

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации



УТВЕРЖДАЮ

Проректор по учебной работе

Н.Г. Зарипов

2017 г.

**ПРОГРАММА
НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ**

Уровень подготовки: высшее образование – специалитет

Специальность

10.05.05 «Безопасность информационных технологий
в правоохранительной сфере»
(код и наименование специальности)

Специализация

Технологии защиты информации в правоохранительной сфере
(наименование специализации)

Квалификация (степень) выпускника

Специалист

Форма обучения

очная

Год начала подготовки – 2013

Уфа 2017

Программа научно-исследовательской работы / сост. В.Е. Кладов – Уфа: УГАТУ, 2017.
– 24 с.

Программа НИР является приложением к Основной профессиональной образовательной программе высшего образования по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» и профилю «Технологии защиты информации в правоохранительной сфере».

Составитель В.Е. Кладов В.Е. Кладов
18.01.2017 г. (подпись)

Программа одобрена на заседании научно-методического совета по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере»
" 19 " 01 2017 г., протокол № 5

Председатель научно-методического совета

Васильев В.И. Васильев В.И. 19.01.2017
личная подпись расшифровка подписи дата

Программа утверждена на заседании кафедры ВТ и ЗИ

" 19 " 01 2017 г., протокол № 8

Заведующий кафедрой ВТ и ЗИ Васильев В.И. Васильев В.И. 19.01.2017
личная подпись расшифровка подписи дата

Начальник ООПБС

Г.Т. Гарипова Г.Т. Гарипова 26.01.2017
личная подпись расшифровка подписи дата

© Кладов В.Е., 2017
© УГАТУ, 2017

Содержание

- 1 Цели и задачи НИР
- 2 Требования к результатам НИР
- 3 Место НИР в структуре ОПОП подготовки специалиста
- 4 Структура и содержание НИР
- 5 Место, сроки и формы проведения НИР
- 6 Формы аттестации
- 7 Учебно-методическое и информационное обеспечение НИР
- 8 Материально-техническое обеспечение НИР
- 9 Реализация НИР лицами с ОВЗ

1. Цели и задачи НИР

Научно-исследовательская работа (НИР) выполняется студентами специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» в десятом семестре на четвертом курсе.

Целью НИР является формирование компетенций, направленных на получение первичных знаний и умений в научно-исследовательской деятельности студентов в области комплексной защиты объектов информатизации, проектирования, введения в эксплуатацию, эксплуатации и совершенствования систем защиты информации, а также в сфере управления информационной безопасностью.

Задачами НИР являются:

- сбор, изучение, систематизация и обобщение научно-технической информации, отечественного и зарубежного опыта по проблемам информационно-аналитической работы и обеспечения защиты информации;
- анализ прикладных проблем информационно-аналитического обеспечения правоохранительной деятельности, защиты информации и обеспечения безопасности информационных технологий;
- разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок;
- проведение экспериментов по заданным методикам.

2. Требования к результатам НИР

ФГОС ВО содержит требования к результату освоения ОПОП в терминах компетенций. В соответствии с ОПОП (раздел 3, подпункты 3.1 и 3.2) указаны общекультурные, общепрофессиональные, профессиональные и профессионально-специализированные компетенции, на которые направлено освоение раздела научно-исследовательской работы.

Общекультурные компетенции:

– **ОК-1** - способность понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы.

В результате освоения данной компетенции студент должен:

Знать:

– мировоззренческие, методологические основы мышления;

Уметь:

- применять понятия с четко определенным содержанием, устанавливать логический смысл суждения;

Владеть:

- навыками анализа социально и профессионально значимых проблем, процессов и явлений.

– **ОК-7** - способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии.

В результате освоения данной компетенции студент должен:

Знать:

– логические основы мышления;

Уметь:

- пользоваться логическими правилами ведения диалога и дискуссии;

Владеть:

- навыками научного мышления, использования приемов логического построения рассуждений, распознавания логических ошибок, методами логического анализа.

– **ОК-12** - способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

В результате освоения данной компетенции студент должен:

Знать:

– основные технологии создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств и информационных и коммуникационных технологий;

Уметь:

– использовать различные информационно - аналитические и справочно-правовые информационные ресурсы и технологии в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;

Владеть:

– навыками поиска, сбора, обработки и систематизации информации различного характера.

Общепрофессиональные компетенции:

– **ОПК-1** - способность анализировать физические явления и процессы для решения профессиональных задач.

В результате освоения данной компетенции студент должен:

Знать:

– особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности.

Уметь:

– применять полученную теоретическую базу для решения конкретных практических задач;

– грамотно работать с научной литературой с использованием новых информационных технологий;

Владеть:

– навыками анализа физических явлений и процессов для решения конкретных профессиональных задач.

Профессиональные компетенции:

–**ПК-18** - способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.

В результате освоения данной компетенции студент должен:

Знать:

– основные методы управления информационной безопасностью;

Уметь:

– разрабатывать предложения по совершенствованию системы управления информационной безопасностью;

Владеть:

– методами управления информационной безопасностью.

–**ПК-20** - способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач.

В результате освоения данной компетенции студент должен:

Знать:

– основные понятия информатики;

– типовые структуры и принципы организации компьютерных сетей;

Уметь:

– применять типовые программные средства для накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности;

Владеть:

– навыками применения технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности.

–ПК-25 - способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования.

В результате освоения данной компетенции студент должен:

Знать:

– лексический и грамматический минимум, необходимый для работы с иноязычными текстами профессиональной направленности и осуществления взаимодействия на иностранном языке;

Уметь:

– читать и переводить иноязычную литературу по профилю подготовки, взаимодействовать и общаться на иностранном языке;

Владеть:

– навыками поиска, сбора, обработки и систематизации научной информации отечественного и зарубежного характера.

–ПК-26 - способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать.

В результате освоения данной компетенции студент должен:

Знать:

– методы проведения экспериментов, методы обработки и анализа полученных данных;

Уметь:

– вести обработку экспериментальных данных с целью повышения точности конечного результата, нахождения различных статистик;

Владеть:

– навыками определения задач исследования, обработки полученных данных, анализа и интерпретирования.

–ПК-27 - способность готовить научные отчеты по результатам выполненных исследований.

В результате освоения данной компетенции студент должен:

Знать:

– способы и средства документирования;

– структуру документов и нормативные требования к их составлению и оформлению;

Уметь:

– квалифицированно исследовать состав документации предприятия (организации);

– руководствоваться нормативными документами по документоведению;

Владеть:

– навыками работы с нормативными правовыми актами;

– навыками работы с документами.

–ПК-28 - способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны.

В результате освоения данной компетенции студент должен:

Знать:

– основы технико-экономического анализа;

– научные основы, цели, принципы и методы управленческой деятельности;

Уметь:

– анализировать экономические показатели деятельности;

Владеть:

– навыками технико-экономического анализа и обоснования проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны.

–ПК-33 - способность проектировать, осуществлять, контролировать и оценивать ре-

зультаты образовательного процесса по дисциплинам (модулям) в области информационных технологий и информационной безопасности в организациях, осуществляющих образовательную деятельность.

В результате освоения данной компетенции студент должен:

Знать:

- иметь представление о роли сознания и бессознательного в регуляции поведения;
- иметь представление о мотивации и психической регуляции поведения и деятельности;
- основы социальной психологии, психологии межличностных отношений, психологии больших и малых групп;

Уметь:

- использовать полученные знания по психологии в своей практической деятельности;
- организовать индивидуальную и групповую деятельность людей с учетом их психологических особенностей;
- управлять мнением и настроением группы, регулировать взаимоотношения людей: убеждать, доказывать, внушать и побуждать людей к необходимым действиям в процессе профессионального общения и совместной деятельности;

Владеть:

- навыками выстраивания эффективных межличностных отношений.

Профессионально-специализированные компетенции:

–**ПСК-1** - способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации.

В результате освоения данной компетенции студент должен:

Знать:

- основные информационные технологии, используемые в автоматизированных системах;
- основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;

Уметь:

- администрировать подсистемы информационной безопасности автоматизированных систем;
- восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;
- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;

Владеть:

- навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;
- методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;
- навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

– навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

–**ПСК-2** - способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей.

В результате освоения данной компетенции студент должен:

Знать:

– принципы построения и функционирования, примеры реализаций современных систем управления базами данных;

– архитектуру систем баз данных;

Уметь:

– разрабатывать и администрировать базы данных;

– создавать объекты базы данных;

– применять средства обеспечения безопасности данных;

Владеть:

– навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;

– навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности.

–**ПСК-3** - способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.

В результате освоения данной компетенции студент должен:

Знать:

– способы повышения надежности систем;

Уметь:

– выбирать и оценивать различные структуры систем с точки зрения надежности;

Владеть:

– способностью планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.

–**ПСК-4** - способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

В результате освоения данной компетенции студент должен:

Знать:

– основы системного программирования, объектно-ориентированного подхода к программированию, технологии разработки алгоритмов и программ;

– архитектуру, принципы построения компьютеров, принципы построения операционных систем и особенностей их применения, аппаратно-программных средств диагностики компьютеров;

Уметь:

– реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;

Владеть:

– навыками разработки аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

3. Место НИР в структуре ОПОП подготовки специалиста

Содержание НИР является логическим продолжением разделов основной образовательной программы (ООП):

- информационные технологии;
- теория информационной безопасности и методология защиты информации;
- искусственный интеллект в системах защиты информации;
- нейросетевые технологии обработки информации;
- программно-аппаратная защита информации;
- инженерно-техническая защита информации.

и др.

и служит основой для последующего изучения разделов ООП:

- комплексная система защиты информации на предприятии;
- проектирование защищенных компьютерных систем;
- администрирование компьютерных систем;

прохождения производственной практики, а также формирования профессиональной компетентности в профессиональной области научно-исследовательской деятельности в области защиты информации.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), сформировавшего данную компетенцию
1	Способность понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы	ОК-1	базовый	Философия, учебная практика, производственная практика
2	Способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии	ОК-7	базовый	Логика, производственная практика
3	Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	ОК-12	базовый	Информатика и информационные технологии в правоохранительной деятельности. Часть 1, информатика и информационные технологии в правоохранительной деятельности. Часть 2, средства вычислительной техники, языки программирования и основы алгоритмизации, технологии и методы программирования, системы и сети передачи данных, специальные информационные правовые системы, специальные информационные технологии в правоохранительной деятельности, нейросетевые технологии обработки информации, информационные технологии, телекоммуникационные технологии, компьютерная графика, безопасность систем баз данных, учебная практика, производственная практика, информационно-аналитическое обеспечение правоохранительной деятельности, искусственный интеллект в системах защиты информации, телевизионные системы контроля, системы видеонаблюдения.

4	Способность анализировать физические явления и процессы для решения профессиональных задач	ОПК-1	базовый	Математика, основы теории надежности, физика1, физика 2 , физические основы защиты информации, математические основы обработки информации, методы оптимизации, элементы математической логики, языки программирования и основы алгоритмизации, технологии и методы программирования, теория информационной безопасности и методология защиты информации, криптографическая защита информации, противодействие информационной разведке, основы криминалистики, безопасность критически важных информационных систем, теория принятия решений в системах защиты информации, модели и мет принятия решений в системах защиты информации оды, основы теории надежности, контроль и диагностика технических средств защиты информации, учебная практика, производственная практика, криминология, экономическая безопасность.
5	Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации	ПК-18	базовый	Управление информационной безопасностью, производственная практика
6	Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	ПК-20	базовый	Информатика и информационные технологии в правоохранительной деятельности. Часть 1, информатика и информационные технологии в правоохранительной деятельности. Часть 2, математические основы обработки информации, элементы математической логики, базы данных, средства вычислительной техники, системы и сети передачи данных, специальные правовые информационные системы, искусственный интеллект в системах защиты информации, нейросетевые технологии обработки информации, информационные технологии, телекоммуникационные технологии, безопасность систем баз данных, учебная практика, производственная практика, информационно-аналитическое обеспечение правоохранительной деятельности.
7	Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования	ПК-25	базовый	
8	Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты	ПК-26	базовый	Математические основы обработки информации, теоретические основы электротехники, основы радиоэлектроники, основы электро-; радиоизмерений

9	Способность готовить научные отчеты по результатам выполненных исследований	ПК-27	базовый	Документоведение
10	Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	ПК-28	базовый	Экономика, управление информационной безопасностью, производственная практика, экономика защиты информации.
11	Способность проектировать, осуществлять, контролировать и оценивать результаты образовательного процесса по дисциплинам (модулям) в области информационных технологий и информационной безопасности в организациях, осуществляющих образовательную деятельность	ПК-33	базовый	Психология и педагогики, производственная практика
12	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ПСК-1	базовый	Системы и сети передачи данных, специальные информационные технологии в правоохранительной деятельности, искусственный интеллект в системах защиты информации, нейросетевые технологии обработки информации, защита информационных процессов в компьютерных системах, телекоммуникационные технологии, безопасность систем баз данных, производственная практика
13	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	ПСК-2	базовый	Системы и сети передачи данных, безопасность систем баз данных, производственная практика, администрирование компьютерных сетей.
14	Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	ПСК-3	базовый	Безопасность критически важных информационных систем, основы теории надежности, контроль и диагностика технических средств защиты информации, производственная практика
15	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	ПСК-4	базовый	Языки программирования и основы алгоритмизации, технологии и методы программирования, организация ЭВМ и систем, производственная практика

Исходящие компетенции

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), сформировавшего данную компетенцию
1	Способность понимать и анализировать мировоззренческие, социально и лично значимые философские проблемы	ОК-1	повышенный	Преддипломная практика, государственная итоговая аттестация
2	Способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии	ОК-7	повышенный	Преддипломная практика, государственная итоговая аттестация
3	Способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	ОК-12	повышенный	Преддипломная практика, государственная итоговая аттестация
4	Способность анализировать физические явления и процессы для решения профессиональных задач	ОПК-1	повышенный	Производственная практика, преддипломная практика, государственная итоговая аттестация.
5	Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации	ПК-18	повышенный	Преддипломная практика, государственная итоговая аттестация
6	Способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач	ПК-20	повышенный	Преддипломная практика, государственная итоговая аттестация
7	Способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования	ПК-25	повышенный	Преддипломная практика, государственная итоговая аттестация
8	Способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать результаты	ПК-26	повышенный	Преддипломная практика, государственная итоговая аттестация

9	Способность готовить научные отчеты по результатам выполненных исследований	ПК-27	повышенный	Преддипломная практика, государственная итоговая аттестация
10	Способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны	ПК-28	повышенный	Преддипломная практика, государственная итоговая аттестация
11	Способность проектировать, осуществлять, контролировать и оценивать результаты образовательного процесса по дисциплинам (модулям) в области информационных технологий и информационной безопасности в организациях, осуществляющих образовательную деятельность	ПК-33	повышенный	Преддипломная практика, государственная итоговая аттестация
12	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ПСК-1	повышенный	Проектирование защищенных компьютерных систем, преддипломная практика, государственная итоговая аттестация
13	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	ПСК-2	повышенный	Преддипломная практика, государственная итоговая аттестация
14	Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	ПСК-3	повышенный	Преддипломная практика, государственная итоговая аттестация
15	Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	ПСК-4	повышенный	Проектирование защищенных компьютерных систем, преддипломная практика, государственная итоговая аттестация

4. Структура и содержание НИР

4.1 Структура НИР

Общая трудоемкость НИР составляет 3 зачетные единицы (108 часов).

№ раздела	Наименование раздела НИР	Виды учебной нагрузки и их трудоемкость, часы		
		Индивидуальное задание	Коллективное задание	Всего часов
1	Планирование НИР (ознакомление с тематикой исследовательских работ, выбор темы исследования, анализ литературных источников, написание реферата с обзором исследовательских работ по избранной теме)	30		30
2	Проведение научно-исследовательских работ в соответствии с индивидуальным планом, в частности проведение математического моделирования, экспериментальных исследований	60		60
3	Оформление отчетных материалов, электронной презентации по результатам НИР	10		10
4	Защита отчета по НИР, представление результатов на научно-технических семинарах и конференциях, публикация в научных изданиях	8		8
Итого		108		108

4.2. Содержание НИР

Индивидуальное задание – 108 часов.

а) Выполнение индивидуального задания имеет своей целью формирование:

представлений:

- о принципах и технологиях, методах и средствах самоорганизации и самообразования;
- об основах и структуре самостоятельной работы;
- о перечне источников научно-технической литературы, нормативных и методических материалов по защите информации;
- об особенностях физических эффектов и явлений, используемых для обеспечения информационной безопасности;
- о принципах организации информационных систем в соответствии с требованиями по защите информации;
- о средствах защиты от несанкционированного доступа;
- о применении межсетевых экранов;
- о средствах контроля контента;
- о средствах анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях;
- о порядке оформления научно-технических отчетов, обзоров, подготовки публикации по результатам выполненных исследований;
- о состоянии законодательной базы и стандарты в области информационной безопасности.

умений:

- организовывать свой умственный труд;
 - пользоваться нормативными документами по защите информации;
 - проводить поиск и критический анализ литературы по необходимому научному направлению;
 - анализировать, оформлять и представлять полученные результаты работы;
 - применять методы математического планирования и моделирования для проведения исследовательских работ;
 - анализировать и оценивать угрозы информационной безопасности объекта;
 - составлять отчетность по проведенной работе;
 - проводить патентные исследования;
- навыков:
- организации и выполнения научно-исследовательских работ;
 - работы с нормативными правовыми актами;
 - поиска нормативной правовой информации необходимой для профессиональной деятельности;
 - подбора и использования научно-технической литературы, нормативных и методических материалов по информационной безопасности для защиты информации на различных объектах информатизации;
 - проведения физического эксперимента и обработки его результатов;
 - экспериментальной оценки защищенности объектов информатизации по заданным методикам технологии обработки результатов, оценки погрешности и достоверности результатов измерений;
 - выявления угроз безопасности автоматизированным системам;
 - составления научно-технических отчетов, статей, презентаций.
- б) данный вид занятий направлен на формирование следующих компетенций:
- **ОК-1** - способность понимать и анализировать мировоззренческие, социально и лично значимые философские проблемы.
 - **ОК-7** - способность к логическому мышлению, аргументировано и ясно строить устную и письменную речь, вести полемику и дискуссии.
 - **ОК-12** - способность работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.
 - **ОПК-1** - способность анализировать физические явления и процессы для решения профессиональных задач.
 - **ПК-18** - способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.
 - **ПК-20** - способность применять технологии получения, накопления, хранения, обработки, анализа, интерпретации и использования информации в ходе профессиональной деятельности, работать с различными источниками информации, информационными ресурсами и технологиями; проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач.
 - **ПК-25** - способность осуществлять поиск, анализировать и систематизировать научную информацию, отечественный и зарубежный опыт по теме исследования.
 - **ПК-26** - способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные данные, анализировать и интерпретировать.
 - **ПК-27** - способность готовить научные отчеты по результатам выполненных исследований.
 - **ПК-28** - способность выполнять предварительный технико-экономический анализ и обоснование проектных решений по созданию систем обеспечения безопасности информации и защиты государственной тайны.

–**ПК-33** - способность проектировать, осуществлять, контролировать и оценивать результаты образовательного процесса по дисциплинам (модулям) в области информационных технологий и информационной безопасности в организациях, осуществляющих образовательную деятельность.

–**ПСК-1** - способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации.

–**ПСК-2** - способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей.

–**ПСК-3** - способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации.

–**ПСК-4** - способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

в) формы проведения НИР:

- выполнение задания научного руководителя в соответствии с утвержденным индивидуальным планом НИР;
- участие в научно-исследовательских семинарах;
- подготовка докладов и выступлений на научных конференциях, семинарах;
- участие в конкурсах научно-исследовательских работ;
- подготовка и публикация научных статей;
- участие в научно-исследовательской работе кафедры.

г) перечень выполняемых работ и их содержание:

№ п/п	Объем, часов	Номер раздела НИР	Наименование этапа НИР	Содержание (раскрываемые вопросы)
1	4	1	Ознакомление с тематикой исследовательских работ	Изучение материалов о проведенных современных исследований в сфере защиты информации. Анализ изученного материала.
2	4	1	Выбор темы исследования	Выбор направления исследования. Поиск подходящей информации, касающейся данной тематики. Оценка возможность реализации исследования на практике в своём научно-исследовательском проекте
3	10	1	Анализ литературных источников	Ознакомление с литературой по выбранной теме. Поиск новейших сведений, источников. Анализ достоверности найденных источников.
4	12	1	Написание реферата с обзором исследовательских работ по избранной теме	Постановка цели и задачи написания реферата. Построение плана реферата. Сбор необходимого материала. Обработка собранного материала. Оформление реферата.
5	30	2	Математическое моделирование	Постановка задачи. Разработка математической модели. Подбор параметров модели. Анализ исходных данных.

6	30	2	Экспериментальные исследования	Планирование эксперимента. Проведения эксперимента. Оценка полученных результатов экспериментов.
7	6	3	Оформление отчетных материалов	Систематизация результатов эксперимента. Подготовка отчета.
8	4	3	Оформление электронной презентации	Выделение основной информации из отчетных материалов. Систематизация результатов эксперимента в форме схем, таблиц и моделей. Подготовка электронной презентации.
9	4	4	Защита отчета по НИР	Представление отчетных материалов о результатах эксперимента. Проверка теоретических знаний в ходе беседы.
10	6	4	Представление результатов на научно-технических семинарах и конференциях	Выступление с демонстрацией презентации. Представление знаний по проведенным экспериментам.

5. Место, сроки и формы проведения НИР

Учебным планом подготовки предусмотрена НИР (V курс, 10 семестр) – выделенная.

Научно-исследовательская работа студентов, обучающихся по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», проводится в учебных и учебно-научных лабораториях кафедры вычислительной техники и защиты информации.

Местом прохождения НИР могут также выступать предприятия и учреждения, осуществляющие инновационную или научно-исследовательскую деятельность. Как правило, такие предприятия являются базой прохождения различных видов практик. Подразделения предприятий, в которых студенты будут осуществлять НИР, должны соответствовать профилю подготовки обучающегося, располагать высококвалифицированными кадрами, необходимой материально-технической и информационной базой, должны быть закреплены приказом по университету и иметь, как правило, договор с университетом о прохождении практики.

К числу таких предприятий, в частности, относятся:

- ЗАО Республиканский центр защиты информации, г. Уфа;
- ЗАО Центр системных исследований "Интегро", г. Уфа;
- Компания «Фродекс».

Научно-исследовательская работа осуществляется под руководством ведущих преподавателей кафедры.

6. Формы аттестации

Контроль прохождения НИР проводится в соответствии с положением о проведении текущего контроля успеваемости и промежуточной аттестации студентов. (Приказ по ФГБОУ ВПО УГАТУ №299-О от 10.03.2015 г.)

Текущий контроль студентов проводится в дискретные временные интервалы руководителем НИР в следующих формах:

- выполнение индивидуальных заданий;
- формирование элементов отчета по НИР.

Контроль по завершении НИР проводится в следующей форме:

- сформированный отчет по НИР;
- защита отчета по НИР перед руководителем НИР в виде устного доклада о результатах

НИР

Отдельно оцениваются личностные качества студента (аккуратность, организованность, исполнительность, инициативность и др.).

По результатам выполнения индивидуального плана НИР на основании представленного отчета научным руководителем проводится аттестация студента в форме дифференцированного зачета в 10 семестре.

При аттестации могут быть учтены также следующие показатели результативности работы

- доклады на конференциях, публикации;
- участие в конкурсах, выставках, олимпиадах и др.;
- заявки на объекты интеллектуальной собственности;
- участие в подготовке и проведении организационно-массовых мероприятий по НИР
- публикации в научных изданиях.

Фонды оценочных средств, включают типовые, индивидуальные и коллективные задания, формы внешнего, внутреннего оценивания и самооценки (для включения в отчет о НИР), позволяющие оценить результаты обучения по НИР.

№ п/п	Контролируемые разделы	Код контролируемой компетенции (или ее части)	Уровень освоения, определяемый этапом формирования компетенции	Наименование оценочного средства
1	Планирование НИР (ознакомление с тематикой исследовательских работ, выбор темы исследования, анализ литературных источников, написание реферата с обзором исследовательских работ по избранной теме)	ОК-1	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ОК-12	повышенный	ИЗ, отчет по НИР, зачет по НИР
2	Проведение научно-исследовательских работ в соответствии с индивидуальным планом, в частности проведение математического моделирования, экспериментальных исследований	ПК-18	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПК-28	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПК-33	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПСК-2	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПСК-3	повышенный	ИЗ, отчет по НИР, зачет по НИР
3	Оформление отчетных материалов, электронной презентации по результатам НИР	ПСК-1	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПСК-3	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПК-27	повышенный	ИЗ, отчет по НИР, зачет по НИР
4	Защита отчета по НИР, представление результатов на научно-технических семинарах и конференциях, публикация в научных изданиях	ОК-7	повышенный	ИЗ, отчет по НИР, зачет по НИР

Комплект оценочных материалов:

Требования к отчету по НИР

Отчет по НИР – научно-технический документ, который содержит систематизированные данные о научно-исследовательской работе, описывает состояние научно-технической проблемы, процесс и/или результаты научного исследования.

Отчет по НИР составляется и предоставляется студентом не позднее последнего дня проведения НИР в 10 семестре. Отчет по НИР должен содержать результаты всех научно-исследовательских работ, проведенных в рамках выполнения индивидуальных в соответствии с поставленной темой исследования.

Отчет по НИР должен быть оформлен согласно ГОСТ 7.32 – 2001 «Отчет о научно-исследовательской работе. Структура и правила оформления». Структурными элементами отчета по НИР являются:

- титульный лист;
- содержание;
- нормативные ссылки;
- обозначения и сокращения;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения.

Титульный лист является первой страницей отчета по НИР и служит источником информации, необходимой для обработки отчета и идентификации автора отчета.

Введение должно содержать основание и исходные данные для разработки темы исследования, обоснование о необходимости проведения НИР; показаны актуальность и новизна темы исследований, связь представленной работы с другими научно-исследовательскими работами.

В основной части отчета приводятся данные, отражающие сущность, методику и основные результаты выполненной НИР. Основная часть отчета может содержать:

а) выбор направления исследований, включающий обоснование направления исследования, методы решения задач и их сравнительную оценку, описание выбранной общей методики проведения НИР;

б) процесс теоретических и (или) экспериментальных исследований, включая определение характера и содержания теоретических исследований, методы исследований, методы расчета, обоснование необходимости проведения экспериментальных работ, принципы действия разработанных объектов, их характеристики;

в) обобщение и оценку результатов исследований, включающих оценку полноты решения поставленной задачи и предложения по дальнейшим направлениям работ, оценку достоверности полученных результатов и их сравнение с аналогичными результатами отечественных и зарубежных работ, обоснование необходимости проведения дополнительных исследований, отрицательные результаты, приводящие к необходимости прекращения дальнейших исследований.

Заключение должно содержать:

- краткие выводы по результатам выполнения НИР в семестре;
- оценку полноты решений поставленных задач.

А также может содержать:

- разработку рекомендаций и исходных данных по конкретному использованию результатов НИР;
- оценку технико-экономической эффективности внедрения;
- оценку научно-технического уровня выполненной НИР в сравнении с лучшими достижениями в данной области.

В приложения рекомендуется включать материалы, связанные с выполненной НИР, которые по каким-либо причинам не могут быть включены в основную часть. В приложения могут быть включены:

- промежуточные математические доказательства, формулы и расчеты;
- таблицы вспомогательных цифровых данных;
- протоколы испытаний;
- описание аппаратуры и приборов, применяемых при проведении экспериментов, измерений и испытаний;
- заключение метрологической экспертизы;
- инструкции, методики, разработанные в процессе выполнения НИР;
- иллюстрации вспомогательного характера;
- копии технического задания на НИР, программы работ, договора или другого исходного документа для выполнения НИР;
- акты внедрения результатов НИР и др.

Вопросы к зачёту:

- 1) организация научно-исследовательской работы в России;
- 2) управление в сфере науки;
- 3) научно-исследовательская работа;
- 4) интеллектуальная деятельность;
- 5) понятие науки и классификация наук;
- 6) понятие научного исследования;
- 7) научная проблема;
- 8) методология научных исследований;
- 9) понятия метода и методологии научных исследований;
- 10) этапы научно-исследовательской работы;
- 11) подготовительный этап научно-исследовательской работы;
- 12) методологические требования к заглавию научной работы;
- 13) методологические требования к содержанию научной работы;
- 14) планирование научно-исследовательской работы;
- 15) сбор научной информации;
- 16) основные источники научной информации;
- 17) изучение литературы;
- 18) оформление библиографического аппарата;
- 19) требования к печатанию рукописи;
- 20) виды научных публикаций;
- 21) особенности подготовки докладов;
- 22) особенности подготовки отчетных материалов по результатам исследований;
- 23) особенности подготовки презентаций для научных докладов.

При реализации научно-исследовательской работы используется балльно-рейтинговая оценка освоения компетенций. Согласно Положению о модульно-рейтинговой системе подготовки студентов ФГБОУ ВПО УГАТУ №689-О от 04.06.12 максимальная сумма баллов за научно-исследовательскую работу устанавливается в 100 баллов, из которой:

- 50 баллов отводятся на контроль хода проведения научно-исследовательской работы;
- 50 баллов отводится на зачет.

Руководитель НИР суммирует баллы, полученные студентом за время ее проведения и при промежуточном контроле, после чего выставляет оценку за НИР по шкале баллов в соответствии со шкалой:

Сумма баллов	Числовой эквивалент
91-100	отлично
74-90	хорошо
61-73	удовлетворительно
0-60	неудовлетворительно

Раздел	Балл за конкретное задание	Число заданий	Баллы	
			Максимальный	Минимальный
Текущий контроль				
Организация и проведение исследования по проблеме в рамках темы исследовательской работы, сбор данных и их интерпретация	15	1	15	0
Написание реферата по выбранной теме исследования	15	1	15	0
Поощрительные баллы				
Выступление на научной конференции по проблеме исследования или на научном семинаре	10	1	10	0
Рубежный контроль				
Формирование элементов отчета по научно-исследовательской работе	10	1	10	0
Зачет с оценкой				
Защита отчета о научно-исследовательской работе	50	1	50	0

Критерии оценки:

- оценка «отлично» выставляется студенту, который:
 - полностью выполнил программу НИР;
 - своевременно сдал отчет по НИР;
 - отчет по НИР полностью соответствует предъявленным требованиям;
 - в ходе защиты отчета по НИР представлено систематическое изложение теоретического вопроса, раскрывающее полно взаимосвязь основных понятий, полностью раскрыты результаты проведенного математического моделирования и экспериментальных исследований, грамотно сформулированы полученные результаты;
 - продемонстрировал отличные знания при ответе на вопросы в ходе зачета по НИР и защиты отчета по НИР;

- оценка «хорошо» выставляется студенту, который:
 - по большей части выполнил программу НИР;
 - своевременно сдал отчет по НИР;
 - к отчету по НИР имеются отдельные замечания;
 - в ходе защиты отчета по НИР представлено систематическое изложение теоретического материала, раскрыты, хотя и с отдельными замечаниями результаты проведенных научно-исследовательских работ, сформулированы полученные результаты;
 - продемонстрировал хорошие знания при ответе на вопросы в ходе зачета по НИР и защиты отчета по НИР.

- оценка «удовлетворительно» выставляется студенту, который:

- более чем на половину выполнил программу НИР;
- своевременно сдал отчет по НИР;
- к отчету по НИР имеются существенные замечания;
- имеются существенные замечания при ответе на вопросы в ходе зачета по НИР и защиты отчета по НИР.

- оценка «неудовлетворительно» выставляется студенту, который:

- не выполнил программу НИР;
- отчет по НИР сдан несвоевременно;
- отчет по НИР выполнен не полностью или не выполнен;
- имеются грубые ошибки при ответе на вопросы в ходе зачета по НИР и защиты отчета по НИР;

7. Учебно-методическое и информационное обеспечение НИР

7.1. Основная литература

1. Кузнецов, Игорь Николаевич. Основы научных исследований [Текст] : / И. Н. Кузнецов .— Москва : Дашков и К, 2014 .— 282 с. Доступ по логину и паролю из сети Интернет .— URL://e.lanbook.com/books/element.php.?pl1_id56264_

2. Кравченко, И. Н. Основы научных исследований [Электронный ресурс]: / Кравченко И.Н., Коломейченко А.В., Логачев В.Н., Тарасов В.А. — Москва : Лань, 2015.— Доступ по логину и паролю из сети Интернет .— ISBN 978-5-8114-1827-5 .— URL:http://e.lanbook.com/books/element.php?pl1_id=56165.

7.2. Дополнительная литература

1. Тихонов, В. А. Научные исследования: концептуальные, теоретические и практические аспекты / В. А. Тихонов, В. А. Ворона .— Москва : Горячая линия-Телеком, 2009 .— 296 с. — URL:http://www.library.ugatu.ac.ru/pdf/diplom/Tixonov_Nauch_issl_2009.pdf.

2. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : [учебное пособие для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника»] / В. Ф. Шаньгин .— Москва : ДМК ПРЕСС, 2012 .— 592 с. — Доступ по логину и паролю из сети УГАТУ .— ISBN 978-5-94074-637-9 .— URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=3032.

3. Мельников Д.А., Информационная безопасность открытых систем [учебник Для студентов государственных образовательных учреждений высшего профессионального образования, обучающихся по направлениям 230700 «Прикладная информатика», 090900 «Информационная безопасность» (ИБ) и 230100 «Информатика и вычислительная техника», а также специальностям 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» и 090305 «Информационно-аналитические системы безопасности»]-М: Издательство Флинта, 2014 -448с - Доступ по логину и паролю из сети УГАТУ https://e.lanbook.com/book/48368?category_pk=1545#authors

4. Гвоздев, В. Е. Словарь терминов в области программных проектов [Электронный ресурс] / В. Е. Гвоздев, А. Е. Колоденкова, О. Я. Бежаева ; УГАТУ .— Учебное электронное издание .— Уфа : УГАТУ, 2009 .— 1 электрон. опт. диск (CD-ROM).

7.3. Периодические издания

Журналы:

1. «Информационные технологии».
2. «Вопросы защиты информации» - [URL: http://i-vimi.ru](URL:http://i-vimi.ru).
3. «Защита информации. INSIDE».
4. «Безопасность информационных технологий»

7.4. Интернет-ресурсы

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

7.5. Программное обеспечение современных информационно-коммуникационных технологий

При выполнении НИР могут использоваться следующие программные продукты:

- 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 Visio Pro (№ договора ЭА-269/0503-16, 50 компьютеров, на которые распространяется право пользования);
- Kaspersky Endpoint Security для бизнеса (лицензии 1055/0503-16, 500 users);
- DLP система Falcongaze (лицензионный договор 05/17/2016-1 от 17.05.2016 с ООО «Фалконгейз», 20 лицензий сроком на 3 года)
- Веб-сервер Apache (freeware)
- программное обеспечение СЗИ Secret Net 7 Клиент (автономный режим работы вариант). Лицензия WWIB-****-****-****-****-****-*00S от 16.01.2017 на 10 компьютеров. Бессрочно.
- программное обеспечение СЗИ «Secret Net LSP». Лицензия 1****А от 16.01.2017 на 10 компьютеров. Бессрочно.
- программное обеспечение Secret Net Studio 8. Комплекс «Максимальная защита» Лицензия 1*****С от 16.01.2017 на 10 компьютеров.
- обманная система Security Studio HoneyPot Manager (договор о сотрудничестве с ООО «Код безопасности»);
- средство защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальных инфраструктур на базе VMware vSphere и Microsoft Hyper-V Security Code VGate R2 Договор о сотрудничестве с ООО «Код безопасности») Лицензия 1****F.
- распределенный межсетевой экран для управления доступом внутри защищаемой сети Trust Access для защиты раб.станций Договор о сотрудничестве с ООО «Код безопасности» Лицензия WWIM-****-****-****-****-****-*00Q ;
- распределенный межсетевой экран для управления доступом внутри защищаемой сети Trust Access для защиты сервера Договор о сотрудничестве с ООО «Код безопасности» Лицензия WWIM-****-****-****-****-****-*00K;
- система защита информации на компьютерах, съемных носителях и внешних устройствах Infowatch Endpoint Security. Договор о сотрудничестве с ООО «Код безопасности» Лицензия WWIS-****-****-****-****-****-*000
- сервер безопасности Dallas Lock 8.0-С. Лицензионный сертификат 181**-****-*57 на 1 сервер. Бессрочно.
- сервер безопасности Dallas Lock 8.0-К. Лицензионный сертификат 181**-****-*13 на один сервер. Бессрочно.
- программное обеспечение Dallas Lock Linux. Лицензионный сертификат 181**-****-*99 на 15 рабочих мест. Бессрочно.
- программное обеспечение Dallas Lock 8.0-К(СЗИ, НСД, СКН, МЭ, СОВ). Лицензионный сертификат 181**-*****33 на 15 рабочих мест. Бессрочно.
- программное обеспечение Dallas Lock 8.0-С(СЗИ, НСД, СКН, МЭ, СОВ). Лицензионный сертификат 181**-*****14 на 15 рабочих мест. Бессрочно.

- программное обеспечение Dallas Lock СЗВИ. Демо-версия, предоставлена разработчиком в соответствии с договором о сотрудничестве с ООО «Конфидент» от 17.11.2016.
- операционная система Astra Linux SE (Special Edition) РУСБ.10015-01 (программный продукт в формате BOX). Лицензионный договор РБТ-14/1318-01-ВУЗ. Бессрочно.
- DLP система «Контур информационной безопасности» SearchInform (Лицензионное соглашение с ООО «Новые поисковые технологии UEI-2349-87, 20 пользователей);
- SearchInform Event Manager. Лицензионный договор 1726811. Срок действия 3 года.
- DLP система Infowatch Traffic Monitor Enterprise Edition. Лицензионное соглашение 932-N-ИВ/2016. 50 лицензий. Договор о сотрудничестве с АО «Инфовотч» от 19.10.2016.
- система защита информации на компьютерах, съемных носителях и внешних устройствах Infowatch Endpoint Security. Соглашение о сотрудничестве 664-ИВ/2016 Лицензия для ФБГТУ ВО УГАТУ
- WAF Positive Technologies Application Firewall Education (лицензионный договор с ЗАО Позитив Технолоджис 72-16/EAF от 21.06.2016)
- сканер безопасности XSpider 7.8 Education. (лицензионный договор с ЗАО Позитив Технолоджис 71-16/EX от 21.06.2016)
- система комплексного анализа информационной безопасности MaxPatrol Education (лицензионный договор с ЗАО Позитив Технолоджис 70-16/EM от 21.06.2016)
- набор лабораторных и практических занятий фирмы Positive Technologies.
- операционная система Mandriva 2010. Бесплатное программное обеспечение
- операционная система OpenSuSe. Бесплатное программное обеспечение

8. Материально-техническое обеспечение НИР

8.1. В ходе НИР студентами используются аудитории 5-301 и 5-314, оснащенные презентационной техникой (проектором, экраном, ноутбуком), дисплейные классы кафедры ВТ и ЗИ, оснащенные пакетами общего назначения (текстовыми, графическими редакторами), специализированным ПО, указанным в п. 7.5, и имеющими выход в интернет.

8.2. Для проведения НИР по согласованию сторон могут использоваться материально-техническое обеспечение предприятий, с которыми кафедра проводит совместные научно-исследовательские работы

8.3. В процессе проведения НИР используются специализированные пакеты программ, практические работы и методическое обеспечение, предоставленные кафедре предприятия Российской Федерации в соответствии с договорами о сотрудничестве.

9. Реализация НИР лицами с ОВЗ

Выбор мест и способов прохождения НИР для обучающихся инвалидов и лиц с ОВЗ осуществляется с учетом требований их доступности, а также рекомендованных условий и видов труда. В таком случае требования к структуре и содержанию НИР адаптируются под конкретные ограничения возможностей здоровья обучающегося, и отражаются в индивидуальном задании на НИР.