УТВЕРЖДЕНО
решением Ученым советом факультета математики, информационных и авиационных технологий
от «21» 06 2019 г., протокол № 9/19
Председатель _____ М.А. Волков
(подпись, расшифровка подписи)
«21» 06 2019 г.

ПРОГРАММА ПРАКТИКИ

Практика	Вид практики: производственная Тип практики: преддипломная (по получению профессиональных умений и опыта профессиональной деятельности в сторонних организациях)
Способ и форма проведения	Способ проведения преддипломной 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	Аббревиатура кафедры (наименование цикла, отделения)	Ученая степень, звание
Иванцов Андрей Михайлович	ИБиТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____ / А.С. Андреев /
(Подпись) *(Ф.И.О.)*
«15» 06 2019 г.

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Цели прохождения преддипломной практики:

- закрепление теоретических и практических знаний, полученных в процессе обучения по специальности «Компьютерная безопасность»;
- подготовка студента к решению задач, относящихся к различных проблемам обеспечения информационной безопасности, и к решению отдельных фундаментальных проблем связанных с компьютерной безопасностью.

Задачи прохождения практики:

- овладение профессиональными навыками работы и решение практических задач;
- выбор направления практической работы;
- изучение литературных и иных источников, необходимых для выполнения данной работы и подготовки выпускной квалификационной работы;
- приобретение опыта работы в коллективе.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

Общая трудоемкость составляет 15 зачетных единиц (540 часов). Продолжительность практики -10 недель в 11 семестре.

Преддипломная практика относится к «Блоку 2» основной профессиональной образовательной программы специалитета - «Практики, в том числе научно-исследовательская работа (НИР)» и базируется на дисциплинах как базовой, так и вариативной части учебного плана основной профессиональной образовательной программы.

Для успешного прохождения практики 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».

Преддипломная практика студентов, обучающихся по учебной программе специальности «Компьютерная безопасность», является составной частью основной образовательной программы высшего образования. Практика студента является средством связи теоретического обучения с практической деятельностью, обеспечивающим прикладную направленность и специализацию обучения и направлена на подготовку студентов с учетом их будущей профессиональной деятельности.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ СТУДЕНТОВ, СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В совокупности с дисциплинами базовой и вариативной частей ФГОС ВО преддипломная практика направлена на формирование следующих компетенций по специальности «Компьютерная безопасность»:

Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
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	**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;

информации, теоретико-числовых методов	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:** основные принципы подбора, изучения и обобщения научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности **Уметь:** осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности **Владеть:** навыками подбора, изучения и обобщения научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности
ПК-2 - способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке	**Знать:** защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита;

защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований	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 компью-	**Знать:** отечественные и зарубежные стандарты в области компьютерной безопасности

терных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	**Уметь:** проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности **Владеть:** навыками анализа безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности
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 **Владеть:** навыками анализа и участия в разработке математических моделей безопасности компьютерных систем
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 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:** 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 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;

	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:** формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; 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 обнару-

	жения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-9 - способностью участвовать в проведении экспериментально-исследова-тельских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	**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-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 сертификации средств защиты информации в компьютерных системах по требованиям безопасности 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; 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:** 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; пользоваться нормативными документами по противодействию технической разведке **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 про-

	граммных средств; навыками настройки межсетевых экранов; методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации
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 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-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 рабо-

	ту 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 уста-	**Знать:** основы Интернет-технологий;

новку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение	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:** организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы 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
ПК-20 - способностью выпол-нять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	**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
ПСК-2.1 - способностью разрабатывать вычислительные ал-	**Знать:** основы Интернет-технологий; типовые структуры и принципы организации компьютер-

горитмы, реализующие современные математические методы защиты информации	ных 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 модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	**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-2.4 – 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

Практика может проводиться 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.

Как исключение, студент может проходить практику самостоятельно по

согласованию с кафедрой.

Время прохождения преддипломной практики: в 11-м семестре.

5. ОБЩАЯ ТРУДОЕМКОСТЬ ПРАКТИКИ

Объем практики		Продолжительность практики
з.е.	**часы**	**недели**
15	540	10

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Разделы (этапы) практики	Виды производственной работы на практике, включая самостоятельную работу студентов	Трудоёмкость (в часах)	Объем часов контактной работы обучающегося с преподавателем	Формы текущего контроля
1	2	3	4	5	6
1	Подготовительный этап	Организационное собрание, инструктаж по ТБ и должностным обязанностям. Определение задач, плана работ и средств по его выполнению.	2/2	2/2	Тест по технике безопасности
2	Экспериментальный этап	Сбор, обработка, систематизация материала по теме исследования. Решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей ВКР. Тестирование программ и оценка качества решения задач.	510/510	12/12	Проверка ведения дневника практики
3	Заключительный этап	Обработка и оформление результатов работы, подготовка и защита отчета по практике.	28/28	6/6	Защита отчета о прохождении практики
	ИТОГО:		540	20	

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

В ходе практики студент должен получить профессиональное представление и приобрести профессиональные навыки работы в отделах, службах и подразделениях, используя теоретические знания, полученные в процессе учебы.

Порядок прохождения практики:

1. Получить отметку в отделе кадров предприятия о прибытии на практику.
2. Получить вводный и первичный инструктаж на рабочем месте по охране труда.
3. Изучить функциональные обязанности инженера отдела (специалиста по защите информации) и практически их выполнять.

4. Изучить информационную систему предприятия.
5. Выполнить задачи, поставленные руководителем практики от предприятия.
6. Заполнять журнал прохождения практики.
7. Подготовить отчет по практике.
8. По окончанию практики получить характеристику и оценку у руководителя практики от предприятия.
9. Получить отметку в отделе кадров предприятия об убытии с предприятия и заверить печатью характеристику и оценку.

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

На преддипломной практике изучаются современные информационные технологии обеспечения информационной безопасности, используемые в технологических и производственных процессах предприятия.

8. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ПРАКТИКИ

После прохождения преддипломной практики студенты в течение 5 дней после официальной даты ее окончания представляют на кафедру ИБиТУ дневник практики, включающий в себя задание, и отчет о прохождении практики.

Руководитель практики проводит контроль над работами студентов, целью которого является:

- обеспечение высокого качества прохождение студентами практики, ее строго соответствия учебным планам и программам;
- согласование программы и графиков прохождения студентами практики с руководителями практики от предприятий, подготовка и выдача студентам индивидуальных заданий на время практики;
- осуществление регулярного контроля за прохождением студентами практики, за соблюдением студентами правил внутреннего трудового распорядка предприятия;
- проведение консультаций по всем возникающим вопросам;
- проверка отчетов и дневников студентов по завершении практики, участие в работе по приемке защиты отчетов о практике.

По окончании практики студент составляет письменный отчет, оформленный в соответствии с установленными требованиями, сдает его руководителям практики от университета и организации – базе практики для предварительной дифференцированной оценки.

Отчет о практике должен содержать сведения о конкретно выполненной студентом работы в период практики.

По результатам аттестации студенту выставляется итоговая дифференцированная оценка за преддипломную практику («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).

Итоги практики подводятся на заседании кафедры. Студент, не выполнивший программу практики, получивший отрицательный отзыв о работе или неудовлетворительную оценку при защите отчета, направляется повторно на практику в период студенческих каникул, либо в свободное от учебы время, либо ставится вопрос об отчислении студента из университета.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

а) Список рекомендуемой литературы:

основная

1. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с. https://biblio-online.ru/viewer/zaschita-informacii-osnovy-teorii-433715.

2. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html.

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

1.2 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

1.3 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.

1.4 Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования (утв. приказом Министерства образования и науки РФ от 27 ноября 2015 г. № 1383). Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_190917/.

2. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. https://gostexpert.ru/gost/gost-27002-2012

3. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт..журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: https://elibrary.ru/contents.asp?id=37279950

учебно-методическая

1.Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). **URL:** http://edu.ulsu.ru/cources/750/interface/

1. Иванцов А. М.

Методические указания для самостоятельной работы по преддипломной практике для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 358 КБ). - Текст: электронный.

http://lib.ulsu.ru/MegaPro/Download/MObject/4266

Согласовано:

Гл. библиотекарь НБ УлГУ	Полежаева И.Ю.		14.06.2019
Должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

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

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИиТ / Клочкова А.В. / подпись / 14.06.2019

Должность сотрудника УИТиТ ФИО дата

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer.
- научно-исследовательское оборудование, которым обладает организация, утвержденная местом прохождения практики.

12. 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.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность 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.п. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1	Андреев А.С.		08.04.2020 Протокол заседания кафедры № 12
2	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
3	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
4	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 1

6. Структура и содержание практики

№ п/п	Разделы (этапы) практики	Виды производственной работы на практике, включая самостоятельную работу студентов	Трудоёмкость (в часах)	Объем часов контактной работы обучающегося с преподавателем	Формы текущего контроля
1	2	3	4	5	6
1	Подготовительный этап	Организационное собрание, инструктаж по ТБ и должностным обязанностям. Определение задач, плана работ и средств по его выполнению.	2/2*	2/2*	Тест по технике безопасности
2	Экспериментальный этап	Сбор, обработка, систематизация материала по теме исследования. Решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей ВКР. Тестирование программ и оценка качества решения задач.	510/510*	12/12*	Проверка ведения дневника практики
3	Заключительный этап	Обработка и оформление результатов работы, подготовка и защита отчета по практике.	28/28*	6/6*	Защита отчета о прохождении практики
	ИТОГО:		540	20	

*Количество часов работы ППС с обучающимися в дистанционном формате с применением электронного обучения.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

Приложение 2

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

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей

Приложение 3

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

а) Список рекомендуемой литературы:

основная

1. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с. https://biblio-online.ru/viewer/zaschita-informacii-osnovy-teorii-433715.

2. Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М.: Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html.

дополнительная

1. Некоммерческая интернет-версия СПС "КонсультантПлюс":

1.1 Федеральный закон от 27.06.2006 N149-ФЗ "Об информации, информационных технологиях и защите информации". Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

1.2 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

1.3 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.

1.4 Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования (утв. приказом Министерства образования и науки РФ от 27 ноября 2015 г. № 1383). Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_190917/.

2. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. https://gostexpert.ru/gost/gost-27002-2012

3. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт..журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: https://elibrary.ru/contents.asp?id=37279950

учебно-методическая

1.Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). **URL:** http://edu.ulsu.ru/cources/750/interface/

1. Иванцов А. М.

Методические указания для самостоятельной работы по преддипломной практике для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск: УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 358 КБ). - Текст: электронный.

http://lib.ulsu.ru/MegaPro/Download/MObject/4266

Согласовано:

Гл. библ-рь НБ УлГУ	Полежаева И.Ю.		14.06.2019
Должность сотрудника научной библиотеки	ФИО	подпись	дата

Приложение 4

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

б) Программное обеспечение

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- Microsoft Office / МойОфис Стандартный.

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

8. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности.

Согласовано:

Зам. нач. УИиТ /Клочкова А.В. / 14.06.2019

Должность сотрудника УИТиТ ФИО подпись дата