


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

УТВЕРЖДЕНО
 Решением Ученого совета факультета
 математики, информационных и авиационных технологий
 от «10» 06 2020 г., протокол №5/20
 Председатель М.А.Волков
 «16» 06 2020г.

ПРОГРАММА ПРАКТИКИ

Практика	Вид практики: производственная практика. Тип практики: практика по получению профессиональных умений и опыта профессиональной деятельности.
Способ и форма проведения	Способ проведения производственной практики: стационарная Форма проведения: непрерывная
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	5


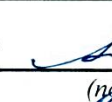
Специальность 10.05.01 «Компьютерная безопасность»
 Специализация «Математические методы защиты информации»
 Форма обучения очная


Дата введения в учебный процесс УлГУ «01» 09 2020г.

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:

Ф.И.О.	Аббревиатура кафедры	Ученая степень, звание
Перцева Ирина Анатольевна	ИБиТУ	к.ф.-м.н.

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/  / <u>Андреев А.С.</u> / (подпись) (Ф.И.О.)	/  / <u>Андреев А.С.</u> / (подпись) (Ф.И.О.)
« 10 » 06 2020г.	« 10 » 06 2020г.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Цели прохождения практики:

- закрепление теоретических и практических знаний, полученных в процессе обучения по специальности «Компьютерная безопасность»;
- подготовка студента к решению задач, относящихся к различным 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;
- сбор необходимой для выполнения данной работы информации по месту прохождения практики, а также при изучении литературных и иных источников;
- приобретение опыта работы в коллективе.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

Для успешного прохождения практики необходимы компетенции, сформированные в ходе изучения дисциплин «Иностранный язык», «Основы управленческой деятельности», «Алгебра», «Геометрия», «Математический анализ», «Дискретная математика», «Математическая логика и теория алгоритмов», «Теория вероятностей и математическая статистика», «Физика», «Теория информации», «Информатика», «Системы и сети передачи информации», «Компьютерные сети», «Аппаратные средства вычислительной техники», «Операционные системы», «Системы управления базами данных», «Основы информационной безопасности», «Теоретико-числовые методы в криптографии», «Криптографические методы защиты информации», «Теория кодирования, сжатия и восстановления информации», «Техническая защита информации», «Организационное и правовое обеспечение информационной безопасности», «Основы построения защищенных компьютерных систем», «Защита в операционных системах», «Модели безопасности компьютерных систем», «Основы построения защищенных баз данных», «Защита программ и данных», «Теория псевдослучайных генераторов», «Психология и педагогика», «Русский язык и культура речи», «Вычислительные методы в алгебре и теории чисел», «Численные методы», «Теория функций комплексного переменного», «Введение в специальность», «Гуманитарные аспекты информационной безопасности», «Основы научных исследований», «Профессиональная этика», «Математические модели информационных систем», «Системный анализ», «Теория игр и исследования операций», «Вейвлет-анализ», «Комбинаторика», «Теория вычислительной сложности», «Проектная деятельность», «Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности».

Производственная 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, СООТНЕСЕННЫХ С

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОПОП ВО

В совокупности с другими дисциплинами базовой и вариативной части ФГОС ВО производственная 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-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: значение информационной безопасности в структуре национальной безопасности; угрозы информационной безопасности в социальной сфере. Уметь: анализировать потребности государства, общества, личности в профессиональной деятельности в области информационной безопасности Владеть: культурой внедрения инновационных методов в профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
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: принципы построения грамотной устной и письменной речи на иностранном языке (по крайней мере, на одном). Уметь: вступать в коммуникацию в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействий. Владеть: техникой перевода иностранной научно-технической литературы на русский язык и способностью к коммуникации в профессиональной сфере (перевод основного содержания работы на иностранный язык) и межличностном общении.
ОК-8 способностью к самоорганизации и самообразованию	Знать: способы самоорганизации и развития своего интеллектуального, культурного, духовного, нравственного, физического и профессионального уровня Уметь: устранять недостатки в состоянии своего общекультурного и профессионального уровней развития посредством самообразования. Владеть: навыками самоорганизации, самостоятельной работы и развития своего потенциала

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
<p>ОПК-2 способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов</p>	<p>Знать: основные понятия и методы математического анализа, аналитической геометрии, линейной и векторной алгебры.</p> <p>Уметь: использовать математические методы в технических приложениях; строить вероятностные модели для конкретных процессов, проводить необходимые расчеты в рамках построенной модели.</p> <p>Владеть: соответствующим математическим аппаратом для решения профессиональных задач.</p>
<p>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</p>	<p>Знать: основные понятия информатики; формы и способы представления данных в персональном компьютере.</p> <p>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.</p> <p>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).</p>
<p>ПК-2 способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры</p>	<p>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,</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
по результатам выполнения исследований	<p>ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; физическую организацию баз данных и принципы (основы) их защиты;</p> <p>защитные механизмы и средства обеспечения сетевой безопасности;</p> <p>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;</p> <p>основные протоколы идентификации и аутентификации абонентов сети;</p> <p>средства и методы предотвращения и обнаружения вторжений;</p> <p>Уметь:</p> <p>использовать средства защиты, предоставляемые системами управления базами данных;</p> <p>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;</p> <p>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;</p> <p>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;</p> <p>Владеть:</p> <p>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;</p> <p>навыками анализа программных реализаций;</p> <p>навыками использования инструментальных средств отладки и дизассемблирования программного кода;</p> <p>криптографической терминологией;</p> <p>методиками анализа сетевого трафика;</p> <p>методиками анализа результатов работы средств обнаружения вторжений;</p> <p>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;</p> <p>навыками настройки межсетевых экранов;</p>
ПК-4 способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	<p>Знать:</p> <p>основные виды политик управления доступом и информационными потоками в компьютерных системах;</p> <p>основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков;</p> <p>Уметь:</p> <p>разрабатывать частные политики безопасности компьютерных</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
	систем, в том числе политики управления доступом и информационными потоками;
<p>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</p>	<p>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;</p> <p>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;</p> <p>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</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
	<p>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;</p>
<p>ПК-6 способностью участвовать в разработке проектной и технической документации</p>	<p>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.</p>
<p>ПК-7 способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем</p>	<p>Знать: требования к шифрам и основные характеристики шифров; архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. Владеть: навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности; методами формирования требований по защите информации; методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем.</p>
<p>ПК-8</p>	<p>Знать:</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
<p>способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы</p>	<p>Требования к обеспечению информационной безопасности компьютерных систем Уметь: Применять нормативно-методическую базу по обеспечению информационной безопасности компьютерной системы Владеть: Практическими навыками разработки подсистемы информационной безопасности компьютерной системы.</p>
<p>ПК-9 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы</p>	<p>Знать: Требования к уровню защищенности компьютерной системы Уметь: Нормативные документы по аттестации объектов с учетом требований к уровню защищенности компьютерной системы Владеть: навыками проведения работ по аттестации объектов с учетом требований к уровню защищенности компьютерной системы</p>
<p>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</p>	<p>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</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
	<p>операционных систем, а также локальных компьютерных сетей, построенных на их основе;</p> <p>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.</p>
<p>ПК-11 способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации</p>	<p>Знать: методологию научного исследования для определения параметров и характеристик средств защиты информации</p> <p>Уметь: применять исследовательский подход в процессе сертификации средств защиты информации</p> <p>Владеть: навыком и практическим опытом проведения научного исследования в процессе сертификации средств защиты информации</p>
<p>ПК-12 способностью проводить инструментальный мониторинг защищенности компьютерных систем</p>	<p>Знать: какие инструментальные средства используются для мониторинга компьютерных систем.</p> <p>Уметь: Использовать и реализовывать современные алгоритмы обработки информации и сигналов в целях обеспечения безопасности систем.</p> <p>Владеть: навыками программной реализации алгоритмов обработки информации и сигналов в целях обеспечения безопасности компьютерных систем.</p>
<p>ПК-13 способностью организовывать работу малых коллективов исполнителей, находить</p>	<p>Знать: особенности профессиональной этики; возможные пути разрешения конфликтных ситуаций в профессиональной деятельности</p> <p>Уметь: в качестве руководителя формировать цели команды,</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
и принимать управленческие решения в сфере профессиональной деятельности	принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность Владеть: навыками работы в коллективе в качестве руководителя и лидера группы сотрудников; методами разрешения конфликтных ситуаций
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	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 орга-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
информационной безопасностью компьютерной системы	<p>низационного 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;</p> <p>правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации.</p> <p>Уметь:</p> <p>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.</p> <p>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.</p>
<p>ПК-16</p> <p>разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем</p>	<p>Знать:</p> <p>основные положения стандартов Единой системы конструкторской документации, Единой системы программной Документации знать правила аттестации автоматизированных систем с учетом нормативных документов</p> <p>Уметь:</p> <p>разрабатывать регламенты, инструкции в области профессиональной деятельности</p> <p>Владеть:</p> <p>навыками разработки документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем</p>
<p>ПК-17</p> <p>способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая</p>	<p>Знать:</p> <p>современное общее и специальное программное обеспечение, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p> <p>Уметь:</p> <p>производить установку, наладку современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
операционные системы, системы управления базами данных, сетевое программное обеспечение	<p>Владеть: Навык тестирования и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p>
<p>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</p>	<p>Знать: Современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации</p> <p>Уметь: Производить установку, наладку 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</p> <p>Владеть: Навыками тестирования и обслуживания 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</p>
<p>ПК-19 способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации</p>	<p>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;</p> <p>Уметь: пользоваться нормативными документами по противодействию технической разведке;</p> <p>Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации;</p>
<p>ПК-20 способностью выполнять работы по восстановлению работоспособности средств защиты информации при</p>	<p>Знать: способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановления ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций;</p> <p>Уметь: применять средства и системы защиты информационно-</p>

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
возникновении нештатных ситуаций	<p>технологических ресурсов автоматизированной системы; восстанавливать ресурсы автоматизированной системы, их работоспособность при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; применять методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям;</p> <p>Владеть: методикой применения средств и систем защиты информационно технологических ресурсов автоматизированной системы; методикой восстановления ресурсов автоматизированной системы, их работоспособности при возникновении нештатных ситуаций</p>
<p>ПСК-2.1 способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации</p>	<p>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.</p> <p>Уметь: организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы данных.</p> <p>Владеть: навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками системного программирования; навыками конфигурирования и администрирования операционных систем.</p>
<p>ПСК-2.2 способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах</p>	<p>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.</p> <p>Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе.</p> <p>Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.</p>
<p>ПСК-2.3 способностью строить математические модели для оценки</p>	<p>Знать: математические модели для оценки безопасности компьютерных систем.</p> <p>Уметь:</p>


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	анализировать компоненты системы безопасности компьютерных систем. Владеть: навыками использования современных математических методов для оценки безопасности компьютерных систем.
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 с 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;

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

- оказывающих услуги обеспечения информационной безопасности;
- занимающихся разработкой программных продуктов.

Как исключение, студент может проходить практику самостоятельно по согласованию с кафедрой.

Время прохождения производственной практики: в 10-м семестре.

5. ОБЩАЯ ТРУДОЕМКОСТЬ ПРАКТИКИ

Объем практики		Продолжительность практики
з.е.	часы	недели
9	324	6


6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

№ п/п	Разделы (этапы) практики	Виды производственной работы на практике, включая самостоятельную работу студентов	Трудоемкость (в часах)	Формы текущего контроля	Объем часов контактной работы обучающегося с преподавателем
1	Подготовительный этап	Организационное собрание, инструктаж по ТБ и должностным обязанностям. Определение задач, плана работ и средств по его выполнению.	4	Тестовые вопросы	4
2	Экспериментальный этап	Сбор, обработка, систематизация материала по теме исследования. Решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей. Тестирование программ и оценка качества решения задач.	306	Проверка ведения дневника практики	24
3	Заключительный этап	Обработка и оформление результатов работы, подготовка и защита отчета по практике.	14	Защита отчета о прохождении практики	8
ИТОГО:			324		36

В ходе практики студент должен получить необходимое профессиональное представление и приобрести профессиональные навыки работы в отделах, службах и подразделениях, используя теоретические знания, полученные в процессе учебы и в результате работы над выполнением задания на практику.

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.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

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

8. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ПРАКТИКИ

После прохождения 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 прохождения 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 выполненных студентом работ в период практики.

По результатам аттестации студенту выставляется итоговая дифференцированная оценка за 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.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

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://biblioonline.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/courses/750/interface/>.
2. Методические указания для самостоятельной работы при прохождении практики для студентов по специальностям 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» очной формы обучения / И. А. Перцева; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 350 КБ). - Текст : электронный. <http://lib.ulsu.ru/MegaPro/Download/MObject/8263>

Согласовано:

Гл. библио-р Полина И.Ю Ю.И.У 05.06.20
 Должность сотрудника научной библиотеки ФИО подпись дата

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

б) Программное обеспечение

Для образовательного процесса студенту необходимо рабочее место с ПК с установленным следующим программным обеспечением: операционная среда ОС Windows/Linux; MS Office.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2020]. – URL: <http://www.iprbookshop.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2020]. - URL: <https://www.biblio-online.ru>. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2020]. – URL: http://www.studentlibrary.ru/catalogue/switch_kit/x2019-128.html. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2020]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2020]. - URL: <http://znanium.com>. – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.6. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: <http://web.a.ebscohost.com/ehost/search/advanced?vid=1&sid=e3ddfb99-a1a7-46dd-a6eb-2185f3e0876a%40sessionmgr4008>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2020].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2020]. – URL: <https://dlib.eastview.com/browse/udb/12>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2020]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный


3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2020]. – URL: <https://id2.action-media.ru/Personal/Products>. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2020]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: <https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741>. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. [Единое окно доступа к образовательным ресурсам](#) : федеральный портал /

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст : электронный.

6.2. [Российское образование](http://www.edu.ru) : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://www.edu.ru>. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотека УлГУ : модуль АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: <http://lib.ulsu.ru/MegaPro/Web>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

7.2. Образовательный портал УлГУ. – URL: <http://edu.ulsu.ru>. – Режим доступа : для зарегистр. пользователей. – Текст : электронный.

Согласовано:

Техническая таб.
Должность сотрудника УИТИТ

Бордужина Ю.С.
ФИО подпись дата

05.06.20
Дата

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ:

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


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;

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф- Рабочая программа		

- 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.

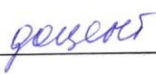
Условия организации и прохождения практики, подготовки отчетных материалов, проведения текущего контроля и промежуточной аттестации по практике обеспечиваются в соответствии со следующими требованиями:

- 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



должность



ФИО