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

УТВЕРЖДЕНО
Ученым советом факультета
математики, информационных и авиационных технологий
от «22» 06 2018 г., протокол №5/18
Председатель _____ Волков М.Н.
«28» 06 2018 г.

РАБОЧАЯ ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Специальность: 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

Факультет математики, информационных и авиационных технологий
Курс 6 Семестр 11 Форма обучения очная

Способ и форма проведения практики (в соответствии с ФГОС ВО 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 01.12.2016 № 1509), а также с учетом рекомендованной примерной образовательной программы.

Сведения о разработчиках:

Ф.И.О.	Аббревиатура кафедры	Ученая степень, звание
Рацеев Сергей Михайлович	ИБиТУ	д.ф-м.н., доцент

Дата введения в учебный процесс УлГУ 01.09.2018

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 _____ / А.С. Андреев / (Подпись) (Ф.И.О.) «28» 06 2018 г.

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Цели преддипломной практики:

- закрепление теоретических и практических знаний, полученных в процессе обучения по специальности «Информационная безопасность автоматизированных систем».
- подготовка студента к решению задач, относящихся к различных проблемам обеспечения информационной безопасности, и к решению отдельных фундаментальных проблем связанных с информационной безопасностью автоматизированных систем.

На этапе преддипломной практики студент решает следующие задачи:

- овладение профессиональными навыками работы и решение практических задач;
- выбор направления практической работы;
- изучение литературных и иных источников, необходимых для выполнения данной работы и подготовки выпускной квалификационной работы;
- приобретение опыта работы в коллективе.

2. МЕСТО ПРЕДДИПЛОМНОЙ ПРАКТИКИ В СТРУКТУРЕ ОПОП ВО

Для успешного прохождения практики 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».

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

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ СТУДЕНТОВ

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

- 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 (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);
- 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 прохождения преддипломной практики студент должен:

Знать:

– принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите государственной тайны;

– виды и состав угроз информационной безопасности;

– конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, потенциальные каналы утечки информации, характерные для этих устройств, способы их выявления и методы оценки опасности, основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации;

– принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;

– виды уязвимости защищаемой информации и формы ее проявления;

– каналы и методы несанкционированного доступа к конфиденциальной информации;

– наиболее уязвимые для атак противника элементы компьютерных систем;

Владеть:

– методами организации и управления деятельностью служб защиты информации на предприятии;

– технологией проектирования, построения и эксплуатации комплексных систем защиты информации;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

Уметь и применять на практике:

– осуществлять комплекс мер по информационной безопасности с учетом его правовой обоснованности;

– разработку математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов;

– проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средствах защиты информации;

– применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;

– проведение инструментального мониторинга защищенности компьютерных систем;

– организацию работ по выполнению требований режима защиты информации, в том числе информации ограниченного доступа (сведений, составляющих

государственную тайну и конфиденциальной информации).

4. МЕСТО И СРОКИ ПРОВЕДЕНИЯ ПРАКТИКИ

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

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

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

Время прохождения производственной практики: в 10-м семестре.

5. ОБЪЕМ ПРАКТИКИ В ЗЕ И ЕЕ ПРОДОЛЖИТЕЛЬНОСТЬ В НЕДЕЛЯХ

Преддипломная практика проходит продолжительностью в 324 часа (9 ЗЕ) в 10-м семестре (6 недель).

6. СТРУКТКРА И СОДЕРЖАНИЕ ПРАКТИКИ

Общая трудоемкость преддипломной практики составляет 9 зачетных единиц, 324 часа.

№ п/п	**Разделы (этапы) практики**	**Виды производственной работы на практике, включая самостоятельную работу студентов**	**Трудоемкость (в часах)**	**Формы текущего контроля**
1	Подготовительный этап	Организационное собрание, инструктаж по ТБ и должностным обязанностям. Определение задач, плана работ и средств по его выполнению.	6	Тест по технике безопасности
2	Экспериментальный этап	Сбор, обработка, систематизация материала по теме исследования. Решение задач, разработка алгоритмов и создание прикладных программ, необходимых для достижения целей выпускной квалификационной работы. Тестирование программ и оценка качества решения задач.	300	Проверка ведения дневника практики
3	Заключительный этап	Обработка и оформление	18	Защита отчета о

		результатов работы, подготовка и защита отчета по практике.		прохождении практики
	ИТОГО		324	

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

Порядок прохождения практики:

1. Получить отметку в отделе кадров предприятия о прибытии на практику.
2. Получить вводный и первичный инструктаж на рабочем месте по охране труда.
3. Изучить функциональные обязанности инженера отдела (специалиста по защите информации) и практически их выполнять.
4. Изучить информационную систему предприятия.
5. Выполнить задачи, поставленные руководителем практики от предприятия.
6. Заполнять журнал прохождения практики.
7. Подготовить отчет по практике.
8. По окончанию практики получить характеристику и оценку у руководителя практики от предприятия.
9. Получить отметку в отделе кадров предприятия об убытии с предприятия и заверить печатью характеристику и оценку.

7. НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЕ И НАУЧНО-ПРОИЗВОДСТВЕННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ НА ПРАКТИКЕ

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

8. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ПРАКТИКИ

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

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

- обеспечение высокого качества прохождение студентами практики, ее строго соответствия учебным планам и программам;
- согласование программы и графиков прохождения студентами практики с руководителями практики от предприятий, подготовка и выдача студентам индивидуальных заданий на время практики;
- осуществление регулярного контроля за прохождением студентами практики, за соблюдением студентами правил внутреннего трудового распорядка предприятия;
- проведение консультаций по всем возникающим вопросам;
- проверка отчетов и дневников студентов по завершении практики, участие в работе по приемке защиты отчетов о практике.

По окончании практики студент составляет письменный отчет, оформленный в соответствии с установленными требованиями, сдает его руководителям практики от университета и организации – базе практики для предварительной дифференцированной

оценки.

Отчет о практике должен содержать сведения о конкретно выполненной студентом работы в период практики.

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

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

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Список используемой литературы

а) основная

1. Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы высшего образования (утв. приказом Министерства образования и науки РФ от 27 ноября 2015 г. № 1383).
2. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М. ДМК Пресс, 2010. - 544 с. ил.
3. Девянин П.Н. Модели безопасности компьютерных систем. Учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2005. – 144 с.
4. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие для вузов. – М.: Академия, 2008. – 336 с.
5. Семкин С.Н. Основы правового обеспечения защиты информации – М: Горячая линия – Телеком, 2008.
6. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник – М: Академия, 2008.
7. Методические указания по разработке типовых документов в области информационной безопасности /А.М. Иванцов. – Ульяновск: УлГУ, 2016 – 63 с.
8. Хореев П.В. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов. – М.: Академия, 2007. – 256 с.
9. 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. 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.

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 ПРАКТИКИ

Во время практики студенты используют научно-исследовательское оборудование, которым обладает организация, утвержденная местом прохождения практики.

Приложение 1

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	ПСК-4.1	ПСК-4.2	ПСК-4.3	ПСК-4.4	ПСК-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 безопасности				+		+		+			+	+			+	+	+										
9	Разработка и эксплуатация защищённых автоматизированных систем				+	+	+	+		+							+	+				+						

8	Программно-аппаратные средства обеспечения информационной безопасности				+	+	+	+	+	+												+						
5	Открытые информационные системы			+			+		+														+	+	+		
7	Криптографические протоколы и стандарты			+	+				+						+		+	+				+		+	+	+		
9	Безопасность открытых информационных систем	+					+		+	+	+		+		+								+	+	+			
7	Виртуальные частные сети															+		+		+								
5	Теоретико-числовые методы в криптографии				+																							
9	Аттестация объектов информатизации								+				+					+	+	+	+							
6-7	Методы принятия оптимальных решений			+	+	+					+																	
6	Основы научных исследований			+	+	+	+																					
8	Модели безопасности компьютерных систем			+	+	+		+	+																			
9	Администрирование сетей ЭВМ					+																+						
7	Профессиональная этика	+	+																									
4	Вычислительные методы в алгебре и теории чисел				+																							
5	Русский язык и культура речи		+																									
7	Системный анализ				+	+		+																				
7	Теория игр и исследование операций				+	+		+																				
9	Методы алгебраической геометрии в криптографии			+	+				+						+		+											
9	Дополнительные главы криптографии			+	+				+						+		+											
3	Объектно-ориентированное программирование					+																						
8	Телекоммуникационные системы				+																							
8	Технические средства обнаружения каналов утечки информации																+	+		+								
9	Инструментальные средства контроля защищенности информации								+					+		+		+		+								
9	Сертификация средств защиты информации																	+										
4	Дифференциальные уравнения				+																							
4	Функциональный анализ				+																							
8-9	Теория кодирования, сжатия и восстановления информации			+	+																							
4	Учебная практика	+	+			+	+					+											+	+	+	+	+	
11	Научно-исследовательская работа	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
6, 10	Производственная практика	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	
11	Преддипломная практика	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
11	ГИА	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	

2. Требования к результатам освоения преддипломной практики

№ 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;	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 при-	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

			основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	кладные физические задачи; анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности; применять математические методы исследования моделей шифров основы физической защиты объектов информатизации выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем	
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; типовые свойства и спосо-	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 имногозначных	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 математическо-

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

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

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

		информационной безопасности автоматизированной системы	основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	и подсистем безопасности 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 автомати-	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

				зированных системах	
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 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 (организа-	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 под-	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

			ционные, правовые, программно-аппаратные, криптографические, технические); основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах	системы с учетом действующих нормативных и методических документов исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем	
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		разрабатывать, реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности разрабатывать предложения по совершенствованию системы управле-	навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с уче-

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

		информационных систем	мерах защиты в открытых информационных системах; о комплексном подходе к построению эшелонированной защиты для открытых информационных систем;	стандартами по оценке защищенных систем; практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений; осуществлять мониторинг и аудит сетевой безопасности; осуществлять администрирование открытых информационных систем;	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
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 участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы	основные стандарты построения виртуальных сетей; принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях; подходы к интеграции виртуальных сетей с открытыми информационными системами;	обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам; применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество; используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем;	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
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

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-7, ОК-8, 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 практике.

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-Гамаля. 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-Гамаля, электронная подпись Шнорра. Электронная подпись на основе симметричных систем шифрования.
14. Криптосистемы на эллиптических кривых.

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

Итоговая оценка	**Традиционная оценка**
90–100	Отлично
70–89	Хорошо
50–69	Удовлетворительно
0–49	Неудовлетворительно

Накопленная оценка текущего контроля *Отек* находится по формуле*:*

$$Отек=Орп+Ору,$$

где *Орп* – оценка руководителя с предприятия, *Ору* – оценка руководителя от университета.

Оценка руководителя с предприятия:

Оценка руководителя с предприятия	**Оценка**	**Количество баллов**
Учитывается содержательный отзыв руководителя практики с предприятия о работе студента и его оценка за практику	Отлично	45–50
	Хорошо	35–44
	Удовлетворительно	25–34
	Неудовлетворительно	0–24

Оценка руководителя от университета:

Критерии оценки руководителя практики от университета	**Количество баллов**		**Оценка**
	За пункт	**Общее**	
Форма и содержание отчета и дневника соответствуют требованиям к работе подобного рода, ошибки отсутствуют	15	45–50	Отлично
Выполненная работа соответствует направлению	15		

образовательной программы			
Устная защита: презентация выполненной работы, даны подробные и полные ответы на вопросы	15–20		
Форма и содержание отчета и дневника в целом соответствуют требованиям к работе подобного рода, присутствуют ошибки	11–15	35–44	Хорошо
Выполненная работа в целом соответствует направлению образовательной программы, но общепрофессиональные и профессиональные компетенции раскрыты не в полной мере	11–14		
Устная защита: презентация выполненной работы, подробные и полные ответы на вопросы	13–15		
Форма и содержание отчета и дневника не соответствуют требованиям к работе подобного рода, присутствуют ошибки	8–10	25–34	Удовлетворительно
Выполненная работа в целом соответствует направлению образовательной программы, но общепрофессиональные и профессиональные компетенции не раскрыты	9–12		
Устная защита: презентация выполненной работы не достаточно подробна, даны ошибочные или недостаточно подробные ответы на вопросы	8–12		
Отчетные документы (дневник и отчет по практике) не предоставлены или их форма и содержание не соответствует требованиям к работе подобного рода	0–8	0–24	Неудовлетворительно
Выполненная работа не соответствует направлению образовательной программы	0–8		
Устная защита: презентация выполненной работы не выполнена, даны ошибочные или недостаточно подробные ответы на вопросы	0–8		

Приложение 2

ТРЕБОВАНИЯ К ОТЧЕТУ ПО ПРАКТИКЕ

Отчет готовится студентом в период прохождения практики с использованием материалов, собранных в организации, являющейся базой практики на основании индивидуального задания.

Структура отчета:

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

Отчет студента по окончании практики должен включать следующие разделы:
– Общая характеристика организации (базового предприятия практики), анализ ее деятельности.
– Обобщение полученной исходной информации по теме дипломной работы: сравнительный анализ возможных вариантов реализации научно-технической информации по теме работы; реализацию некоторых из возможных путей решения поставленной задачи;
– Выводы и рекомендации.

Приложение 3. Титульный лист отчета по преддипломной практике

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

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

ОТЧЕТ
по преддипломной практике

10.05.03 «Информационная безопасность автоматизированных систем»

Специализация:
«Безопасность открытых информационных систем»

Выполнил студент _____ _____ _____
группа подпись Ф.И.О.

Руководитель практики от УлГУ:

_____
(ФИО, должность, подпись)

Руководитель практики от предприятия:

_____
(ФИО, должность, подпись)

_____
(наименование предприятия практики)

_____
оценка

_____
дата

УЛЬЯНОВСК – 20__