МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по организации и проведению учебной практики
ЭКСПЕРИМЕНТАЛЬНО-ИССЛЕДОВАТЕЛЬСКАЯ ПРАКТИКА
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь, 2026

ВВЕДЕНИЕ

Практики студентов для специальности 10.05.01 «Компьютерная безопасность» являются составной частью основной образовательной программы высшего образования и представляют собой одну из форм организации учебного процесса, которая заключается в профессионально-практической подготовке студентов на базах практики. Цели, объёмы и виды практики определяются Положением о практической подготовке обучающихся по образовательным программам бакалавриата, специалитета, магистратуры, аспирантуры, ординатуры в ФГАОУ ВО «Северо-Кавказский федеральный университет» с учетом интересов и возможностей организаций и подразделений, в которых она проводится. Проведение практики организуется дирекцией и выпускающей кафедрой. Местом проведения практики могут быть предприятия, организации и фирмы любой организационно-правовой формы - промышленные предприятия; государственные и муниципальные учреждения; банки и финансовые учреждения; коммерческие фирмы, имеющие практический опыт в организации современного бизнеса, сложившиеся сферы деятельности, структуру управления и информационные системы управления. При этом базы практик должны соответствовать следующим требованиям:

− сфера деятельности организации (или подразделения организации), соответствует специальности 10.05.01 «Компьютерная безопасность»;

− организация обладает необходимой материально-технической базой, позволяющей обучающимся выполнить программу экспериментально-исследовательской практики;

− организация обладает компетентными, квалифицированными специалистами для обеспечения руководства практикой.

При определении базы прохождения практики приоритет отдается организациям, с которыми Договорами оформлено долгосрочное сотрудничество. Направление студента на практику осуществляется на основании приказа с указанием закрепления каждого обучающегося за структурным подразделением Университета или профильной организацией, руководителем практики от Университета, а также с указанием вида и срока прохождения практики. Проекты приказов о направлении обучающихся на практику готовятся институтами за 1 месяц до начала практики, согласовываются учебно-методическим управлением, правовым управлением. Приказы о направлении обучающихся на практику подписывает проректор по направлению. Издает и регистрирует приказы учебно-методическое управление. Если практика проводится на кафедре, которая отвечает за реализацию программы практики, основанием для формирования приказа о направлении обучающихся на практику является представление кафедры. Направление обучающихся на практику в структурные подразделения СКФУ осуществляется по согласованию с руководителем структурного подразделения, принимающего на практику обучающихся, на основании ходатайства. Договор о практической подготовке в этом случае не заключается. Направление обучающихся в сторонние организации для прохождения всех видов практики, предусмотренных ОПОП ВО, осуществляется только на основе договоров о практической подготовке. Договоры о практической подготовке составляются в двух экземплярах на основе типового «Договора о практической подготовке» и заключаются, как правило, в период планирования учебной деятельности на учебный год, но не позднее, чем за 2 месяца до начала практики. Регистрацию, учет и хранение оригиналов всех Договоров, заключенных Университетом, осуществляет Учебно-методическое управление. Копии зарегистрированных Договоров хранятся на кафедрах, реализующих соответствующую практику. Допускается возможность направления на практику в индивидуальном порядке обучающихся, желающих пройти практику в организациях по собственному выбору, если эти организации соответствуют требованиям, определенным выпускающей кафедрой. В этом случае обучающийся за 2 месяца до начала практики направляет заведующему выпускающей кафедры заявление, в котором указывает наименование, реквизиты и контактные данные организации - предполагаемого индивидуального места прохождения

практики. При несвоевременности предоставления обучающимся сведений, необходимых для оформления договора о практической подготовке, он направляется на практику в организацию, определенную руководителем практики от СКФУ. Ответственность за достоверность данных, указанных в индивидуальном Договоре о практической подготовке, несет руководитель практики от СКФУ. Для студентов очной формы обучения программа предусматривает проведение Экспериментально-исследовательской практики продолжительностью 2 недели в 6 семестре.

1. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Целями учебной практики экспериментально-исследовательская практика по специальности 10.05.01 «Компьютерная безопасность «являются получение основ теоретической подготовки обучающегося, приобретение им начальных практических навыков и компетенций, а также опыта самостоятельной профессиональной деятельности.

Общей задачей практики является приобретение начальных практических знаний и опыта работы по направлению подготовки, проверка профессиональной готовности будущего специалиста к самостоятельной трудовой деятельности.

Задачами практики являются:

1. Изучение основных правил организации научно-исследовательской и проектной работы в организации, а также управления коллективом.
2. Приобретение практических навыков в организации и проведении научных исследований, а также подготовки данных для составления обзоров, отчетов и научных публикаций.
3. Приобретение практических навыков в работе по обоснованию структуры и проектированию сложных систем и комплексов управления информационной безопасностью с учетом особенностей объектов защиты.
4. Проведение анализа угроз информационной безопасности объектов и разработка методов противодействия им.
5. Осуществление сбора, обработки, анализа и систематизации научно-технической информации по теме исследования.
6. Приобретение практических навыков в оформлении научно-технических отчётов, обзоров и подготовке публикаций по результатам выполненных исследований.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРАКТИКИ

Для освоения программы учебной Экспериментально-исследовательской практики, обучающиеся должны владеть следующими компетенциями: частично сформированной компетенцией ОПК-4 (способностью анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности); частично сформированной компетенцией ОПК-6 (Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю); частично сформированной компетенцией ОПК-9 (Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации); ОПК-11 (Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности

информации и требований по защите информации); ОПК-12 (Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения); ОПК-13 (Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности); ОПК-14 (Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации); ОПК-6.1 (Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов); ОПК-6.2 (Способен проводить экспертные исследования вычислительной техники и компьютерных носителей информации в рамках информационно-аналитической и технической экспертизы компьютерных систем); ОПК-6.3 (Способен в качестве привлекаемого эксперта при проведении следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной криминалистики), УК-1 (Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий), УК-6 (Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни).

Для освоения программы учебной Экспериментально-исследовательской практики, обучающиеся должны владеть следующими знаниями и компетенциями:

– углубить и закрепить знания, полученные при изучении теоретическом обучении:

– руководящих документов по вопросам программного, информационного и технического обеспечения реализации необходимых информационных технологий;

– организационной структуры учреждения, порядка взаимодействия элементов этой структуры в ходе выполнения информационных задач;

– самостоятельного выполнения отдельных функциональных и должностных обязанностей по предназначению;

– работы на штатных средствах вычислительных систем организации, применять в ходе выполнения штатных обязанностей новые информационные технологии;

– навыками работы с компьютером как средством управления информацией;

– методами управления проектами и готовностью к их реализации с использованием современного программного обеспечения;

– средствами программного обеспечения анализа и количественного моделирования систем управления;

– освоить компетенции ОПК-4, ОПК-6, ОПК-9, ОПК-,11 ОПК-12, ОПК-13, ОПК-14, ОПК-6.1, ОПК-6.2, ОПК-6.3, УК-1, УК-6.

3. ПЕРЕЧЕНЬ ОСВАИВАЕМЫХ КОМПЕТЕНЦИЙ

В результате прохождения учебной Экспериментально-исследовательской практики студенты получают знания и овладевают практическими навыками в рамках следующих компетенций:

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты, характеризующие этапы формирования компетенций, индикаторов
ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования	ИД-3 ОПК-4 использует стандартные методы и средства проектирования цифровых узлов и устройств, анализирует и синтезирует электронные	Способен использовать стандартные методы и средства проектирования цифровых узлов и устройств, анализировать и синтезировать электронные схемы

микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности	схемы	
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-1 ОПК-6 определяет критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Способен определять критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	ИД-2 ОПК-6 разрабатывает проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа	Способен разрабатывать проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ИД-1 ОПК-9 настраивает операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации	Способен настраивать операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации
	ИД-2 ОПК-9 использует методы и средства технической защиты информации	Способен использовать в профессиональной деятельности методы и средства технической защиты информации
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ИД-1 ОПК-11 разрабатывает частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками	Способен разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	ИД-2 ОПК-11 составляет комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в компьютерной системе	Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в компьютерной системе
ОПК-12 Способен	ИД-1 ОПК-12 использует	Способен использовать системные

администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения	системные приложения для управления настройками операционных систем	приложения для управления настройками операционных систем
	ИД-2 ОПК-12 выполняет резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения	Способен выполнять резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности	ИД-2 ОПК-13 проводит анализ уязвимостей программных и программно-аппаратных средств системы защиты информации компьютерной системы	Способен проводить анализ уязвимостей программных и программно-аппаратных средств системы защиты информации компьютерной системы
ОПК-14 Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации	ИД-1 ОПК-14 проектирует системы управления базами данных с учетом требований по обеспечению защиты информации	Способен проектировать системы управления базами данных с учетом требований по обеспечению защиты информации
	ИД-2 ОПК-14 настраивает и применяет современные системы управления базами данных, пользуется средствами защиты, предоставляемыми системами управления базами данных	Способен настраивать и применять современные системы управления базами данных, пользоваться средствами защиты, предоставляемыми системами управления базами данных
ОПК-6.1 Способен использовать технологии поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов	ИД-1 ОПК-6.1 определяет причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения	Способен определять причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения
	ИД-2 ОПК-6.1 применяет инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов	Способен применять инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов
ОПК-6.2 Способен проводить экспертные исследования вычислительной техники и компьютерных носителей информации в рамках информационно-аналитической и технической экспертизы компьютерных систем	ИД-3 ОПК-6.2 составляет экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации	Способен составлять экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации
ОПК-6.3 Способен в качестве привлекаемого эксперта при проведении	ИД-1 ОПК-6.3 применяет нормативные правовые акты, методические документы,	Способен применять нормативные правовые акты, методические документы, основы компьютерной

следственных и судебных действий применять нормативные правовые акты, методические документы, основы компьютерной криминалистики	основы компьютерной криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем	криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем
	ИД-2 ОПК-6.3 подготавливает экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем	Способен подготавливать экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИД-3 УК-1 определяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации	Определяет и оценивает риски возможных вариантов решений проблемной ситуации, вырабатывает стратегию действий по решению проблемной ситуации
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	ИД-3 УК-6 критически оценивает эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности	Способен критически оценивать эффективность использования своего времени и других ресурсов при решении задач, поставленных в избранной сфере профессиональной деятельности

4. ОБЯЗАННОСТИ СТУДЕНТА-ПРАКТИКАНТА

4.1. Студенты в период прохождения практики:

− выполняют в полном объеме индивидуальные задания, предусмотренные программами практики;

− соблюдают правила внутреннего трудового распорядка;

− соблюдают требования охраны труда и пожарной безопасности;

− ведут дневник учебной практики, где фиксируются все виды работ, выполняемых в течение рабочего дня.

4.2. При наличии в организации вакантной должности, работа на которой соответствует требованиям к содержанию практики, с обучающимся может быть заключен срочный трудовой договор о замещении такой должности. Допускается проведение практики в составе специализированных, сезонных или студенческих отрядов и в порядке индивидуальной подготовки у специалистов, имеющих соответствующую квалификацию;

4.3. Студенты, совмещающие обучение с трудовой деятельностью, вправе проходить учебную, учебную, в том числе учебную практики, по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям к содержанию практики.

4.4. С момента зачисления студентов в период практики в качестве практикантов на рабочие места на них распространяются правила охраны труда и правила внутреннего распорядка, действующие в организации, с которыми они должны быть ознакомлены в установленном в организации порядке.

5. ОБЯЗАННОСТИ РУКОВОДИТЕЛЯ ПРАКТИКИ ОТ УНИВЕРСИТЕТА

И/ИЛИ ПРЕДПРИЯТИЯ

Для руководства практикой, проходящей в структурных подразделениях СКФУ, назначаются руководители практики от соответствующих кафедр из числа лиц, относящихся к профессорско-преподавательскому составу.

Для руководства практикой, проводимой в профильной организации, назначаются руководители практики от соответствующих кафедр из числа лиц, относящихся к профессорско-преподавательскому составу, и руководители практики из числа работников профильной организации (далее - руководитель практики от профильной организации). Закрепление каждого обучающегося за руководителем практики из числа работников профильной организации осуществляется на основе распоряжения по институту.

5.1 . Обязанности руководителя практики от кафедры:

5.1.1 До начала практики:

– **со**ставляет рабочий график (план) проведения практики;

– разрабатывает индивидуальные задания для обучающихся, выполняемые в период практики;

– устанавливает связь с руководителями практики от профильной организации;

– проводит с обучающимися организационные мероприятия, связанные с проведением практики, в том числе инструктаж по технике безопасности (сведения о прохождении обучающимися инструктажа отражаются в журнале учета инструктажа);

– не позднее чем за 3 дня до начала практики, студентам выдается пакет документов: направление на практику, задание на практику и методические рекомендации по прохождению практики

5.1.2 В период проведения практики:

– проводит, предусмотренные программой практики, занятия;

– участвует в распределении обучающихся по рабочим местам и видам работ в организации;

– осуществляет контроль за соблюдением сроков проведения практики и соответствием ее содержания установленным образовательной программой и рабочей программой практики требованиям;

– проводит индивидуальные консультации и оказывает методическую помощь обучающимся при выполнении ими индивидуальных заданий и подготовки отчетов, а также при сборе материалов к выпускной квалификационной работе в ходе учебной практики;

– оказывает методическую помощь организации, принимающей на практику обучающихся.

– доводит до сведения заведующего кафедрой все случаи нарушения обучающимися дисциплины на базе практики;

– рассматривает отчет обучающихся о практике.

5.1.3 После завершения практики:

– в составе комиссии оценивает результаты прохождения практики обучающимися;

– принимает участие в заседаниях кафедры, посвященных обсуждению итогов выполнения практикантами программы практики.

– Руководитель практики от профильной организации:

– − согласовывает индивидуальные задания, содержание и планируемые результаты практики;

– предоставляет рабочие места обучающимся;

– обеспечивает безопасные условия прохождения практики обучающимся, отвечающие санитарным правилам и требованиям охраны труда;

– проводит инструктаж обучающихся по ознакомлению с требованиями охраны труда, техники безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка.

6. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

Прохождение учебной практики, является одним из обязательных и неотъемлемых элементов программы обучения в вузе по специальности 10.05.01 «Компьютерная безопасность». В результате прохождения практики студент знакомиться со способами обработки получаемых данных и их интерпретацией, этапами обработки и анализа полученной информации, формулирование выводов, а именно:

1. Организационно-правовой анализ трудовых отношений в организации.
2. Правовой анализ договорных отношений в организации.
3. Анализ стратегий и целей организации.
4. Маркетинговый анализ (Оценка положения организации на рынке).
5. Характеристика особенностей учетной политики организации.
6. Анализ нормативно-правовой базы, регламентирующей функционирование организации.
7. Анализ результатов деятельности организации.
8. Анализ программного, технического и телекоммуникационного обеспечения организации.
9. Характеристика информационного обеспечения.
10. Документооборот.

Структура отчета по практике:

1. Задания.

Изучить и провести анализ следующих вопросов:

– изучение деятельности и аналитическая оценка предприятия, как объекта информатизации;

– изучение конкретной финансовой, инвестиционной, биржевой, производственной и другой деловой документации;

– изучение технологии сбора, регистрации и обработки экономической информации на данном предприятии;

– изучение организационной структуры базы практики, особенностей функционирования объекта, представление организационных структур в виде схем;

– освоение на практике методов предпроектного обследования объекта информатизации, проведение системного анализа результатов обследования при построении модели информационной системы;

– анализ функций предприятия, участка, отдела, службы, выявление функциональной структуры подразделений, представление функциональных структур в виде схем и информационных моделей;

– изучение особенностей, имеющихся на предприятии информационных систем, а также средств сбора, обработки и передачи информации;

– изучение состояния экономических информационных систем на предприятии с выдачей оценки научно-технического уровня системы;

– определить перечень задач, решаемых средствами и в рамках автоматизированных информационных технологий;

– выполнить классификацию функциональных подсистем и задач ИС;

– определить продолжительность жизненного цикла различных подсистем, задач;

– ознакомление с системой классификации и кодирования информации в условиях экономических информационных систем.

2. Индивидуальное задание.

1. Анализ инструментальных средств обратного инжиниринга.
2. Средства отладки и дизассемблирования.
3. Шестнадцатеричные редакторы.
4. Описание функций встроенного языка IDA Pro.
5. Теоретические основы исследования программных реализаций.
6. Описание функций встроенного языка OLYDB.
7. Основы программирования на ассемблере в Windows.
8. Работа с машинными командами и командами ассемблера с помощью отладчика Debug.
9. Представление данных в памяти компьютера.
10. Изучение техники работы с отладчиками и дизассемблерами.
11. Изучение защитных механизмов программного обеспечения.
12. Изучение недокументированных возможностей по повышению привилегий пользователя в ОС Windows.
13. Обеспечение безопасности операционных систем семейства Linux.
14. Мандатная сущностно-ролевая ДП модель управления доступом и информационными потоками в операционных системах Linux.
15. Управление доступом. Задание мандатного управления доступом для состояния системы.
16. Управление доступом. Задание мандатного контроля целостности.
17. Управление безопасностью операционной системы специального назначения.
18. Мандатное управление доступом.
19. Мандатный контроль целостности.
20. Управление доступом к объектам графической подсистемы.
21. Сетевое взаимодействие в ОССН (операционной системы специального назначения).
22. Основные определения и понятия экспертизы вычислительной техники и носителей компьютерной информации.
23. Классификация и виды экспертиз вычислительной техники и носителей компьютерной информации.
24. Основные законы, регламентирующие деятельность эксперта. Уголовно-процессуальный кодекс: 47, 42, 57, 162, 195-207
25. Основные законы, регламентирующие деятельность эксперта. Уголовно-процессуальный кодекс: 235, 269, 271-275, 282-283.
26. Оформление отчетов криминалистической экспертизы.
27. Правила и инструкции первичного осмотра компьютерной системы.
28. Внутренний осмотр компьютерной техники, информация о результатах внешнего осмотра.
29. Информация о результатах исследования информационного пространства носителей информации и их пригодности для проведения исследования.
30. Понятие криптоконтейнеров и зашифрованных файлов на компьютере.
31. Алгоритмы поиска зашифрованных файлов.
32. Основные определения и термины компьютерных преступлений и инцидентов в информационной безопасности.
33. Обзор принципов, методов и технологий выявления факта свершения компьютерного преступления.
34. Экспертные системы. Основные возможности данных систем, их плюсы, минусы, сравнительный обзор параметров и технических особенностей.
35. Аппаратное обеспечение для проведения расследования компьютерных преступлений и инцидентов. Типы доверенных операционных систем. Требования к хранилищам данных и АРМ, на которых производится расследование.

36. Поиск уликовой информации и следов компьютерных преступлений при помощи экспертной системы EnCase Forensic.

37. Поиск уликовой информации и следов компьютерных преступлений при помощи экспертной системы Belkasoft Evidence Center.

38. Мошенничество в системах дистанционного банковского обслуживания. Принципы. Способы хищения денежных средств.

39. Кража конфиденциальной информации. Методы и средства. Применение специального ПО. Средства удалённого управления.

40. Технологии совершения компьютерных преступлений на конечных устройствах банковского обслуживания (вирусы для банкоматов, терминалов и т.д.),

41. Технологии и принципы исследования дампов оперативной памяти. Специализированное ПО для выполнения данного исследования.

42. Обзор технологий хранения данных (магнитные носители информации, оптические носители информации, полупроводниковые носители информации).

43. Логика хранения данных (формат и структура файлов, двоичные редакторы).

44. Способы надежного хранения данных (зазеркаливание и копирование файлов, RAID- избыточный массив независимых дисков).

45. Причины потерь данных (аппаратные проблемы, нарушение логической структуры данных).

46. Восстановление информации (тактика восстановления данных, программные и программно-аппаратные средства восстановления данных).

47. Автоматическое и ручное восстановление (средства автоматического восстановления, приемы восстановления вручную).

48. Восстановление данных с жестких дисков (принцип работы жестких дисков, диагностика аппаратных неисправностей, программные средства диагностики).

49. Восстановление данных с массивов RAID (обзор программ для работы с RAID, причины потерь данных и тактика их восстановления).

50. Восстановление данных с флеш-накопителей (принцип работы, устройство и причины потери данных с полупроводниковых накопителей; восстановление данных с карт памяти, извлечение информации с карт памяти и их образов).

51. Восстановление данных с дисков SSD (особенности устройства и структуры твердотельных накопителей, тактика и практика восстановления данных со встроенных дисков).

52. Восстановление данных с SIM-карт (архитектура SIM-карты, тактика и практика восстановления данных SIM карт).

53. Восстановление данных с лазерных дисков (причины потерь данных, восстановление данных при физических повреждениях, программное восстановление данных).

54. Подготовка теоретического материала для учебно-лабораторного стенда «Устройство жесткого диска».

55. Подготовка теоретического материала для учебно-лабораторного стенда «Устройство привода оптических дисков».

56. Подготовка теоретического материала для учебно-лабораторного стенда «Устройство дисковода для гибких магнитных дисков».

3. Список использованной литературы:

1. Учебная практика: методические рекомендации по прохождению учебной практики / сост. Гимбицкий В.А., Куликов В.В. — Ставрополь: Изд-во СКФУ, 2013. – 28 с.

2. Делопроизводство: образцы, документы, организация и технология работы: с учетом нового ГОСТ Р 6.30-2003 "Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов": [более 120 документов / В. В. Галахов, канд.ист.наук, доц. и др.;

под ред.: И. К. Корнеева, канд.эконом.наук, доц., В. А. Кудряева, канд. эконом.наук, проф.]. - 3-е изд., перераб. и доп. - Москва: Проспект, 2010. - 479 с.: ил., табл.; 24. - (Профессиональные юридические системы Кодекс). - ISBN 978-5-392-00563-5

3. Защита компьютерной информации. Эффективные методы и средства /Шаньгин В. Ф. - М. ДМК Пресс, 2010. - 544 с. ил.

4. Девянин П.Н. Модели безопасности компьютерных систем. Учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия»,2005. – 144 с.

5. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для вузов. – М.: Академия, 2008. – 336 с.

6. Семкин С.Н. Основы правового обеспечения защиты информации – М: Горячая линия – Телеком, 2008.

7. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник – М: Академия, 2008.

8. Методические указания по разработке типовых документов в области информационной безопасности /А.М. Иванцов. – Ульяновск: УлГУ, 2016 – 63 с.

9. Хореев П.В. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов. – М.: Академия, 2007. – 256 с.

10. 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

11. А.И., Ушаков Д.В. - М.: Горячая линия-Телеком, 2008. - 558 с.

4.Приложения (копии документов, бланки, формы).

7. ЗАДАНИЯ И ПОРЯДОК ИХ ВЫПОЛНЕНИЯ

Индивидуальное задание определяется научным руководителем с учетом интересов студентов. Задание должно содержать четкую формулировку намечаемых целей и ожидаемых результатов. Из целей должна следовать постановка конкретной задачи, предлагаемой для решения студенту, а также должно быть указано место этой задачи в общем комплексе задач.

Индивидуальное задание по Экспериментально-исследовательской практике должно, как правило, включать следующие основные разделы:

1. Анализ и описание исследуемого объекта информационной системы.

2. Выбор (разработка) и обоснование методов решения поставленных конкретных задач.

3. Рекомендации по повышению эффективности функционирования исследуемого объекта.

8. ФОРМА ПРЕДОСТАВЛЕНИЯ ОТЧЕТА ПО ПРАКТИКЕ

По результатам прохождения практики студент представляет руководителю практики от кафедры следующие отчетные документы, заверенные подписью руководителя и печатью организации:

− отчет;

− дневник экспериментально-исследовательской практики;

− отзыв руководителя практики от профильной организации или структурного подразделения СКФУ в случае, когда практика проводится на базе Университета.

По окончании практики студент составляет письменный отчет. Отчет проверяется и подписывается непосредственным руководителем практики от Университета и руководителем практики от профильной организации. Подпись руководителя практики от профильной организации должна быть заверена печатью организации. Содержание и

оформление отчета должны соответствовать требованиям, разработанным выпускающей кафедрой.

Информационные блоки отчета должны быть представлены в следующем порядке:

1. Титульный лист.

2. Содержание.

3. Введение (цели и задачи практики, краткая характеристика базы и места практики, описание основных видов деятельности, выполняемых практикантом).

4. Разделы и подразделы (сведения о конкретно выполненной студентом работе в период практики в соответствии с заданием или описание деятельности, выполняемой в процессе прохождения практики; достигнутые результаты).

5. Заключение (выводы о результатах практики и анализ возникших проблем)

6. Список литературы.

7. Приложения (по необходимости).

Дневник учебной практики включает:

− задание на практику;

− индивидуальное задание;

− календарный план прохождения практики и краткое описание ежедневных видов работ, выполненных практикантам;

− анкета обучающегося по итогам практики. Отзыв руководителя практики от организации или структурного подразделения СКФУ в случае, когда практика проводится на базе Университета может быть оформлен следующим образом:

− либо в виде письма на официальном бланке организации за подписью руководителя практики от организации или руководителя подразделения 15

− либо в виде письма на листе А4 за подписью за подписью руководителя практики от организации или руководителя подразделения и печатью организации.

Во время практики студент ведет дневник практики, в котором описывает свою деятельность на рабочем месте, заносит записи, чертит схемы и т.д.

В конце практики студент использует этот дневник для собственной оценки общей характеристики деятельности предприятия и составления отчета о практике, график написания, сдачи и защиты которого составляется и утверждается кафедрой.

Студент самостоятельно, непосредственно на предприятии, составляет отчет о практике в соответствии с программой технологической практики. Отчет о практике и все приложения к нему просматриваются руководителем практики от предприятия, который даёт отзыв – характеристику, содержащую данные о сроках практики; названии подразделения предприятия, где и в каком качестве работал студент; краткое описание работы, выполненной студентом; личностная характеристика студента-практиканта и его отношение к работе, участии в общественной жизни. Далее дается оценка выполнения практикантом программы практики и индивидуальных заданий. Отзыв руководителя практики от предприятия обязательно заверяется печатью предприятия.

Студент-практикант при прохождении практики обязан:

- полностью выполнять задания, предусмотренные программой практики;
- подчиняться действующим в организации правилам внутреннего распорядка;
- изучить и строго соблюдать правила охраны труда и учебной санитарии.

Общий объем отчета должен составлять не менее 20 листов, но не превышать 50–55 листов формата А4 (210х297 мм), в том числе введение – не более 2–3 листов.

Текст должен иметь следующие параметры:

- формат бумаги А4 (210×297 мм), бумага белая;
- поля: верхнее, нижнее – 20 мм, левое – 30 мм, правое – 15 мм;
- межстрочное расстояние – полуторное (т. е. на одной странице должно быть не более 29 строк и 60±2 знака в одной строке, учитывая пробелы);
- переплет 0 см;
- ориентация книжная;

− шрифт Times New Roman Cyr (Arial Cyr);
− размер шрифта 14 пунктов;
− красная строка – 1,25 см;
− выравнивание основного текста должно быть по ширине;
− формулы выравниваются по центру, их нумерация по правому краю в круглых скобках;
− рисунки нумеруются снизу (Рисунок 1 – Название), таблицы – сверху (таблица 1 – Название);
− страницы нумеруются снизу, по центру;
− необходимо различать в тексте дефис (-) (например, черно-белый, бизнес-план) и тире (–);
− если вы используете кавычки, они должны иметь вид так называемых «ёлочек» («»).

9. КРИТЕРИИ ВЫСТАВЛЕНИЯ ОЦЕНОК

После окончания практики студенты должны защитить отчет по практике комиссии.

Итоги практики оцениваются на защите индивидуально по пятибалльной шкале. Оценка по практике приравнивается к оценкам по теоретическому обучению и учитывается при подведении итогов общей успеваемости студентов и предполагает оценку: «отлично», «хорошо», «удовлетворительно», которая проставляется в ведомость и зачетную книжку. Оценка «неудовлетворительно», полученная студентом по итогам практики, в зачетную книжку не выставляется. При оценке итогов работы студента принимаются во внимание выполнение программы практики и реализация поставленных задач в полном объеме, активность, ответственность и творческий подход практиканта к работе, качественная характеристика продуктивности деятельности, качество итоговой документации и представление ее в установленные сроки. Кроме этого, при подведении итогов работы студента принимается во внимание оценка, данная ему руководителем практики от учреждения.

Оценка «**отлично**» выставляется обучающему, если студент

На высоком уровне: способен использовать стандартные методы и средства проектирования цифровых узлов и устройств, анализировать и синтезировать электронные схемы; способен определять критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; способен разрабатывать проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа; способен настраивать операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации; способен использовать в профессиональной деятельности методы и средства технической защиты информации; способен разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в компьютерной системе; способен использовать системные приложения для управления настройками операционных систем; способен выполнять резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения; способен проводить анализ уязвимостей программных и программно-аппаратных средств системы защиты информации компьютерной системы; способен проектировать системы управления базами данных с учетом требований по обеспечению защиты информации; способен настраивать и применять современные системы управления базами данных,

пользоваться средствами защиты, предоставляемыми системами управления базами данных способен определять причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения; способен применять инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; способен составлять экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; способен применять нормативные правовые акты, методические документы, основы компьютерной криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем; способен подготавливать экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем.

Оценка «**хорошо**» выставляется обучающему, если студент

На среднем уровне: способен использовать стандартные методы и средства проектирования цифровых узлов и устройств, анализировать и синтезировать электронные схемы; способен определять критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; способен разрабатывать проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа; способен настраивать операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации; способен использовать в профессиональной деятельности методы и средства технической защиты информации; способен разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в компьютерной системе; способен использовать системные приложения для управления настройками операционных систем; способен выполнять резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения; способен проводить анализ уязвимостей программных и программно-аппаратных средств системы защиты информации компьютерной системы; способен проектировать системы управления базами данных с учетом требований по обеспечению защиты информации; способен настраивать и применять современные системы управления базами данных, пользоваться средствами защиты, предоставляемыми системами управления базами данных способен определять причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения; способен применять инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; способен составлять экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; способен применять нормативные правовые акты, методические документы, основы компьютерной криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем; способен подготавливать экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем

Оценка «**удовлетворительно**» выставляется обучающему, если студент

На минимальном уровне: способен использовать стандартные методы и средства проектирования цифровых узлов и устройств, анализировать и синтезировать электронные

схемы; способен определять критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; способен разрабатывать проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа; способен настраивать операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации; способен использовать в профессиональной деятельности методы и средства технической защиты информации; способен разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в компьютерной системе; способен использовать системные приложения для управления настройками операционных систем; способен выполнять резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения; способен проводить анализ уязвимостей программных и программно-аппаратных средств системы защиты информации компьютерной системы; способен проектировать системы управления базами данных с учетом требований по обеспечению защиты информации; способен настраивать и применять современные системы управления базами данных, пользоваться средствами защиты, предоставляемыми системами управления базами данных способен определять причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения; способен применять инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; способен составлять экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; способен применять нормативные правовые акты, методические документы, основы компьютерной криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем; способен подготавливать экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем.

Оценка «**неудовлетворительно**» выставляется обучающему, который

С грубыми ошибками: способен использовать стандартные методы и средства проектирования цифровых узлов и устройств, анализировать и синтезировать электронные схемы; способен определять критерии технологических процессов защиты информации для сопоставления с требованиями нормативных документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; способен разрабатывать проекты инструкций, регламентов, положений и приказов по защите информации ограниченного доступа в организации; определяет политику контроля доступа работников к информации ограниченного доступа; способен настраивать операционные системы, системы управления базами данных и компьютерные сети с учетом требований по обеспечению защиты информации; способен использовать в профессиональной деятельности методы и средства технической защиты информации; способен разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в компьютерной системе; способен использовать системные приложения для управления настройками операционных систем; способен выполнять резервное копирование и аварийное восстановление работоспособности прикладного и системного программного обеспечения; способен

проводить анализ уязвимостей программных и программно-аппаратных средств системы защиты информации компьютерной системы; способен проектировать системы управления базами данных с учетом требований по обеспечению защиты информации; способен настраивать и применять современные системы управления базами данных, пользоваться средствами защиты, предоставляемыми системами управления базами данных способен определять причины, цели и условия изменения свойств (состояния) программного и аппаратного обеспечения; способен применять инструментальные средствами поиска, фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов; способен составлять экспертное заключение в соответствии с требованиями, предъявляемыми к работе привлекаемого эксперта при проведении следственных и судебных действий; обращаться с инструментальными средствами проведения экспертиз вычислительной техники и носителей компьютерной информации; способен применять нормативные правовые акты, методические документы, основы компьютерной криминалистики при проведении следственных и судебных действий по информационно-аналитической и технической экспертизе компьютерных систем; способен подготавливать экспертные заключения по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем.

Не выполнившие программу практики или не предоставившие её результаты в установленные сроки, считается не аттестованным. При выставлении оценки по результатам практики студента необходимо учитывать следующие показатели:

− оценка понимания студентом целей и задач, стоящих перед современным специалистом по информационным технологиям в образовании;

− оценка технологической готовности студента к работе в современных условиях (оценивается общая дидактическая, методическая, техническая подготовка по проведению научных исследований);

− оценка умений планировать свою деятельность (учитывается умение студента прогнозировать результаты своей деятельности учитывать реальные возможности и все резервы, которые можно привести в действие для реализации намеченного);

− оценка исследовательской деятельности студента (выполнение экспериментальных и исследовательских программ, степень самостоятельности, качество обработки полученных данных, их интерпретация, достижение цели);

− оценка работы студента над повышением своего профессионального уровня (оценивается поиск эффективных методик и технологий исследования);

− оцениваются личностные качества студента (культура общения, уровень интеллектуального, нравственного развития и др.).

10. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

Основная литература:

1. Котляревская, И.В. Организация и проведение практик: учебно-методическое пособие / И.В. Котляревская, М.А. Илышева, Н.Ф. Одинцова; Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. - Екатеринбург: Издательство Уральского университета, 2014. - 93 с.: ил., табл. - Библиогр. в кн. - ISBN 978-5-7996-1091-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276361

Дополнительная литература:

1. Барсуков, В. С. Современные технологии безопасности / В. С. Барсуков, В. В. Водолазкий. – М.: Нолидж, 2000. – 496 с.: ил., табл. – Библиогр.: с. 490-493. – ISBN 5-89251-073-5.

2. Гришин, В. Н. Информационные технологии в профессиональной деятельности: учебник для студентов сред. проф. образования / В.Н. Гришин, Е.Е. Панфилова. – М.: ИД

Форум: Инфра-М, 2011. – 416 с.: прил. – (Профессиональное образование). – Библиогр.: с. 408-409. – ISBN 978-5-8199-0175-5. – ISBN 978-5-16-002310-6.

3. Девянин, П.Н. Модели безопасности компьютерных систем: учеб. пособие для студентов вузов / П.Н. Девянин. – М.: Академия, 2005. – 144 с.: ил., табл. – (Высшее профессиональное образование). – Гриф: Доп. УМО. – Библиогр.: с. 139-140. – ISBN 5-7695-2053-1.

4. Завгородний, В.И. Комплексная защита информации в компьютерных системах: учеб. пособие вузов / В.И. Завгородний. – М.: Логос, 2001. – 264 с.: ил. – Гриф: Рек. УМО для студентов вузов. – Библиогр.: с. 259-263. – ISBN 5-94010-088-0.

5. Северин, В.А. Правовое обеспечение информационной безопасности предприятия: Учебно-практическое пособие / МГУ. – М.: Городец, 2000. – 192с. – ISBN 5-9258-0009-5.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по практике:

1. Методические рекомендации по экспериментально-исследовательской практике для студентов специальности 10.05.01 Компьютерная безопасность

Интернет-ресурсы:

1. Национальный открытый университет ИНТУИТ. http://www.intuit.ru/.
2. Интернет портал компании «Бизнес инжиниринговые технологии» betec.ru
3. Интернет портал компании SAP AG - sap.com
4. Интернет портал компании IBM - ibm.com
5. Интернет-портал компании MICROSOFT - Microsoft.com
6. Интернет портал компании ORACLE – oracle.com
7. Интернет портал компании GMCS – gmcs.ru.

11. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы не требуются.

Программное обеспечение:

Windows 8, Microsoft Office 2010, Visual Studio 2010, Firefox, MS SQL Server 2014, MongoDB, доступ к интернет-ресурсам, система MS Internet Explorer

12. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Компьютерный класс (корпус 9, аудитория 402А). 26 ЭВМ со следующими характеристиками: Intel Core i3 /ОЗУ 8 Гб/HDD 1 Тб/SSD 128Гб/DVD-RW.