

# ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:  
Заведующий выпускающей  
кафедрой

ЮУрГУ	Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП	
Кому выдан: Шестакова Л. И.	
Пользователь: shestakovali	
Дата подписания: 30.05.2023	

Л. И. Шестакова

## РАБОЧАЯ ПРОГРАММА

**дисциплины 1.Ф.М0.08 Технологии защиты информации**

**для направления 38.04.02 Менеджмент**

**уровень Магистратура**

**магистерская программа Геоинформационные системы в управлении**

**форма обучения очно-заочная**

**кафедра-разработчик Международные отношения, политология и регионоведение**

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 38.04.02 Менеджмент, утверждённым приказом Минобрнауки от 12.08.2020 № 952

Зав.кафедрой разработчика,  
к.техн.н., доц.

ЮУрГУ	Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП	
Кому выдан: Шестакова Л. И.	
Пользователь: shestakovali	
Дата подписания: 30.05.2023	

Л. И. Шестакова

Разработчик программы,  
к.филол.н., доцент

ЮУрГУ	Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП	
Кому выдан: Дудина Ю. А.	
Пользователь: dudinaya	
Дата подписания: 30.05.2023	

Ю. А. Дудина

Челябинск

## 1. Цели и задачи дисциплины

Цель изучения дисциплины — получить базовые знания в области защиты информации, хранящейся на рабочих станциях и серверах, подключенных к сети Интернет, а также при ее передаче по открытым каналам Интернет. Задачи изучения дисциплины:

- освоение практических приемов защиты рабочих станций и серверов;
- получение навыков проектирования программно защищенных каналов передачи информации.

## Краткое содержание дисциплины

Защищенность информационной среды организации — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности информационной среды должен быть неотъемлемой частью системы управления любой организации. В настоящее время, персональные компьютеры (рабочие станции) пользователей, как правило, подключены к глобальной сети Интернет. Знания и умения пользователя по обеспечению информационной безопасности персонального компьютера, работающего в «агрессивной» сетевой среде, становятся одними из самых востребованных и необходимых. Данная дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем, практическими приемами защиты рабочих станций и серверов.

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

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Знает: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации Умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения Имеет практический опыт: владения методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации
ПК-2 способность управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями	Знает: теоретические основы криптографии, корпоративную стратегию, программы организационного развития Умеет: применять практические приемы защиты рабочих станций и серверов

	Имеет практический опыт: работы с инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем
ПК-7 способность использовать количественные и качественные методы для проведения прикладных исследований и управления бизнес-процессами, готовить аналитические материалы по результатам их применения	Знает: основы разработки корпоративной стратегии, программы организационного развития Умеет: применять практические приемы защиты рабочих станций и серверов Имеет практический опыт: владения инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем

### 3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Компьютерные технологии в научных исследованиях, Анализ бизнес-данных, Системный анализ в экономике и управлении, Управление проектами в информационных технологиях, Педагогика высшей школы, Производственная практика (научно-исследовательская работа) (2 семестр)	Информационные технологии для эффективного управления, Принципы современных профессиональных коммуникаций

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

Дисциплина	Требования
Анализ бизнес-данных	Знает: принципы построения математических моделей; математические методы, используемые для информационной поддержки принятия управленческих решений по оптимизации хозяйственных рисков, управлению запасами, сбытом, товарными потоками, в том числе в условиях конфликта целей; об основных направлениях исследований, направленных на развитие методологии и математических методов обоснования и информационной поддержки принятия управленческих решений применительно к различным объектам бизнеса; о теоретических и прикладных проблемах, ограничивающих применение математических методов в бизнесе и управлении, и о перспективах их решения Умеет: интерпретировать формальные записи изученных экономико-математических моделей, модифицировать их применительно к специфике

	<p>конкретного объекта приложения, объяснять их содержание в процессе профессиональной коммуникации; обосновывать конкретные управленческие решения на основе применяемых математических методов; оценивать адекватность и достоверность результатов применения изученных экономико-математических методов в бизнесе и управлении Имеет практический опыт: профессиональной коммуникации со специалистами в области математических методов экономики; применения программного обеспечения при решении прикладных задач математической поддержки принятия решений, входящих в состав MS EXCEL</p>
Управление проектами в информационных технологиях	<p>Знает: современное состояние в сфере проектной деятельности в информационных технологиях, специфику управления ИТ-проектами, типовые ошибки менеджмента ИТ-проектов; ролевую (организационную) структуру управления ИТ-проектом, программой, портфелем проектов; метрики оценки трудоемкости и времени разработки программного обеспечения; модели жизненного цикла ИТ-решений и их соотнесение с этапами жизненного цикла проекта Умеет: проводить самостоятельные исследования в соответствии с разработанной программой, адаптировать модель жизненного цикла ИТ-проекта в зависимости от решаемых задач и особенностей программного обеспечения; оценивать трудоемкость и время разработки программного обеспечения; реализовывать модели жизненного цикла ИТ-решений и их соотнесение с этапами жизненного цикла проекта Имеет практический опыт: владении программными средствами формирования научного отчета, статьи, доклада, работы с информационными системами управления проектами и портфелями проектов, метриками оценки трудоемкости и времени, методами календарного, ресурсного и сетевого планирования</p>
Системный анализ в экономике и управлении	<p>Знает: определения, свойства, классификацию систем, основные свойства и закономерности их эволюции; основные положения, принципы, процедуры и методологию системного анализа; основы теории системных исследований, методологию формирования (представления) и анализа экономических ситуаций; современные технологии работы с информацией; методы организации вычислительного эксперимента на имитационной модели. Умеет: идентифицировать и структурировать системы; применять средства визуализации и инструменты принятия решений в процессе анализа систем; создавать имитационные модели; применять</p>

	<p>положения и методологические процедуры системного подхода при исследовании проблем в теории и практике; корректно выполнять сбор и анализ статистических показателей моделируемых процессов; на основе критического анализа вырабатывать стратегию действий для решения проблемных ситуаций с применением инструментария системного подхода. Имеет практический опыт: применения положений системного подхода и системного анализа при исследовании проблемных ситуаций в теории и практике; проведения исследования экономических процессов с применением инструментария системного анализа; имитационного моделирования для решения проблемных ситуаций и интерпретации полученных результатов; принятия решений на основе результатов имитационного исследования.</p>
<p>Компьютерные технологии в научных исследованиях</p>	<p>Знает: количественные и качественные методы для проведения прикладных исследований и управления бизнес-процессами, готовить аналитические материалы по результатам их применения Умеет: готовить аналитические материалы по результатам применения методов для проведения прикладных исследований и управления бизнес-процессами Имеет практический опыт: использования количественных и качественных методов при проведении прикладных исследований и в управлении бизнес-процессами</p>
<p>Педагогика высшей школы</p>	<p>Знает: - технологию аналитической, оценочной и рефлексивной деятельности по организации образовательного процесса в высшей школе; - теоретические и методологические основы формирования образовательной среды в высшей школе, организации и реализации образовательного процесса в высшем образовании в соответствии с требованиями ФГОС ВО Умеет: -научно-обоснованными способами выявлять в суждениях (в т. ч. критических) идеи, принципы, модели, ценности педагогики высшей школы, анализировать современное состояние педагогической науки и тенденции в совершенствовании содержания и структуры образования, анализировать федеральный государственный стандарт по направлению подготовки, разрабатывать рабочую программу дисциплины по направлению профессиональной деятельности, планировать и осуществлять свою педагогическую деятельность с учетом современных тенденций развития науки и образования Имеет практический опыт: - критического анализа проблемных ситуаций на основе системного подхода, выработки стратегии</p>

	действий по педагогике высшей школы; проектирования и реализации образовательного процесса в высшей школе с учетом индивидуальных особенностей и образовательных потребностей обучающихся в соответствии с требованиями федерального стандарта высшего образования
Производственная практика (научно-исследовательская работа) (2 семестр)	Знает: современные подходы сбора и анализ научной информации для проведения исследований, количественные и качественные методы для проведения прикладных исследований и управления бизнес-процессами, как готовить аналитические материалы по результатам их применения Умеет: готовить отчеты на основании аналитических материалов, готовить отчеты на основании аналитических материалов Имеет практический опыт: подготовки аналитических материалов по результатам проведенных исследований, применения количественных и качественных методов для проведения прикладных исследований и управления бизнес-процессами

#### 4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 38,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		3
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>		
Лекции (Л)	8	8
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	24	24
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	69,75	69,75
Изучение государственного стандарта 28147-89. Изучение государственного стандарта Р34.10-2001. Изучение государственного стандарта Р34.11-94	10	10
Подготовка к зачету	9,75	9.75
Изучение характерных проблем, связанных с безопасностью, при использовании компьютерных сетей. Изучение правил обеспечения безопасности рабочей станции	20	20
Алгоритм RSA, схема Диффи-Хеллмана, стандарт цифровой подписи DSS. Отечественные стандарты алгоритмов с открытым ключом	20	20
Подготовка к тестированию	10	10
Консультации и промежуточная аттестация	6,25	6,25

## 5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Основные понятия и термины, относящиеся к информационной безопасности. Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей. Классификация атак. Сервисы безопасности. Правила обеспечения безопасности рабочей станции.	4	2	2	0
2	Криптография. Основные понятия и термины. Алгоритмы симметричного шифрования. Факторы безопасности алгоритмов симметричного шифрования. Примеры алгоритмов симметричного шифрования и их программная реализация.	6	2	4	0
3	Криптография с открытым ключом. Термины. Основные требования к алгоритмам асимметричного шифрования. Способы использования алгоритмов с открытым ключом. Примеры алгоритмов с открытым ключом и их программная реализация.	6	2	4	0
4	Использование криптографических программных средств (на примере open source). Gpg, Pgp (Pgp sdk), Openssl, TrueCrypt. Примеры создания криптографических модулей.	5	1	4	0
5	Криптографические стандарты. Цифровые сертификаты. Иерархия центров авторизации. Серверные и клиентские сертификаты. Безопасные коммуникации.	7	1	6	0
6	Лингвистический криптоанализ	4	0	4	0

### 5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Основные понятия и термины, относящиеся к информационной безопасности. Характерные проблемы, связанные с безопасностью, при использовании компьютерных сетей. Классификация атак. Сервисы безопасности. Правила обеспечения безопасности рабочей станции	2
2	2	Криптография. Криптоанализ. Определения. Термины. Стеганография, примеры использования. Факторы безопасности алгоритмов симметричного шифрования. Абсолютно стойкий шифр. Структура блочного алгоритма симметричного шифрования; Симметричное шифрование блока; Алгоритмы DES, AES; Алгоритм ГОСТ 28147-89; Режимы симметричного блочного шифрования длинных сообщений	2
3	3	Основные требования к алгоритмам асимметричного шифрования (шифрования с открытым ключом). Терминология в алгоритмах асимметричного шифрования. Понятие односторонней функции с секретом. Правила модульной арифметики. Способы использования алгоритмов с открытым ключом (зашифровывание/расшифровывание). Цифровая подпись (прямая, арбитражная)	2
4	4	Криптографические хэш-функции. Основные требования. Программные реализации. Программные реализации алгоритмов с открытым ключом (на примере Gpg, Pgp, TrueCrypt).	1

5	5	Цифровые сертификаты Стандарт X.509. Спецификации РКИ Иерархия центров авторизации цифровых сертификатов Серверные и клиентские сертификаты. Безопасные коммуникации на основе SSL.	1
---	---	---	---

## 5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Настройка и проверка защищенности Internet-коммуникаций	2
2	2	Использование и защита почтовых протоколов	4
3	3	Использование PGP и GPG для обеспечения конфиденциальности электронной почты и шифрования файлов	4
4	4	Криptoанализ зашифрованного текста	4
5	5	Использование РКИ (инфраструктуры открытых ключей) для защиты электронной почты и web-коммуникаций	6
6	6	Лингвистический криptoанализ	4

## 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
Изучение государственного стандарта 28147-89. Изучение государственного стандарта Р34.10-2001. Изучение государственного стандарта Р34.11-94	P:\PREP\Wan\Security\Лабораторные работы\lab0.doc – lab6.doc http://protect.gost.ru/document.aspx?control=7&id=139177 http://protect.gost.ru/document.aspx?control=7&id=131131 http://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_%D0%A0_34.11-94	3
Подготовка к зачету	Суховилов, Б. М. Защита информации в корпоративных информационных системах Текст учеб. пособие к практ. работам по направлению "Приклад. информатика" Б. М. Суховилов ; Юж.-Урал. гос. ун-т, Каф. Информатика ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 39, [1] с. ил. электрон. версия Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире Пер. с англ. Б. Шнайер. - СПб. и др.: Питер: Питер прнт, 2003. - 368 с.	3
Изучение характерных проблем, связанных с безопасностью, при использовании компьютерных	Суховилов Б.М. Презентации к лекциям по информационной безопасности	3

сетей. Изучение правил обеспечения безопасности рабочей станции		
Алгоритм RSA, схема Диффи-Хеллмана, стандарт цифровой подписи DSS. Отечественные стандарты алгоритмов с открытым ключом	Кошкаров В.Н. Презентации к лекциям по информационной безопасности	3
Подготовка к тестированию	P:\PREP\Wan\Secu-riaty\Лекции\ Основы_информационной_безопасно-сти.ppt (с.1-70)	3

## 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	Учи-тыва-ется в ПА
1	3	Текущий контроль	Тест	1	10	Тест состоит из 10 вопросов. Каждый правильный ответ оценивается в 1 балл. Время на выполнение заданий -15 минут	зачет
2	3	Текущий контроль	Выступление на практических занятиях по вопросам	1	5	При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Оценка: - «отлично» (5 баллов): при ответе показано всестороннее и глубокое знание учебного материала; демонстрируется взаимосвязь основных понятий дисциплины в их значении для исследуемой проблемы; - «хорошо» (4 балла): демонстрируется полное знание основных тем программы; усвоена основная литература, рекомендованная в программе; показывается стабильный характер знаний и умений и способность к их самостоятельному применению и обновлению; - «удовлетворительно» (3	зачет

						балла): знание основного программного материала в достаточном объеме; знакомство с основной литературой, рекомендованной программой; допускаются неточности в ответе на экзамене, но в основном студент владеет необходимыми знаниями и умениями; - «неудовлетворительно» (0 баллов): показаны существенные пробелы в знаниях основного учебного материала по программе; допущены принципиальные ошибки при ответе на вопросы.	
3	3	Промежуточная аттестация	сдача зачета	-	2	Показатели оценивания: 2 балла – правильные и развернутые ответы на вопросы в билете 1 балл – неправильные ответы на 1 вопрос в билете 0 баллов – отсутствие правильных ответов на вопросы в билете	зачет

## 6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Студенты, имеющие 60% и более по балльно-рейтинговой системе, полученные ими за выполнение заданий текущего контроля, получают зачет. Те, кто не имеет необходимого минимума, сдают зачет. Устный ответ по билетам. В билете 2 вопроса. На подготовку ответов студенту дается 45 минут, после чего происходит индивидуальная беседа с преподавателем. В случае некорректно или неправильно данных ответов студенту могут быть заданы уточняющие вопросы из этой темы.	В соответствии с пп. 2.5, 2.6 Положения

## 6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ		
		1	2	3
УК-1	Знает: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации	+++		
УК-1	Умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения	+++		
УК-1	Имеет практический опыт: владения методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации	+++		
ПК-2	Знает: теоретические основами криптографии, корпоративную стратегию, программы организационного развития	+	+	

ПК-2	Умеет: применять практические приемы защиты рабочих станций и серверов	+++
ПК-2	Имеет практический опыт: работы с инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем	++ +
ПК-7	Знает: основы разработки корпоративной стратегии, программы организационного развития	++
ПК-7	Умеет: применять практические приемы защиты рабочих станций и серверов	+++
ПК-7	Имеет практический опыт: владения инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем	+ +

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### Печатная учебно-методическая документация

*а) основная литература:*

Не предусмотрена

*б) дополнительная литература:*

Не предусмотрена

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

Не предусмотрены

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

1. Методическое пособие для работы по дисциплине "Технологии защиты информации"

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

1. Методическое пособие для работы по дисциплине "Технологии защиты информации"

### Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Андианова, Е. Г. Корпоративные информационные системы : методич (дата обращения: 16.02.2022). — Режим доступа: для авториз. пользователей.
2	Основная литература	Электронно-библиотечная система издательства Лань	Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — М. : Издательство Лань, 2018. — 256 с.
3	Основная литература	Электронно-библиотечная	Скудис, Э. Противостояние хакерам. Пошаговое руководство по компьютерной безопасности (дата обращения: 16.02.2022). — Режим доступа: для авториз. пользователей.

		система издательства Лань	
4	Основная литература	Электронно-библиотечная система издательства Лань	Нортон, П. Полное руководство по Microsoft Windows XP: руководство для авториз. пользователей.
5	Основная литература	Электронно-библиотечная система издательства Лань	Аверченков, В. И. Аудит информационной безопасности : учебное пособие. Режим доступа: для авториз. пользователей.
6	Основная литература	Электронно-библиотечная система издательства Лань	Современные методы обеспечения защиты информации: учебное пособие
7	Основная литература	Электронно-библиотечная система издательства Лань	Ермакова, А. Ю. Криптографические методы защиты информации : учебное пособие для авториз. пользователей.
8	Основная литература	Электронный каталог ЮУрГУ	<a href="http://virtua.lib.susu.ru/cgi-bin/gw_2011_1_4/chameleon?sessionid=2022021603565602598&amp;skin=def4%0%be%d1%80%0%bc%d0%b0%d1%86%d0%b8%d0%be%d0%bd%d1%82%20%d1%83%d1%87%d0%b5%d0%b1.%20%d0%bf%d0%be%d1%0%b8%20%d0%ba%d1%80%d0%b5%d0%b4%d0%b8%d1%82%22%20%0%bb%d0%be%d0%b2%d0%b0%20%3b%20%d0%ae%d0%b6.-%d0%a3%d1%82,%20%d0%9a%d0%b0%d1%84.%20%d0%98%d0%bd%d1%84%0">http://virtua.lib.susu.ru/cgi-bin/gw_2011_1_4/chameleon?sessionid=2022021603565602598&amp;skin=def4%0%be%d1%80%0%bc%d0%b0%d1%86%d0%b8%d0%be%d0%bd%d1%82%20%d1%83%d1%87%d0%b5%d0%b1.%20%d0%bf%d0%be%d1%0%b8%20%d0%ba%d1%80%d0%b5%d0%b4%d0%b8%d1%82%22%20%0%bb%d0%be%d0%b2%d0%b0%20%3b%20%d0%ae%d0%b6.-%d0%a3%d1%82,%20%d0%9a%d0%b0%d1%84.%20%d0%98%d0%bd%d1%84%0</a>

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(31.12.2022)

## 8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стеллы, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	160 (1)	компьютер, проектор, экран
Самостоятельная работа студента	162а (1)	16 компьютеров, проектор, экран
Практические занятия и семинары	160 (1)	компьютер, проектор, экран