

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

УТВЕРЖДЕНО
Ученым советом факультета
Математики, информационных и авиационных технологий
от «20» 06 2017 г., протокол № 6/17
Председатель 18/17
120 06 2017 г.

РАБОЧАЯ ПРОГРАММА НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»
Факультет математики, информационных и авиационных технологий
Курс 5 Семестр 10 Форма обучения очная
Форма отчетности: диф. зачет

Сведения о разработчиках:

ФИО	Аббревиатура кафедры (наименование цикла, отделения)	Ученая степень, звание
Перцева Ирина Анатольевна	ИБиТУ	к.ф.-м.н., доцент
Рацеев Сергей Михайлович	ИБиТУ	д.ф.-м.н., доцент

Дата введения в учебный процесс УлГУ 01.09.2017

Программа актуализирована на заседании кафедры: протокол №__ от _____ 20__ г.

Программа актуализирована на заседании кафедры: протокол №__ от _____ 20__ г.

Программа актуализирована на заседании кафедры: протокол №__ от _____ 20__ г.

Программа актуализирована на заседании кафедры: протокол №__ от _____ 20__ г.

СОГЛАСОВАНО:	
Заведующий кафедрой	
<u></u> (Подпись)	/ <u>А.С. Андреев</u> / (Ф.И.О.)
« <u>13</u> » <u>06</u>	20 <u>17</u> г.

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

1. ЦЕЛИ И ЗАДАЧИ НИР

Цели научно-исследовательской работы:

- 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 научно-исследовательской работы:

- 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 НИР В СТРУКТУРЕ ОПОП ВО

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

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

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

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ВЫПОЛНЕНИИ НИР СТУДЕНТОВ

В совокупности с дисциплинами базовой и вариативной части ФГОС ВО по специальности «Информационная безопасность автоматизированных систем» научно-исследовательская работа направлена на формирование следующих компетенций:

- способностью понимать социальную значимость своей будущей профессии, обладать

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

- высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- 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 (ОК-7);
 - способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);
 - способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
 - способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
 - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);
 - способностью создавать и исследовать модели автоматизированных систем (ПК-2);
 - способностью проводить анализ защищенности автоматизированных систем (ПК-3);
 - способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
 - способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
 - способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
 - способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);
 - способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
 - способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
 - способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);
 - способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
 - способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации (ПК-16);
 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);
 - способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);
 - способностью администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

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

- способностью управлять информационной безопасностью автоматизированной системы (ПК-28).
- способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);
- способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);
- способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);
- способностью участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);
способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5).

В результате выполнения научно исследовательской работы студент должен:

- знать порядок и методы проведения и оформления научных исследований;
- уметь пользоваться периодическими реферативными и справочно-информационными изданиями по профилю работы;
- владеть навыками самостоятельной работы с литературой и приобрести опыт использования современной вычислительной техники для решения задач по защите информации;

4. МЕСТО И СРОКИ ПРОВЕДЕНИЯ НИР

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

- занимающихся проектированием вычислительных машин, систем, комплексов и сетей с применением новых информационных технологий и средств математического обеспечения;
- проектно-конструкторских и научно-исследовательских учреждениях, занимающихся производством средств вычислительной техники, разработкой информационных систем и технологий;
- проектно-конструкторских и научно-исследовательских учреждениях, использующих средства вычислительной техники, программное обеспечение, информационные системы и технологии;
- оказывающих услуги обеспечения информационной безопасности;
- занимающихся разработкой программных продуктов.

Время прохождения НИР: в 10-м семестре.

5. ОБЪЕМ НИР В ЗАЧЕТНЫХ ЕДИНИЦАХ (ЗЕ) И ЕЕ ПРОДОЛЖИТЕЛЬНОСТЬ В НЕДЕЛЯХ

Объем НИР составляет 6 ЗЕ (10-й семестр).

6. СТРУКТУРА И СОДЕРЖАНИЕ НИР

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

Общая трудоемкость НИР составляет 6 зачетных единиц, 216 часов.

4.1. Примерный календарный план выполнения НИР

№ п/п	Раздел НИР	Трудоемкость (в часах)
1.	Организационные мероприятия	4
2.	Теоретический (аналитический) этап	100
	Практический этап	100
3.	Обобщение материалов и оформление отчета по НИР	12
	ИТОГО:	216

4.2. Примерное распределение часов по видам работы:

№ п/п	Раздел НИР	Количество (час)
1.	Определение задач, плана работ и средств для его выполнения.	10
2.	Сбор, обработка, систематизация фактического материала по теме исследования	40
3.	Решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей НИР	70
4.	Тестирование программ и оценка качества решения задач	30
5.	Проведение вычислительного эксперимента	30
6.	Обработка и оформление результатов работы,	24
7.	Подготовка и защита отчета по НИР.	12
	Всего:	216

Примечание. Распределение часов по видам работы может варьироваться в зависимости от темы НИР студента. Целесообразно тему НИР увязывать с темой ВКР.

7. НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЕ И НАУЧНО-ПРОИЗВОДСТВЕННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ В НИР

В процессе НИР руководителями от кафедры (руководителем от организации) должны применяться современные образовательные и научно-производственные технологии:

- мультимедийные технологии, для чего ознакомительные лекции и инструктаж студентов по НИР проводятся в помещениях, оборудованных экраном, видеопроектором, персональными компьютерами;
- дистанционная форма консультаций во время прохождения конкретных этапов НИР;
- компьютерные технологии и программные продукты, необходимые для сбора и систематизации информации, проведения требуемых программой НИР расчетов и т.д.

8. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ НИР

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

Научно-исследовательская работа выполняется студентом под руководством научного руководителя.

Направление научно-исследовательских работ студента определяется в соответствии с темой выпускной квалификационной работы.

Обсуждение плана и промежуточных результатов НИР проводится на выпускающей кафедре.

Результаты научно-исследовательской работы должны быть оформлены в письменном виде (отчет) и представлены для утверждения научному руководителю. НИР должна быть законченным научным материалом, иметь факты и данные, раскрывающие взаимосвязь между явлениями, процессами, аргументами, действиями и содержать нечто новое: обобщение обширной литературы, материалы самостоятельных исследований, в которых появляется авторское видение проблемы и ее решение. Образец титульного листа отчета о научно-исследовательской работе приводится в приложении. В приложении могут быть представлены ксерокопии статей, тезисов докладов и др..

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

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

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НИР

Список используемой литературы

а) основная

1. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М. ДМК Пресс, 2010. - 544 с. ил.
2. Девянин П.Н. Модели безопасности компьютерных систем. Учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2005. – 144 с.
3. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для вузов. – М.: Академия, 2008. – 336 с.
4. Семкин С.Н. Основы правового обеспечения защиты информации – М: Горячая линия – Телеком, 2008.
5. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник – М: Академия, 2008.
6. Методические указания по разработке типовых документов в области информационной безопасности /А.М. Иванцов. – Ульяновск: УлГУ, 2016 – 63 с.
7. Хореев П.В. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов. – М.: Академия, 2007. – 256 с.
8. Информационная безопасность открытых систем: учебник для вузов по спец. 075500 (090105) - "Комплексное обеспечение информационной безопасности автоматизированных систем": в 2 т. /Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В.. - М.: Горячая линия-Телеком, 2008. - 558 с.

б) дополнительная

1. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента.
2. Методологические основы построения защищенных автоматизированных систем. Учебное пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др. – Воронеж: ВГУИТ, 2013. – 263 с.

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

в) программное обеспечение

Для образовательного процесса студенту необходимо рабочее место с ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования: Visual Studio 2012/Qt.

г) базы данных, информационно-справочные и поисковые

Электронный каталог библиотеки УлГУ.

Система ГАРАНТ: электронный периодический справочник [Электронный ресурс].

Consultplus: справочно-поисковая система [Электронный ресурс].

Система IPRBooks: электронно-библиотечная система [Электронный ресурс].

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ НИР

В процессе НИР студенты используют научно-исследовательское оборудование, которым обладает организация (учреждение), либо кафедра информационной безопасности и теории управления.

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

Приложение 1. ФОС

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ФОС)

1. Перечень компетенций по дисциплине (модулю) для обучающихся по направлению подготовки (специальности) с указанием этапов их формирования в процессе освоения ОПОП ВО

№ семестра	Наименование	ОК-5	ОК-7	ОПК-1	ОПК-2	ОПК-3	ПК-1	ПК-2	ПК-3	ПК-4	ПК-5	ПК-7	ПК-8	ПК-9	ПК-11	ПК-12	ПК-13	ПК-14	ПК-16	ПК-17	ПК-21	ПК-26	ПК-28	ПК-4.1	ПК-4.2	ПК-4.3	ПК-4.4	ПК-4.5	
1-4	Иностранный язык		+																										
8	Основы управленческой деятельности	+	+																			+							
1-3	Математический анализ				+	+																							
3-4	Теория вероятностей и математическая статистика				+	+																							
1-2	Алгебра и геометрия				+	+																							
4	Дискретная математика				+	+																							
7	Теория информации					+																							
1-2	Математическая логика и теория алгоритмов					+																							
1-3	Физика				+																								
2	Инженерная графика											+		+		+	+												
3-4	Электроника и схемотехника					+																		+					
2-3	Языки программирования					+	+																	+					
7-8	Организация ЭВМ и вычислительных систем		+		+																			+					
6	Сети и системы передачи информации				+			+																					
2-3	Технологии и методы программирования					+	+						+											+					
5	Основы информационной безопасности																							+					
6	Криптографические методы защиты информации				+	+	+	+	+	+					+		+	+						+					
4-5	Безопасность операционных систем						+	+				+												+					
8	Безопасность сетей ЭВМ					+	+	+				+												+	+				
6-7	Безопасность систем баз данных					+						+	+	+									+						
6	Техническая защита информации				+					+	+	+							+	+	+	+							
6	Управление информационной безопасностью				+	+		+				+	+		+	+	+	+				+	+		+				
5	Организационное и правовое обеспечение информационной					+		+		+		+	+				+	+	+										

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

2. Требования к результатам освоения НИР

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны:		
			знать	уметь	владеть
1	2	3	4	5	6
1.	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	основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые события истории России и мира с древности до наших дней, выдающихся деятелей отечественной истории; различные оценки и периодизации Отечественной истории;	соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; извлекать уроки из исторических событий и на их основе принимать осознанные решения; осуществлять эффективный поиск информации и критику источников; получать, обрабатывать и сохранять источники информации; формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории; анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав	представлениями о событиях российской и всемирной истории, основанными на принципе историзма; навыками анализа исторических источников; приемами ведения дискуссии и полемики; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности
2.	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		осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий	навыками работы с технической документацией на ЭВМ и вычислительные системы
3.	ОПК-1	способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	основные законы механики; основные законы термодинамики и молекулярной физики; основные законы электричества и магнетизма; основы теории колебаний и волн, оптики; основы квантовой физики и физики твёрдого тела; физические явления и эффекты, используемые при обработке, хранении, передаче, уничтожении и защите информации основные методы управления информационной безопасностью; основные угрозы безопас-	определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач строить математические модели физических явлений и процессов; решать типовые прикладные физические зада-	навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры навыками построения дискретных моделей при решении профессиональных задач методами теоретического исследования физических явлений и процессов; навыками проведения физического эксперимента и обработки его результатов

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

			ности информации и модели нарушителя в автоматизированных системах	чи; анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; применять математические методы исследования моделей шифров основы физической защиты объектов информатизации выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем	
4.	ОПК-2	способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	возможности координатного метода для исследования различных геометрических объектов, основные задачи векторной алгебры и аналитической геометрии, основные виды уравнений простейших геометрических объектов, основные свойства важнейших алгебраических структур, основы линейной алгебры над произвольными полями, векторные пространства над полями и их свойства основы комбинаторного анализа; метод включения-исключения; производящие функции; основные понятия теории автоматов; основные понятия и алгоритмы теории графов; основные дискретные структуры: конечные автоматы, графы, комбинаторные структуры; методы перечисления для основных дискретных структур; основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи основные понятия математической логики и теории алгоритмов; язык и средства современной математической логики, представления булевых функций и способы минимизации формул; типичные свойства и способы задания функций много-	строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач, определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач, исследовать простейшие геометрические объекты по их уравнениям в различных системах координат, оперировать с числовыми и конечными полями, многочленами, матрицами, решать основные задачи линейной алгебры, в частности системы линейных уравнений над полями применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач; решать задачи периодичности и эквивалентности для конечных автоматов; применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач; решать оптимизационные задачи на графах; находить и исследовать свойства представлений булевых многозначных функций формулами в	навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике, методами линейной алгебры навыками построения дискретных моделей при решении профессиональных задач; навыками применения языка и средств дискретной математики; навыками решения комбинаторных и теоретико-графовых задач; навыками применения математического аппарата для решения прикладных теоретико-информационных задач; навыками использования языка современной символической логики; навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач; навыками упрощения формул алгебры высказываний и алгебры предикатов; навыками составления программ на машинах Тьюринга; навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач; навыками использования стандартных методов и моделей математического анализа и их примене-

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

			<p>значной логики.</p> <p>различные подходы к определению алгоритма и доказательства алгоритмической неразрешимости отдельных массовых задач,</p> <p>подходы к оценкам сложности алгоритмов,</p> <p>методы построения эффективных алгоритмов,</p> <p>возможности применения общих логических принципов в математике и профессиональной деятельности</p> <p>основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики</p> <p>основные положения теории пределов и непрерывных функций, теории числовых и функциональных рядов;</p> <p>основные теоремы дифференциального и интегрального исчисления функций одной и нескольких переменных;</p> <p>основные понятия теории функций комплексной переменной;</p> <p>основные методы решения простейших дифференциальных уравнений и систем дифференциальных уравнений</p> <p>основные понятия теории информации: энтропия, взаимная информация, источники сообщений, каналы связи, коды;</p> <p>основные теоремы о кодировании при наличии и отсутствии шума;</p> <p>основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи</p> <p>эталонную модель взаимодействия открытых систем</p> <p>основные задачи и понятия криптографии;</p> <p>частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки</p> <p>основные информационные технологии, используемые в автоматизированных системах;</p> <p>автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;</p> <p>методы, способы, средства, последовательность и содер-</p>	<p>различных базисах;</p> <p>оценивать сложность алгоритмов и вычислений;</p> <p>классифицировать алгоритмы по классам сложности;</p> <p>применять методы математической логики и теории алгоритмов к решению задач математической кибернетики;</p> <p>строить и изучать математические модели конкретных явлений и процессов для решения расчётных и исследовательских задач;</p> <p>определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач;</p> <p>применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;</p> <p>пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач</p> <p>строить и изучать математические модели конкретных явлений и процессов для решения расчётных и исследовательских задач;</p> <p>определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач;</p> <p>решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды</p> <p>вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность);</p> <p>решать типовые задачи кодирования и декодирования;</p> <p>работать с научно-технической литературой по тематике дисциплины</p>	<p>ния к решению прикладных задач;</p> <p>навыками решения задач с применением аппарата теории функций комплексной переменной;</p> <p>навыками использования стандартных методов решения типовых дифференциальных уравнений;</p> <p>навыками пользования библиотеками прикладных программ для решения прикладных математических задач</p> <p>основами построения математических моделей систем передачи информации;</p> <p>навыками применения математического аппарата для решения прикладных теоретико-информационных задач</p> <p>методами формирования требований по защите информации</p> <p>методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем</p> <p>методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;</p> <p>навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;</p> <p>навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</p> <p>навыками программирования с использованием эффективных реализаций структур данных и алгоритмов</p>
--	--	--	--	--	--

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

			<p>жание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>способы кодирования информации</p> <p>современные технологии и методы программирования</p> <p>методы анализа и синтеза электронных схем</p> <p>язык программирования высокого уровня (объектно-ориентированное программирование);</p> <p>возможности, классификацию и область применения макрообработки</p>	<p>разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем</p> <p>применять на практике методы анализа электрических цепей</p>	
5.	ОПК-3	<p>способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p>	<p>принципы построения и функционирования, примеры реализаций современных операционных систем</p> <p>принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей</p> <p>основные информационные технологии, используемые в автоматизированных системах</p> <p>показатели качества программного обеспечения</p> <p>язык программирования высокого уровня (объектно-ориентированное программирование);</p> <p>возможности, классификацию и область применения макрообработки;</p> <p>способы обработки исключительных ситуаций</p>	<p>создавать объекты базы данных;</p> <p>выполнять запросы к базе данных;</p> <p>разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных</p> <p>исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений</p> <p>формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения</p> <p>работать с интегрированной средой разработки программного обеспечения;</p> <p>использовать шаблоны классов и средства макрообработки;</p> <p>использовать динамически подключаемые библиотеки</p>	<p>навыками использования ЭВМ в анализе простейших шифров</p> <p>навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;</p> <p>навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ</p> <p>навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;</p> <p>навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;</p> <p>навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</p> <p>навыками проектирования программного обеспечения с использованием средств автоматизации;</p> <p>навыками разработки программной документации</p>
6.	ПК-1	<p>способностью осуществлять поиск, изучение, обобщение и систематизацию научнотехнической информации, нормативных и</p>	<p>разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом</p>	<p>навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках</p>	<p>Разработка и эксплуатация защищенных автоматизированных систем</p>

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

		методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	действующих нормативных и методических документов		
7.	ПК-2	способностью создавать и исследовать модели автоматизированных систем	<p>модели шифров и математические методы их исследования</p> <p>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</p> <p>основные характеристики сигналов электросвязи, спектры и виды модуляции;</p> <p>эталонную модель взаимодействия открытых систем;</p> <p>принципы построения и функционирования систем и сетей передачи информации</p>	<p>разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений</p>	<p>навыками математического моделирования в криптографии</p> <p>методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;</p> <p>навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем</p> <p>навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;</p> <p>навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</p>
8.	ПК-3	способностью проводить анализ защищенности автоматизированных систем	<p>требования к шифрам и основные характеристики шифров;</p> <p>модели шифров и математические методы их исследования</p> <p>программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях</p> <p>технические каналы утечки информации;</p> <p>возможности технических средств перехвата информации;</p> <p>организацию защиты информации от утечки по техническим каналам на объектах информатизации</p>	<p>разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем</p> <p>исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений</p>	<p>навыками математического моделирования в криптографии</p> <p>методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;</p> <p>навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем</p> <p>навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;</p> <p>навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем</p> <p>навыками организации и обеспечения режима секретности</p>
9.	ПК-4	способностью разрабатывать модели угроз и модели нарушителя информационной	<p>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</p> <p>основные меры по защите</p>	<p>разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности</p>	

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

		безопасности автоматизированной системы	информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	автоматизированных систем анализировать и оценивать угрозы информационной безопасности объекта	
10.	ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы	требования к шифрам и основные характеристики шифров	анализировать и оценивать угрозы информационной безопасности объекта	
11.	ПК-7	способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	принципы построения и функционирования, примеры реализаций современных операционных систем	разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации; разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов	навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности
12.	ПК-8	способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	средства обеспечения безопасности данных основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации показатели качества программного обеспечения; методологии и методы проектирования программного обеспечения; методы тестирования и отладки ПО; принципы организации документирования разработки, процесса сопровождения программного обеспечения; основные структуры данных и способы их реализации на языке программирования; основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности	формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения; планировать разработку сложного программного обеспечения; проводить комплексное тестирование и отладку программных систем; проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования; реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования; проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач; работать с интегрированной средой разработки программного обеспечения оценивать информационные риски в автоматизированных системах	навыками участия в экспертизе состояния защищенности информации на объекте защиты навыками проектирования программного обеспечения с использованием средств автоматизации; навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования; навыками разработки программной документации; навыками программирования с использованием эффективных реализаций структур данных и алгоритмов

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

13.	ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	принципы построения и функционирования, примеры реализаций современных систем управления базами данных; архитектуру систем баз данных; основные модели данных; физическую организацию баз данных; последовательность и содержание этапов проектирования баз данных	разрабатывать и администрировать базы данных; выделять сущности и связи предметной области; отображать предметную область на конкретную модель данных; нормализовывать отношения при проектировании реляционной базы данных применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации
14.	ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	основные задачи и понятия криптографии основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем разрабатывать частные политики информационной безопасности автоматизированных систем	навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности
15.	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы		применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации оценивать информационные риски в автоматизированных системах	навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации навыками участия в экспертизе состояния защищенности информации на объекте защиты
16.	ПК-13	способностью участвовать в проектировании средств защиты информации автоматизированной системы	требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; основные меры по защите информации в автоматизированных системах (организационные, правовые, про-	применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом дейст-	криптографической терминологией методами формирования требований по защите информации методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем методами и средствами технической защиты информации

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

			граммно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	вующих нормативных и методических документов исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений разрабатывать частные политики информационной безопасности автоматизированных систем	
17.	ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	требования к шифрам и основные характеристики шифров основные информационные технологии, используемые в автоматизированных системах	контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем	навыками участия в экспертизе состояния защищенности информации на объекте защиты навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем методами расчета и инструментального контроля показателей технической защиты информации навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков
18.	ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации	возможности технических средств перехвата информации		
19.	ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	технические каналы утечки информации		методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
20.	ПК-21	способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем		разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности разрабатывать предложения по совершенствованию системы управления информационной	навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению

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

				безопасностью автоматизированных систем	печению информационной безопасности
21.	ПК-26	способностью администрировать подсистему информационной безопасности автоматизированной системы	<p>типичные шифры с открытыми ключами;</p> <p>технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования</p> <p>источники и классификацию угроз информационной безопасности;</p> <p>программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях</p> <p>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;</p> <p>содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;</p> <p>основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);</p> <p>основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах</p> <p>современные технологии и методы программирования</p>	<p>планировать политику безопасности операционных систем;</p> <p>применять средства обеспечения безопасности данных;</p> <p>классифицировать и оценивать угрозы информационной безопасности для объекта информатизации</p> <p>администрировать подсистемы информационной безопасности автоматизированных систем</p>	<p>навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;</p> <p>навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;</p> <p>навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;</p> <p>навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ</p> <p>навыками работы с технической документацией на ЭВМ и вычислительные системы</p> <p>профессиональной терминологией в области информационной безопасности;</p> <p>навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплексу документации;</p> <p>навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы</p> <p>навыками разработки программной документации</p>
22.	ПК-28	способностью управлять информационной безопасностью автоматизированной системы	основные методы управления информационной безопасностью	разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	методами управления информационной безопасностью автоматизированных систем
23.	ПСК-4.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем	основные методы и средства реализации удаленных сетевых атак на открытые информационные системы; о политиках безопасности и мерах защиты в открытых	реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по	терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей;

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

			информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем;	оценке защищенных систем; практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений; осуществлять мониторинг и аудит сетевой безопасности; осуществлять администрирование открытых информационных систем;	навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
24.	ПСК-4.2	способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	о политиках безопасности и мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем;	проектировать защищенные открытые информационные системы; определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя Виртуальные частные сети Аудит информационных технологий и систем обеспечения информационной безопасности информационной безопасности для открытых информационных систем; выявлять и устранять уязвимости в основных компонентах открытых информационных систем;	терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах
25.	ПСК-4.3	способностью участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы	принципы построения современных виртуальных локальных и частных сетей и направления их развития; виды виртуальных сетей и их преимущества при конкретном применении; политику безопасности для виртуальных сетей;	осуществлять управление информационной безопасностью в открытых информационных системах; применять стандартные решения для защиты информации в виртуальных сетях и квалифицированно оценивать их качество;	навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
26.	ПСК-4.4	способностью	основные стандарты	обнаруживать, прерывать	навыками анализа угроз

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

		участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	построения виртуальных сетей; принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях; подходы к интеграции виртуальных сетей с открытыми информационными системами;	и предотвращать удаленные сетевые атаки по их характерным признакам; применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество; используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем;	информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей
27.	ПСК-4.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	базовые вопросы построения открытых информационных систем; основные криптографические протоколы и стандарты; основные стандарты построения и взаимодействия открытых систем; о политиках безопасности и мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем;	проектировать защищенные открытые информационные системы; определять и устранять основные угрозы информационной безопасности для открытых информационных систем; строить модель нарушителя информационной безопасности для открытых информационных систем; выявлять и устранять уязвимости в основных компонентах открытых информационных систем;	терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей; навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах; навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей

3. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы/темы практики	Индекс контролируемой компетенции	Наименование оценочного средства
1.	Раздел. Основы информационной безопасности	ПК-26	ОС-1. Контрольные вопросы №№ 1-8
2.	Раздел. Криптографические методы защиты информации	ОПК-1, ОПК-2, ОПК-3, ПК-1, ПК-2, ПК-3, ПК-5, ПК-11, ПК-13, ПК-14, ПК-26	ОС-1. Контрольные вопросы №№ 9-14.
3.	Раздел. Техническая защита информации	ОПК-1, ПК-1, ПК-3, ПК-4, ПК-5, ПК-13, ПК-14, ПК-16, ПК-17	ОС-1. Контрольные вопросы №№ 15-17

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

4.	Раздел. Организационное и правовое обеспечение информационной безопасности	ОПК-2, ПК-1, ПК-3, ПК-7, ПК-8, ПК-12, ПК-13, ПК-14	ОС-1. Контрольные вопросы №№ 18-23
5.	Отчет по практике	ОК-5, ОК-7, ПК-7, ПК-8, ПК-9, ПК-28, ПСК-4.1, ПСК-4.2, ПСК-4.3, ПСК-4.4., ПСК-4.5	ОС-2. Отчет по НИР.

ОС-1. Контрольные вопросы

4. Контрольные вопросы для оценки результатов прохождения практики

1. Классификация угроз информации. Источники угроз информационной безопасности РФ. Модель действий нарушителя.

2. Понятие информационной войны. Составные части и методы информационного противоборства. Информационное оружие.

3. Концепция защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности.

4. Направления защиты от несанкционированного доступа (НСД). Основные способы НСД. Структура системы защиты информации от НСД, назначение и функции элементов.

5. Правила разграничения доступа к информации. Мандатная и дискреционная модели управления доступом.

6. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Основные методы аутентификации.

7. Технология межсетевых экранов (МЭ). Виды МЭ.

8. Основные понятия и функции виртуальных частных сетей (VPN).

9. Симметричные блочные шифры. Шифры Фейстеля и их обратимость. Российский стандарт шифрования ГОСТ Р 34.12-2015. Режимы использования симметричных блочных шифров.

10. Ассиметричные блочные шифры. Схема Диффи-Хеллмана. Шифр RSA. Шифр Эль-Гамала. Шифр Шамира.

11. Хеш-функции. Требования, предъявляемые к хеш-функциям. Криптографические хеш-функции. Способы построения криптографических хеш-функций.

12. Коды аутентификации. Понятие имитации и подмены сообщения. Нижние оценки для вероятностей успеха имитации и подмены. Критерий достижимости нижних оценок. Оптимальные коды аутентификации.

13. Электронная подпись. Электронная подпись на основе асимметричных систем шифрования: электронная подпись RSA, электронная подпись Фиата-Шамира, электронная подпись Эль-Гамала, электронная подпись Шнорра. Электронная подпись на основе симметричных систем шифрования.

14. Криптосистемы на эллиптических кривых.

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

15. Общие положения инженерно-технической защиты информации. Классификация технических каналов утечки информации.

16. Скрытие демаскирующих признаков при противодействии техническим средствам разведки (ТСР).

17. Физические и технические основы противодействия видовой разведке. Технический контроль эффективности противодействия видовой разведке.

18. Информация как объект правоотношений. Законодательство РФ в области информационной безопасности.

19. Виды и содержание тайн. Законодательная база охраны государственной, коммерческой и служебной тайн.

20. Основные нормативные документы, разрабатываемые на предприятии по защите персональных данных и первоочередные мероприятия по созданию системы защиты персональных данных на предприятии.

21. Виды деятельности, подлежащие лицензированию. Порядок получения лицензии в области защиты информации.

22. Методы и средства инженерной защиты объектов информатизации.

23. Программные и аппаратные средства защиты информации от несанкционированного доступа.

5. Критерии оценивания

Формой промежуточной аттестации по итогам НИР является дифференцированный зачет.

Критерии оценки работы следующие:

«Отлично»: тема полностью раскрыта, использовано оптимальное количество источников и литературы, автор продемонстрировал высокий уровень владения исследовательскими методиками. Научная работа правильно оформлена. Защита прошла успешно, автор содержательно выступил и ответил на поставленные вопросы. График представления работы соблюден.

«Хорошо»: тема в целом раскрыта, однако работа имеет недостатки и ошибки в проведенном исследовании. Защита прошла неубедительно, автор не сумел ответить на ряд вопросов. Есть ошибки в оформлении. График представления работы соблюден.

«Удовлетворительно»: работа несамостоятельная, носит откровенно реферативный характер, то есть переписана из нескольких книг с минимальной авторской работой с источниками или вообще без оной. Число источников, статей и книг, к которым обратился автор, явно недостаточно для качественного раскрытия темы. Работа является «подражательной». Неубедительная защита. Отсутствие ответов на большинство вопросов комиссии. Ошибки в оформлении. Допущены нарушения графика представления работы.

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

Приложение 2. Требования к отчету

ТРЕБОВАНИЯ К ОТЧЕТУ ПО НИР

Отчет готовится студентом в период выполнения НИР с использованием материалов на основании индивидуального задания.

Структура отчета:

- Титульный лист;
- Оглавление;
- Введение;
- Основное содержание отчета;
- Заключение;
- Список литературы;
- Приложения (при необходимости);

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

Приложение 3. Титульный лист отчета о НИР



**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

Факультет математики, информационных и авиационных технологий
Кафедра информационной безопасности и теории управления

НАЗВАНИЕ ТЕМЫ

научно-исследовательская работа

10.05.03 «Информационная безопасность автоматизированных систем»

Специализация :

«Безопасность открытых информационных систем»

Выполнил студент	_____	_____	_____
	группа	подпись, дата	Ф.И.О.
Руководитель НИР	_____	_____	_____
	степень, звание	подпись, дата	Ф.И.О.

			оценка

			дата

УЛЬЯНОВСК – 20__