedded, Visio, Project, OneNote, SQL Server, BizTalk Server, SharePoint Server)(04.08.2019)

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

## 8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия и семинары	203 (3)	ПК в составе (12 шт): Корпус MidiTower Inwin C583 350W Grey Процессор Intel Core 2 Duo E4600, 2,4GHz, 2Mb, 800MHz Socket-775 BOX. Мат.плата ASUS P5KPL-VM, Socket 775.Память 1024Mb PC2-5300(667Mhz) SEC-1. Жесткий диск 160,0 Gb HDD Seagate (ST3160815AS) Barracuda7200.10 8Mb SATA-300 Привод DVD±RW Samsung SH-S202J. Клавиатура Genius (KB-06XE), PS/2, White. Мышь Genius NetScroll 110 white optical (800dpi) PS/2. Монитор 17" Samsung 720N VKS TFT; Системный блок (1 шт): "Стандарт" * (без фильтра для ethernet, без считывателя); Монитор (1 шт): MONITOR Acer V193WV Cb; Проектор (1 шт) Acer X1263; Проекционный экран (1 шт).
Лекции	203 (3)	ПК в составе (12 шт): Корпус MidiTower Inwin C583 350W Grey Процессор Intel Core 2 Duo E4600, 2,4GHz, 2Mb, 800MHz Socket-775 BOX. Мат.плата ASUS P5KPL-VM, Socket 775.Память 1024Mb PC2-5300(667Mhz) SEC-1. Жесткий диск 160,0 Gb HDD Seagate (ST3160815AS) Barracuda7200.10 8Mb SATA-300 Привод DVD±RW Samsung SH-S202J. Клавиатура Genius (KB-06XE), PS/2, White. Мышь Genius NetScroll 110 white optical (800dpi) PS/2. Монитор 17" Samsung 720N VKS TFT; Системный блок (1 шт): "Стандарт" * (без фильтра для ethernet, без считывателя); Монитор (1 шт): MONITOR Acer V193WV Cb; Проектор (1 шт) Acer X1263; Проекционный экран (1 шт).
Самостоятельная работа студента	202 (3)	ПК в составе (12 шт): Корпус MidiTower Inwin C583 350W Grey Процессор Intel Core 2 Duo E4600, 2,4GHz, 2Mb, 800MHz Socket-775 BOX. Мат.плата ASUS P5KPL-VM, Socket 775.Память 1024Mb PC2-5300(667Mhz) SEC-1. Жесткий диск 160,0 Gb HDD Seagate

	(ST3160815AS) Barracuda7200.10 8Mb SATA-300 Привод DVD±RW Samsung SH-S202J. Клавиатура Genius (KB-06XE), PS/2, White. Мышь Genius NetScroll 110 white optical (800dpi) PS/2. Монитор 17" Samsung 720N VKS TFT; Системный блок (1 шт): "Стандарт" * (без фильтра для ethernet, без считывателя); Монитор (1 шт): MONITOR Acer V193WV Cb; Проектор (1 шт) Acer X1263; Проекционный экран (1 шт).
--	--