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
"2" _____ 2016 г.

ПРОГРАММА
НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Уровень подготовки: высшее образование – бакалавриат

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Направленность подготовки (профиль)
Безопасность автоматизированных систем
(наименование профиля подготовки)

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Год начала подготовки – 2015

Уфа 2016

Программа научно-исследовательской работы / сост. В.Е. Кладов – Уфа: УГАТУ, 2016. - 26 с.

Программа НИР является приложением к Основной профессиональной образовательной программе высшего образования по направлению 10.03.01 «Информационная безопасность» и профилю «Безопасность автоматизированных систем».

Составитель _____ В.Е. Кладов
(подпись)
25.12.2016 г.

Программа одобрена на заседании научно-методического совета по УГСН 10.00.00 «Информационная безопасность»
"28" 12 2016г., протокол № 4

Председатель научно-методического совета
_____ Васильев В.И. 28.12.2016
личная подпись *расшифровка подписи* *дата*

Программа утверждена на заседании кафедры ВТ и ЗИ
"26" 12 2016г., протокол № 7

Заведующий кафедрой ВТ и ЗИ _____ Васильев В.И. 26.12.2016
личная подпись *расшифровка подписи* *дата*

Начальник ООПБС _____ Г.Т. Гарипова 29.12.2016
личная подпись *расшифровка подписи* *дата*

Содержание

1. Цели и задачи НИР
2. Требования к результатам НИР
3. Место НИР в структуре ОПОП подготовки бакалавра
4. Структура и содержание НИР
5. Место, сроки и формы проведения НИР
6. Формы контроля
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 направлению подготовки 10.03.01 «Информационная безопасность» в шестом семестре на третьем 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 защиты информации и обеспечения безопасности информационных технологий;
- разработка заданий, планов, программ проведения прикладных научных исследований и технических разработок;
- проведение экспериментов по заданным методикам;
- выполнение прикладных научных исследований, подготовка статей, отчетов, докладов на научно–практических семинарах и конференциях.

2. Требования к результатам НИР

Компетенция ОК-7 – способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности.

В результате освоения данной компетенции студент должен:

Знать:

- русский и иностранный языки в объеме, достаточном для устной и письменной коммуникации для решения задач межличностного и межкультурного взаимодействия.

Уметь:

- в устной и письменной формах решать задачи межличностного и межкультурного взаимодействия на русском и иностранном языках.

Владеть:

- устной и письменной формами русского и иностранного языков для решения задач межличностного и межкультурного взаимодействия.

Компетенция ОК-8 – способность к самоорганизации и самообразованию.

В результате освоения данной компетенции студент должен:

Знать:

- принципы и технологии, методы и средства самоорганизации и самообразования;
- основы и структуру самостоятельной работы.

Уметь:

- организовывать свой умственный труд.

Владеть:

- навыками организации и выполнения научно-исследовательских работ.

Компетенция 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:

- анализировать, оформлять и представлять полученные результаты работы.

Владеть:

- навыками проведения физического эксперимента и обработки его результатов.

Компетенция ОПК-2 – способность применять соответствующий математический аппарат для решения профессиональных задач.

В результате освоения данной компетенции студент должен:

Знать:

- основные понятия и методы информации математической логики и теории алгоритмов, теории информации и кодирования;

Уметь:

- применять методы математического планирования и моделирования для проведения исследовательских работ;

Владеть:

- владеть навыками экспериментальной оценки защищенности объектов информатизации по заданным методикам технологии обработки результатов, оценки погрешности и достоверности результатов измерений.

Компетенция ОПК-3 – способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач.

В результате освоения данной компетенции студент должен:

Знать:

- принципы построения систем и средств связи;
- методы анализа электрических цепей;
- принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них;
- основы схемотехники.

Уметь:

- применять на практике положения электротехники, электроники, схемотехники для решения профессиональных задач.

Владеть:

- навыками чтения электронных схем.

Компетенция ОПК-5 – способность использовать нормативные правовые акты в профессиональной деятельности.

В результате освоения данной компетенции студент должен:

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области.

Уметь:

- пользоваться нормативными документами по защите информации.

Владеть:

- навыками работы с нормативными правовыми актами;
- навыками поиска нормативной правовой информации необходимой для профессиональной деятельности;
- основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации.

Компетенция ОПК-7 – способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате освоения данной компетенции студент должен:

Знать:

- принципы организации информационных систем в соответствии с требованиями по защите информации;
- средства защиты от несанкционированного доступа,
- средства контроля контента,
- средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях.

Уметь:

- анализировать и оценивать угрозы информационной безопасности объекта.

Владеть:

- методами и средствами выявления угроз безопасности автоматизированным системам.
- методами анализа и формализации информационных процессов объекта и связей между ними;
- навыками работы с компьютером как средством защиты информации,
- навыками работы с информацией в глобальных компьютерных сетях.

Компетенция ПК-2 – способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

В результате освоения данной компетенции студент должен:

Знать:

- методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;
- современные средства разработки и анализа программного обеспечения на языках высокого уровня;
- аппаратные средства вычислительной техники;
- операционные системы персональных ЭВМ;
- основы администрирования вычислительных сетей.

Уметь:

- выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;
- составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные.

Владеть:

- навыками безопасного использования программных и инструментальных средств в профессиональной деятельности;
- навыками создания прикладного программного обеспечения;
- навыками работы с программно-техническими средствами диалога человека с профессионально-ориентированными информационными системами;
- основными принципами организации и взаимодействия программных компонент.

Компетенция ПК-4 – способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты.

В результате освоения данной компетенции студент должен:

Знать:

- принципы и методы организационной защиты информации;
- политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации.

Уметь:

- формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- реализовывать на практике принципы политики безопасности.

Владеть:

- навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
- навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации.

Компетенция ПК-7 – способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

В результате освоения данной компетенции студент должен:

Знать:

- методы проектирования защищенных компьютерных систем;
- подходы обоснования затрат на информационную безопасность;
- методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности.

Уметь:

- обосновывать принимаемые проектные решения;
- использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности;
- определять зависимость между затратами на ИБ и уровнем защищенности.

Владеть:

- основными методами, способами и средствами получения хранения, переработки и передачи информации;
- навыками определения затрат компании на ИБ.

Компетенция ПК-8 – способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.

В результате освоения данной компетенции студент должен:

Знать:

- порядок оформления научно-технических отчетов, обзоров, подготовки публикации по результатам выполненных исследований.

Уметь:

- составлять отчетность по проведенной работе.

Владеть:

- навыками составления научно-технических отчетов, статей, презентаций.

Компетенция ПК-9 – способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

В результате освоения данной компетенции студент должен:

Знать:

- перечень источников научно-технической литературы, нормативных и методических

материалов по защите информации.

Уметь:

- проводить поиск и критический анализ литературы по необходимому научному направлению.

Владеть:

- опытом подбора и использования научно-технической литературы, нормативных и методических материалов по информационной безопасности для защиты информации на различных объектах информатизации.

Компетенция ПК-10 – способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

В результате освоения данной компетенции студент должен:

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области.

Уметь:

- пользоваться нормативными документами по защите информации;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.

Владеть:

- навыками работы с нормативными правовыми актами;
- методами формирования требований по защите информации;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Компетенция ПК-11 – способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

В результате освоения данной компетенции студент должен:

Знать:

- основные принципы экспериментальных исследований;
- соотношение теоретического и экспериментального знания.

Уметь:

- проводить физические эксперименты и обрабатывать их результатов.

Владеть:

- методами количественного анализа процессов обработки, поиска и передачи информации;
- основными методами исследования функций и навыками формулирования и решения простейших задач об отыскании экстремума функции.

Компетенция ПК-12 – способность принимать участие в проведении экспериментальных исследований системы защиты информации.

В результате освоения данной компетенции студент должен:

Знать:

- теоретические основы научного исследования;
- основные принципы экспериментальных исследований;
- соотношение теоретического и экспериментального знания.

Уметь:

- проводить патентные исследования;

- ориентироваться в современной и вновь создаваемой технике с целью ее быстрого освоения, внедрения и эффективного использования в практической деятельности.

Владеть:

- навыками проведения физических экспериментов и обработки их результатов.

Компетенция ПК-13 – способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

В результате освоения данной компетенции студент должен:

Знать:

- общеметодологические принципы теории информационной безопасности;
- возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.
- состояние законодательной базы и стандарты в области информационной безопасности.

Уметь:

- обосновывать организационно-технические мероприятия по защите информации;
- использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.

Владеть:

- навыками выявления и устранения угроз информационной безопасности;
- навыками во внедрении, адаптации и настройке средств защиты прикладных ИС.

Компетенция 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:

- особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации.

Уметь:

- применять типовые проектные решения для создания защищенных информационных систем и технологий в профессиональной деятельности.

Владеть:

- навыками защиты информации в базах данных и сетях;
- навыками анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;
- навыками разработки комплекса мер для управления информационной безопасностью.

Компетенция 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:

- методы и средства управления защитой информации в операционных системах, базах данных и прикладных программах;
- настройки и конфигурирования программных средства борьбы со злонамеренным программным обеспечением.

Уметь:

- настраивать, конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, используемых в организации;
- настраивать антивирусные программы и другие средства борьбы с программными закладками.

Владеть:

- методами и инструментарием конфигурирования и настройки средств защиты информации в ОС, СУБД, прикладных системах.

Компетенция 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:

- теоретические основы оценки надежности и помехоустойчивости коммуникационного оборудования и аппаратуры обработки данных;
- критерии и меры надежности;
- возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации.

Уметь:

- рассчитывать характеристики надежности технических комплексов;
- обосновывать организационно-технические мероприятия по защите информации;
- использовать возможности и особенности организационных, аппаратных и программных средств защиты информации.

Владеть:

- навыками выявления и устранения угроз информационной безопасности;
- навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий.

3. Место НИР в структуре ОПОП подготовки бакалавра

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

- информационные технологии;
- организационное и правовое обеспечение информационной безопасности;
- искусственный интеллект в системах защиты информации;
- нейросетевые технологии обработки информации;
- программно-аппаратная защита информации;
- техническая защита информации;

и др.

и служит основой для последующего изучения разделов ООП:

- теория принятия решений в системах защиты информации;
- информационные технологии моделирования интеллектуальных систем;
- моделирование технических систем компьютерная техническая экспертиза;

и др.

прохождения производственной практики, а также формирования профессиональной компетентности в профессиональной области защиты информации.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), сформировавшего данную компетенцию
1	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	ОК-7	базовый	Культура делового человека, русский язык, иностранный язык, иностранный язык в профессиональной деятельности
2	Способность к самоорганизации и самообразованию	ОК-8	пороговый	Основы управленческой деятельности, Психология и педагогика, культура делового человека, учебная практика, физическая культура
3	Способность анализировать физические явления и процессы для решения профессиональных задач	ОПК-1	базовый	Физика, физические основы защиты информации, электротехника, электроника и схе-мотехника, учебная практика
4	Способность применять соответствующий математический аппарат для решения профессиональных задач	ОПК-2	базовый	Линейная алгебра и аналитическая геометрия, математический анализ, теория вероятностей и математическая статистика, криптографические методы защиты информации, методы оптимизации, математическая логика и теория алгоритмов, теория нечетких систем, математические основы теории надежности; теория информации
5	Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	ОПК-3	базовый	технические средства охраны, теория автоматов, организация ЭВМ и систем, электрорадиоизмерения, основы метрологии, электротехника, электротехника и схемотехника
6	Способность использовать нормативные правовые акты в профессиональной деятельности	ОПК-5	пороговый	Организационное и правовое обеспечение информационной безопасности
7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОПК-7	пороговый	Основы информационной безопасности, программно-аппаратные средства защиты информации
8	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2	пороговый	Информатика, языки программирования, технологии и методы программирования, математическая логика и теория алгоритмов, программно-аппаратные средства защиты информации, криптографические методы защиты информации, информационные технологии, телекоммуникационные технологии, организация ЭВМ и систем, компьютерная графика,Web-дизайн

9	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7	пороговый	Экономика, линейная алгебра и аналитическая геометрия, математический анализ, теория вероятностей и математическая статистика, дискретная математика, основы информационной безопасности, теория принятия решений, теория нечетких систем, методы оптимизации
10	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8	пороговый	Документоведение, защита и обработка документов ограниченного доступа
11	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9	базовый	Основы информационной безопасности, организационное и правовое обеспечение информационной безопасности, документоведение
12	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10	пороговый	Стандарты информационной безопасности и аудит
13	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11	базовый	Линейная алгебра и аналитическая геометрия, математический анализ, теория вероятностей и математическая статистика, дискретная математика
14	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12	базовый	Физические основы защиты информации, математические основы теории надежности, электрорадиоизмерения, основы метрологии
15	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13	пороговый	Организационное и правовое обеспечение информационной безопасности, техническая защита информации, технические средства охраны
16	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ПСК-1	пороговый	Сети и системы передачи информации, информационные технологии, телекоммуникационные технологии
17	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	ПСК-2	базовый	Программно-аппаратные средства защиты информации, сети и системы передачи информации

18	Способность планировать и организовывать комплекс мероприятий по защите информации связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	ПСК-3	пороговый	Математические основы теории надежности

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), сформировавшего данную компетенцию
1	Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	ОК-7	повышенный	Производственная практика, преддипломная практика, государственная итоговая аттестация
2	Способность к самоорганизации и самообразованию	ОК-8	базовый	Основы управленческой деятельности, производственная практика, преддипломная практика, государственная итоговая аттестация
3	Способность анализировать физические явления и процессы для решения профессиональных задач	ОПК-1	повышенный	Производственная практика, преддипломная практика, государственная итоговая аттестация
4	Способность применять соответствующий математический аппарат для решения профессиональных задач	ОПК-2	повышенный	Теория принятия решений в системах защиты информации, информационные технологии моделирования интеллектуальных систем, моделирование технических систем, производственная практика, преддипломная практика, государственная итоговая аттестация
5	Способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач	ОПК-3	повышенный	Производственная практика, преддипломная практика, государственная итоговая аттестация
6	Способность использовать нормативные правовые акты в профессиональной деятельности	ОПК-5	базовый	Информационное право, право интеллектуальной собственности, компьютерная техническая экспертиза, производственная практика, преддипломная практика, государственная итоговая аттестация
7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОПК-7	базовый	Безопасность критически важных информационных систем, комплексная система защиты информации на предприятии, управление информационной безопасностью, защита информационных процессов в компьютерных системах, проектирование защищенных компьютерных систем, производственная практика, преддипломная практика, государственная итоговая аттестация
8	Способность применять про-	ПК-2	базовый	Защита информационных процессов

	граммные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач			в компьютерных системах, компьютерно-техническая экспертиза, методы искусственного интеллекта, информационные технологии моделирования интеллектуальных систем, современные банковские технологии, безопасность систем электронной торговли, производственная практика, преддипломная практика, государственная итоговая аттестация
9	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	ПК-4	базовый	Управление информационной безопасностью, комплексная система защиты информации на предприятии, современные банковские технологии, безопасность систем электронной торговли, производственная практика, преддипломная практика, государственная итоговая аттестация
10	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ПК-7	базовый	Экономика защиты информации, проектирование защищенных компьютерных систем, моделирование технических систем, имитационное моделирование, теория принятия решений в системах защиты информации, модели и методы принятия решений в системах защиты информации, производственная практика, преддипломная практика, государственная итоговая аттестация
11	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8	базовый	Проектирование защищенных компьютерных систем, производственная практика, преддипломная практика, государственная итоговая аттестация
12	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ПК-9	повышенный	Производственная практика, преддипломная практика, государственная итоговая аттестация
13	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10	базовый	Преддипломная практика, государственная итоговая аттестация
14	Способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11	повышенный	Завершается формирование компетенции
15	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12	повышенный	Катастрофоустойчивость информационных систем, безопасность критически важных информационных систем, преддипломная практика, государственная итоговая аттестация

16	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13	базовый	Основы управленческой деятельности, управление информационной безопасностью, комплексная система защиты информации на предприятии, информационное право, право интеллектуальной собственности, производственная практика, преддипломная практика, государственная итоговая аттестация
17	Способность учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	ПСК-1	базовый	Защита информационных процессов в компьютерных системах, методы искусственного интеллекта, информационные технологии моделирования интеллектуальных систем, современные банковские технологии, безопасность систем электронной торговли, преддипломная практика, государственная итоговая аттестация
18	Способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	ПСК-2	повышенный	Защита информационных процессов в компьютерных системах, преддипломная практика, государственная итоговая аттестация
19	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	Катастрофоустойчивость информационных систем, безопасность критически важных информационных 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 соответствие 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-7 – способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;
- ОК-8 – способность к самоорганизации и самообразованию;
- ОПК-1 – способность анализировать физические явления и процессы для решения профессиональных задач;
- ОПК-2 – способность применять соответствующий математический аппарат для решения профессиональных задач;
- ОПК-3 – способность применять положения электротехники, электроники и схемотехники для решения профессиональных задач;
- ОПК-5 – способность использовать нормативные правовые акты в профессиональной деятельности;
- ОПК-7 – способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
- ПК-2 – способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
- ПК-4 – способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- ПК-7 – способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- ПК-8 – способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;
- ПК-9 – способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
- ПК-10 – способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- ПК-11 – способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов;
- ПК-12 – способность принимать участие в проведении экспериментальных исследований системы защиты информации;
- ПК-13 – способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации;
- 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.

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 (III курс, 6 семестр) – выделенная.

Научно-исследовательская работа студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», 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 конце 6 семестра.

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)	ОПК-5	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПК-9	повышенный	ИЗ, отчет по НИР, зачет по НИР
2	Проведение научно-исследовательских работ в соответствие с индивидуальным планом, в частности проведение математического моделирования, экспериментальных исследований	ОПК-2	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ОПК-7	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПК-7	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПСК-1	базовый	ИЗ, отчет по НИР, зачет по НИР
		ОК-8	базовый	ИЗ, отчет по НИР, зачет по НИР
		ОПК-1	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ОПК-3	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПК-2	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПК-4	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПК-11	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПК-12	повышенный	ИЗ, отчет по НИР, зачет по НИР
		ПК-13	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПСК-2	повышенный	ИЗ, отчет по НИР, зачет по НИР
3	Оформление отчетных материалов, электронной презентации по результатам НИР	ПК-10	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПСК-3	базовый	ИЗ, отчет по НИР, зачет по НИР
		ПК-8	базовый	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 6 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	10	1	10	0
Написание реферата по выбранной теме исследования	20	1	20	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 НИРl
- 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 полученными 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. Власов К. П**.** Методы исследований и организация экспериментов / К. П. Власов [и др.] ; под ред. К. П. Власова .— 2-е изд., перераб. и доп. — Харьков : Гуманитарный Центр, 2013 .— 412 с. : ил. ; 21 см .— Библиогр.: с. 400-402 (33 назв.) .— ISBN 978-617-7022-11-3 .— <URL:http://www.library.ugatu.ac.ru/pdf/teach/Metody_issled_Vlasov_2izd_2013.pdf>.

7.3. Периодические издания

Журналы:

1. «Информационные технологии».
2. «Вопросы защиты информации» - <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 обеспчение СЗИ «Secret Net LSP». Лицензия 1****A от 16.01.2017 на 10 компьютеров. Бессрочно.
- программное обеспечение Secret Net Studio 8. Комплекс «Максимальная защита» Лицензия 1*****C 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-C. Лицензионный сертификат 181**-****-*57 на 1 сервер. Бессрочно.
- сервер безопасности Dallas Lock 8.0-K. 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-K(СЗИ, НСД, СКН, МЭ, СОВ). Лицензионный сертификат 181**-****33 на 15 рабочих мест. Бессрочно.
- программное обеспечение Dallas Lock 8.0-C(СЗИ, НСД, СКН, МЭ, СОВ). Лицензионный сертификат 181**-****14 на 15 рабочих мест.Бессрочно.
- программное обеспечение Dallas Lock СЗВИ. Демо-версия, предоставлена разработчиком в соответствие 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.