Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____ Хагуров Т.А.
подпись
«27» апреля 2018г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Б1.Б.20 «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ЭКОНОМИЧЕСКИХ СИСТЕМ»

Направление подготовки 09.03.03 Прикладная информатика

Профиль Прикладная информатика в экономике

Программа подготовки Академическая

Форма обучения Очная

Квалификация выпускника Бакалавр

Краснодар 2018

Рабочая программа дисциплины «Безопасность информационных экономических систем» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.03.03 Прикладная информатика профиль Прикладная информатика в экономике

Программу составили:

А.Х. Арутюнян, преподаватель

подпись

М.Х. Уртенов, заведующий кафедрой
д.ф.-м.н., профессор

подпись

Рабочая программа дисциплины «Безопасность информационных экономических систем» утверждена на заседании кафедры прикладной математики протокол № 7 «18» апреля 2018г.

Заведующий кафедрой Уртенов М.Х.

подпись

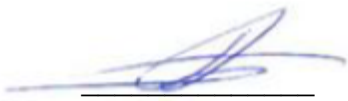
Рабочая программа обсуждена на заседании кафедры прикладной математики протокол № 7 «18» апреля 2018г.

Заведующий кафедрой Уртенов М.Х.

подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 1 «20» апреля 2018г.

Председатель УМК факультета Малыхин К.В.



подпись

Рецензенты:

Шапошникова Татьяна Леонидовна.
Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Директор института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

Марков Виталий Николаевич.
Доктор технических наук. Профессор кафедры информационных систем и программирования института компьютерных систем и информационной безопасности (ИКСиИБ) ФГБОУ ВО «КубГТУ».

1, Цели и задачи учебной дисциплины

1.1 Цели освоения дисциплины

Целью освоения учебной дисциплины «Безопасность информационных экономических систем» является приобретение теоретических и практических умений и навыков применения современных информационных технологий для использования в профессиональной деятельности по защите информации.

1.2 Задачи дисциплины:

- формирование у обучающихся общего представления о современных концепциях информационной безопасности;
- знакомство с различными методами защиты информации от несанкционированного доступа;
- изучение криптографических средств, как основного инструмента обеспечения сохранности компьютерной информации;
- приобретение практических навыков работы с современными аппаратными и программными средствами защиты информации;

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность информационных экономических систем» относится к базовой части Блока 1 «Дисциплины» учебного плана.

Данная дисциплина (Безопасность информационных экономических систем) тесно связана со следующими дисциплинами базовой части Блока 1: Информационные системы и технологии. Она направлена на формирование знаний и умений обучающихся разрабатывать и использовать защищенные ЭИС. Обеспечивает способность у обучающихся к созданию моделей безопасности и их применение, таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Компетенции обучающегося, формируемые в результате освоения курса «Безопасность информационных экономических систем»:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК–4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создания ИС	оценивать и выбирать современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создание ИС	способностью применять системный подход и математические методы для защиты электронных информационных систем

2. Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 5 зач.ед. (180 часов), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)			
		7			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	72	72	-	-	-
Занятия лекционного типа	36	36	-	-	-
Лабораторные занятия	36	36	-	-	-
Занятия семинарского типа (семинары, практические занятия)	-	-	-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)	8	8	-	-	-
Промежуточная аттестация (ИКР)	0,5	0,5	-	-	-
Самостоятельная работа, в том числе:					

Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		40	40	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		20	20	-	-	-
Реферат				-	-	-
Подготовка к текущему контролю		3,8	3,8	-	-	-
Контроль:						
Подготовка к экзамену		35,7	35,7			
Общая трудоемкость	**час.**	**180**	**180**	**-**	**-**	**-**
	в том числе контактная работа	**80,5**	**80,5**			
	зач. ед	**5**	**5**			

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
	Общие представления об информационной безопасности	52	13		13	26
	Защита от утечек информации	16	4		4	8
	Программные средства защиты	67,8	19		19	29,8
	Итого по дисциплине:		**36**		**36**	**63,8**

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
	Общие представления об информационной безопасности.	*Тема 1. Основные понятия информационной безопасности и защиты информации.* Понятие информации, информации безопасности, защиты информации. Общие концептуальные положения информационной безопасности. *Тема 2. Требования, предъявляемые к защите информации.* Требование к системам общего пользования. Мероприятия по обеспечению защиты в системах общего пользования. *Тема 3. Аспекты информационной безопасности.* Доступность, целостность и конфиденциальность информационной безопасности. *Тема 4. Угрозы. Основные понятия и определения.* Понятие угрозы. Системная классификация угроз. *Тема 5. Множество причин нарушения целостности информации (ПНЦИ).* Взаимодействие параметров угроз информации. Безопасность в базах данных. *Тема 6. Множество каналов несанкционированного получения информации (КНПИ).* Каналы утечки информации. Классификация каналов утечки информации. Источники образования каналов утечки. *Тема 7. Оценка угроз информации.* Сущность оценки угроз информации. Задачи оценки угроз информации. *Тема 8. Показатели уязвимости информации.* Анализ уязвимости. Модель нарушителей. Особо важные зоны. *Тема 9. Вероятностная модель расчета уязвимости информации.* Декомпозиция компонента информационной системы. Оценка базовой уязвимости. *Тема 10. Методы определения требований к защите информации.* Множество задач защиты информации. Задачи, возникающие при определении требований к защите информации. Оценка параметров. Классификация информации по важности. *Тема 11. Классификация способов и средств защиты информации. Технические средства.* Средства защиты от речевой информации. Методы поиска электронных устройств перехвата информации.	1. Подготовка рефератов, презентаций, выступлений. 2. Резюме, аналитический обзор по проблеме.

	Защита от утечек информации	*Тема 1. Защита от утечки по визуально-оптическим каналам.* Общие положения. Факторы утечки информации. Средства и способы защиты. *Тема 2. Защита от утечки по акустическим каналам.* Общие положения. Факторы утечки информации. Средства и способы защиты. *Тема 3. Защита от утечки по электромагнитным каналам.* Общие положения. Факторы утечки информации. Средства и способы защиты. *Тема 4. Защита от утечки по материально-вещественным каналам.* Общие положения. Факторы утечки информации. Средства и способы защиты.	1. Опрос по результатам индивидуального задания
	Программные средства защиты	*Тема 1. Вредоносное программное обеспечение.* Классификация вредоносного программного обеспечения. Программные закладки. Ловушка, люк, червь, троянский конь, бомба. *Тема 2. Вирусы.* Общее представление о вирусах. Этапы функционирования. Классификация вирусов. *Тема 3. Антивирусные средства.* Классификация антивирусных программных средств. Детекторы, полифаги, ревизоры, сторожа, вакцины. *Тема 4. Сетевые атаки.* Понятие сетевой атаки. Классификация сетевых атак. Группы атак. *Тема 5. Межсетевые экраны.* Понятие межсетевого экрана. Классификация межсетевых экранов. Группы атак. *Тема 6. Контроль целостности ПО и информации.* Целостность данных. Электронно-цифровая подпись. *Тема 7. Методы идентификации и аутентификации.* Функции идентификации и аутентификации. Процедуры идентификации и аутентификации. *Тема 8. Способы контроля и разграничения доступа к информации.* Аппаратные и программные средства разграничения доступа. Методы разграничения доступа. *Тема 9. Защита операционных систем.* Механизмы защиты информации в операционных системах. Классификация средств защиты информации.	1. Защита проектного задания.

2.3.2 Семинарские занятия – не предусмотрены

2.3.3 Лабораторные занятия

№ п/п	Наименование раздела	Наименование лабораторных работ	Форма текущего контроля

	Программные средства защиты	Программные закладки. Ловушка, люк, червь, троянский конь, бомба.	Проверка выполнения лабораторных работ № 1
		Этапы функционирования. Классификация вирусов.	Проверка выполнения лабораторных работ № 2
		Антивирусные программныесредства. Детекторы, полифаги, ревизоры, сторожа, вакцины.	Проверка выполнения лабораторных работ № 3
		Сетевые атаки.	Проверка выполнения лабораторных работ № 4
		Межсетевые экраны.	Проверка выполнения лабораторных работ № 5
		Контроль целостности ПО и информации.	Проверка выполнения лабораторных работ № 6
		Методы идентификации и аутентификации.	Проверка выполнения лабораторных работ № 7
		Способы контроля и разграничения доступа к информации.	Проверка выполнения лабораторных работ № 8
		Защита операционных систем.	Проверка выполнения лабораторных работ № 9

2.3.4 Курсовые работы – не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающегося по дисциплине

Целью самостоятельной работы студента является углубление знаний, полученных в результате аудиторных занятий. Вырабатываются навыки самостоятельной работы. Закрепляются опыт и знания полученные во время лабораторных занятий.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка и повторение лекционного материала, материала учебной и научной литературы, подготовка к семинарским занятиям	Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
2	Подготовка к лабораторным занятиям	Методические указания по выполнению лабораторных работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
3	Подготовка к решению задач и тестов	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
4	Подготовка докладов	Методические указания для подготовки эссе, рефератов, курсовых работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
5	Подготовка к решению расчетно-графических заданий (РГЗ)	Методические указания по выполнению расчетно-графических заданий, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
6	Подготовка к текущему контролю	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.

3. Образовательные технологии

С точки зрения применяемых методов используются как традиционные информационно-объяснительные лекции, так и интерактивная подача материала с мультимедийной системой. Компьютерные технологии в данном случае обеспечивают возможность разнопланового отображения алгоритмов и демонстрационного материала. Такое сочетание позволяет оптимально использовать отведенное время и раскрывать логику и содержание дисциплины.

Лекции представляют собой систематические обзоры нечетких и нейросетевых технологий с подачей материала в виде презентаций.

Лабораторное занятие позволяет научить студента применять теоретические знания при решении и исследовании конкретных задач. Лабораторные занятия проводятся в

компьютерных классах, при этом практикуется работа в группах. Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы. Это обусловлено тем, что в процессе исследования часто встречаются задачи, для которых единых подходов не существует. Каждая конкретная задача при своем исследовании имеет множество подходов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Занятия, проводимые с использованием интерактивных технологий

№	Наименование разделов (тем)	Количество часов	
		всего ауд. часов	интерактивные часы
1	2	3	4
1.	Общие представления об информационной безопасности	26	2
2.	Защита от утечек информации	8	4
3.	Программные средства защиты	38	10
	Итого по дисциплине:	72	16

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1 Фонд оценочных средств для проведения текущего контроля

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа студентов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе.

Фонд оценочных средств дисциплины состоит из средств текущего контроля (см. список лабораторных работ, задач и вопросов) и итоговой аттестации (экзамена).

В качестве оценочных средств, используемых для текущего контроля успеваемости, предлагается перечень вопросов, которые прорабатываются в процессе освоения курса. Данный перечень охватывает все основные разделы курса, включая знания, получаемые во время самостоятельной работы. Кроме того, важным элементом технологии является самостоятельное решение студентами и сдача заданий. Это полностью индивидуальная форма обучения. Студент рассказывает свое решение преподавателю, отвечает на дополнительные вопросы.

Примерные задания на лабораторные работы

1. Общие представления об информационной безопасности.

Задание 1. Зашифрование и расшифрование информации с помощью шифра Цезаря.

Задание 2. Зашифрование и расшифрование информации с помощью шифра Виженера.

Задание 3. Анализ одноалфавитных систем шифрования: частотный анализ.

Задание 4. Анализ одноалфавитных систем шифрования: метод полосок.

Задание 5. Анализ многоалфавитных систем шифрования: сведение к анализу одноалфавитных систем.

Задание 6. Анализ многоалфавитных систем шифрования: Метод Казиски.

Задание 7. Зашифрование и расшифрование информации с помощью шифра Виженера.

Задание 8. Протестировать антивирусное ПО с помощью тестового вируса http: //www. eicar. org/anti_virus_test_file. htm.

Задание 9. Определить дату выпуска антивирусных баз, при необходимости обновить их.

Задание 10. Зашифрование и расшифрование информации с помощью шифра Гронсфельда.

Задание 11. Зашифрование и расшифрование информации с помощью шифра Хилла.

2. Защита от утечек информации

Задание 1. Изучить интерфейс представленного антивирусного ПО - Kaspersky Internet Security.

Задание 2. Проанализировать назначение каждого компонента входящего в состав KIS.

Задание 3. Произвести настройку каждого компонента входящего в состав KIS на оптимальный уровень.

Задание 4. Провести полную проверку компьютера на наличие вредоносного ПО.

3. Программные средства защиты

Задание 1. Провести выборочную проверку компьютера на наличие вредоносного ПО.

Задание 2. Установить пароль на вход в ОС.

Задание 3. Зашифровать файлы криптоалгоритмом DES single (8 byte).

Задание 4. Зашифровать файлы криптоалгоритмом DES double (8 byte).

Задание 5. Зашифровать файлы криптоалгоритмом AES.

Задание 6. С помощью менеджера паролей сгенерировать пароль.

Задание 7. Установить пароль на файл архива.

Задание 8. Создать учетную запись пользователя.

Задание 9. С помощью утилиты восстановления забытых паролей проанализировать защищенный документ на предмет подбора пароля.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Примерный перечень вопросов к экзамену

1. Основные понятия информационной безопасности и защиты информации.
2. Требования, предъявляемые к защите информации.
3. Аспекты информационной безопасности.
4. Угрозы. Основные понятия и определения.
5. Системная классификация угроз.
6. Множество причин нарушения целостности информации (ПНЦИ).
7. Множество каналов несанкционированного получения информации (КНПИ).
8. Оценка угроз информации.
9. Показатели уязвимости информации.
10. Вероятностная модель расчета уязвимости информации.
11. Методы определения требований к защите информации.
12. Множество задач защиты информации.
13. Классификация способов и средств защиты информации.
14. Технические средства.
15. Системы охранной сигнализации.
16. Системы контроля вскрытия аппаратуры.
17. Защита информации на носителях. Способы уничтожения информации.
18. Защита от утечки по визуально-оптическим каналам.

19. Защита от утечки по акустическим каналам.
20. Защита от утечки по электромагнитным каналам.
21. Защита от утечки по материально-вещественным каналам.
22. Программные средства защиты.
23. Вредоносное программное обеспечение.
24. Вирусы.
25. Антивирусные средства.
26. Сетевые атаки.
27. Межсетевые экраны.
28. Контроль целостности ПО и информации.
29. Методы идентификации и аутентификации.
30. Способы контроля и разграничения доступа к информации.
31. Защита операционных систем.
32. Организационные средства защиты информации.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература:

1. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278.

2. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург : Лань, 2017. — 324 с. — Режим доступа: https://e.lanbook.com/book/90153.

3. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2016. — 296 с. — Режим доступа: https://e.lanbook.com/book/82817.

4. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс] : учеб. пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Режим доступа: https://e.lanbook.com/book/91449.

5.2 Дополнительная литература:

1. Ерохин, В.В. Безопасность информационных систем [Электронный ресурс] : учебное пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. – Электрон. дан. – М. : ФЛИНТА, 2015. – 184 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=62972.

2. Беломойцев, Д.Е. Основные методы криптографической обработки данных: учеб. пособие [Электронный ресурс] : / Д.Е. Беломойцев, Т.М. Волосатова, С.В. Родионов. – Электрон. дан. – М. : МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2014. – 80 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=58438.

3. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : . – Электрон. дан. – СПб. : СПбГПУ (Санкт-Петербургский государственный политехнический университет), 2014. – 322 с. – Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=64809.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронно-библиотечная система Издательство «Лань». http://e.lanbook.com

7. Методические рекомендации по организации изучения дисциплины

Контрольная работа представляет собой самостоятельную реферативную работу студентов. Каждый студент выполняет работу по одной теме.

Для написания реферата необходимо подобрать литературу. Общее количество литературных источников, включая тексты из Интернета, (публикации в журналах), должно

составлять не менее 10 наименований. Учебники, как правило, в литературные источники не входят.

Рефераты выполняют на листах формата А4. Страницы текста, рисунки, формулы нумеруют, рисунки снабжают подрисуночными надписями. Текст следует печатать шрифтом №14 с интервалом между строками в 1,5 интервала, без недопустимых сокращений. В конце реферата должны быть сделаны выводы.

В конце работы приводят список использованных источников.

Реферат должен быть подписан бакалавром с указанием даты ее оформления.

Работы, выполненные без соблюдения перечисленных требований, возвращаются на доработку.

Выполненная бакалавром работа определяется на проверку преподавателю в установленные сроки. Если у преподавателя есть замечания, работа возвращается и после исправлений либо вновь отправляется на

проверку, если исправления существенные, либо предъявляется на зачете, где происходит ее защита.

Темы презентаций

- Презентация «Вредоносное ПО».
- Презентация «Антивирусное ПО».

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1 Перечень информационных технологий

1. Проверка домашних заданий и консультирование посредством электронной почты.
2. Использование электронных презентаций при проведении лекционных занятий.

8.2 Перечень необходимого программного обеспечения

1. Операционная система MS Windows (раздел 1 дисциплины).
2. Интегрированное офисное приложение MS Office (раздел 2 дисциплины).
3. Программное обеспечение для организации управляемого коллективного и безопасного доступа в Интернет (раздел 2 дисциплины).
4. Среда разработки CodeGear RAD studio Delphi 2010 (раздел 3 дисциплины).

8.3 Перечень информационных справочных систем

1. Электронная библиотечная система eLIBRARY.RU(http://www.elibrary.ru)

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория А305, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук), соответствующим программным обеспечением, а также необходимой мебелью (доска, столы, стулья).
2.	Лабораторные занятия	Лаборатория 102, укомплектованная специализированной мебелью, техническими средствами обучения (современными ПЭВМ на базе процессоров Intel или AMD, объединёнными локальной сетью) с выходом в глобальную сеть Интернет, а также современным лицензионным

		программным обеспечением (операционная система Windows 8/10, пакет Microsoft Office, среды программирования MS Visual Studio и Delphi) ПО: 1. Microsoft Windows 8, 10 "№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510" 2. Microsoft Office Professional Plus "№73–АЭФ/223-ФЗ/2018 Соглашение Microsoft ESS 72569510"
3.	Групповые (индивидуальные) консультации	Аудитория 131 для групповых и индивидуальных консультаций, укомплектованная необходимой мебелью (доска, столы, стулья).
4.	Текущий контроль, промежуточная аттестация	Аудитория 131 для текущего контроля и промежуточной аттестации, укомплектованная необходимой мебелью (доска, столы, стулья).
5.	Самостоятельная работа	Кабинет 102а для самостоятельной работы, оснащённая компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета, необходимой мебелью (доска, столы, стулья).