


|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |

**УТВЕРЖДЕНО**  
решением Ученого совета факультета математики,  
информационных и авиационных технологий

от «16» 06 2020 г. протокол № 120  
Председатель \_\_\_\_\_ М.А. Волков \_\_\_\_\_  
(подпись, расшифровка подписи)  
«16» 06 2020 г.

### ПРОГРАММА ПРАКТИКИ

|                           |   |
|---------------------------|---|
| Практика                  | Вид практики: производственная<br>Тип практики: преддипломная (по получению профессиональных умений и опыта профессиональной деятельности в сторонних организациях) |
| Способ и форма проведения | Способ проведения преддипломной практики: стационарная<br>Форма проведения: непрерывная   |
| Факультет                 | Математики, информационных и авиационных технологий (ФМИАТ)   |
| Кафедра                   | Информационной безопасности и теории управления (ИБиТУ)   |
| Курс                      | 6   |

Специальность: 10.05.01 «Компьютерная безопасность»

Специализация: «Математические методы защиты информации»

Форма обучения: очная

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

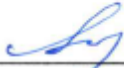
Программа актуализирована на заседании кафедры: протокол № 12 от 08.04.2020 г.


Программа актуализирована на заседании кафедры: протокол № 14 от 27.05.2020 г.

Программа актуализирована на заседании кафедры: протокол № \_\_\_\_\_ от \_\_\_\_\_ 20 \_\_\_\_\_ г.

Сведения о разработчиках:

| ФИО                       | Аббревиатура кафедры<br>(наименование цикла,<br>отделения) | Ученая степень, звание            |
|---------------------------|--|-----------------------------------|
| Иванцов Андрей Михайлович | ИБиТУ  | Кандидат технических наук, доцент |
|                           |  |                                   |

|   |           |                 |
|---|-----------|-----------------|
| <b>СОГЛАСОВАНО:</b>   |           |                 |
| Заведующий выпускающей кафедрой<br>«Информационная безопасность и теория<br>управления» |           |                 |
|     | /         | А.С. Андреев /  |
| (Подпись)   |           | (Ф.И.О.)        |
| « <u>10</u> »   | <u>06</u> | 20 <u>20</u> г. |

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

## 1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

### Цели прохождения преддипломной практики:

- закрепление теоретических и практических знаний, полученных в процессе обучения по специальности «Компьютерная безопасность»;
- подготовка студента к решению задач, относящихся к 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;
- изучение литературных и иных источников, необходимых для выполнения данной работы и подготовки выпускной квалификационной работы;
- приобретение опыта работы в коллективе.


## 2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

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

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

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


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

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |


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

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


| Индекс и наименование реализуемой компетенции  | Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций  |
|--|--|
| ОК-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 | <p><b>Знать:</b><br/>цели, задачи, принципы и основные направления обеспечения информационной безопасности;<br/>основные термины по проблематике информационной безопасности;<br/>роль и место информационной безопасности в системе национальной безопасности страны;<br/>угрозы информационной безопасности государства;<br/>содержание информационной войны, методы и средства ее ведения</p> <p><b>Уметь:</b><br/>пользоваться современной научно-технической информацией по исследуемым проблемам и задачам</p> <p><b>Владеть:</b><br/>навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности</p> |
| 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  | <p><b>Знать:</b><br/>свойства, функции и признаки документа, в том числе как объекта нападения и защиты;<br/>основы документационного обеспечения управления</p> <p><b>Уметь:</b><br/>квалифицированно исследовать состав документации предприятия (организации)</p> <p><b>Владеть:</b><br/>методами формирования требований по защите информации</p>  |

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |


|  |  |
|--|--|
| <p>ОК-8 - способностью к самоорганизации и самообразованию</p>   | <p><b>Знать:</b><br/>основные методы управления информационной безопасностью</p> <p><b>Уметь:</b><br/>оценивать информационные риски в информационных системах;<br/>разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем</p> <p><b>Владеть:</b><br/>методами управления информационной безопасностью информационных систем;<br/>методами оценки информационных рисков</p>  |
| <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><b>Знать:</b><br/>основные понятия и задачи векторной алгебры и аналитической геометрии;<br/>основные свойства алгебраических структур;<br/>основы линейной алгебры над произвольными полями;<br/>основы теории групп и теории групп подстановок;<br/>свойства векторных пространств;<br/>свойства кольца многочленов;<br/>основные понятия и задачи векторной алгебры и аналитической геометрии;<br/>основные понятия и методы дискретной математики;<br/>основные понятия математической логики и теории алгоритмов;<br/>абстрактный интеграл Лебега и его основные свойства;<br/>основные положения теории пределов функций, теории рядов;<br/>основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных;<br/>понятие меры, измеримые функции и их свойства;<br/>алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах;<br/>основные понятия и методы теории вероятностей, математической статистики и теории случайных процессов;<br/>основные понятия и методы теории информации;</p> <p><b>Уметь:</b><br/>решать основные задачи векторной алгебры и аналитической геометрии;<br/>решать системы линейных уравнений над полями;<br/>решать основные задачи векторной алгебры и аналитической геометрии;<br/>использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечисленных задач;</p> |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|  |  |
|--|--|
|  | <p>находить представление и исследовать свойства булевых и многозначных функций формулами в различных базах;</p> <p>определять возможности применения методов математического анализа;</p> <p>решать основные задачи теории пределов функций, дифференцирования, интегрирования и разложения функций в ряды;</p> <p>проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;</p> <p>применять стандартные методы и модели к решению теоретико-вероятностных и статистических задач;</p> <p>вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность);</p> <p><b>Владеть:</b></p> <p>навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;</p> <p>навыками решения систем линейных уравнений над полем и кольцом вычетов;</p> <p>навыками решения стандартных задач в векторных пространствах;</p> <p>навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;</p> <p>навыками решения задач дискретной математики;</p> <p>навыками использования языка математической логики;</p> <p>навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач;</p> <p>навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.</p> <p>основами построения математических моделей текстовой информации и моделей систем передачи информации</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</p> | <p><b>Знать:</b></p> <p>основные понятия информатики;</p> <p>формы и способы представления данных в персональном компьютере</p> <p><b>Уметь:</b></p> <p>использовать расчетные формулы, таблицы, графики, компьютерные программы при решении математических задач;</p> <p>пользоваться сетевыми средствами и внешними носителями информации для обмена данными;</p> <p>применять персональные компьютеры для обработки различных видов информации</p> <p><b>Владеть:</b></p> <p>навыками пользования библиотеками прикладных про-</p>  |

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

|  |   |
|--|---|
| иных источниках информации   | грамм и пакетами программ для решения прикладных математических задач;<br>навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов)   |
| ПК-1 - способностью осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности                  | <b>Знать:</b><br>основные принципы подбора, изучения и обобщения научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности<br><b>Уметь:</b><br>осуществлять подбор, изучение и обобщение научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности<br><b>Владеть:</b><br>навыками подбора, изучения и обобщения научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности   |
| ПК-2 - способностью участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований | <b>Знать:</b><br>защитные механизмы и средства обеспечения безопасности операционных систем;<br>средства и методы хранения и передачи аутентификационной информации;<br>требования к подсистеме аудита и политике аудита;<br>основные средства и методы анализа программных реализаций;<br>основные виды симметричных и асимметричных криптографических алгоритмов;<br>математические модели шифров;<br>основные виды политик управления доступом и информационными потоками в компьютерных системах;<br>основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков;<br>физическую организацию баз данных и принципы (основы) их защиты;<br>защитные механизмы и средства обеспечения сетевой безопасности;<br>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br>основные протоколы идентификации и аутентификации абонентов сети;<br>средства и методы предотвращения и обнаружения вторжений<br><b>Уметь:</b><br>использовать средства защиты, предоставляемые системами управления базами данных;<br>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br><b>Владеть:</b><br>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;<br>навыками анализа программных реализаций;<br>навыками использования инструментальных средств отладки и дизассемблирования программного кода; |


|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

|  |   |
|--|---|
|  | <p>криптографической терминологией;<br/>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками настройки межсетевых экранов</p>  |
| ПК-3 - способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности  | <p><b>Знать:</b><br/>отечественные и зарубежные стандарты в области компьютерной безопасности</p> <p><b>Уметь:</b><br/>проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности</p> <p><b>Владеть:</b><br/>навыками анализа безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности</p>   |
| ПК-4 - способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем  | <p><b>Знать:</b><br/>основные виды политик управления доступом и информационными потоками в компьютерных системах;<br/>основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков</p> <p><b>Уметь:</b><br/>разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками</p> <p><b>Владеть:</b><br/>навыками анализа и участия в разработке математических моделей безопасности компьютерных систем</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><b>Знать:</b><br/>защитные механизмы и средства обеспечения безопасности операционных систем;<br/>средства и методы хранения и передачи аутентификационной информации;<br/>требования к подсистеме аудита и политике аудита;<br/>основные средства и методы анализа программных реализаций;<br/>основные виды симметричных и асимметричных криптографических алгоритмов;<br/>математические модели шифров;<br/>физическую организацию баз данных и принципы (основы) их защиты;<br/>защитные механизмы и средства обеспечения сетевой безопасности;<br/>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/>основные протоколы идентификации и аутентификации абонентов сети;<br/>средства и методы предотвращения и обнаружения вторжений;</p> <p><b>Уметь:</b><br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br/>корректно применять симметричные и асимметричные криптографические алгоритмы;<br/>использовать средства защиты, предоставляемые системами управления базами данных;<br/>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и ап-</p> |


|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

|   |   |
|---|---|
|   | <p>паратных средств защиты;<br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;<br/>навыками анализа программных реализаций;<br/>навыками использования инструментальных средств отладки и дизассемблирования программного кода;<br/>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);<br/>криптографической терминологией;<br/>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками настройки межсетевых экранов</p> |
| ПК-6 - способностью участвовать в разработке проектной и технической документации | <p><b>Знать:</b><br/>защитные механизмы и средства обеспечения безопасности операционных систем;<br/>средства и методы хранения и передачи аутентификационной информации;<br/>требования к подсистеме аудита и политике аудита;<br/>основные средства и методы анализа программных реализаций;<br/>основные виды симметричных и асимметричных криптографических алгоритмов;<br/>математические модели шифров;<br/>физическую организацию баз данных и принципы (основы) их защиты;<br/>защитные механизмы и средства обеспечения сетевой безопасности;<br/>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/>основные протоколы идентификации и аутентификации абонентов сети;<br/>средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;</p>   |




|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |


|   |   |
|---|---|
|   | <p>корректно применять симметричные и асимметричные криптографические алгоритмы;</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><b>Владеть:</b></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>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);</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> |
| <p>ПК-7 - способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем</p> | <p><b>Знать:</b></p> <p>защитные механизмы и средства обеспечения безопасности операционных систем;</p> <p>средства и методы хранения и передачи аутентификационной информации;</p> <p>требования к подсистеме аудита и политике аудита;</p> <p>основные средства и методы анализа программных реализаций;</p> <p>основные виды симметричных и асимметричных криптографических алгоритмов;</p> <p>математические модели шифров;</p> <p>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 аобо-</p>   |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|  |   |
|--|---|
|  | <p>нентов сети;<br/>средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br/>корректно применять симметричные и асимметричные криптографические алгоритмы;<br/>использовать средства защиты, предоставляемые системами управления базами данных;<br/>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе сетевых средств обмена информацией);<br/>криптографической терминологией;<br/>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками настройки межсетевых экранов</p> |
| ПК-8 - способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы | <p><b>Знать:</b><br/>защитные механизмы и средства обеспечения безопасности операционных систем;<br/>средства и методы хранения и передачи аутентификационной информации;<br/>требования к подсистеме аудита и политике аудита;<br/>основные средства и методы анализа программных реализаций;<br/>основные виды симметричных и асимметричных криптографических алгоритмов;<br/>математические модели шифров;<br/>основные виды политик управления доступом и информационными потоками в компьютерных системах;<br/>основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолирован-</p>   |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|  |  |
|--|--|
|  | <p>ной программной среды и безопасности информационных потоков;</p> <p>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><b>Уметь:</b></p> <p>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;</p> <p>корректно применять симметричные и асимметричные криптографические алгоритмы;</p> <p>разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;</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><b>Владеть:</b></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>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);</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> |
|--|--|

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |


|   |   |
|---|---|
|   | <p>навыками настройки межсетевых экранов;</p> <p><b>Знать:</b><br/>основы Интернет-технологий;<br/> типовые структуры и принципы организации компьютерных сетей;<br/> эталонную модель взаимодействия открытых систем;<br/> основы системного программирования;<br/> принципы построения современных операционных систем и особенности их применения;<br/> физическую организацию баз данных и принципы (основы) их защиты;<br/> характеристики и типы систем баз данных</p> <p><b>Уметь:</b><br/> организовывать удаленный доступ к базам данных;<br/> осуществлять нормализацию отношений при проектировании реляционной базы данных</p> <p><b>Владеть:</b><br/> навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/> навыками системного программирования;<br/> навыками конфигурирования и администрирования операционных систем;<br/> методикой составления запросов для поиска информации в базах данных;</p>  |
| <p>ПК-9 - способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы</p>   | <p><b>Знать:</b><br/> защитные механизмы и средства обеспечения безопасности операционных систем;<br/> средства и методы хранения и передачи аутентификационной информации;<br/> требования к подсистеме аудита и политике аудита;<br/> основные средства и методы анализа программных реализаций;<br/> основные виды симметричных и асимметричных криптографических алгоритмов;<br/> математические модели шифров;<br/> физическую организацию баз данных и принципы (основы) их защиты;<br/> защитные механизмы и средства обеспечения сетевой безопасности;<br/> механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/> основные протоколы идентификации и аутентификации абонентов сети;<br/> средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/> формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br/> корректно применять симметричные и асимметричные крип-</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><b>Знать:</b><br/> защитные механизмы и средства обеспечения безопасности операционных систем;<br/> средства и методы хранения и передачи аутентификационной информации;<br/> требования к подсистеме аудита и политике аудита;<br/> основные средства и методы анализа программных реализаций;<br/> основные виды симметричных и асимметричных криптографических алгоритмов;<br/> математические модели шифров;<br/> физическую организацию баз данных и принципы (основы) их защиты;<br/> защитные механизмы и средства обеспечения сетевой безопасности;<br/> механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/> основные протоколы идентификации и аутентификации абонентов сети;<br/> средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/> формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br/> корректно применять симметричные и асимметричные крип-</p> |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|  |   |
|--|---|
|  | <p>тографические алгоритмы;<br/>использовать средства защиты, предоставляемые системами управления базами данных;<br/>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;<br/>навыками анализа программных реализаций;<br/>навыками использования инструментальных средств отладки и дизассемблирования программного кода;<br/>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);<br/>криптографической терминологией;<br/>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>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><b>Знать:</b><br/>защитные механизмы и средства обеспечения безопасности операционных систем;<br/>средства и методы хранения и передачи аутентификационной информации;<br/>требования к подсистеме аудита и политике аудита;<br/>основные средства и методы анализа программных реализаций;<br/>основные виды симметричных и асимметричных криптографических алгоритмов;<br/>математические модели шифров;<br/>физическую организацию баз данных и принципы (основы) их защиты;<br/>защитные механизмы и средства обеспечения сетевой безопасности;<br/>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/>основные протоколы идентификации и аутентификации абонентов сети;</p>   |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |

|  |  |
|--|--|
|  | <p>средства и методы предотвращения и обнаружения вторжений;</p> <p>возможности технических средств перехвата информации;</p> <p>организацию защиты информации от утечки по техническим каналам на объектах информатизации;</p> <p>способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;</p> <p>технические каналы утечки информации</p> <p><b>Уметь:</b></p> <p>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;</p> <p>корректно применять симметричные и асимметричные криптографические алгоритмы;</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>пользоваться нормативными документами по противодействию технической разведке</p> <p><b>Владеть:</b></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>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);</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> <p>методами и средствами технической защиты информации;</p> <p>методами расчета и инструментального контроля показа-</p> |
|--|--|


|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |

|  |  |
|--|--|
|  | телей технической защиты информации  |
| ПК-12 - способностью проводить инструментальный мониторинг защищенности компьютерных систем                        | <p><b>Знать:</b><br/>защитные механизмы и средства обеспечения сетевой безопасности;<br/>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/>основные протоколы идентификации и аутентификации абонентов сети;<br/>средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками настройки межсетевых экранов</p> |
| ПК-14 - способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа | <p><b>Знать:</b><br/>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;<br/>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;<br/>правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;</p> <p><b>Уметь:</b><br/>пользоваться нормативными документами по противодействию технической разведке;<br/>применять действующую законодательную базу в области обеспечения компьютерной безопасности;<br/>применять нормативные правовые акты и нормативные методические документы в области обеспечения инфор-</p>          |


|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

|  |  |
|--|--|
|  | <p>мационной безопасности;<br/>применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;<br/>разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации</p> <p><b>Владеть:</b><br/>методами организации и управления деятельностью служб защиты информации на предприятии;<br/>методами формирования требований по защите информации.<br/>навыками организации и обеспечения режима секретности;<br/>навыками работы с нормативными правовыми актами</p>   |
| ПК-15 - способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы | <p><b>Знать:</b><br/>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;<br/>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;<br/>правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях</p> <p><b>Уметь:</b><br/>пользоваться нормативными документами по противодействию технической разведке;<br/>применять действующую законодательную базу в области обеспечения компьютерной безопасности;<br/>применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;<br/>применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;<br/>разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации</p> <p><b>Владеть:</b><br/>методами организации и управления деятельностью служб защиты информации на предприятии;</p> |




|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |


|  |  |
|--|--|
|  | <p>методами формирования требований по защите информации.</p> <p>навыками организации и обеспечения режима секретности;</p> <p>навыками работы с нормативными правовыми актами</p>   |
| <p>ПК-16 - разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем</p> | <p><b>Знать:</b></p> <p>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;</p> <p>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;</p> <p>правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях</p> <p><b>Уметь:</b></p> <p>пользоваться нормативными документами по противодействию технической разведке;</p> <p>применять действующую законодательную базу в области обеспечения компьютерной безопасности;</p> <p>применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;</p> <p>применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;</p> <p>разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации</p> <p><b>Владеть:</b></p> <p>методами организации и управления деятельностью служб защиты информации на предприятии;</p> <p>методами формирования требований по защите информации.</p> <p>навыками организации и обеспечения режима секретности;</p> <p>навыками работы с нормативными правовыми актами</p> |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|  |   |
|--|---|
| <p>ПК-17 - способностью производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение</p>   | <p><b>Знать:</b><br/>основы Интернет-технологий;<br/> типовые структуры и принципы организации компьютерных сетей;<br/> эталонную модель взаимодействия открытых систем;<br/> основы системного программирования;<br/> принципы построения современных операционных систем и особенности их применения;<br/> физическую организацию баз данных и принципы (основы) их защиты;<br/> характеристики и типы систем баз данных</p> <p><b>Уметь:</b><br/> организовывать удаленный доступ к базам данных;<br/> осуществлять нормализацию отношений при проектировании реляционной базы данных</p> <p><b>Владеть:</b><br/> организовывать удаленный доступ к базам данных;<br/> осуществлять нормализацию отношений при проектировании реляционной базы данных</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><b>Знать:</b><br/> защитные механизмы и средства обеспечения безопасности операционных систем;<br/> средства и методы хранения и передачи аутентификационной информации;<br/> требования к подсистеме аудита и политике аудита;<br/> основные средства и методы анализа программных реализаций;<br/> основные виды симметричных и асимметричных криптографических алгоритмов;<br/> математические модели шифров;<br/> физическую организацию баз данных и принципы (основы) их защиты;<br/> защитные механизмы и средства обеспечения сетевой безопасности;<br/> механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/> основные протоколы идентификации и аутентификации абонентов сети;<br/> средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/> формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br/> корректно применять симметричные и асимметричные криптографические алгоритмы;<br/> использовать средства защиты, предоставляемые системами управления базами данных;<br/> осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и ап-</p> |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|   |   |
|---|---|
|   | <p>паратных средств защиты;<br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;<br/>навыками анализа программных реализаций;<br/>навыками использования инструментальных средств отладки и дизассемблирования программного кода;<br/>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);<br/>криптографической терминологией;<br/>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками настройки межсетевых экранов</p> |
| ПК-19 - способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации | <p><b>Знать:</b><br/>возможности технических средств перехвата информации;<br/>организацию защиты информации от утечки по техническим каналам на объектах информатизации;<br/>способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;<br/>технические каналы утечки информации</p> <p><b>Уметь:</b><br/>пользоваться нормативными документами по противодействию технической разведке</p> <p><b>Владеть:</b><br/>методами и средствами технической защиты информации;<br/>методами расчета и инструментального контроля показателей технической защиты информации</p>   |

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |

|  |  |
|--|--|
| <p>ПК-20 - способностью выпол-нять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций</p> | <p><b>Знать:</b><br/>защитные механизмы и средства обеспечения безопасности операционных систем;<br/>средства и методы хранения и передачи аутентификационной информации;<br/>требования к подсистеме аудита и политике аудита;<br/>основные средства и методы анализа программных реализаций;<br/>основные виды симметричных и асимметричных криптографических алгоритмов;<br/>математические модели шифров;<br/>физическую организацию баз данных и принципы (основы) их защиты;<br/>защитные механизмы и средства обеспечения сетевой безопасности;<br/>механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня;<br/>основные протоколы идентификации и аутентификации абонентов сети;<br/>средства и методы предотвращения и обнаружения вторжений</p> <p><b>Уметь:</b><br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;<br/>корректно применять симметричные и асимметричные криптографические алгоритмы;<br/>использовать средства защиты, предоставляемые системами управления базами данных;<br/>осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;<br/>применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;<br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;<br/>навыками анализа программных реализаций;<br/>навыками использования инструментальных средств отладки и дизассемблирования программного кода;<br/>навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);<br/>криптографической терминологией;</p> |
|--|--|

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |


|   |  |
|---|--|
|   | <p>методиками анализа сетевого трафика;<br/>методиками анализа результатов работы средств обнаружения вторжений;<br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками настройки межсетевых экранов</p>  |
| <p>ПСК-2.1 - способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации</p>   | <p><b>Знать:</b><br/>основы Интернет-технологий;<br/> типовые структуры и принципы организации компьютерных сетей;<br/> эталонную модель взаимодействия открытых систем;<br/> основы системного программирования;<br/> принципы построения современных операционных систем и особенности их применения</p> <p><b>Уметь:</b><br/>организовывать удаленный доступ к базам данных;<br/>осуществлять нормализацию отношений при проектировании реляционной базы данных</p> <p><b>Владеть:</b><br/>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;<br/>навыками системного программирования;<br/>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><b>Знать:</b><br/>защитные механизмы и средства обеспечения безопасности операционных систем;<br/>средства и методы хранения и передачи аутентификационной информации;<br/>требования к подсистеме аудита и политике аудита;<br/>основные средства и методы анализа программных реализаций</p> <p><b>Уметь:</b><br/>формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе</p> <p><b>Владеть:</b><br/>навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств</p>  |

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

|   |   |
|---|---|
| ПСК-2.3 – способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов                | <p><b>Знать:</b><br/>основные виды политик управления доступом и информационными потоками в компьютерных системах;<br/>основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков</p> <p><b>Уметь:</b><br/>разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками</p> <p><b>Владеть:</b><br/>методами формирования требований по защите информации</p>   |
| ПСК-2.4 – способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации                            | <p><b>Знать:</b><br/>основные виды политик управления доступом и информационными потоками в компьютерных системах;<br/>основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков</p> <p><b>Уметь:</b><br/>разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками</p> <p><b>Владеть:</b><br/>методами формирования требований по защите информации</p>   |
| ПСК-2.5 – способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации | <p><b>Знать:</b><br/>возможности технических средств перехвата информации;<br/>организацию защиты информации от утечки по техническим каналам на объектах информатизации;<br/>способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;<br/>технические каналы утечки информации</p> <p><b>Уметь:</b><br/>пользоваться нормативными документами по противодействию технической разведке</p> <p><b>Владеть:</b><br/>методами и средствами технической защиты информации;<br/>методами расчета и инструментального контроля показателей технической защиты информации</p> |

#### 4. МЕСТО И СРОКИ ПРОХОЖДЕНИЯ ПРАКТИКИ

Практика может проводиться в структурных подразделениях (деятельность которых связана с информационной безопасностью) на предприятиях, в учреждениях и организациях:

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

- занимающихся проектированием вычислительных машин, систем, комплексов и сетей с применением новых информационных технологий и средств математического обеспечения;

- проектно-конструкторских и научно-исследовательских учреждениях, занимающихся производством средств вычислительной техники, разработкой информационных систем и технологий;

- проектно-конструкторских и научно-исследовательских учреждениях, использующих средства вычислительной техники, программное обеспечение, информационные системы и технологии;

- оказывающих услуги обеспечения информационной безопасности;

- занимающихся разработкой программных продуктов.

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

Время прохождения преддипломной практики: в 11-м семестре.

### 5. ОБЩАЯ ТРУДОЕМКОСТЬ ПРАКТИКИ

| Объем практики |      | Продолжительность практики |
|----------------|------|----------------------------|
| з.е.           | часы | недели                     |
| 15             | 540  | 10                         |

### 6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ


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

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

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

Порядок прохождения практики:

1. Получить отметку в отделе кадров предприятия о прибытии на практику.

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

2. Получить вводный и первичный инструктаж на рабочем месте по охране труда.
3. Изучить функциональные обязанности инженера отдела (специалиста по защите информации) и практически их выполнять.
4. Изучить информационную систему предприятия.
5. Выполнить задачи, поставленные руководителем практики от предприятия.
6. Заполнять журнал прохождения практики.
7. Подготовить отчет по практике.
8. По 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 преддипломной практике изучаются современные информационные технологии обеспечения информационной безопасности, используемые в технологических производственных процессах предприятия.

## **8. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ПРАКТИКИ**

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

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

- обеспечение высокого качества 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 выполненной студентом работы в период практики.

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

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



|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

отчисления студента из университета.

## 9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

### а) Список рекомендуемой литературы:

#### основная

1. Защита информации: основы теории: учебник для бакалавриата и магистратуры / Щеглов А. Ю., Щеглов К. А. – М.: Издательство Юрайт, 2019. – 309 с. <https://biblionline.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/](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/](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/](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/](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>

1. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт. журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: [http://journals.tsu.ru/pdm/&journal\\_page=archive&id=1823](http://journals.tsu.ru/pdm/&journal_page=archive&id=1823)

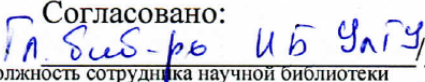
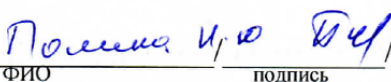
#### учебно-методическая


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. Иванцов А. М.

Методические указания для самостоятельной работы по преддипломной практике для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана; Непубликованный ресурс. - Электрон. текстовые дан. (1 файл : 359 КБ). - Текст : электронный.

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

Согласовано:  
  05.06.2020  
 Должность сотрудника научной библиотеки \_\_\_\_\_ ФИО \_\_\_\_\_ подпись \_\_\_\_\_ дата \_\_\_\_\_

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

## **б) Программное обеспечение**

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

## **в) Профессиональные базы данных, информационно-справочные системы**

### **1. Электронно-библиотечные системы:**

1.1. IPRbooks : 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](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. /Компания «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](http://window.edu.ru/) : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст :

|  |       |  |
|--|-------|--|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |  |

электронный.

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

7. **Электронная библиотека диссертаций РГБ** [Электронный ресурс]: электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2020]. - Режим доступа: <https://dvs.rsl.ru>.

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

**9. Образовательные ресурсы УлГУ:**

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

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

Согласовано:

Зам.нач. УИТиТ  
должность сотрудника УИТиТ

/ Клочкова А.В.  
ФИО

/   
подпись

/ 05.06.2020  
дата

**11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:**

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

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


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

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

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

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

|  |       |   |
|--|-------|---|
| Министерство науки и высшего образования РФ<br>Ульяновский государственный университет | Форма |  |
| Ф- Рабочая программа   |       |   |

нахождение указанным лицом своего рабочего места и выполнение индивидуального задания;

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

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

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


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

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





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

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

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

Разработчик:  Иванцов Андрей Михайлович  
подпись должность ФИО

## ЛИСТ ИЗМЕНЕНИЙ

| №<br>п/п | Содержание изменения или ссылка на прилагаемый текст изменения  | ФИО<br>заведующего<br>кафедрой,<br>реализующей<br>дисциплину/вы<br>-<br>пускающей<br>кафедрой | Подпись   | Дата  |
|----------|---|---|---|---|
| 1        | Внесение изменений в п.п. 4.2 Объем дисциплины по видам учебной работы п. «Общая трудоемкость дисциплины» с оформлением приложения 1  | Андреев А.С.  |    | 08.04.2020<br>Протокол заседания кафедры № 12 |
| 2        | Внесение изменений в п. 13 «Специальные условия для обучающихся с ограниченными возможностями здоровья» с оформлением приложения 2  | Андреев А.С.  |    | 08.04.2020<br>Протокол заседания кафедры № 12 |
| 3        | Внесение изменений в п/п а) Список рекомендуемой литературы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 3                                | Андреев А.С.  |   | 27.05.2020<br>Протокол заседания кафедры № 14 |
| 4        | Внесение изменений в п/п в) Профессиональные базы данных, информационно-справочные системы п. 11 «Учебно-методическое и информационное обеспечение дисциплины» с оформлением приложения 4 | Андреев А.С.  |  | 27.05.2020<br>Протокол заседания кафедры № 14 |
|          |   |   |   |   |

## 6. Структура и содержание практики

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

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

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

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

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

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

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

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

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

## 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://biblionline.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/](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/](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/](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/](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.

<http://gostexpert.ru/gost/gost-27002-2012>

1. Прикладная дискретная математика [Электронный ресурс]: Междунар. ежекварт. журнал. –Томск., 2017-2019.- ISSN 2311-2263. - Режим доступа: [http://journals.tsu.ru/pdm/&journal\\_page=archive&id=1823](http://journals.tsu.ru/pdm/&journal_page=archive&id=1823)

#### 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. Иванцов А. М.

Методические указания для самостоятельной работы по преддипломной практике для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения / А. М. Иванцов; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2020. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 359 КБ). - Текст : электронный.

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

Согласовано:  
 П.А. Суб-ро ИБ УлГУ \_\_\_\_\_ Попова И.Ю. ДЧ, 05.06.2020  
 Должность сотрудника научной библиотеки \_\_\_\_\_ ФИО \_\_\_\_\_ подпись \_\_\_\_\_ дата \_\_\_\_\_



## 9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

### б) Программное обеспечение

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

### в) Профессиональные базы данных, информационно-справочные системы

#### 1. Электронно-библиотечные системы:

1.1. IPRbooks : 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](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. /Компания «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://ebco.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 /  
учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: <http://window.edu.ru/>. – Текст :

электронный.

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

7. Электронная библиотека диссертаций РГБ [Электронный ресурс]:  
электронная библиотека / ФГБУ РГБ. - Электрон. дан. – Москва, [2020]. - Режим доступа:  
<https://dvs.rsl.ru>.

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

**9. Образовательные ресурсы УлГУ:**

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

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

Согласовано:

Зам.нач. УИТиГ  
должность сотрудника УИТиГ

/ Клочкова А.В.  
ФИО

/   
подпись

/ 05.06.2020  
дата