Некоммерческое частное образовательное учреждение
высшего образования

КУБАНСКИЙ ИНСТИТУТ ИНФОРМЗАЩИТЫ

Кафедра информационной безопасности

ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

для обучающихся по направлению подготовки
10.03.01 **Информационная безопасность**

Квалификация (степень) выпускника
«Бакалавр»

Обсуждена и одобрена на заседании кафедры «Информационной безопасности» (протокол № 4 от 28 ноября 2017 г.). Утверждена на заседании Ученого Совета (протокол № 4 от 28 ноября 2017 г.)

Краснодар
2017

Содержание

1. Цель и задачи преддипломной практики

Цель преддипломной практики - формирование профессионально важных качеств, закрепление профессиональных знаний, умений и навыков, полученных в результате теоретической подготовки и приобретение опыта самостоятельной работы в соответствии с профилем подготовки. Преддипломная практика проводится для выполнения выпускной квалификационной работы и является обязательной в соответствии с требованиями ФГОС ВО.

Задачи преддипломной практики

Основной задачей преддипломной (как вида производственной) практики является приобретение опыта в исследовании и решении актуальной научной проблемы, а также подбор информационных материалов, необходимых для выполнения выпускной квалификационной работы.

Задачами преддипломной практики являются:

– анализ научной и практической значимости проводимых исследований;

– закрепление и углубление теоретических и практических знаний обучающихся по специальным дисциплинам учебного плана;

– приобретение более глубоких практических навыков по направлению подготовки и профилю будущей работы;

– закрепление навыков в постановке и проведении исследовательских работ;

– расширение опыта общения с современной техникой обработки защищенных данных по всему технологическому циклу работы ЭВМ (ПК), обслуживающих объект практики;

– введение учета и составление элементов рабочей документации защищенной информационной системы;

– совершенствование автоматизированного документооборота в организации (базе практики), формулирование требований к содержанию и построению системы защиты технической и организационно- распорядительной документации;

– практическое ознакомление с методами и техническими средствами обеспечения информационной безопасности систем и объектов;

– ознакомление обучающихся с организацией службы охраны труда и вопросами техники безопасности при эксплуатации защищенных автоматизированных информационных систем;

– развитие умений использовать знания при решении конкретных научно-исследовательских задач;

– сбор материалов и проведение исследований, необходимых для выполнения выпускной квалификационной работы.

Для успешного решения данных задач, во время преддипломной практики обучающийся должен изучить:

– информационные источники по разрабатываемой теме с целью их использования при выполнении выпускной квалификационной работы;

– методы моделирования и исследования вопросов информационной безопасности;

– методы анализа и обработки данных, являющихся входными для проведения научного исследования;

– информационные технологии, применяемые в научных исследованиях, программные продукты, относящиеся к профессиональной сфере;

– требования к оформлению научно-технической документации;

а также, выполнить: анализ, систематизацию и обобщение информации по теме исследований; сравнение результатов исследования объекта разработки с отечественными и зарубежными аналогами.

Преддипломная практика организуется и проводится в организациях (предприятиях, учреждениях) по профилю подготовки выпускников НЧОУ ВО КИИЗ. Прохождение преддипломной практики для обучающегося является обязательным. Ввиду специфики направления подготовки и особенностей института, преддипломная практика может проводиться

на базе института КИИЗ с привлечением обучающихся для ее прохождения в качестве специалистов, техников, занимающихся разработкой и эксплуатацией средств защиты информации и защищенных автоматизированных систем различного назначения (при этом необходимо в полном объеме использовать возможности компьютерных классов, учебных лабораторий института).

На кафедре Информационной безопасности, в организации, в которой проводится практика, разрабатываются и ведутся документы в соответствии с перечнем документов по организации и проведению практики. Достигнутые результаты практики также отражаются в индивидуальных портфолио обучающихся на сайте НЧОУ ВО «Кубанский институт информзащиты» (раздел «Электронная информационно-образовательная среда»).

Выбор мест прохождения практик для лиц с ограниченными возможностями здоровья производится с учетом состояния здоровья обучающихся и требований по доступности.

2. Место практики в структуре ОП

Преддипломная практика входит в Блок 2 «Практики», который в полном объеме относится к вариативной части образовательной программы (ОП).

Программа преддипломной практики обучающихся предусмотрена учебным планом направления 10.03.01 Информационная безопасность.

В процессе прохождения практики студенты окончательно закрепляют знания и умения, полученные в ходе освоения дисциплин вариативной части учебного плана, в том числе, дисциплин выпускного (последнего) курса обучения: Техническая защита информации, Защита и обработка конфиденциальных документов, Защита электронного документооборота, Безопасность операционных систем, Безопасность баз данных, Комплексные системы защиты информации на предприятии, Экономическая и финансы защита информации (Организация и управление службой защиты информации), Технические средства охраны (Технические средства безопасности).

3. Требования к результатам прохождения преддипломной практики

Прохождение преддипломной практики направлено на формирование у обучающихся следующих компетенций:

профессиональных

способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способностью осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-10);

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими

документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);

профессионально-специализированных

способностью проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-1).

В результате прохождения преддипломной практики обучающийся должен:

знать:

– принципы и правила концептуального представления и построения структуры защищенных автоматизированных информационных систем;

– принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации);

– методы и средства контроля эффективности технической защиты информации;

– основные методы управления информационной безопасностью;

– порядок обработки, движения, хранения и использования конфиденциальных документов в ведомственных архивах;

– организацию работы руководителей, специалистов и технического персонала с конфиденциальными документами на любом носителе информации;

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;

– технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;

– основы организационного и правового обеспечения информационной безопасности;

***уметь*:**

– применять инструментарий концептуального проектирования защищенных автоматизированных информационных систем при принятии решения о создании таких систем, разработке концепции их функционирования, эффективно применяя при этом принципы и правила представления защищенной информации;

– оценивать информационные риски в информационных системах организаций (предприятий);

– работать с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности;

– разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем;

– формулировать задачи по разработке требований к автоматизированным системам в части обработки и хранения конфиденциальных документов;

– разрабатывать эффективные технологические схемы рационального документооборота с использованием современных систем и способов обработки и хранения конфиденциальных документов;

– руководить службой конфиденциальной документации;

– контролировать и анализировать уровень организационной и технологической защищенности документов;

– анализировать и оценивать угрозы информационной безопасности объекта;

– применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

– пользоваться нормативными документами по защите информации;

– применять отечественные и зарубежные стандарты в области компьютерной безопасности при проектировании, разработке и проведении оценки защищенности компьютерных систем;

владеть:

–навыками работы с инструментарием концептуального проектирования защищенных автоматизированных информационных систем;

– навыками работы с нормативными правовыми актами и конфиденциальными документами;

– методами и средствами выявления угроз безопасности автоматизированным системам;

– методами технической защиты информации;

– методами формирования требований по защите информации;

– методами расчета и инструментального контроля показателей технической защиты информации;

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

– методами управления информационной безопасностью информационных систем;

– методами выполнения типовых расчетов и моделирования процессов с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации;

– методами оценки информационных рисков и экономических рисков, обусловленных потерей защищенности объектов защиты в организации;

– профессиональной терминологией.

4. Формы проведения преддипломной практики

Преддипломная практика является обязательной видом производственной практики и ее форма выражается в работе по избранной профессии в подразделении организации.

Способы проведения практики: стационарная и выездная.

Все информационные ресурсы созданные обучающимися в ходе прохождения практики систематизируются, собираются, наиболее значимые позиции отражаются в индивидуальных портфолио, хранятся на кафедре наряду с другими работами, которые могут характеризовать уровень профессиональной компетентности обучающихся.

5. Место и время проведения преддипломной практики

Преддипломная практика обучающихся может проходить:

–в научных лабораториях, лабораториях НИИ, заводов, учреждений, предприятий, филиалов организаций;

–в центрах поддержки информационных систем различных фирм, организаций и предприятий;

–при кафедрах и в научных лабораториях вуза, оснащенных информационными системами, или занимающихся разработкой информационных систем;

–в организациях (предприятиях) на рабочем месте (для тех обучающихся, которые уже работают).

При наличии вакантных должностей обучающиеся могут быть зачислены на период прохождения практики на работу, если работа соответствует требованиям программы практики.

Руководителями преддипломной практики от КИИЗ назначаются ведущие преподаватели выпускающей кафедры Информатики и вычислительной техники, имеющие как правило, ученую степень и (или) ученое звание.

В организациях (учреждениях, предприятиях), на базе которых проводится преддипломная практика, назначаются лица, ответственные за практику.

Обучающиеся проходят преддипломную практику продолжительностью 6 недель (9 зачетных единиц) в 8-м (последнем учебном) семестре.

Для инвалидов I, II, III групп и лиц с ограниченными возможностями здоровья форма проведения практики в институте устанавливается по индивидуальному плану с учетом особенностей психофизического развития и состояния их здоровья.

6. Объем преддипломной практики и виды учебной работы

Общая трудоемкость преддипломной практики составляет 9 зачетных единиц (324 часа).

Вид учебной работы	Всего часов	Распределение часов	
		ОФО, 4 курс	ОЗФО, 5 курс
Аудиторные занятия (всего)	**2**	**2**	**2**
В том числе:			
Лекции (Л)	2	2	2
Практические занятия (ПЗ)	-	-	-
Лабораторные работы (ЛР)	-	-	-
Контрольные работы (КР)	-	-	-
Самостоятельная работа (всего)	**322**	**322**	**322**
В том числе:			
Составление отчета	24	24	24
Расчётно-графические работы	-	-	-
Коллоквиум	-	-	-
Выполнение индивидуального задания	40	40	40
Домашнее задание	-	-	
Другие виды самостоятельной работы (работа с литературой, технической документацией)	258	258	258
Вид промежуточной аттестации и его трудоемкость	**-**	**Зачет с оценкой**	**Зачет с оценкой**
Общая трудоёмкость часов	**324**	**324**	**324**
зачетных единиц	**9**	**9**	**9**

7. Содержание преддипломной практики

7.1. Содержание разделов (тем) практики

№ п/п	Наименование раздела	Содержание раздела	Трудоемкость (час.)
Семестр 8			
1.	Проектирование защищенных автоматизированных информационных систем	Установочная лекция. Факторы, влияющие на выбор компонентов КСЗИ. Объекты защиты и основные требования, предъявляемые к выбору методов и средств защиты. Понятие модели объекта, основные виды моделей и их характеристика. Выбор структуры КСЗИ и ее функциональная и организационная модели. Характеристика основных стадий создания КСЗИ. Предпроектное обследование, технический проект, рабочий проект, ввод в эксплуатацию. Определение состава кадрового обеспечения функционирования КСЗИ. Распределение функций по защите информации и взаимодействие между ними. Разработка нормативных документов, регламентирующих деятельность персонала по защите информации. Подбор и обучение персонала. Определение состава материально-технического обеспечения, его зависимость от структуры КСЗИ. Значение нормативно-методического обеспечения функционирования КСЗИ. Состав нормативно-методических документов по обеспечению функционирования КСЗИ, их назначение, структура и содержание. Порядок разработки и внедрения документов.	70
2.	Защита документооборота, обработка документов, в т.ч., конфиденциальных	Назначение и задачи защиты составления и ведения электронных документов. Особенности формы электронного документа (ЭД), применяемые на практике. Состав операций защиты и обработки ЭД. Идентификация средств защиты электронных документов. Состав требований, предъявляемых к выбору систем защиты и заполнения ЭД. Характеристика структуры и особенностей технологии работы с системой защиты составления электронных документов. Назначение защиты системы управления электронными документами (СУД), функции, выполняемые СУД в процессах управления системой. Структура СУД и назначение ее компонентов. Методы организации защиты хранения документов в СУД. Практика применения методов защиты поиска и их характеристика. Характеристика адаптивного метода защиты распознавания и поиска (APRP). Средства и способы доставки конфиденциальной информации. Уничтожение конфиденциальных	70

		документов. Прием и учет конфиденциальных документов входного потока. Порядок рассмотрения и исполнения документов входного потока. Контроль исполнения документов в организации. Организационные и методические проблемы автоматизации делопроизводственных операций по документам. Системы электронного документооборота (СЭД). Защита конфиденциальных документов в СЭД	
3.	Управление процессом защиты информации. Общая организация работы службы защиты информации	Понятие и цели, принципы управления процессом защиты информации. Структура и содержание общей технологии управления процессом защиты информации. Факторы, влияющие на выбор принципов и способов организации защиты информации. Понятие и виды, методы контроля функционирования защищенных автоматизированных систем. Особенности проведения контроля в организации. Факторы, влияющие на принятие решений в условиях чрезвычайной ситуации. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций. Особенности подбора персонала на должности, связанные с конфиденциальной информацией. Состав документов, необходимых при подборе и приеме работников на должности, связанные с доступом к конфиденциальной информации. Понятия «номенклатуры должностей». Понятия «допуска». Формы допусков, их назначение, порядок оформления допусков. Методы проверки кандидатов; особенности документирования трудовых отношений. Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации.	70
4.	Технические, программно-аппаратные средства защиты информации в организации	Объектовые средства обнаружения (датчики) Особенности использования физических свойств нарушителя для выбора и обоснования применения технических средств охраны. Технические средства обнаружения (датчики) – объектовые. Периметровые средства обнаружения (датчики) Внешние и внутренние рубежи охраны. Требования к их оборудованию. Технические средства обнаружения – периметровые. Технические средства (приборы) визуального наблюдения. Средства управления доступом Телевизионные системы наблюдения. Приборы визуального наблюдения. Выбор технических средств наблюдения. Требования по применению. Порядок эксплуатации и допуска личного состава к техническим средствам безопасности.. Методика определения варианта оборудования объекта техническими средствами охраны. Практическая реализация систем ТСО. Охрана режимных помещений.	60

5.	Экономика защиты информации	Применение методик определения затрат на информационную безопасность организации на практике. Составление модели объектов защиты в условиях ограниченности денежных средств и независимости ущербов. Вопросы эффективности функционирования системы организации службы безопасности на предприятии. Оценка экономической эффективности защиты интеллектуальной собственности организации. Оценка информационного риска.	54

7.2 Разделы практики и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ разделов практики, необходимые для изучения обеспечиваемых (последующих) дисциплин		
		преддипломная практика (семестр 8)		
		1	2	3
1.	Выпускная квалификационная работа	+	+	+
2.	Государственная итоговая аттестация	+	+	+

8. Практические работы

8.1 Содержание практических работ

Основную часть времени преддипломной практики обучающиеся работают на рабочих местах в качестве стажеров, техников. Наряду с выполнением обязанностей на рабочем месте они углубленно изучают отдельные технические вопросы согласно индивидуальному заданию.

На практике студентами могут выполняться следующие работы:

№ п/п	Наименование работ	Трудоемкость (час.)
Преддипломная практика (семестр 8)		
1	изучение новых научных результатов, научной литературы или научно-исследовательских проектов связанных с развитием средств и методов применения вычислительной техники (ВТ) в защищенных автоматизированных информационных системах	50
2	изучение защищенных информационных систем методами прогнозирования и системного анализа	30
3	методы и средства контроля эффективности технической защиты информации	30
4	исследование и разработка математических моделей, алгоритмов, методов, программного обеспечения, инструментальных средств по	50

	защите информации в сложных объектах	
5	составление научных обзоров, рефератов и библиографии по тематике проводимых исследований	40
6	участие в работе научных семинаров, научно-тематических конференций, симпозиумов	30
7	подготовка научных публикаций, документов для регистрации компьютерных программ	30
	Итого	260

9. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по преддипломной практике

Прохождение преддипломной практики направлено на формирование у обучающихся следующих компетенций:

способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способностью осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности ПК-10);

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ПК-15);

способностью проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-1).

По результатам прохождения практики обучающимся разрабатывается и составляется отчет. Отчет является основным документом, по которому определяется качество работы обучающегося в период практики. Отчет должен составляться индивидуально.

Работа по подбору материалов и составлению отчета должна проводиться в течение всего периода практики.

Отчет, заверенный руководителем практики от предприятия, подлежит проверке и защите на кафедре Информатики и вычислительной техники в установленные учебным графиком сроки.

Теоретические вопросы для защиты отчета по преддипломной практике

Теоретические вопросы (ПК-4,ПК-7,ПК-9,ПК-10,ПК-13, ПК-14,ПК-15**):**

Блок вопросов № 1

1. Понятия информации, информатики, информационной технологии.
2. Этапы развития информационной технологии.
3. Понятие информационной системы, информационного ресурса.
4. Системы счисления. Основание и базис.
5. Понятия вычислительного прибора, вычислительной машины, ЭВМ.
6. Схема обработки информации на компьютере (взаимодействие устройств).
7. Периферийные устройства компьютера.
8. Классификация программного обеспечения (классы и подклассы).
9. Назначение системных программ. Привести примеры.
10. Назначение систем программирования. Привести примеры.
11. Назначение и классификация прикладных программ. Привести примеры.
12. Операционная система (назначение и функции).
13. Компьютерные вирусы и защита от них.
14. Текстовые редакторы, назначение. Microsoft Word. (запуск программы; элементы окна; меню; панели инструментов, работа).
15. Электронные таблицы: назначение и области применения. Microsoft Excel. Запуск программы; вид окна после запуска.
16. Понятие и свойства операционной системы. Примеры. Общая характеристика объектов ОС
17. Понятие открытой информационной системы. Эволюция архитектурных моделей ОС
18. Признаки классификации локальных ОС: назначение, методы построения, типы аппаратных платформ, типы алгоритмов управления объектами. Примеры.
19. Понятие сетевой ОС. Общая характеристика взаимодействия открытых информационных систем на основе модели клиент/сервер.
20. Принцип распределенного управления объектами ОС. Взаимодействие открытых информационных систем на основе модели клиент/агент/сервер.
21. Типовая структура современной ОС (на примере ОС UNIX: файл, процесс, поток данных, поток управления, непривилегированный и привилегированный пользователи, командный и программный интерфейсы).
22. Системные структуры данных. Механизм взаимодействия ядра ОС с платформой. Прерывания ОС UNIX.
23. Системные структуры данных процесса в ОС UNIX. Пространство процесса. Таблица процессов.
24. Понятие дескриптора и контекста процесса. Характеристика пользовательского, регистрового и системного контекстов.
25. Функции управления состоянием процесса в ОС UNIX. Синхронное взаимодействие процессов.
26. Основные этапы загрузки ОС. Примеры. Порядок порождения процессов в ОС UNIX.
27. Планирование и диспетчеризация процессов в многозадачных ОС: задачи, алгоритмы, параметры. Примеры.
28. Планирование процессов на основе принципа «карусели с многоуровневой обратной связью».
29. Планирование процессов в ОС реального времени.
30. Классификация способов взаимодействия процессов (в локальных и сетевых ОС). Примеры.
31. Основные примитивы (средства) локального взаимодействия процессов.
32. Взаимодействие процессов на основе механизмов разделяемой памяти, семафоров, очередей сообщений.
33. Взаимодействие процессов на основе механизма программных каналов. Неименованные

и именованные каналы.

34. Основные примитивы (средства) удаленного взаимодействия процессов.
35. Типизация данных в ОС. Примеры.
36. Проблемы представления и адресации данных в ОС. Функции управления данными.
37. Методы распределения памяти без использования дискового пространства.
38. Базовая архитектура файловой системы. Файлы и атрибуты файлов. Типизация файлов. Адресация (именование) файлов. Примеры.
39. Способы логической и физической организации файлов. Примеры.
40. Общая модель файловой системы. Проблемы доступа к файлам. Избирательный и мандатный доступ. Отображение файлов в память.
41. Обобщенная архитектура файловой системы. Понятие локальной, сетевой, виртуальной файловой системы. Примеры.
42. Трехуровневая модель СУБД, предложенная ANSI (American National Standards Institute).
43. Иерархическая, сетевая и реляционная модели данных.
44. Нормализация реляционной базы данных.
45. Классическая архитектура «клиент-сервер».
46. Архитектура «клиент-сервер», основанная на Web-технологии (Intranet-архитектура).
47. Работа Web-сервера.
48. Способы передачи данных между CGI-программой и СУБД.
49. Доступ к серверу СУБД напрямую (Технология ActiveX).
50. Прохождение запроса к БД.

Блок вопросов № 2

1. Необходимость и цели защиты информации.
2. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
3. Методы создания безопасных систем обработки информации.
4. Автоматизация процесса обработки конфиденциальной информации.
5. Противодействие угрозам безопасности путем устранения. предпосылок их осуществления.
6. Стандарты информационной безопасности и их роль.
7. Основные понятия и определения политики информационной безопасности.
8. Угрозы безопасности компьютерных систем (КС).
9. Методы взлома компьютерных систем.
10. Защита компьютерной системы от взлома.
11. Защита КС от программных закладок.
12. Программные закладки.
13. Воздействия программных закладок на компьютеры.
14. Защита от программных закладок.
15. Политика безопасности.
16. Модель КС. Понятие монитора безопасности.
17. Обеспечение гарантий выполнения политики безопасности.
18. Коммерческая тайна.
19. Требования по защите конфиденциальной информации в документах предприятия.
20. Классификация компьютерных преступлений.
21. Компьютерные преступлениями против личных прав и частной сферы.
22. Компьютерные преступления против государственных и общественных интересов.
23. Основные виды преступлений, связанных с вмешательством в работу компьютеров.
24. Правовые методы обеспечения информационной безопасности Российской Федерации.
25. Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна».

26. Субъект доступа к информации, носитель информации это, собственник информации, владелец информации, пользователь (потребитель) информации.

27. Право доступа к информации, правило доступа к информации.

28. Виды угроз информационной безопасности Российской Федерации.

29. Экономическая оценка последствий нарушения информационной безопасности.

30. Методические подходы к проектированию защищенных информационных систем (экономический аспект).

Блок вопросов № 3

1. Законодательство РФ в области информационной безопасности
2. Лицензирование и сертификация в информационной сфере
3. Закон РФ «О персональных данных».
4. Закон РФ от 21.07.93 "О государственной тайне" № 5485-1
5. Постановление Правительства РФ от 24.12.94 № 1418 "О лицензировании отдельных видов деятельности"
6. Закон РФ "Об информации, информационных технологиях и защите информации".
7. Указ Президента РФ № 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации"
8. Постановление Правительства РФ от 26.06.95 № 608 "О сертификации средств защиты информации"
9. Закон РФ "Об участии в международном информационном обмене" от 5 июня 1996 года N 85-ФЗ.
10. Информационная безопасность объекта при осуществлении международного сотрудничества
11. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
12. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
13. Правовая защита информации.
14. Понятие и содержание конфиденциальной информации.
15. Защита интеллектуальной собственности
16. Компьютерные правонарушения
17. Международное законодательство в области защиты информации
18. Постановление Правительства РФ № 2195-1 "О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)".
19. Понятие и содержание конфиденциальной информации

Блок вопросов № 4 (компетенция ПСК-1)

1. Принципы формирования организационно-распорядительной документации по защите информации.
2. Оценка соответствия при обработке и защите персональных данных.
3. Понятие об оценке соответствия.
4. Сертификация средств защиты информации в ИС персональных данных.
5. Аттестация объектов информатизации по требованиям безопасности информации.
6. Государственный контроль и надзор при обработке и защите персональных данных.
7. Административный регламент РКН.
8. Типовой регламент проверок ФСБ.
9. Аутсорсинг при обработке и защите персональных данных.
10. Концепция безопасности баз данных
11. Угрозы безопасности баз данных: общие и специфичные.

12. Требования безопасности баз данных.
13. Защита от несанкционированного доступа.
14. Защита от вывода. Целостность баз данных.
15. Доступность (готовность) баз данных. Аудит.
16. Средства обеспечения целостности баз данных
17. Угрозы целостности информации. Способы противодействия.
18. Понятие транзакции. Основные свойства транзакций. Журнал транзакций. Механизм блокировок.
19. Декларативная и процедурная ссылочные целостности. Способы поддержания ссылочной целостности. Триггеры и правила.
20. Средства обеспечения конфиденциальности баз данных
21. Угрозы конфиденциальности информации.
22. Средства идентификации и аутентификации в СУБД.
23. Средства управления доступом. Виды привилегий.
24. Использование механизма ролей. Метки безопасности.
25. Использование представлений для обеспечения конфиденциальности информации.
26. Аудит связанных с безопасностью событий. Регистрация действий пользователя.
27. Управление набором регистрируемых событий.
28. Ведение специализированно аудита с использованием механизма триггеров.
29. Анализ данных аудита.

В ходе прохождения преддипломной практики обучающийся должен также продемонстрировать и закрепить ранее полученные навыки:

1. Соблюдения правила охраны труда и техники безопасности
2. Соблюдения эксплуатации средств вычислительной техники, исследовательских установок, имеющихся в подразделении, а также их обслуживания
3. Выполнения правил трудового распорядка предприятия (организации)
4. Соблюдения этики при работе в подразделения предприятия (организации)
5. Выполнения заданий, предусмотренных программой практики - назначенных руководителем подразделения предприятия (организации)
6. Взаимодействия с коллегами для выполнения задания подразделения предприятия (организации)
7. Представления результатов заданий руководителем подразделения предприятия (организации)
8. Освоение отдельных компьютерных программ и информационных систем, используемых в профессиональной деятельности
9. Работы с периодическими, реферативными и справочными информационными изданиями по прикладной математике и информатике
10. Работы с периодическими, реферативными и справочными информационными изданиями для составления отчетов по результатам исследования, практики
11. Проведения научных исследований в составе научного коллектива в соответствии с профилем объекта профессиональной деятельности
12. Исследования и разработки моделей и алгоритмов в составе научного коллектива в соответствии с профилем объекта профессиональной деятельности;
13. Исследования и разработки инструментальных средств по тематике проводимых научно-исследовательских проектов;
14. Участия в научных конференциях, семинарах
15. Подготовки научных и научно-технических публикаций.

10 Формы отчетности по практике

Для защиты отчета по преддипломной практике обучающемуся необходимо оформить и представить нижеперечисленные документы (формы заявления, задания на ВКР определены в Руководстве по выполнению и защите выпускных квалификационных работ по направлению 10.03.01 – Информационная безопасность):

1. Заявление на ВКР.
2. Задание на ВКР.
3. Копию договора о преддипломной практике.
4. Отзыв (приложение Б).
5. Отчет по преддипломной практике (приложение А).

Для защиты отчетов на кафедре создается комиссия в количестве трех преподавателей под председательством заведующего кафедрой.

Защита отчета по преддипломной практике оценивается комиссионно дифференцированно по пятибалльной системе с учетом представленных документов и ответов на теоретические вопросы для защиты отчета по преддипломной практике (см. подраздел 9). При оценке учитывается качество отчета о преддипломной практики и результаты защиты, а также, характеристика студента с места практики, указанная в отзыве.

10.1 Примерная структура и содержание отчета

По результатам прохождения практики студентом разрабатывается и составляется отчет. Отчет должен быть результатом **самостоятельной** творческой работы обучающегося. Изложение должно быть содержательным, но кратким.

Собранные во время прохождения преддипломной практики материалы могут быть использованы для разработки и защиты выпускной квалификационной работы. Обучающийся, как правило, в период преддипломной практики, выявляет технологическую проблему предприятия с учетом своей темы выпускной работы и намечает пути решения проблемы (см. Руководство по выполнению и защите выпускных квалификационных работ по направлению 10.03.01 – Информационная безопасность).

Для ознакомления с необходимыми материалами и использования их в процессе подготовки отчета обучающийся обязан обратиться за разрешением к руководству организации.

Требования к составлению и оформлению отчета

Отчет является основным документом, по которому определяется качество работы обучающегося в период практики. Отчет должен составляться индивидуально каждым обучающимся.

Работа по подбору материалов и составлению отчета должна проводиться в течение всего периода практики.

Работа над дневником и отчетом по практике должна быть закончена во время практики. Эти документы должны быть просмотрены и подписаны руководителем практики от производства, который дает отзыв о работе обучающегося и его отчете. В отзыве отмечается выполнение обучающимся программы практики, отношение к работе, трудовая дисциплина, приобретенные производственные навыки и участие в общественной жизни коллектива предприятия.

Отчет и дневник сдаются обучающимся на кафедру информатики и вычислительной техники в течение первой недели после окончания преддипломной практики.

Отчет пишется на одной стороне листа бумаги формата А 4 по ГОСТ 2.105-95 и с учетом требований стандартов. Чертежи и схемы могут быть выполнены карандашом.

При подготовке отчета желательно использовать текстовый редактор Word. При подготовке отчета следует использовать шрифт - Times New Roman, кегль 14, межстрочный интервал - одинарный.

Поля должны оставляться по всем четырем сторонам листа. Размер левого поля 30 мм, правого – не менее 10 мм, размер верхнего и нижнего полей - не менее 20 мм. Объем отчета по преддипломной практике должен составлять не менее 25 страниц, но не более 35 страниц машинописного текста. Статистический материал (формы, таблицы и т. п.) приводятся в приложениях.

10.2 Рабочее место и обязанности обучающегося на практике

Во время практики обучающийся обязан:

- выполнять служебные обязанности на рабочем месте (как стажер);
- вести конспект теоретических занятий;
- выполнять индивидуальное задание и оформлять отчет.

Находясь на практике, студенты обязаны руководствоваться должностными инструкциями работников в соответствии с занимаемой должностью.

С момента зачисления студентов на оплачиваемые рабочие места и должности в период преддипломной практики на них распространяется общее трудовое законодательство, правила охраны труда и внутреннего распорядка, действующие в данной организации. На студентов, не зачисленных на рабочие места, распространяются правила охраны труда и режим рабочего дня, действующие в данной организации.

Охрана труда и техника безопасности

Практика обучающегося начинается с изучения правил техники безопасности в организации в целом и на конкретных рабочих местах, на которых обучающимся предстоит работать с оформлением необходимых документов. Изучение правил и сдача зачета проводится в отделе техники безопасности.

Формы и методы контроля

Руководство и ответственность за организацию практики несет заведующий кафедрой и ответственный за практику на кафедре информатики и вычислительной техники.

Учебно-методическое руководство практикой обучающегося осуществляется ответственным за практику. В его обязанности входит контроль распределения студентов по рабочим местам, контроль выполнения плана практики и проведение необходимых консультаций. Оперативное руководство практикой осуществляют руководители практики от организации – базы практики.

Подведение итогов

Подведение итогов практики осуществляется в несколько этапов.

1. Отчет, заверенный руководителем практики от предприятия, подлежит проверке и защите в установленные учебным графиком сроки. Защита отчета по преддипломной практике оценивается руководителем практики от института по пятибалльной системе, о чем делается запись в экзаменационную ведомость и зачетную книжку студента с учетом балла. При оценке учитывается качество отчета и результаты защиты, а также, характеристика обучающегося с места практики.

Непредставление отчета в срок, неудовлетворительное прохождение практики или неудовлетворительная защита, влекут за собой повторное прохождение практики.

2. Ответственный за практику проверяет материалы практики, предоставленные руководителями, обобщает их замечания и предложения и составляет сводный отчет, содержащий сведения о сроках практики, задействованных преподавателях, общем количестве обучающихся, замечаниях и предложениях.

3. Сводный отчет ответственного за практику заслушивается и обсуждается на специальном заседании кафедры и утверждается перечень мероприятий по устранению недостатков (если они имели место) и реализации предложений по повышению качества проведения практики.

Методические указания руководителю практики

Ответственный за практику и руководители практик назначаются заведующим кафедрой информационной безопасности. В период практики ее руководители подчиняются непосредственно ответственному за практику. В обязанности руководителя практики входит:

- выдача заданий студентам,
- контроль за посещаемостью и выполнением программы практики,
- сдача всех материалов практики ответственному за практику.

11 Учебно-методическое обеспечение дисциплины

11.1 Основная литература

1. Об информации, информационных технологиях и о защите информации. Федеральный закон РФ от 27.07.2006 №149-ФЗ.

2. О персональных данных. Федеральный закон от 27 июля 2006 года № 152-ФЗ // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451

3. Федотова, Е.Л. Информационные технологии и системы: Учеб. пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 352 с.: ил. - (Высшее образование).

4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В.Г.Олифер, Н.А. Олифер. - 4-е изд. – СПб.: Питер, 2011. – 944 с.

5. Краковский, Ю.М. Информационная безопасность и защита информации : Учеб. пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с.

6. Гвоздева, В.А. Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 544 с.: ил. - (Профессиональное образование)

7. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : / ВУ.Ф. Шаньгин. – М. : ДМК Пресс, 2010 .— 544 с.

8. Проскурин, В.Г. Защита в операционных системах: Учеб. пособие для вузов / В.Г. Проскурин. - СПб: Горячая линия-Телеком, 2014.-192 с.

9. Гончаров, И.В. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков . - Воронеж : Воронежская областная типография, 2015.-180 с.

10. Методические указания и требования по выполнению и защите выпускной квалификационной работы по направлению 10.03.01 – Информатика и вычислительная техника / Сост.: Р.Р. Саакян, В.П. Зайков. – Краснодар: КИИЗ, 2017. – 60 с.

11. Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва : Дашков и Ко, 2012. — 244 с. <URL:http://biblioclub.ru/index.php?page=book&id=112247>

11.2 Дополнительная литература

1. Вдовенко, Л.А. Информационная система предприятия: Учеб. пособие / Л.А. Вдовенко. – М.: ИНФРА-М, 2010. – 237 с.

2. Основы управления информационной безопасностью: Учеб. пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой - М.: Горячая линия-Телеком, 2012.

4. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учеб. пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой - М.: Горячая линия- Телеком, 2012.

5. Сычев А.Н. Защита и передача интеллектуальной собственности: Учеб. пособие / А.Н.Сычев / Томский государственный университет систем управления и радиоэлектроники. - Томск : ТУСУР, 2010.

6. Зенин, И.А. Право интеллектуальной собственности: Учебник / И.А.Зенин. - М.:. Издательство Юрайт, 2011.

7. Малюк, А.А. Введение в защиту информации в автоматизированных системах: Учеб. пособие для вузов / А.А. Малюк, С.В. Пазизин, Н.С. Погожин - 4-е изд., стереотип. - М.: Горячая линия - Телеком, 2011.

8. Баскаков, И.В. Защита информации в информационных системах: Учеб. пособие / И.В. Баскаков, В.Л. Евсеев, А.В. Пролетарский, А.М. Суровов. М.: 2011.

9. Голенищев, Э.П. Информационное обеспечение систем управления: Учеб. пособие / Э.П. Голенищев, И.В. Клименко. – Ростов н/Д: Феникс, 2010. – 315 с.

10. Ищейнов, В.Я. Защита конфиденциальной информации : Учеб. пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с.

11. Избачков, З.Ю. Информационные системы: Учебник для вузов / З.Ю. Избачков, В.Петров . – СПб: Питер, 2006.

12. Хетагуров, Я.А. Проектирование автоматизированных систем обработки информации и управления: Учебник / А.Я. Хетагуров. – М.: Высш.шк., 2006.

13. Партыка, Т.Л. Операционные системы, среды и оболочки: Учеб. пособие / Т.Л. Партыка, И.И. Попов. – 3-е изд. перераб. и доп. – М.: ФОРУМ, 2010.- 544 с.

14. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 // Российская газета, № 136, 26.06.2013.

15. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 // Российская газета, № 107, 22.05.2013.

11.3 Периодические издания

Отечественные периодические издания:

1. Журнал «Информационные технологии и вычислительные системы»
2. Проблемы информационной безопасности. Компьютерные системы.

Зарубежные периодические издания:

1. Международный научн.-техн. Журнал Проблемы управления и информатики.

12 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения практики

1. http://www.znanium.ru
2. http://elibrary.ru (для препод.)
3. http://www.diclib.com
4. http://www.encyclopedia.ru
5. http://ru.wikipedia.org
6. http: //www.iprbookshop .ru/
7. http://citforum.ru/

8. http://www.intuit.ru/
9. http://www.bezpeka.com/ru/
10. http://www.microsoft.com/rus/
11. http://www.infoforum.ru/
12. hptt;//www.rupto.ru
13. http://www.ixbt.com/nw/

13 Перечень информационных технологий

Программное обеспечение

1. Операционные системы MS Windows, Linux;
2. Пакеты программ Open Office, MS Office
3. VirtualBox.

Базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex, Rambler.

14 Материально-техническое обеспечение преддипломной практики

ПЭВМ типа IBM PC (процессор Intel Pentium (Celeron) не ниже 1500 МГц, ОЗУ не менее 1024 Mb RAM, HDD не менее 200 Gb), подключенная к ИВС ОП (Internet), ЛВС, принтер.

15 Дополнения и изменения в рабочей программе преддипломной практики

Приложение А

НЕКОММЕРЧЕСКОЕ ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
КУБАНСКИЙ ИНСТИТУТ ИНФОРМЗАЩИТЫ

Кафедра Информационной безопасности

ОТЧЕТ
по преддипломной практике

Выполнил обучающийся: _____
(фамилия, имя, отчество)

Учебная группа: _____
Форма обучения: _____

Проверила комиссия: _____
(подпись, фамилия, инициалы)

_____
(подпись, фамилия, инициалы)

_____
(подпись, фамилия, инициалы)

_____
(подпись, фамилия, инициалы)

Оценка: _____

Краснодар
(год)

Приложение Б

О Т З Ы В ОРГАНИЗАЦИИ
о прохождении практики обучающимся

_____

(фамилия, имя, отчество)

проходившего преддипломную практику в

_____

_____

_____

с «___»_____20____ года

по «___»_____20____ года

Администрация организации (предприятия, учреждения) удостоверяет следующие сведения об обучающимся:

1.Правила техники безопасности изучил и сдал экзамен (зачет) _____
«___» _____ 2017 года

(Указать какая квалификационная группа по ТБ присвоена и выдано ли удостоверение, имелись ли нарушения ТБ.)

_____

_____

_____

_____

2. Во время практики работал в качестве кого (по какой профессии, по какому разряду и в какой должности)

_____

_____

_____

_____

3. Освоенные виды выполненных работ (качество, самостоятельность выполнения, интерес, инициатива, способность работать с технической документацией и т.д.)

_____

_____

_____

_____

4. Трудовая и исполнительская дисциплина (конкретные случаи нарушений, взыскания, поощрения и за что)

5. Общий уровень теоретической подготовки

6. Участие в общественной работе, поведение практиканта в нерабочее время, коммуникабельность

7. Особые замечания руководителя практики от предприятия:

8. Возможная перспектива трудоустройства выпускника на предприятии после окончания института

9. Качество составления и оформление отчета по практике

10. Оценка за прохождение практики

_____

М.П.

Руководитель практики от организации_____
Представитель института КИИЗ_____