УТВЕРЖДЕНО
Решением Ученого совета факультета
математики, информационных и авиационных технологий
от «27» 06 2019 г., протокол № 5/19
Председатель Восиков М.Н.
«27» 06 2019 г.

ПРОГРАММА ПРАКТИКИ

Практика	Вид практики: производственная Тип практики: научно-исследовательская работа
Способ и форма проведения	Способ проведения практики: стационарная Форма проведения: непрерывная
Факультет	Математики, информационных и авиационных технологий (ФМИАТ)
Кафедра	Информационной безопасности и теории управления (ИБиТУ)
Курс	6

Специальность: 10.05.01 «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Форма обучения: очная

Дата введения в учебный процесс УлГУ « 01 » 09 2018 г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.
Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Рацеев Сергей Михайлович	ИБиТУ	профессор, д.ф.-м.н., доцент

СОГЛАСОВАНО:
Заведующий кафедрой _____ / А.С. Андреев / (Подпись) (Ф.И.О.) « 13 » 06 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Цели прохождения практики:

- закрепление и углубление теоретической подготовки студентов;
- приобретение навыков научно-исследовательской работы;
- расширение и углубление практических умений и навыков по дисциплинам, формирующим будущую профессию;
- овладение практическими навыками в области организации и управления при проведении исследований.

Задачи прохождения практики:

- приобретение студентами навыков сбора, обработки, анализа и систематизации научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности;
- участие в теоретических и экспериментальных исследованиях по оценке защищенности автоматизированных систем;
- изучение и обобщение опыта работы предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;
- разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к блоку Б2 образовательной программы и проводится в 11-м семестре студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного выполнения научно-исследовательской работы необходимы компетенции, сформированные в ходе изучения дисциплин «Криптографические методы защиты информации», «Основы информационной безопасности», «Операционные системы», «Компьютерные сети», «Модели безопасности компьютерных систем», «Защита программ и данных», «Техническая защита информации», «Основы построения защищенных компьютерных сетей», «Защита в операционных системах», «Криптографические протоколы».

НИР предполагает исследовательскую работу, направленную на развитие у студентов способности к самостоятельным теоретическим и практическим суждениям и выводам, умений объективной оценки научной информации, свободы научного поиска и стремления к применению научных знаний в образовательной деятельности. НИР предполагает индивидуальную программу, направленную на выполнение конкретного задания.

Прохождение практики (НИР) предшествует прохождению преддипломной практики, написанию и защите выпускной квалификационной работы в соответствии с выбранным направлением научного исследования.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ СТУДЕНТОВ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОПОП ВО

В совокупности с дисциплинами базовой и вариативной части математического и

естественнонаучного цикла ФГОС ВО научно-исследовательская работа направлена на формирование компетенций по специальности «Компьютерная безопасность».

Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
ОК-5 – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности; основные термины по проблематике информационной безопасности; роль и место информационной безопасности в системе национальной безопасности страны; угрозы информационной безопасности государства; содержание информационной войны, методы и средства ее ведения; Уметь: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам Владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
ОК-7 – способностью 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	Знать: свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления Уметь: квалифицированно исследовать состав документации предприятии (организации) Владеть: методами формирования требований по защите информации
ОК-8 – способностью к самоорганизации и самообразованию	Знать: основные методы управления информационной безопасностью Уметь: оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем Владеть: методами управления информационной безопасностью информационных систем; методами оценки информационных рисков
ОПК-2 – способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать: основные понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основы теории групп и теории групп подстановок; свойства векторных пространств; свойства кольца многочленов; основные понятия и задачи векторной алгебры и аналитической геометрии; основные понятия и методы дискретной математики; основные понятия математической логики и теории алгоритмов; абстрактный интеграл Лебега и его основные свойства; основные положения теории пределов функций, теории рядов; основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; понятие меры, измеримые функции и их свойства; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; основные понятия и методы теории вероятностей, математической статистики и теории случайных процессов;

	основные понятия и методы теории информации; Уметь: решать основные задачи векторной алгебры и аналитической геометрии; решать системы линейных уравнений над полями; решать основные задачи векторной алгебры и аналитической геометрии; использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; находить представление и исследовать свойства булевых и многозначных функций формулами в различных базисах; определять возможности применения методов математического анализа; решать основные задачи теории пределов функций, дифференцирования, интегрирования и разложения функций в ряды; проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; применять стандартные методы и модели к решению теоретико-вероятностных и статистических задач; вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); Владеть: навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения систем линейных уравнений над полем и кольцом вычетов; навыками решения стандартных задач в векторных пространствах; навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения задач дискретной математики; навыками использования языка математической логики; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов. основами построения математических моделей текстовой информации и моделей систем передачи информации;
ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации	Знать: основные понятия информатики; формы и способы представления данных в персональном компьютере; Уметь: использовать расчетные формулы, таблицы, графики, компьютерные программы при решении математических задач; пользоваться сетевыми средствами и внешними носителями информации для обмена данными; применять персональные компьютеры для обработки различных видов информации; Владеть: навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач; навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов)
ПК-1 – способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов**,** отечественного и зарубежного опыта по проблемам компьютерной безопасности	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; физическую организацию баз данных и принципы (основы) их защиты;

	защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-2 – способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений;

	навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-3 – способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;
ПК-4 – способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;
ПК-5 – способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;

ПК-6 – способностью участвовать в разработке проектной и технической документации	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-7 – способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений

	для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-8 – способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-9 – способностью участвовать в проведении экспериментально-	Знать: основы Интернет-технологий; типовые структуры и принципы организации компьютерных сетей;

исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	эталонную модель взаимодействия открытых систем; основы системного программирования; принципы построения современных операционных систем и особенности их применения; физическую организацию баз данных и принципы (основы) их защиты; характеристики и типы систем баз данных; Уметь: организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы данных; Владеть: навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками системного программирования; навыками конфигурирования и администрирования операционных систем; методикой составления запросов для поиска информации в базах данных;
ПК-10 – способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-11 – способностью участвовать в проведении экспериментально-исследовательских работ при проведении	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций;

сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-12 – способностью проводить инструментальный мониторинг защищенности компьютерных систем	Знать: защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-14 – способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Знать: организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопас-

	ности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; Уметь: пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения компьютерной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации Владеть: методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации. навыками организации и обеспечения режима секретности; навыками работы с нормативными правовыми актами;
ПК-15 – способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знать: организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; Уметь: пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения компьютерной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации Владеть: методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации. навыками организации и обеспечения режима секретности; навыками работы с нормативными правовыми актами;
ПК-16 – разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем	Знать: организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;

	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; Уметь: пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения компьютерной безопасности; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации Владеть: методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации. навыками организации и обеспечения режима секретности; навыками работы с нормативными правовыми актами;
ПК-17 – способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	Знать: основы Интернет-технологий; типовые структуры и принципы организации компьютерных сетей; эталонную модель взаимодействия открытых систем; основы системного программирования; принципы построения современных операционных систем и особенности их применения; физическую организацию баз данных и принципы (основы) их защиты; характеристики и типы систем баз данных; Уметь: организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы данных; Владеть: навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками системного программирования; навыками конфигурирования и администрирования операционных систем; методикой составления запросов для поиска информации в базах данных;
ПК-18 – способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений

	для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-19 – способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Знать: возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; технические каналы утечки информации; Уметь: пользоваться нормативными документами по противодействию технической разведке; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации;
ПСК-2.1 – способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знать: основы Интернет-технологий; типовые структуры и принципы организации компьютерных сетей; эталонную модель взаимодействия открытых систем; основы системного программирования; принципы построения современных операционных систем и особенности их применения; Уметь: организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы данных; Владеть: навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками системного программирования; навыками конфигурирования и администрирования операционных систем;
ПСК-2.2 – способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;
ПСК-2.3 – способностью строить математические	Знать: основные виды политик управления доступом и информационными потоками в компь-

модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	ютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; Владеть: методами формирования требований по защите информации
ПСК-2.4 – способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; Владеть: методами формирования требований по защите информации
ПСК-2.5 – способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации	Знать: возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; технические каналы утечки информации; Уметь: пользоваться нормативными документами по противодействию технической разведке; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации;

4. МЕСТО И СРОКИ ПРОХОЖДЕНИЯ ПРАКТИКИ

Научно-исследовательская работа может проводиться на кафедре информационной безопасности и теории управления УлГУ, а также в структурных подразделениях (деятельность которых связана с информационной безопасностью) на предприятиях, в учреждениях и организациях:

- занимающихся проектированием вычислительных машин, систем, комплексов и сетей с применением новых информационных технологий и средств математического обеспечения;
- проектно-конструкторских и научно-исследовательских учреждениях, занимающихся производством средств вычислительной техники, разработкой информационных систем и технологий;
- проектно-конструкторских и научно-исследовательских учреждениях, использующих средства вычислительной техники, программное обеспечение, информационные системы и технологии;
- оказывающих услуги обеспечения информационной безопасности;
- занимающихся разработкой программных продуктов.

Время прохождения НИР: в 11-м семестре.

5. ОБЩАЯ ТРУДОЕМКОСТЬ ПРАКТИКИ

Объем практики		Продолжительность практики
з.е.	часы	недели

6	216	4

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Разделы (этапы) прохождения практики	Виды работ на практике, включая самостоятельную работу обучающихся	Трудоемкость (в часах)	Объем часов контактной работы обучающегося с преподавателем	Формы текущего контроля
1	Организационные мероприятия	Определение задач, плана работ и средств для его выполнения.	4	2	Тест по технике безопасности
2	Теоретический (аналитический) этап	Сбор, обработка, систематизация фактического материала по теме исследования	100	10	Проверка ведения дневника практики
3	Практический этап	Решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей НИР. Тестирование программ и оценка качества решения задач. Проведение вычислительного эксперимента	100	10	Проверка ведения дневника практики
4	Обобщение материалов и оформление отчета по НИР	Обработка и оформление результатов работы. Подготовка и защита отчета по НИР.	12	2	Защита отчета о прохождении практики
	Итого		216	24	

7. НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЕ И НАУЧНО-ПРОИЗВОДСТВЕННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ НА ПРАКТИКЕ

В процессе НИР руководителями от кафедры (руководителем от организации) должны применяться современные образовательные и научно-производственные технологии:

- мультимедийные технологии, для чего ознакомительные лекции и инструктаж студентов во время НИР проводятся в помещениях, оборудованных экраном, видеопроектором, персональными компьютерами;
- дистанционная форма консультаций во время прохождения конкретных этапов НИР;
- компьютерные технологии и программные продукты, необходимые для сбора и систематизации информации, проведения требуемых программой НИР расчетов и т.д.

8. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ПРАКТИКИ

Научно-исследовательская работа выполняется студентом под руководством научного руководителя.

Направление научно-исследовательских работ студента определяется в соответствии с темой выпускной квалификационной работы.

Обсуждение плана и промежуточных результатов НИР проводится на выпускающей кафедре.

Результаты научно-исследовательской работы должны быть оформлены в письменном виде (отчет) и представлены для утверждения научному руководителю. НИР должна быть завершенным научным материалом, иметь факты и данные, раскрывающие взаимосвязь между явлениями, процессами, аргументами, действиями и содержать нечто новое: обобщение обширной литературы, материалы самостоятельных исследований, в которых появляется авторское видение проблемы и ее решение. Образец титульного листа отчета о научно-исследовательской работе приводится в приложении. В приложении могут быть представлены ксерокопии статей, тезисов докладов.

Студенты, не предоставившие в срок отчет о научно-исследовательской работе и не получившие зачета, к сдаче экзаменов и защите ВКР не допускаются.

По результатам выполнения научно-исследовательской работы студента выставляется итоговая оценка.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

а) Список рекомендуемой литературы

основная

1. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для студентов вузов по спец. 075200 "Компьютер. безопасность" и 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" . М.: Академия. 2005. 144 с.
2. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности : учеб. пособие для вузов по спец. 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" и 075200 "Компьютер. безопасность" / Соболев А.Н., В. М. Кириллов. М. : Гелиос АРВ, 2004. 224 с.
3. Щеглов А.Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. Москва : Издательство Юрайт, 2019. 309 с. (Серия : Бакалавр и магистр. Академический курс). ISBN 978-5-534-04732-5. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/433715

дополнительная

1. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт..журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: https://elibrary.ru/contents.asp?id=37279950
2. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:
   2.1. ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-27001-2006
   2.2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
   2.1. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2017. 40 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915
2. Иванцов А. М. Методические указания для самостоятельной работы студентов по научно-исследовательской работе для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 253 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4677

Согласовано:

Гл. библ-рь ИБ УлГУ	Полина И.Ю.	20.05.2019
должность сотрудника научной библиотеки	ФИО	подпись дата

б) Программное обеспечение

Для образовательного процесса студенту необходимо рабочее место с ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования: Code::Blocks.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5. Znanium.com [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/ 20.05.2019
должность сотрудника УИТиТ	ФИО	подпись	дата

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Помещение 3/317. Аудитория для проведения практических и лабораторных занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций с набором демонстрационного оборудования для обеспечения тематических иллюстраций. Помещение укомплектовано ученической доской и комплектом мебели (посадочных мест – 24). Генератор шума для акустического зашумления помещения.

Сканирующий радиоприемник АР 3000 А. Широкополосная антенна. Осциллограф АСК 2102. Прибор В6-9 (селективный вольтметр). Генератор НЧ Г3-118. Поисковый прибор ST 032 «Пиранья». Имитатор закладных устройств ИМФ-2. Универсальный акустический излучатель к генератору акустического шума OMS-2000. Универсальный электромагнитный излучатель к генератору акустического шума. Генератор электромагнитного зашумления Гром-ЗИ4. Детектор поля D 006. Экран настенный, мультимедийный проектор. Информационные плакаты. Компьютер, Wi-Fi с доступом к сети «Интернет», ЭИОС, ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106 (3 корпус).

Аудитория -24б для проведения лекционных, лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 корпус

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров.

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

11. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ (ОВЗ) И ИНВАЛИДОВ

Обучающиеся с ОВЗ и инвалиды проходят практику совместно с другими обучающимися (в учебной группе) или индивидуально (по личному заявлению обучающегося).

Определение мест прохождения практики для обучающихся с ОВЗ и инвалидов осуществляется с учетом состояния здоровья и требований к их доступности для данной категории обучающихся. При определении мест и условий (с учётом нозологической группы и группы инвалидности обучающегося) прохождения учебной и производственной практик для данной категории лиц учитываются индивидуальные особенности обучающихся, а также рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации, относительно рекомендованных условий и видов труда.

При определении места практики для обучающихся с ОВЗ и инвалидов особое внимание уделяется безопасности труда и оснащению (оборудованию) рабочего места. Рабочие места на практику предоставляются профильной организацией в соответствии со следующими требованиями:

– **для обучающихся с ОВЗ и инвалидов по зрению-слабовидящих:** оснащение специального рабочего места общим и местным освещением, обеспечивающим беспрепятственное нахождение указанным лицом своего рабочего места и выполнение индивидуального задания; наличие видеоувеличителей, луп;

– **для обучающихся с ОВЗ и инвалидов по зрению-слепых:** оснащение специального рабочего места тифлотехническими ориентирами и устройствами, с возможностью использования крупного рельефно-контрастного шрифта и шрифта Брайля, акустическими навигационными средствами, обеспечивающими беспрепятственное нахождение указанным лицом своего рабочего места и выполнение индивидуального задания;

– **для обучающихся с ОВЗ и инвалидов по слуху-слабослышащих:** оснащение (оборудование) специального рабочего места звукоусиливающей аппаратурой, телефонами для слабослышащих;

– **для обучающихся с ОВЗ и инвалидов по слуху-глухих:** оснащение специального рабочего места визуальными индикаторами, преобразующими звуковые сигналы в световые,

речевые сигналы в текстовую бегущую строку, для беспрепятственного нахождения указанным лицом своего рабочего места и выполнения индивидуального задания;

– **для обучающихся с ОВЗ и инвалидов с нарушением функций опорно-двигательного аппарата:** оборудование, обеспечивающее реализацию эргономических принципов (максимально удобное для инвалида расположение элементов, составляющих рабочее место); механизмы и устройства, позволяющие изменять высоту и наклон рабочей поверхности, положение сиденья рабочего стула по высоте и наклону, угол наклона спинки рабочего стула; оснащение специальным сиденьем, обеспечивающим компенсацию усилия при вставании, специальными приспособлениями для управления и обслуживания этого оборудования.

Условия организации и прохождения практики, подготовки отчетных материалов, проведения текущего контроля и промежуточной аттестации по практике обеспечиваются в соответствии со следующими требованиями:

– Объем, темп, формы выполнения индивидуального задания на период практики устанавливаются индивидуально для каждого обучающегося указанных категорий. В зависимости от нозологии максимально снижаются противопоказанные (зрительные, звуковые, мышечные и др.) нагрузки.

– Учебные и учебно-методические материалы по практике представляются в различных формах так, чтобы обучающиеся с ОВЗ и инвалиды с нарушениями слуха получали информацию визуально (документация по практике печатается увеличенным шрифтом; предоставляются видеоматериалы и наглядные материалы по содержанию практики), с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

– Форма проведения текущего контроля успеваемости и промежуточной аттестации для обучающихся с ОВЗ и инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно, при помощи компьютера, в форме тестирования и т.п.). При необходимости обучающемуся предоставляется дополнительное время для подготовки ответа и (или) защиты отчета.

Разработчик _____ / Ганеев С.М. /
подпись ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1	Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
2	Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14
3	Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4	Андреев А.С.		27.05.2020 Протокол заседания кафедры № 14

Приложение 2

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающиеся с ОВЗ и инвалиды проходят практику совместно с другими обучающимися (в учебной группе) или индивидуально (по личному заявлению обучающегося).

Определение мест прохождения практики для обучающихся с ОВЗ и инвалидов осуществляется с учетом состояния здоровья и требований к их доступности для данной категории обучающихся. При определении мест и условий (с учётом нозологической группы и группы инвалидности обучающегося) прохождения учебной и производственной практик для данной категории лиц учитываются индивидуальные особенности обучающихся, а также рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации, относительно рекомендованных условий и видов труда.

При определении места практики для обучающихся с ОВЗ и инвалидов особое внимание уделяется безопасности труда и оснащению (оборудованию) рабочего места. Рабочие места на практику предоставляются профильной организацией в соответствии со следующими требованиями:

– **для обучающихся с ОВЗ и инвалидов по зрению-слабовидящих:** оснащение специального рабочего места общим и местным освещением, обеспечивающим беспрепятственное нахождение указанным лицом своего рабочего места и выполнение индивидуального задания; наличие видеоувеличителей, луп;

– **для обучающихся с ОВЗ и инвалидов по зрению-слепых:** оснащение специального рабочего места тифлотехническими ориентирами и устройствами, с возможностью использования крупного рельефно-контрастного шрифта и шрифта Брайля, акустическими навигационными средствами, обеспечивающими беспрепятственное нахождение указанным лицом своего рабочего места и выполнение индивидуального задания;

– **для обучающихся с ОВЗ и инвалидов по слуху-слабослышащих:** оснащение (оборудование) специального рабочего места звукоусиливающей аппаратурой, телефонами для слабослышащих;

– **для обучающихся с ОВЗ и инвалидов по слуху-глухих:** оснащение специального рабочего места визуальными индикаторами, преобразующими звуковые сигналы в световые, речевые сигналы в текстовую бегущую строку, для беспрепятственного нахождения указанным лицом своего рабочего места и выполнения индивидуального задания;

– **для обучающихся с ОВЗ и инвалидов с нарушением функций опорно-двигательного аппарата:** оборудование, обеспечивающее реализацию эргономических принципов (максимально удобное для инвалида расположение элементов, составляющих рабочее место); механизмы и устройства, позволяющие изменять высоту и наклон рабочей поверхности, положение сиденья рабочего стула по высоте и наклону, угол наклона спинки рабочего стула; оснащение специальным сиденьем, обеспечивающим компенсацию усилия при вставании, специальными приспособлениями для управления и обслуживания этого оборудования.

Условия организации и прохождения практики, подготовки отчетных материалов, проведения текущего контроля и промежуточной аттестации по практике обеспечиваются в соответствии со следующими требованиями:

– Объем, темп, формы выполнения индивидуального задания на период практики устанавливаются индивидуально для каждого обучающегося указанных категорий. В зависимости от нозологии максимально снижаются противопоказанные (зрительные, звуковые, мышечные и др.) нагрузки.

– Учебные и учебно-методические материалы по практике представляются в различных формах так, чтобы обучающиеся с ОВЗ и инвалиды с нарушениями слуха получали информацию визуально (документация по практике печатается увеличенным шрифтом; предоставляются видеоматериалы и наглядные материалы по содержанию практики), с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

– Форма проведения текущего контроля успеваемости и промежуточной аттестации для обучающихся с ОВЗ и инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно, при помощи компьютера, в форме тестирования и т.п.). При необходимости обучающемуся предоставляется дополнительное время для подготовки ответа и (или) защиты отчета.

Приложение 3

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для студентов вузов по спец. 075200 "Компьютер. безопасность" и 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" . М.: Академия. 2005. 144 с.
2. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности : учеб. пособие для вузов по спец. 075500 "Комплексное обеспечение информ. безопасности автоматиз. систем" и 075200 "Компьютер. безопасность" / Соболев А.Н., В. М. Кириллов. М. : Гелиос АРВ, 2004. 224 с.
3. Щеглов А.Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. Москва : Издательство Юрайт, 2019. 309 с. (Серия : Бакалавр и магистр. Академический курс). ISBN 978-5-534-04732-5. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/433715

дополнительная

1. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт..журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: https://elibrary.ru/contents.asp?id=37279950
2. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности:
   2.1. ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2008. — URL: https://gostexpert.ru/gost/gost-27001-2006
   2.2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
   2.1. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012

учебно-методическая

1. Андреев А. С. Методические указания по написанию курсовых и дипломных работ для студентов специальности "Компьютерная безопасность" : учеб.-метод. пособие / А. С. Андреев, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2017. 40 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/915
2. Иванцов А. М. Методические указания для самостоятельной работы студентов по научно-исследовательской работе для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / А. М. Иванцов, С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 253 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4677

Согласовано:

Гл. библ-рь ИБ УлГУ	Полина И.Ю.		20.05.2019
должность сотрудника научной библиотеки	ФИО	подпись	дата

Приложение 4

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1. Электронно-библиотечные системы:

1.1. **IPRbooks** [Электронный ресурс]: электронно-библиотечная система / группа компаний Ай Пи Эр Медиа . - Электрон. дан. - Саратов , [2019]. - Режим доступа: http://www.iprbookshop.ru.

1.2. **ЮРАЙТ** [Электронный ресурс]: электронно-библиотечная система / ООО Электронное издательство ЮРАЙТ. - Электрон. дан. – Москва , [2019]. - Режим доступа: https://www.biblio-online.ru.

1.3. **Консультант студента** [Электронный ресурс]: электронно-библиотечная система / ООО Политехресурс. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://www.studentlibrary.ru/pages/catalogue.html.

1.4. **Лань** [Электронный ресурс]: электронно-библиотечная система / ООО ЭБС Лань. - Электрон. дан. – С.-Петербург, [2019]. - Режим доступа: https://e.lanbook.com.

1.5. Znanium.com [Электронный ресурс]: электронно-библиотечная система / ООО Знаниум. - Электрон. дан. – Москва, [2019]. - Режим доступа: http://znanium.com.

2. **КонсультантПлюс** [Электронный ресурс]: справочная правовая система. /Компания «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2019].

3. **База данных периодических изданий** [Электронный ресурс] : электронные журналы / ООО ИВИС. - Электрон. дан. - Москва, [2019]. - Режим доступа: https://dlib.eastview.com/browse/udb/12.

4. **Национальная электронная библиотека** [Электронный ресурс]: электронная библиотека. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://нэб.рф.

5. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2019]. - Режим доступа: https://dvs.rsl.ru.

6. Федеральные информационно-образовательные порталы:

6.1. Информационная система Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru

6.2. Федеральный портал Российское образование. Режим доступа: http://www.edu.ru

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ. Режим доступа : http://lib.ulsu.ru/MegaPro/Web

7.2. Образовательный портал УлГУ. Режим доступа : http://edu.ulsu.ru

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	/ 20.05.2019
должность сотрудника УИТиТ	ФИО	подпись	дата