

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«__» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1156870	Защита информации в информационно-управляющих системах

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Информационная безопасность телекоммуникационных систем 2. Информационно-аналитические системы безопасности	Код ОП 1. 10.05.02/22.01 2. 10.05.04/22.01
Направление подготовки 1. Информационная безопасность телекоммуникационных систем; 2. Информационно-аналитические системы безопасности	Код направления и уровня подготовки 1. 10.05.02; 2. 10.05.04

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	
2	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ

Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Защита информации в информационно-управляющих системах

1.1. Аннотация содержания модуля

Модуль «Защита информации в информационно управляющих системах» обобщает полученные знания и навыки в области информационной безопасности телекоммуникационных систем и сетей, систематизирует и определяет основные требования к средствам защиты систем.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Управление информационной безопасностью	3
2	Безопасность автоматизированных информационно-управляющих систем	4
ИТОГО по модулю:		7

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	1. Управление информационной безопасностью
Постреквизиты и кореквизиты модуля	1. Защита информации

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Безопасность автоматизированных информационно-управляющих систем	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе,	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства

	<p>их значение для обеспечения объективных потребностей личности, общества и государства</p> <p>(Информационная безопасность телекоммуникационных систем)</p>	<p>З-2 - Описать психологические аспекты информационной безопасности в современном обществе</p> <p>З-3 - Сделать обзор основных методов обеспечения информационной безопасности</p> <p>У-1 - Работать с различными источниками информации</p> <p>У-2 - Осуществлять сбор и анализ полученной информации</p> <p>У-3 - Систематизировать и классифицировать полученную информацию</p> <p>П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности</p>
	<p>ОПК-6 - Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p> <p>(Информационно-аналитические системы безопасности)</p>	<p>З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа</p> <p>З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации</p> <p>У-1 - Систематизировать и классифицировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах</p> <p>П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа</p>
	<p>ПК-5 - Способен разработать и смоделировать</p>	<p>З-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД</p>

	<p>программно-технические средства защиты информации от несанкционированного доступа</p>	<p>З-2 - Характеризовать современные информационные технологии (операционные системы, базы данных, вычислительные сети)</p> <p>З-3 - Характеризовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах</p> <p>З-4 - Различать основные классы и виды уязвимостей программного обеспечения</p> <p>З-5 - Объяснять методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее</p> <p>З-6 - Характеризовать (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее</p> <p>З-7 - Характеризовать методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий</p> <p>З-8 - Характеризовать средства контроля защищенности информации от несанкционированного доступа</p> <p>З-9 - Характеризовать методики контроля защищенности информации от несанкционированного доступа</p> <p>З-10 - Характеризовать средства проектирования электронных схем</p> <p>У-1 - Составлять техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее</p> <p>У-2 - Составлять проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее</p>
--	--	--

		<p>У-3 - Составлять программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее</p> <p>П-1 - Иметь опыт практической разработки технического (эскизного) проекта программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее</p> <p>П-2 - Иметь опыт практического испытания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее</p> <p>П-3 - Иметь опыт практической разработки рабочей и эксплуатационной документации на техническое средство защиты</p>
Управление информационно й безопасностью	<p>ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства</p> <p>(Информационная безопасность телекоммуникационных систем)</p>	<p>З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства</p> <p>З-2 - Описать психологические аспекты информационной безопасности в современном обществе</p> <p>З-3 - Сделать обзор основных методов обеспечения информационной безопасности</p> <p>У-1 - Работать с различными источниками информации</p> <p>У-2 - Осуществлять сбор и анализ полученной информации</p> <p>У-3 - Систематизировать и классифицировать полученную информацию</p> <p>П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности</p>
	ОПК-6 - Способен при решении профессиональных задач	З-1 - Различать правовые и организационные меры защиты

	<p>проверить выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p> <p>(Информационно-аналитические системы безопасности)</p>	<p>информации, в том числе информации ограниченного доступа</p> <p>З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации</p> <p>У-1 - Систематизировать и классифицировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах</p> <p>П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа</p>
--	--	--

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Управление информационной
безопасностью

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	
2	Поршнев Сергей Владимирович	д.т.н., профессор	директор Учебно- научного центра "Информаци онная безопасност ь"	УНЦ ИБ
3	Синадская Ольга Юрьевна	без ученой степени, без ученого звания	Старший преподавате ль	Учебно-научный центр "Информационная безопасность"

Рекомендовано учебно-методическим советом института Радиозлектроники и информационных технологий - РТФ

Протокол № 9 от 20.09.2021 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- Пономарева Ольга Алексеевна, Старший преподаватель,
- Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ
- Синадская Ольга Юрьевна, Старший преподаватель, Учебно-научный центр "Информационная безопасность"

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
 - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*

Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Обеспечение режима защиты информации персональных данных (ПДн), и безопасности ПДн в организации	Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных». Меры, по обеспечению безопасности ПДн при их обработке. Понятие угроз безопасности ПДн. Определение уровня защищенности ПДн.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Формирование информационно й культуры в	целенаправленная работа с информацией	Технология самостоятельной работы	ОПК-1 - Способен оценивать роль информации,	З-1 - Изложить сущность и понятие

сети интернет	для использования в практических целях		информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства
---------------	--	--	---	--

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью

Электронные ресурсы (издания)

1. Шкундин, С. З.; Теория информационных процессов и систем : учебное пособие.; Горная книга, Москва; 2012; <https://biblioclub.ru/index.php?page=book&id=229031> (Электронное издание)

Печатные издания

1. Бакланов, В. В., Гайдамакин, Н. А.; Защита компьютерной информации в клиентских приложениях : учеб. пособие [для вузов].; [УГТУ-УПИ], Екатеринбург; 2006 (3 экз.)

2. , Белов, Е. Б., Лось, В. П., Мещеряков, Р. В., Шелупанов, А. А.; Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности.; Горячая линия - Телеком, Москва; 2006 (26 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (<http://минобрнауки.рф>).

Федеральный портал _Российское образование (<http://www.edu.ru>).

ООО Научная электронная библиотека (<http://elibrary.ru>).

Зональная научная библиотека УрФУ(<http://lib.urfu.ru>).

Электронный научный архив УрФУ (<https://elar.urfu.ru>).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Управление информационной безопасностью

Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащённость специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	<ol style="list-style-type: none">1. Компьютерный класс.2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.3. Сертифицированный программно-аппаратный комплекс межсетевое экранирования.4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Практические занятия	<ol style="list-style-type: none">1. Компьютерный класс.2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.3. Сертифицированный программно-аппаратный комплекс межсетевое экранирования.4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
3	Консультации	<ol style="list-style-type: none">1. Компьютерный класс.2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.3. Сертифицированный программно-аппаратный комплекс межсетевое экранирования.	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	
4	Самостоятельная работа студентов	<p>1. Компьютерный класс.</p> <p>2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.</p> <p>3. Сертифицированный программно-аппаратный комплекс межсетевое экранирования.</p> <p>4. Общесистемное и прикладное программное обеспечение, средства защиты информации:</p>	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Текущий контроль и промежуточная аттестация	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Доска аудиторная</p> <p>Периферийное устройство</p> <p>Персональные компьютеры по количеству обучающихся</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p> <p>Подключение к сети Интернет</p>	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Безопасность автоматизированных
информационно-управляющих систем

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Гайдамакин Николай Александрович	доктор технических наук, профессор	Профессор	
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	
3	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно- научного центра "Информаци онная безопасност ь"	УНЦ ИБ

Рекомендовано учебно-методическим советом института Радиоэлектроники и информационных технологий - РТФ

Протокол № 9 от 20.09.2021 г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- Гайдамакин Николай Александрович, Профессор,
- Пономарева Ольга Алексеевна, Старший преподаватель,
- Поршнев Сергей Владимирович, директор Учебно-научного центра "Информационная безопасность", УНЦ ИБ

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
 - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*

Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Состав, структура и функции автоматизированных информационноуправляющих систем	Общие сведения об автоматизированном управлении, особенности технических систем как объектов управления и автоматизированных систем управления ими. Классификация технических систем как объектов управления. Основные особенности централизованных, децентрализованных и иерархических систем управления, декомпозиция системы управления на подсистемы, приоритет подсистем в принятии решений, самоуправление и координация, агрегирование информации, передаваемой на верхние уровни. Функции отдельных уровней иерархической системы управления. Оперативнокалендарное планирование, координация работы отдельных подсистем, оптимальное распределение

		ресурсов, Оперативное управление, контроль, цифровое управление.
2	Алгоритмическое обеспечение автоматизированных информационноуправляющих систем	Основные понятия и определения. Способы записи алгоритмов. Ввод непрерывных сигналов в микропроцессорные средства. Задача оценки интервалов дискретизации непрерывных технологических параметров. Первичная обработка информации, введенной в микропроцессорные средства контроля и управления. Алгоритмы цифрового регулирования. Структура цифровой системы регулирования
3	Программное и информационное обеспечение автоматизированных информационноуправляющих систем	Состав и структура программного обеспечения. Общее программное обеспечение и прикладное. Операционные системы реального времени. Системы и языки программирования промышленных микропроцессорных контроллеров. Технологическое программирование. Программные пакеты, используемые для решения задач оптимального управления. Применение метода имитационного моделирования для анализа сложных систем. Информационное обеспечение автоматизированных систем. Основные тенденции развития и совершенствования автоматизированного управления в технических системах

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология самостоятельной работы	ОПК-6 - Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа

			и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	
--	--	--	--	--

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность автоматизированных информационно-управляющих систем

Электронные ресурсы (издания)

1. Трофимов, В. Б.; Интеллектуальные автоматизированные системы управления технологическими объектами: учебно-практическое пособие : учебное пособие.; Инфра-Инженерия, Москва, Вологда; 2016; <https://biblioclub.ru/index.php?page=book&id=444175> (Электронное издание)
2. Галатенко, В. А., Бетелин, В. Б.; Программирование в стандарте POSIX: Курс лекций : учебное пособие.; Интернет-Университет Информационных Технологий (ИНТУИТ), Москва; 2004; <https://biblioclub.ru/index.php?page=book&id=233064> (Электронное издание)

Печатные издания

1. , Белов, Е. Б., Лось, В. П., Мещеряков, Р. В., Шелупанов, А. А.; Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности.; Горячая линия - Телеком, Москва; 2006 (26 экз.)
2. Гайдамакин, Н. А.; Разграничение доступа к информации в компьютерных системах; Издательство Уральского университета, Екатеринбург; 2003 (3 экз.)
3. , Гайдамакин, Н. А.; Сборник нормативных правовых актов по компьютерной и информационной безопасности Т. 1. Законодательные акты РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ; Гриф, Екатеринбург; 2006 (1 экз.)
4. Гайдамакин, Н. А.; Разграничение доступа к информации в компьютерных системах; Изд-во Урал. ун-та, Екатеринбург; 2003 (23 экз.)

Профессиональные базы данных, информационно-справочные системы

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

Министерство образования и науки Российской Федерации (<http://минобрнауки.рф>).

Федеральный портал _Российское образование (<http://www.edu.ru>).

ООО Научная электронная библиотека (<http://elibrary.ru>).

Зональная научная библиотека УрФУ(<http://lib.urfu.ru>).

Электронный научный архив УрФУ (<https://elar.urfu.ru>).

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Безопасность автоматизированных информационно-управляющих систем

Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащённость специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевое экранирования. 4. Общесистемное и прикладное программное обеспечение, средства защиты информации:	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
2	Практические занятия	1. Компьютерный класс. 2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном. 3. Сертифицированный программно-аппаратный комплекс межсетевое экранирования. 4. Общесистемное и прикладное программное	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

		обеспечение, средства защиты информации:	
3	Консультации	<p>1. Компьютерный класс.</p> <p>2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.</p> <p>3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.</p> <p>4. Общесистемное и прикладное программное обеспечение, средства защиты информации:</p>	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
4	Самостоятельная работа студентов	<p>1. Компьютерный класс.</p> <p>2. Персональный компьютер преподавателя с мультимедиа-проектором и экраном.</p> <p>3. Сертифицированный программно-аппаратный комплекс межсетевого экранирования.</p> <p>4. Общесистемное и прикладное программное обеспечение, средства защиты информации:</p>	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES
5	Текущий контроль и промежуточная аттестация	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Доска аудиторная</p> <p>Периферийное устройство</p> <p>Персональные компьютеры по количеству обучающихся</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p>	Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES

