


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

### «Производственная практика» «Научно-исследовательская работа»

по специальности 10.05.01 «Компьютерная безопасность»  
специализация «Математические методы защиты информации»

#### 1. Цели и задачи практики

##### Цели прохождения практики:

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

##### Задачи прохождения практики:

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


#### 2. Место практики в структуре ОПОП ВО

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

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

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

Прохождение практики (НИР) предшествует прохождению преддипломной


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

практики, написанию и защите выпускной квалификационной работы в соответствии с выбранным направлением научного исследования.


### 3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

В совокупности с дисциплинами базовой и вариативной части математического и естественнонаучного цикла ФГОС ВО научно-исследовательская работа направлена на формирование компетенций по специальности «Компьютерная безопасность».


Индекс и наименование реализуемой компетенции	Перечень планируемых результатов прохождения практики, соотнесенных с индикаторами достижения компетенций
ОК-5 – способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности; основные термины по проблематике информационной безопасности; роль и место информационной безопасности в системе национальной безопасности страны; угрозы информационной безопасности государства; содержание информационной войны, методы и средства ее ведения; Уметь: пользоваться современной научно-технической информацией по исследуемым проблемам и задачам Владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
ОК-7 – способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	Знать: свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления Уметь: квалифицированно исследовать состав документации предприятия (организации) Владеть: методами формирования требований по защите информации
ОК-8 – способностью к самоорганизации и самообразованию	Знать: основные методы управления информационной безопасностью Уметь: оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем Владеть: методами управления информационной безопасностью информационных систем; методами оценки информационных рисков
ОПК-2 – способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории	Знать: основные понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основы теории групп и теории групп подстановок; свойства векторных пространств; свойства кольца многочленов; основные понятия и задачи векторной алгебры и аналитической геометрии; основные понятия и методы дискретной математики; основные понятия математической логики и теории алгоритмов;

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

<p>вероятностей, математической статистики, теории информации, теоретико-числовых методов</p>	<p>абстрактный интеграл Лебега и его основные свойства; основные положения теории пределов функций, теории рядов; основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; понятие меры, измеримые функции и их свойства; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; основные понятия и методы теории вероятностей, математической статистики и теории случайных процессов; основные понятия и методы теории информации; Уметь: решать основные задачи векторной алгебры и аналитической геометрии; решать системы линейных уравнений над полями; решать основные задачи векторной алгебры и аналитической геометрии; использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечисленных задач; находить представление и исследовать свойства булевых и многозначных функций формулами в различных базисах; определять возможности применения методов математического анализа; решать основные задачи теории пределов функций, дифференцирования, интегрирования и разложения функций в ряды; проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ; применять стандартные методы и модели к решению теоретико-вероятностных и статистических задач; вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); Владеть: навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения систем линейных уравнений над полем и кольцом вычетов; навыками решения стандартных задач в векторных пространствах; навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения задач дискретной математики; навыками использования языка математической логики; навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач; навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов. основами построения математических моделей текстовой информации и моделей систем передачи информации;</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; Уметь: использовать расчетные формулы, таблицы, графики, компьютерные программы при решении математических задач; пользоваться сетевыми средствами и внешними носителями информации для обмена данными; применять персональные компьютеры для обработки различных видов информации; Владеть: навыками пользования библиотеками прикладных программ и пакетами программ для решения прикладных математических задач; навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов)</p>
<p>ПК-1 – способностью осуществлять подбор, изучение и обобщение</p>	<p>Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации;</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		


<p>научно-технической информации, нормативных, правовых и методических материалов, отечественного и зарубежного опыта по проблемам компьютерной безопасности</p>	<p>требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;</p>
<p>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</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, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		


	<p>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-3 – способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	<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 систем, в том числе политики управления доступом и информационными потоками;</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 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>Знать:</p> <p>защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; 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 абонентов сети;</p> <p>средства и методы предотвращения и обнаружения вторжений;</p> <p>Уметь:</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>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</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

	<p>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>
ПК-6 – способностью участвовать в разработке проектной и технической документации	<p>Знать:</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 абонентов сети;</p> <p>средства и методы предотвращения и обнаружения вторжений;</p> <p>Уметь:</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>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>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>
ПК-7 – способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем	<p>Знать:</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>


Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

	<p>основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;</p>
<p>ПК-8 – способностью участвовать в разработке подсистемы информационной безопасности компьютерной системы</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 операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информации);</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

	ей); криптографической терминологией; методиками анализа сетевого трафика; методиками анализа результатов работы средств обнаружения вторжений; навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов;
ПК-9 – способностью участвовать в проведении экспериментально-исследовательских работ при аттестации объектов с учетом требований к уровню защищенности компьютерной системы	Знать: основы Интернет-технологий; типовые структуры и принципы организации компьютерных сетей; эталонную модель взаимодействия открытых систем; основы системного программирования; принципы построения современных операционных систем и особенности их применения; физическую организацию баз данных и принципы (основы) их защиты; характеристики и типы систем баз данных; Уметь: организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы данных; Владеть: навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками системного программирования; навыками конфигурирования и администрирования операционных систем; методикой составления запросов для поиска информации в базах данных;
ПК-10 – способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знать: защитные механизмы и средства обеспечения безопасности операционных систем; средства и методы хранения и передачи аутентификационной информации; требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров; физическую организацию баз данных и принципы (основы) их защиты; защитные механизмы и средства обеспечения сетевой безопасности; механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; корректно применять симметричные и асимметричные криптографические алгоритмы; использовать средства защиты, предоставляемые системами управления базами данных; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; навыками анализа программных реализаций; навыками использования инструментальных средств отладки и дизассемблирования программного кода; навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией); криптографической терминологией;




Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		


	<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-11 – способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации</p>	<p>Знать:</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 абонентов сети;</p> <p>средства и методы предотвращения и обнаружения вторжений;</p> <p>Уметь:</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>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>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-12 – способностью проводить инструментальный мониторинг защищенности компьютерных систем</p>	<p>Знать:</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>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>методиками анализа сетевого трафика;</p> <p>методиками анализа результатов работы средств обнаружения вторжений;</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		


	<p>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;</p> <p>навыками настройки межсетевых экранов;</p>
<p>ПК-14 – способностью организовать работы по выполнению режима защиты информации, в том числе ограниченного доступа</p>	<p>Знать:</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>Уметь:</p> <p>пользоваться нормативными документами по противодействию технической разведке; 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>Владеть:</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>
<p>ПК-15 – способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p>	<p>Знать:</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>Уметь:</p> <p>пользоваться нормативными документами по противодействию технической разведке; 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>Владеть:</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>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

	<p>навыками работы с нормативными правовыми актами;</p> <p><b>ПК-16 – разрабатывать проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем</b></p>
	<p><b>Знать:</b> 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;</p> <p><b>Уметь:</b> 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><b>Владеть:</b> 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><b>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</b></p>
	<p><b>Знать:</b> основы Интернет-технологий; типовые структуры и принципы организации компьютерных сетей; эталонную модель взаимодействия открытых систем; основы системного программирования; принципы построения современных операционных систем и особенности их применения; физическую организацию баз данных и принципы (основы) их защиты; характеристики и типы систем баз данных;</p> <p><b>Уметь:</b> организовывать удаленный доступ к базам данных; осуществлять нормализацию отношений при проектировании реляционной базы данных;</p> <p><b>Владеть:</b> навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств; навыками системного программирования; навыками конфигурирования и администрирования операционных систем; методикой составления запросов для поиска информации в базах данных;</p>
	<p><b>ПК-18 – способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы,</b></p>
	<p><b>Знать:</b> 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;</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	<p>основные протоколы идентификации и аутентификации абонентов сети; средства и методы предотвращения и обнаружения вторжений;</p> <p>Уметь:</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; использовать средства защиты, предоставляемые системами управления базами данных; 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>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>
ПК-19 – способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации	<p>Знать:</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>Уметь:</p> <p>пользоваться нормативными документами по противодействию технической разведке;</p> <p>Владеть:</p> <p>методами и средствами технической защиты информации;</p> <p>методами расчета и инструментального контроля показателей технической защиты информации;</p>
ПСК-2.1 – способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	<p>Знать:</p> <p>основы Интернет-технологий;</p> <p>типовые структуры и принципы организации компьютерных сетей;</p> <p>эталонную модель взаимодействия открытых систем;</p> <p>основы системного программирования;</p> <p>принципы построения современных операционных систем и особенности их применения;</p> <p>Уметь:</p> <p>организовывать удаленный доступ к базам данных;</p> <p>осуществлять нормализацию отношений при проектировании реляционной базы данных;</p> <p>Владеть:</p> <p>навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств;</p> <p>навыками системного программирования;</p> <p>навыками конфигурирования и администрирования операционных систем;</p>
ПСК-2.2 – способностью на основе анализа применяемых	<p>Знать:</p> <p>защитные механизмы и средства обеспечения безопасности операционных систем;</p> <p>средства и методы хранения и передачи аутентификационной информации;</p>

Министерство науки и высшего образования Российской Федерации Ульяновский государственный университет	Форма	
Ф – Аннотация рабочей программы дисциплины		

математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	требования к подсистеме аудита и политике аудита; основные средства и методы анализа программных реализаций; Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; Владеть: навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств;
ПСК-2.3 – способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; Владеть: методами формирования требований по защите информации
ПСК-2.4 – способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; Уметь: разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; Владеть: методами формирования требований по защите информации
ПСК-2.5 – способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации учетом современных и перспективных математических методов защиты информации	Знать: возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; технические каналы утечки информации; Уметь: пользоваться нормативными документами по противодействию технической разведке; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации;

#### 4. Общая трудоемкость практики

Общая трудоемкость НИР составляет 6 зачетных единиц (216 часа)

#### 5. Образовательные технологии

НИР носит теоретический и практический характер. При ее проведении используются стандартные образовательные технологии: лекции, экскурсии, а также самостоятельная работа студентов. Кроме того, проводится установочная и итоговая конференции, работа с информационными ресурсами, программным обеспечением.

#### 6. Контроль успеваемости

Программой НИР предусмотрены следующие виды текущего контроля: текущая проверка разделов отчета по НИР.

Итоговая аттестация проводится в форме: доклад и защита.