МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Уровень подготовки: высшее образование – магистратура

Направление подготовки
10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(код и наименование направления подготовки)

Направленность подготовки
Информационная безопасность
(наименование программы подготовки)

Квалификация (степень) выпускника
Магистр
Форма обучения
очная

Разработана в соответствии

с ФГОС ВПО, Приказ МОиН РФ от 28.10.2009, № 497

Актуализирована в соответствии

с ФГОС ВО, Приказ МОиН РФ от 01.12.2016, № 1513

Уфа 2016

Исполнители:

к.т.н., доцент _____ А.Р.Амиров

ст.преподаватель _____ С.Н.Зарипов
должность *подпись* *расшифровка подписи*

Заведующий кафедрой

ВТиЗИ _____ В.И.Васильев
наименование кафедры *личная подпись* *расшифровка подписи*

1. Место дисциплины в структуре образовательной программы

Дисциплина "Теоретические основы компьютерной безопасности" является обязательной дисциплиной вариативной части ОПОП по направлению подготовки 10.04.01 Информационная безопасность, направленность: Информационная безопасность.

Рабочая программа составлена в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 090900 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 28 октября 2009 г. № 497;

Рабочая программа актуализирована в соответствии с требованиями:

- Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки 10.04.01 Информационная безопасность (квалификация "магистр"), утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. № 1513.

Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Дисциплина "Теоретические основы компьютерной безопасности" имеет целью обучить студентов принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем (АС). Знания и практические навыки, полученные из курса "Теоретические основы компьютерной безопасности", используются обучаемыми при изучении специальных дисциплин, при разработке курсовых и дипломных работ.

Задачи дисциплины – усвоение обучаемым знаний:

– устройства и принципов функционирования защищенных АС;
– методологии проектирования и построения защищенных АС;
– критериев и методов оценки защищенности АС;
– средств и методов несанкционированного доступа (НСД) к информации АС.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	базовый уровень освоения компетенции параллельный этап	Дисциплина по выбору: Методы цифровой обработки видеоизображений
2	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества		базовый уровень освоения компетенции параллельный этап	Дисциплина по выбору: Биометрические системы безопасности

- **пороговый уровень дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;*

*-**базовый уровень** позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;*

*-**повышенный уровень** предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.*

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	повышенный уровень освоения компетенции шестой этап	Подготовка магистерской диссертации
2	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента		повышенный уровень освоения компетенции пятый этап	Научно-исследовательская работа
3	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента		повышенный уровень освоения компетенции третий этап	Защищенные информационно-вычислительные системы
	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	ПК-7	базовый уровень освоения компетенции третий этап	дисциплины по выбору: 1. Методы многомерного анализа данных в задачах защиты информации 2. Методы кластеризации при мониторинге автоматизированных систем
	способность проводить экспериментальные	ПК-7	базовый уровень освоения	дисциплины по выбору: 1. Параллельное

	исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента		компетенции второй этап	программирование 2. Программная инженерия

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента	**ПК-7**	– основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем; – о перспективных направлениях развития теории безопасности АС; – о методах анализа угроз информации; об архитектуре электронных систем обработки данных и архитектуре защищенных АС; – о принципах и методах построения защищенных автоматизированных систем;	– осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; – проводить анализ АС с точки зрения обеспечения компьютерной безопасности; – применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС; – реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС: – организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения компьютерной безопасности;	– работы с АС распределенных вычислений и обработки информации; – управления процессами функционировани я систем защиты; – работы с документацией АС; – использования критериев оценки защищенности АС;

2	способность анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества	**ПК-5**	– методы концептуального проектирования технологий обеспечения информационной безопасности; – методологические и технологические основы комплексного обеспечения безопасности АС;	– обосновывать принципы организации технического, программного и информационного обеспечения защищенных информационных систем; – разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы;	– навыками управления информационной безопасностью простых объектов; – построения формальных моделей систем защиты информации АС.

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.	
	1 семестр 180 часов /5 ЗЕ	**2 семестр**
Лекции (Л)	16	-
Практические занятия (ПЗ)	30	-
Лабораторные работы (ЛР)	8	-
КСР	5	-
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	85	-
Контроль	36	-
Вид итогового контроля (зачет, экзамен)	экзамен	-

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	**Структура теории компьютерной безопасности**: Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Понятие «формальной модели». Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Архитектура электронных систем обработки данных. Основные уровни защиты информации. Защита машинных носителей информации. Защита представления информации. Защита содержания информации. Основные виды атак на АС.	4	6	4		20	34	Р 6.1 Р 6.2	лекция-визуализация, проблемное обучение, обучение на основе опыта
2	**Методология построения защищенных автоматизированных систем**: Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от НСД. Построение парольных систем. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Построение парольных систем. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Модель политики контроля целостности. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации. Методы верификации.	4	8	4		20	36	Р 6.1 Р 6.2	лекция-визуализация, проблемное обучение, обучение на основе опыта

	Построение системы защиты от угрозы доступности информации. Эксплутационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы. Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации. Методология обследования и проектирования систем защиты АС. Управление процессами функционирования систем защиты. Теория безопасных систем.								
3	**Политика безопасности:** Понятие политики безопасности. Политика безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности. Формальные модели, лежащие в основе систем защиты АС. Модели безопасности. Понятие модели безопасности. Описание систем защиты с помощью матрицы доступа. Разрешимость проблемы безопасности. Модель распространения прав доступа. Основная теорема безопасности модели. Эквивалентные подходы к определению безопасности.	4	8			20	32	Р 6.1 Р 6.2	лекция-визуализация, проблемное обучение, обучение на основе опыта
4	**Классы защищенности АС:** Отечественные и зарубежные стандарты по оценке защищенных систем. Основные критерии оценки защищенности АС. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценки защищенности АС. Стандарт оценки безопасности компьютерных систем	4	8		5	25	42	Р 6.1 Р 6.2	лекция-визуализация, проблемное обучение, обучение на основе опыта

	TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC. Концепция защиты АС и СВТ по руководящим документам ФСТЭК России. Классификация СВТ по документам ФСТЭК России. Классификация АС по документам Правительства и ФСТЭК России, требования классов защиты. Единые критерии безопасности информационных технологий (Common Criteria). Основные положения «Единых критериев». Требования безопасности. Профили защиты..								

Занятия, проводимые в интерактивной форме, составляют 0% от общего количества аудиторных часов по дисциплине.

Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	**1**	Анализ угроз информационной безопасности.	4
2	**2**	Аудит комплексной защиты информации предприятия.	4

Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Основные понятия теории компьютерной безопасности.	2
2	1	Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы.	4
3	2	Построение систем защиты от угрозы нарушения конфиденциальности информации.	4
4	2	Теория безопасных систем.	4
5	3	Дискреционная и мандатная политики разграничения доступа.	4
6	3	Модели безопасности.	4
7	4	Основные критерии оценки защищенности АС.	4
8	4	Концепция защиты АС и СВТ и их классификация СВТ по документам Правительства и ФСТЭК России.	4

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: / П. Н. Девянин - Москва: Горячая линия-Телеком, 2013 - 338 с.

2. Шаньгин В. Ф. Информационная безопасность: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2014.

6.2 Дополнительная литература

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях: / Шаньгин В.Ф. - Москва: ДМК Пресс, 2012.

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступ к м электронным ресурсам и информационным справочным системам, перечисленным в таблице

Таблица

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
1.	ЭБС «Лань» http://e.lanbook.com/	41716	С любого компьютера, имеющего выход в Интернет, после регистрации в ЭБС по сети УГАТУ	Договор № ЕД – 1185/0208-16 от 08.08.2016
2.	ЭБС Ассоциации «Электронное образование Республики Башкортостан» http://e-library.ufa-rb.ru	1225	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Учредительный договор Ассоциации образовательных организаций «Электронное образование Республики Башкортостан» от 29.11.2013
3.	Консорциум аэрокосмических вузов России http://elsau.ru/	1235	С любого компьютера, имеющего выход в Интернет, после регистрации в АБИС «Руслан» на площадке библиотеки УГАТУ	Договор о сетевом взаимодействии от 15.12.2014
4.	Электронная коллекция образовательных ресурсов УГАТУhttp://www.library.ugatu.ac.ru/cgi-bin/zgate.exe?Init+ugatu-fulltxt.xml,simple-fulltxt.xsl+rus	528	С любого компьютера по сети УГАТУ	Свидетельство о регистрац. №2012620618 от 22.06.2012
5.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №2255/0208-15 от 23.12.2015
6.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и дипломных работ	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-

				технической библиотекой России (далее ГПНТБ России) Сублиц. договор №ProQuest/151 52/0208-16 от 02.06.2016
7.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор 3К-2318/0106-15 от 30.12.2015
8.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208-16 от 15.03.2016
9.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии-1место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
10.	Научная электронная библиотека eLIBRARY* http://elibrary.ru/	9919 полнотекстовых журналов	С любого компьютера, имеющего выход в Интернет, после регистрации в НЭБ на площадке библиотеки УГАТУ	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
11.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор№Questel/15 146/0208-16 от 02.06.2016
12.	Научные полнотекстовые журналы издательства Taylor& Francis Group*	1700 наимен. журнал.	С любого компьютера по сети УГАТУ,	В рамках Государственного контракта от

	http://www.tandfonline.com/		имеющего выход в Интернет	17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №T&F/151 44/0208-16 от 02.06.2016
13.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. жрнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
14.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OUP-151 43/0208-16 от 02.06.2016
15.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наим. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016

16.	Научный полнотекстовый журнал Science The American Association for the Advancement of Science http://www.sciencemag.org	1 наимен. журнала.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151 45/0208-16 от 02.06.2016
17.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016
18.	Научные полнотекстовые ресурсы Optical Society of America* http://www.opticsinfobase.org/	19 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
19.	База данных GreenFile компании EBSCO* http://www.greeninfoonline.com	5800 библиографич записей, частично с полными текстами	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)

20.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич записей		В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
21.	Архив научных полнотекстовых журналов зарубежных издательств*- http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849– 1995) SAGE Publications (1800-1998) цифровой архив журнала Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

* Периодические издания получены по Гранту и на баланс библиотеки не принимались.

7. Образовательные технологии

При реализации дисциплины «Теоретические основы компьютерной безопасности» применяются классические образовательные технологии. Формы работы студентов: лекционные занятия, практические и лабораторные занятия, написание рефератов, выполнение контрольных работ (преимущественно в тестовой форме), решение кейс-задач во время лабораторных работ. В процессе проведения практических занятий рекомендуется использовать интерактивные формы проблемного обучения.

Дисциплина «Теоретические основы компьютерной безопасности» разбита на контролируемые разделы, комплексы знаний и умений в составе которых, подлежат контролю.

Контроль включает в себя выполнение письменных контрольных работ, преимущественно в тестовой форме, защиты лабораторных работ и представление рефератов.

Подбор вопросов для очередного тестирования (контрольной работы) осуществляется на основе изученного теоретического материала.

В качестве основной формы контролируемой самостоятельной работы магистранта рекомендуется использовать написание рефератов по выбранной заранее тематике. При написании реферата магистрант должен в соответствии с требованиями к оформлению работ сформулировать

проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

Для успешной подготовки к итоговому контролю в форме экзамена необходимо выполнить следующие контрольные мероприятия:

1. Выполнить тестовые задания по материалам каждого раздела учебного курса.

2. Выполнить все лабораторные работы по дисциплине с последующей защитой. Защита лабораторных работ требует заполнения отчетов, которые составляются в электронном (или печатном) виде. Файлы отчетов с материалами выполненных заданий лабораторных работ должны быть представлены преподавателю. В отчетах должна быть представлена следующая информация: тема работы; цель работы; общая постановка задачи; результаты выполнения работы с программными фрагментами скриншотами; ответы на контрольные вопросы.

3. Представить реферат и ответить на контрольные вопросы преподавателя по его теме.

Экзамен проводится в аудитории по экзаменационным билетам. Экзаменационные билеты содержат три теоретических вопроса по различным разделам курса.

9 . Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации: 5-301, 5-314. Лекционные аудитории оборудованы мультимедийным проектором (1шт.) и ПК (1 шт) с установленными:

- программным комплексом – операционная система Microsoft Windows (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования)
- программным комплексом – Microsoft Office (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования)

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-313 – Компьютерный класс №2 (ПК 6 шт., коммутатор 1 шт.);

Вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

- компьютерная техника:
  - Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150 / PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5” 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;
- программное обеспечение:
  - Программный комплекс – операционная система Microsoft Windows (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Office (№ договора ЭА-269/0503-16 , 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Project Professional (№ договора ЭА-269/0503-16 , 50 компьютеров, на которые распространяется право пользования)
  - Kaspersky Endpoint Security для бизнеса (лицензии 1055/0503-16, 500 users).
  - Dr.Web® Desktop Security Suite (КЗ) +ЦУ (AH99-VCUN-TPPJ-6k3L, 415 рабочих станций).
  - ESET Smart Security Business (EAV-8424791, 500 пользователей).

Для самостоятельной работы обучаемых используется ауд. 5-221 (Кабинет для самостоятельной работы студентов), оборудованная двумя персональными компьютерами, подключенными к локальной сети через ауд. 5-223.

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

10. Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.