УТВЕРЖДЕНО
решением Ученого совета факультета математики,
информационных и авиационных технологий
от «16» 06 2020 г., протокол №5/20
Председатель _____ / М.А. Волков /
(подпись, расшифровка подписи)
«16» 06 2020 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	5

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация: «Безопасность открытых информационных систем»

Форма обучения: очная

Дата введения в учебный процесс УлГУ «01» 09 2020 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.
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.)* «16» 06 2020 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

Для успешного выполнения научно-исследовательской работы необходимы компетенции, сформированные в ходе изучения дисциплин «Криптографические методы защиты информации», «Основы информационной безопасности», «Криптографические протоколы и стандарты», «Техническая защита информации», «Программно-аппаратные средства обеспечения информационной безопасности», «Информационная безопасность открытых систем», «Сети и системы передачи информации», «Безопасность операционных систем», «Безопасность систем баз данных», «Разработка и эксплуатация защищенных автоматизированных систем»..

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.

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 ФГОС ВО по специальности «Информационная безопасность автоматизированных систем» научно-исследовательская работа направлена на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), 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: основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней, выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории; Уметь: соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории; анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав Владеть: представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приемами ведения дискуссии и полемики; 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	Уметь: осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий Владеть: навыками работы с технической документацией на ЭВМ и вычислительные системы
ОПК-1 – способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	Знать: основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела; физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации основные методы управления информационной безопасностью; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Уметь: определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач строить математические модели физических явлений и процессов; решать типовые прикладные физические задачи; анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; применять математические методы исследования моделей шифров основы физической защиты объектов информатизации выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем Владеть: навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры навыками построения дискретных моделей при решении профессиональных задач методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов
ОПК-2 – способностью	Знать:

корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	возможности координатного метода для исследования различных геометрических объектов, основные задачи векторной алгебры и аналитической геометрии, основные виды уравнений простейших геометрических объектов, основные свойства важнейших алгебраических структур, основы линейной алгебры над произвольными полями, векторные пространства над полями и их свойства основы комбинаторного анализа; метод включения-исключения; производящие функции; основные понятия теории автоматов; основные понятия и алгоритмы теории графов; основные дискретные структуры: конечные автоматы, графы, комбинаторные структуры; методы перечисления для основных дискретных структур; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи основные понятия математической логики и теории алгоритмов; язык и средства современной математической логики, представления булевых функций и способы минимизации формул; типовые свойства и способы задания функций многозначной логики. различные подходы к определению алгоритма и доказательства алгоритмической неразрешимости отдельных массовых задач, подходы к оценкам сложности алгоритмов, методы построения эффективных алгоритмов, возможности применения общих логических принципов в математике и профессиональной деятельности основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики основные положения теории пределов и непрерывных функций, теории числовых и функциональных рядов; основные теоремы дифференциального и интегрального исчисления функций одной и нескольких переменных; основные понятия теории функций комплексной переменной; основные методы решения простейших дифференциальных уравнений и систем дифференциальных уравнений основные понятия теории информации: энтропия, взаимная информация, источники сообщений, каналы связи, коды; основные теоремы о кодировании при наличии и отсутствии шума; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи эталонную модель взаимодействия открытых систем основные задачи и понятия криптографии; частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки основные информационные технологии, используемые в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем способы кодирования информации современные технологии и методы программирования методы анализа и синтеза электронных схем язык программирования высокого уровня (объектно-ориентированное программирование); возможности, классификацию и область применения макрообработки Уметь: строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач, исследовать простейшие геометрические объекты по их уравнениям в различных системах координат, оперировать с числовыми и конечными полями, многочленами, матрицами, решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями применять стандартные методы дискретной математики и теории автоматов для реше-

	ния профессиональных задач; решать задачи периодичности и эквивалентности для конечных автоматов; применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; решать оптимизационные задачи на графах; находить и исследовать свойства представлений булевых имногозначных функций формулами в различных базисах; оценивать сложность алгоритмов и вычислений; классифицировать алгоритмы по классам сложности; применять методы математической логики и теории алгоритмов к решению задач математической кибернетики; строить и изучать математические модели конкретных явлений и процессов для решения расчётных и исследовательских задач; определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач; пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач строить и изучать математические модели конкретных явлений и процессов для решения расчётных и исследовательских задач; определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); решать типовые задачи кодирования и декодирования; работать с научно-технической литературой по тематике дисциплины разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем применять на практике методы анализа электрических цепей Владеть: навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры навыками построения дискретных моделей при решении профессиональных задач; навыками применения языка и средств дискретной математики; навыками решения комбинаторных и теоретико-графовых задач; навыками применения математического аппарата для решения прикладных теоретико-информационных задач; навыками использования языка современной символической логики; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками составления программ на машинах Тьюринга; навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками решения задач с применением аппарата теории функций комплексной переменной; навыками использования стандартных методов решения типовых дифференциальных уравнений; навыками пользования библиотеками прикладных программ для решения прикладных математических задач основами построения математических моделей систем передачи информации; навыками применения математического аппарата для решения прикладных теоретико-информационных задач методами формирования требований по защите информации методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;

	навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем навыками программирования с использованием эффективных реализаций структур данных и алгоритмов
ОПК-3 – способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	Знать: принципы построения и функционирования, примеры реализаций современных операционных систем принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей основные информационные технологии, используемые в автоматизированных системах показатели качества программного обеспечения язык программирования высокого уровня (объектно-ориентированное программирование); возможности, классификацию и область применения макрообработки; способы обработки исключительных ситуаций Уметь: создавать объекты базы данных; выполнять запросы к базе данных; разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения работать с интегрированной средой разработки программного обеспечения; использовать шаблоны классов и средства макрообработки; использовать динамически подключаемые библиотеки Владеть: навыками использования ЭВМ в анализе простейших шифров навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках; навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем навыками проектирования программного обеспечения с использованием средств автоматизации; навыками разработки программной документации
ПК-1 – способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	Знать: разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов Уметь: навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках Владеть: Разработка и эксплуатация защищенных автоматизированных систем
ПК-2 – способностью создавать и исследовать модели автоматизированных систем	Знать: модели шифров и математические методы их исследования основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные характеристики сигналов электросвязи, спектры и виды модуляции; эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации Уметь: разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений Владеть:

	навыками математического моделирования в криптографии методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем
ПК-3 – способностью проводить анализ защищенности автоматизированных систем	Знать: требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации Уметь: разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений Владеть: навыками математического моделирования в криптографии методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации; навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем навыками организации и обеспечения режима секретности
ПК-4 – способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах Уметь: разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем анализировать и оценивать угрозы информационной безопасности объекта
ПК-5 – способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров Уметь: анализировать и оценивать угрозы информационной безопасности объекта
ПК-7 – способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знать: принципы построения и функционирования, примеры реализаций современных операционных систем Уметь: разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов Владеть: навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности
ПК-8 – способностью разрабатывать и анализировать проектные решения по обеспечению безопасности	Знать: средства обеспечения безопасности данных основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты ин-

автоматизированных систем	формации показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы тестирования и отладки ПО; принципы организации документирования разработки, процесса сопровождения программного обеспечения; основные структуры данных и способы их реализации на языке программирования; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности Уметь: формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; планировать разработку сложного программного обеспечения; проводить комплексное тестирование и отладку программных систем; проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; работать с интегрированной средой разработки программного обеспечения оценивать информационные риски в автоматизированных системах Владеть: навыками участия в экспертизе состояния защищенности информации на объекте защиты навыками проектирования программного обеспечения с использованием средств автоматизации; навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов
ПК-9 – способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Знать: принципы построения и функционирования, примеры реализаций современных систем управления базами данных; архитектуру систем баз данных; основные модели данных; физическую организацию баз данных; последовательность и содержание этапов проектирования баз данных Уметь: разрабатывать и администрировать базы данных; выделять сущности и связи предметной области; отображать предметную область на конкретную модель данных; нормализовывать отношения при проектировании реляционной базы данных; применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации Владеть: навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации
ПК-11 – способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать: основные задачи и понятия криптографии основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах Уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем Владеть:

	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности
ПК-12 – способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Уметь: применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации оценивать информационные риски в автоматизированных системах Владеть: навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации навыками участия в экспертизе состояния защищенности информации на объекте защиты
ПК-13 – способностью участвовать в проектировании средств защиты информации автоматизированной системы	Знать: требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах Уметь: применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем Владеть: криптографической терминологией методами формирования требований по защите информации методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем методами и средствами технической защиты информации
ПК-14 – способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать: требования к шифрам и основные характеристики шифров основные информационные технологии, используемые в автоматизированных системах Уметь: контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем Владеть: навыками участия в экспертизе состояния защищенности информации на объекте защиты навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем методами расчета и инструментального контроля показателей технической защиты информации навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков
ПК-16 – способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных	Знать: возможности технических средств перехвата информации

требований по защите информации	
ПК-17 – способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Знать: технические каналы утечки информации Владеть: методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-21 – способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Уметь: разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем Владеть: навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности
ПК-26 – способностью администрировать подсистему информационной безопасности автоматизированной системы	Знать: типовые шифры с открытыми ключами; технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования источники и классификацию угроз информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах современные технологии и методы программирования Уметь: планировать политику безопасности операционных систем; применять средства обеспечения безопасности данных; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации администрировать подсистемы информационной безопасности автоматизированных систем Владеть: навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности; навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ навыками работы с технической документацией на ЭВМ и вычислительные системы профессиональной терминологией в области информационной безопасности; навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации; навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы навыками разработки программной документации
ПК-28 – способностью управлять информационной безопасностью автоматизированной системы	Знать: основные методы управления информационной безопасностью Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем Владеть:

	методами управления информационной безопасностью автоматизированных систем
ПСК-4.1 – способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	Знать: основные методы и средства реализации удаленных сетевых атак на открытые информационные системы; о политиках безопасности и мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем; Уметь: реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по оценке защищенных систем; практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений; осуществлять мониторинг и аудит сетевой безопасности; осуществлять администрирование открытых информационных систем Владеть: терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
ПСК-4.2 – способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	Знать: о политиках безопасности и мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем Уметь: проектировать защищенные открытые информационные системы; определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя Виртуальные частные сети Аудит информационных технологий и систем обеспечения информационной безопасности информационной безопасности для открытых информационных систем; выявлять и устранять уязвимости в основных компонентах открытых информационных систем; Владеть: терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах
ПСК-4.3 – способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	Знать: принципы построения современных виртуальных локальных и частных сетей и направления их развития; виды виртуальных сетей и их преимущества при конкретном применении; политику безопасности для виртуальных сетей; Уметь: осуществлять управление информационной безопасностью в открытых информационных системах; применять стандартные решения для защиты информации в виртуальных сетях и квалифицированно оценивать их качество; Владеть: навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
ПСК-4.4 – способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	Знать: основные стандарты построения виртуальных сетей; принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях; подходы к интеграции виртуальных сетей с открытыми информационными системами; Уметь: обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам; применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество; используя современные методы и средства, разрабатывать и оценивать модели и

	политику безопасности для открытых информационных систем; Владеть: навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
ПСК-4.5 – способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	Знать: базовые вопросы построения открытых информационных систем; основные криптографические протоколы и стандарты; основные стандарты построения и взаимодействия открытых систем; о политиках безопасности и мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем; Уметь: проектировать защищенные открытые информационные системы; определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя информационной безопасности для открытых информационных систем; выявлять и устранять уязвимости в основных компонентах открытых информационных систем; Владеть: терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей

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 10-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 по 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 и др.

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

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

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: http://journals.tsu.ru/pdm/
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.
   2.2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012.
   2.3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013.

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:** ftp://10.2.96.134/Text/Andreev_2017.pdf
2. Андреев А. С. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", "Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", "Системный анализ и управление" / А. С. Андреев, С. М. Бородин, А. М. Иванцов; УлГУ, ФМиИТ. Ульяновск : УлГУ, 2015. 54 с.- **URL:** ftp://10.2.96.134/Text/Andreev2015.pdf
3. 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:

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

7. Федеральные информационно-образовательные порталы:

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

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

8. Образовательные ресурсы УлГУ:

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

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

Согласовано:

Зам.нач. УИТиТ /Клочкова А.В. /_____/_____/
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 -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 _____/_____/

подпись ФИО