МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «**ЗАЩИЩЕННЫЕ ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ**»
для студентов направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2022

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине Защищенные локальные вычислительные сети направлена на формирование следующих **компетенций**:

Код	Формулировка:
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
3 семестр					
ПК-4 ПК-2	Самостоятельное изучение литературы и источников	Собеседование	37,17	4,13	41,3
ПК-4 ПК-2	Подготовка к практическим занятиям	Защита ПР	2,43	0,27	2,7
ПК-4 ПК-2	Написание реферата/доклада	Защита доклада	9	1	10
	Итого за 3 семестр		48,6	5,4	54
4 семестр					
ПК-4 ПК-2	Самостоятельное изучение литературы и источников	Собеседование	49,32	5,48	54,8
ПК-4 ПК-2	Подготовка к практическим занятиям	Защита ПР	2,43	0,27	2,7
ПК-4 ПК-2	Написание реферата/доклада	Защита доклада	9	1	10
	Итого за 4 семестр		**60,75**	**6,75**	**67,5**
	Итого		**109,35**	**12,15**	**121,5**

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить, как сами сведения, излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь сокращать и обобщать своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механических навыков без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

- Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.
- Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.
- Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса
- Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.
- Приложение (при необходимости).

Требования к оформлению:

- текст с одной стороны листа;
- шрифт Times New Roman;
- кегль шрифта 14;
- межстрочное расстояние 1,5;
- поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
- доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

- соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде

оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими и информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь отдельные не существенные поручения в групповом проекте.	Проект не сдан.

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

33. Текущее контрольное мероприятие считается сданным, если студент получил за него не

менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо вовремя ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1 Воронцова, В. Л. Лекции по системному и прикладному программному обеспечению: Учебное пособие / В. Л. Воронцова, И. А. Журавлева; Ставроп. гос. ун-т. – Ставрополь: СГУ, 2004. – 208 с. – Библиогр: с. 205-206

2 Защита информации в операционных системах: лабораторные работы: учеб.- метод. пособие / М. В. Романкова / сост.: И. В. Зайцева / Федеральное агентство по образованиюСтавроп. гос. ун-т. – Ставрополь : Изд-во СГУ, 2008. – 99 с. – Библиогр.: с. 96-97

3 Программно-аппаратные средства обеспечения информационной безопасности: учеб.пособие / сост. В. И. Петренко, Н. В. Куклева ; Федер. агентство по образованию,Ставроп. гос. ун-т, Ч. 2, Защита в операционных системах. – Ставрополь: Изд-во СГУ,2007. – 154 с. – Библиогр: с. 154

Дополнительная литература:

1 Безручко, В. Т. Практикум по курсу "Информатика". Работа в Windows, Word, Excel [Учеб.пособие для вузов*]. – М.: Финансы и статистика, 2004. – 272с.: ил. – Библиогр.: 265. – ISBN 5-279-02436-8

2 Грищенко, Ю.Б. Операционные системы: в 2-х ч. / Ю.Б. Грищенко ; Федеральное агентст по образованию, Томский межвузовский центр дистанционного образования (ТУСУРКафедра автоматизации обработки информации (АОИ). Томск: Томский государственный университет систем управления и радиоэлектроники, 2009. – Ч. 2. – 2 с.– Режим доступа: поподписке.– URL: http://biblioclub.ru/index.ph page=book&id=208655

Методические рекомендации для самостоятельной работы студентов по дисциплине

1. Методические рекомендации по выполнению лабораторных работ по дисциплине «Защищенные локальные вычислительные сети».

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине «Защищенные локальные вычислительные сети».

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Цифровая грамотность и обработка больших данных»

2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии

3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине
«ЗАЩИЩЕННЫЕ ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1. Цель и задачи изучения дисциплины

Целью изучения дисциплины «Защищенные локальные вычислительные сети» является обучение принципам построения защиты информации в операционных системах (ОС) и анализа надежности защиты ОС, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность»

2. Оборудование и материалы

Для проведения практических занятий необходимо следующее материально-техническое обеспечение: персональный компьютер; проектор; возможность выхода в сеть Интернет для поиска по образовательным сайтам и порталам; интерактивная доска.

3. Наименование лабораторных работ

Не предусмотрено рабочим планом

5.4 Наименование практических занятий

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
	3 семестр		
Тема 1: Безопасность компьютерных сетей			
1	«Конфигурирование и проверка IPsec VPN между двумя пунктами с помощью интерфейса командной строки	1,5	
1	Настройка межсетевого экрана Cisco ASA 5505	1,5	
Тема 3: Протоколирование и аудит			
3	Исследование процессов создания бюджетов пользователей в ОС Windows NT и Unix	1,5	
3	Исследование методов интеграции сетей Microsoft и Unix с использованием сервера Samba	1,5	
Тема 5: Системы безопасности ОС Linux			
5	Изучение базовых команд ОС Linux	3	
Тема 7: Модели безопасности основных операционных систем			
7	Классификация защиты семейства ОС Windows	4,5	
	4 семестр		
Тема 11. Архитектура ОС Linux			
11	Настройка ОС Linux	1.5	1.5
11	Работа с файлами в Linux	1.5	1.5
11	Работа с файлами в Linux	1.5	1.5
Тема 12. Архитектура ОС Windows			
12	Работа с реестром Windows	1.5	1.5
12	Работа в командной строке	1.5	1.5

12	Пакетные файлы	1.5	1.5
12	Оснастки консоли	1.5	1.5
Тема 14. Управление файлами и вводом-выводом в ОС			
14	Файловая система Windows	1.5	1.5
14	Файловая система UNIX и Linux	1.5	1.5
	Итого за 4 семестр	**13.5**	13.5
	Итого	**13.5**	13.5

4. Содержание практических работ

Практическая работа 1 «Конфигурирование и проверка IPsec VPN между двумя пунктами с помощью интерфейса командной строки

В ходе лабораторной работы: требуется построить соответствующий проект в Cisco Packet Tracer, топология сети включает три маршрутизатора. Ваша задача заключается в том, чтобы настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (при передаче трафика между соответствующими локальными сетями. Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. Маршрутизатор R2 играет роль транзитного узла и не имеет информации о VPN. IPSec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям.

Практическая работа 2 «Настройка межсетевого экрана Cisco ASA 5505»

Целью лабораторной работы является изучение работы межсетевогоэкрана Cisco ASA 5505 конфигурации. В ходе выполнения лабораторной работы необходимо активировать пользовательские порты на R1 и S1. Настроить Ethernet интерфейсы персональных компьютеров. Настроить сетевые интерфейсы PC1, PC2, PC3, PC4. Создать VLAN'ы согласно топологии сети. Произвести базовую настройку межсетевой экран Cisco ASA 5505 Результаты о проделанной работе показать преподавателю. Раздел «Итоговый контроль» представляет собой самостоятельное выполнения заданий по вариантам. Каждый вариант содержит по 3 задания, и дана общая топология сети для всех вариантов. В разделе «Литература» написаны учебные пособия и книги по дисциплине «Безопасность компьютерных сетей», которые помогут освоить дисциплину. Раздел «Оборудование». Описывается лаборатория, компьютерный класс, и весь технический парк на котором будет производиться работы по обучению студентов и подготовки их к WorldSkills Russia.

Технопарк оснащён следующим оборудованием:

- маршрутизаторы Cisco 2911 (количество 6);
- маршрутизаторы Cisco 2811 (количество 9);
- коммутаторы Cisco Catalyst 2960 (количество 9);

•межсетевые экраны Cisco ASA 5505 (количество 6);
•блейд-система HP c7000;
•сервер HP ProLiant BL 460c G7 2x 5675;
•консольный сервер;
•12 рабочих мест;
•IP-телефоны Cisco CP-7961G (количество 6).

Маршрутизатор Cisco 2911/K9 — это устройство нового поколения, относящееся к семейству ISR G2. Модель позволяет создавать безопасное широкополосное подключение к сети, производить передачу мультимедийных данных, видео, осуществлять беспроводную связь, а также применять множество дополнительных функций при минимальном уровне затрат на приобретение и содержание. Маршрутизатор Cisco 2911/K9 со встроенными сетевыми сервисами на 3 порта идеально подходит для создания сетей малых и средних организаций и предприятий. Модель имеет 512 Мб встроенной и 526 Мб флеш-памяти, возможность поддержки PoE на портах 10/100/1000 Ethernet, а также поддержку протокола VPN и туннелирования для осуществления надежной и безопасной передачи при построении удаленных VPN сетей. Маршрутизатор Cisco 2811 — маршрутизатор с интеграцией сервисов, обеспечивающий все потребности небольших офисов и филиалов (до 36 рабочих мест) в современных коммуникациях.

Может выполнять функции:

маршрутизатора доступа и маршрутизатора локальной сети;

центра IP-телефонии и голосовой почты (в вариантах Voice bundle и Voice Security bundle);

интегрированного решения для обеспечения безопасности (в вариантах Security bundle и Voice Security bundle);

• межсетевого экрана;
• систему предотвращения вторжений;
• шифрования и создания VPN-туннелей;
• система Cisco NAC и фильтрация по Uniform Resource Locator (URL);

Коммутатор Cisco Catalyst 2960 — линейка ведущих продуктов среди коммутаторов второго уровня. Эти коммутаторы позволяют снизить совокупную стоимость владения при развертываниях с использованием IP- телефонов Cisco, точек доступа к беспроводной сети (WLAN) Cisco Aironet или других устройств, совместимых с IEEE 802.3af. Технология PoE позволя- ет устранить потребность в обеспечении питания устройств с поддержкой PoE от сети электропитания и исключить затраты на дополнительные электрические кабели, которые в противном случае необходимы при развертываниях IP-телефонов и сетей WLAN. Их использование позволяет упростить эксплуатацию ИТ-инфраструктуры, повысить уровень безопасности бизнес-процессов, обеспечить устойчивую работу сети, а также предоставить пользователям возможность работы в «сетях без границ». Каждый спаренный порт каскадирования состоит из одного порта Ethernet RJ-45 и одного порта GE для подключения SFP, при этом активен может быть только один из двух портов, возможность подключения настольных компьютеров к 24 портам Fast Ethernet, широкий набор

программных средств, обеспечивающих простоту эксплуатации, защиту бизнес-процессов, устойчивость и работу в «сетях без границ». Межсетевой экран Cisco ASA 5505 — современное многофункциональное устройство для защиты локальных сетей от внешних атак и вторжений. Основная функция межсетевого экрана Cisco (файрвол) — защита сети от вторжений, вирусов, спама, шпионских программ, контентная фильтрация трафика пользователей. Построенные на базе аппаратной платформы сетевые

Практическая работа 3: Исследование процессов создания бюджетов пользователей в ОС Windows NT и Unix

Цель работы и содержание: освоить процессы создания бюджетов пользователей в ОС Windows NT и Unix

Теоретическая часть

Организационные требования к системе защиты предусматривают реализацию совокупности административных и процедурных мероприятий. Требования по обеспечению сохранности должны выполняться прежде всего на административном уровне. Организационные мероприятия, проводимые с целью повышения эффективности защиты информации, должны предусматривать следующие процедуры:

- ограничение несопровождаемого доступа к вычислительной системе (регистрация и сопровождение посетителей);
- осуществление контроля за изменением в системе программного обеспечения;
- выполнение тестирования и верификации изменений в системе программного обеспечения и программах защиты;
- организацию и поддержку взаимного контроля за выполнением правил защиты данных;
- ограничение привилегии персонала, обслуживающего ИС;
- осуществление записи протокола о доступе к системе;
- гарантию компетентности обслуживающего персонала;

• разработку последовательного подхода к обеспечению сохранности информации для всей организации;

• организацию четкой работы службы ленточной и дисковой библиотек;

• комплектование основного персонала на базе интегральных оценок и твердых знаний;

• организацию системы обучения и повышения квалификации обслуживающего персонала. С точки зрения обеспечения доступа к ИС необходимо выполнить следующие процедурные мероприятия:

• разработать и утвердить письменные инструкции на загрузку и остановку работы операционной системы;

• контролировать использование магнитных лент, дисков, карт, листингов, порядок изменения программного обеспечения и доведение этих изменений до пользователя;

• разработать процедуру восстановления системы при отказах; • установить политику ограничений при разрешенных визитах в вычислительный центр и определить объем выдаваемой информации;

• разработать систему протоколирования использования ЭВМ, ввода данных и вывода результатов;

• обеспечить периодическую чистки архивов и хранилищ носителей информации для исключения и ликвидации неиспользуемых; • поддерживать

документацию вычислительного центра в соответствии с установленными стандартами. Требования к подсистемам защиты информации (400) В общем случае СЗИ целесообразно условно разделить на подсистемы:

- управления доступом к ресурсам ИС (включает также функции управления системой защиты в целом);
- регистрации и учета действий пользователей (процессов);
- криптографическую;
- обеспечения целостности информационных ресурсов и конфигурации ИС. Для каждой из них определяются требования в виде:
- перечня обеспечиваемых подсистемой функций защиты;
- основных характеристик этих функций;
- перечня средств, реализующих эти функции. Подсистема управления доступом должна обеспечивать:
- идентификацию, аутентификацию и контроль за доступом пользователей (процессов) к системе, терминалам, узлам сети, каналам связи, внешним устройствам, программам, каталогам, файлам, записям и т.д.;
- управление потоками информации;
- очистку освобождаемых областей оперативной памяти и внешних накопителей. Подсистема регистрации и учета выполняет:
- регистрацию и учет: доступа в ИС, выдачи выходных документов, запуска программ и процессов, доступа к защищаемым файлам; передачу данных по линиям
- и каналам связи;
- регистрацию изменения полномочий доступа, создание объектов доступа, подлежащих защите;
- учет носителей информации;
- оповещение о попытках нарушения защиты. Криптографическая подсистема предусматривает:
- шифрование конфиденциальной информации.
- шифрование информации, принадлежащей разным субъектам доступа (группам субъектов), с использованием разных ключей.
- использование аттестованных (сертифицированных) криптографических средств. Подсистема обеспечения целостности осуществляет:
- обеспечение целостности программных средств и обрабатываемой информации,
- физическую охрану средств вычислительной техники и носителей информации,
- наличие администратора (службы) защиты информации в ИС,
- периодическое тестирование СЗИ,
- наличие средств восстановления СЗИ,
- использование сертифицированных средств защиты,
- контроль за целостностью:
- программных средств защиты информации при загрузке операционной среды,
- операционной среды перед выполнением процессов,
- функционального ПО и данных,
- конфигурации ИС,
- оперативное восстановление функций СЗИ после сбоев,
- тестирование средств защиты информации,
- обнаружение и блокирование распространения вирусов,
- резервное копирование программного обеспечения и данных,

- контроль доступа и обеспечение уверенность в том, что только авторизованный пользователь использует имеющиеся рабочие программы и информацию,

• контроль действий с персональной авторизацией, запрещающий операции, которые делают операционную среду уязвимой,

• защиту программного обеспечения, исключающую повреждение инсталлированных программ,

• использование только лицензионного программного продукта с целью обеспечения защиты от встроенных модулей разрушения информационной среды и дискредитации систем защиты;

• защиту коммуникаций для обеспечения недоступности передаваемой информации. Требования к техническому обеспечению В этой группе формулируются требования к таким параметрам:

• месту применения средств защиты;

• способам их использования (например, реализация требований по защищенности должна достигаться без применения экранирования помещений, активные средства могут применяться только для защиты информации главного сервера и т.п.);

• размерам контролируемой зоны безопасности информации;

• требуемой величине показателей защищенности, учитывающей реальную обстановку на объектах ИС;

• применению способов, методов и средств достижения необходимых показателей

• защищенности.

• проведению специсследования оборудования и технических средств, целью которого является измерение показателей ЭМИ;

• проведению спецпроверки технических объектов ИС, целью которой является

• выявление специальных электронных (закладных) устройств. Требования к программному обеспечению Программные средства защиты информации должны обеспечивать контроль доступа, безопасность и целостность данных и защиту самой системы защиты. Для этого необходимо выполнить следующие условия:

• объекты защиты должны идентифицироваться в явном виде при использовании паролей, пропусков и идентификации по голосу;

• система контроля доступа должна быть достаточно гибкой для обеспечения многообразных ограничений и различных наборов объектов;

• каждый доступ к файлу данных или устройству должен прослеживаться через систему контроля доступа для того, чтобы фиксировать и документировать любое обращение. Безопасность данных может обеспечиваться следующей системой мероприятий:

• объекты данных идентифицируются и снабжаются информацией службы безопасности. Целесообразно эту информацию размещать не в отдельном каталоге, а вместе с информацией, имеющей метки;

• кодовые слова защиты размещаются внутри файлов, что в значительной мере повышает эффективность защиты;

• доступ к данным целесообразен с помощью косвенных ссылок, например списка пользователей, допущенных владельцем файла к размещенным в нем данным;

• данные и программы могут преобразовываться (кодироваться) внутренним способом для хранения.

• Система защиты информации должна быть защищена от воздействия окружающей среды. С этой целью выполняется следующая совокупность мероприятий:

• информация по отрицательным запросам не выдается;

• повторные попытки доступа после неудачных обращений должны иметь предел;

• при умолчании конфигурации системы или при ее тестировании функции защиты сохраняются;

• никакие изменения таблиц безопасности, кроме изменения со специального устройства или пульта управления, не разрешаются. Требования по применению способов, методов и средств защиты Рекомендуется применение следующих способов, методов и средств, которые предполагают использование:

• интерфейсов с передачей сигналов в виде последовательного кода и в режиме многократных повторений;

• мультиплексных режимов обработки информации, а также СВТ и системного обеспечения, базирующихся на многоразрядных платформах, интерфейсов с передачей сигналов в виде многоразрядного параллельного кода;

• рациональных способов монтажа, при которых обеспечивается минимальная протяженность электрических связей и коммуникаций;

• технических средств, в состав которых входят устойчивые к самовозбуждению схемы, развязывающие и фильтрующие элементы, комплектующие с низкими уровнями ЭМИ;

• сетевых фильтров для блокирования утечки информации по цепям электропитания, а также линейных (высокочастотных) фильтров для блокирования утечки

• информации по линиям связи;

• технических средств в защищенном исполнении;

• средств пространственного и линейного “зашумления”;

• средств локального либо общего экранирования;

• способов оптимального размещения технических средств с целью минимизации контролируемой зоны безопасности информации. Требования к документированию Можно выделить три группы требований к документированию системы защиты информации. Это протоколирование, тестирование программ и обработка угроз. При разработке системы протоколирования следует учитывать следующие специфические требования:

• необходимость записей всех движений, защищаемых данных;

• возможность воссоздания при необходимости ретроспективы использования защищаемого объекта, для реализации которой обеспечивается запоминание состояний программы и окружающей среды;

• накопление статистики по протоколам использования информации в системе. Существенной особенностью тестирования программ системы защиты информации должно быть наличие специальной программы генерации ложных адресов, несанкционированных попыток доступа к данным, моделирования сбойных ситуаций и других специфических свойств. При тестировании системы защиты информации необходимо также обратить внимание на тщательную проверку таблиц безопасности, системы паролей и программ доступа.

Аппаратура и материалы Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор Intel Pentium-сов– месстимый с тактовой частотой 800 МГц и выше, оперативная память – не менее 512 Мбайт, свободное дисковое пространство – не менее 2 Гбайт, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов от 256) с диагональю не менее 15″. Программное обеспечение – операционная система Windows XP с пакетом обновлений SP2 и выше, ассемблер MASM версии 6.14 и выше, дизассемблер IDA Pro Free версии 4.9 и выше. Указания по технике безопасности Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров, самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металлическими предметами; рабочее место пользователя

персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Практическая работа 4: Исследование методов интеграции сетей Microsoft и Unix с использованием сервера Samba

Цель работы и содержание: освоить методы интегрирования сетей Microsoft и Unix с использованием сервера Samba

Теоретическая часть При избирательном разграничении доступа определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. Большинство ОС реализуют именно избирательное разграничение доступа (discretionary access control).

Полномочное разграничение доступа заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов. Избирательное разграничение доступа Система правил избирательного разграничения доступа формулируется следующим образом.

1. Для любого объекта ОС существует владелец.

2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой тройки субъект—объект—метод возможность доступа определена однозначно.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа. Привилегированный пользователь не может игнорировать разграничение доступа к объектам. Например, в Windows NT администратор для обращения к чужому объекту (принадлежащему другому субъекту) должен сначала объявить себя владельцем этого объекта, использовав привилегию администратора объявлять себя владельцем любого объекта, затем дать себе необходимые права и только после этого может обратиться к объекту. Последнее требование введено для реализации механизма удаления потенциально недоступных объектов. При создании объекта его владельцем назначается субъект, создавший данный объект. В дальнейшем субъект, обладающий необходимыми правами, может назначить объекту нового владельца. При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя. Такое ограничение вводится для того, чтобы владелец объекта не мог отдать «владение» объектом другому

субъекту и тем самым снять с себя ответственность за некорректные действия с объектом. Для определения прав доступа субъектов к объектам при избирательном разграничении доступа используются такие понятия, как матрица доступа и домен безопасности. С концептуальной точки зрения текущее состояние прав доступа при избирательном разграничении доступа описывается матрицей, в строках которой перечислены субъекты доступа, в столбцах — объекты доступа, а в ячейках — операции, которые субъект может выполнить над объектом. Домен безопасности (protection domain) определяет набор объектов и типов операций, которые могут производиться над каждым объектом ОС. Возможность выполнять операции над объектом есть право доступа, каждое из которых есть упорядоченная пара . Таким образом, домен есть набор прав доступа. Например, если домен D имеет право доступа , это означает, что процесс, выполняемый в домене D, может читать или писать в файл F, но не может выполнять других операций над этим объектом Связь конкретных субъектов, функционирующих в ОС, может быть организована следующим образом:

• каждый пользователь может быть доменом. В этом случае набор объектов, к которым может быть организован доступ, зависит от идентификации пользователя;

• каждый процесс может быть доменом. В этом случае набор доступных объектов определяется идентификацией процесса;

• каждая процедура может быть доменом. В этом случае набор доступных объектов соответствует локальным переменным, определенным внутри процедуры. Заметим, что, когда процедура выполнена, происходит смена домена. Модель безопасности, специфицированная выше (см. рис. 8.1), имеет вид матрицы и называется матрицей доступа. Столбцы этой матрицы представляют собой объекты, строки — субъекты. В каждой ячейке матрицы хранится совокупность прав доступа, предоставленных данному субъекту на данный объект. Поскольку реальная матрица доступа очень велика (типичный объем для современной ОС составляет несколько десятков мегабайтов), матрицу доступа никогда не хранят в системе в явном виде. В общем случае эта матрица будет разреженной, т. е. большинство ее клеток будут пустыми. Матрицу доступа можно разложить по столбцам, в результате чего получаются списки прав доступа ACL (access control list). В результате разложения матрицы по строкам получаются мандаты возможностей (capability list, или capability tickets). Список прав доступа ACL. Каждая колонка в матрице может быть реализована как список доступа для одного объекта. Очевидно, что пустые клетки могут не учитываться. В результате для каждого объекта имеем список упорядоченных пар , который определяет все домены с непустыми наборами прав для данного объекта. Элементами

списка прав доступа ACL могут быть процессы, пользователи или группы пользователей. При реализации широко применяется предоставление доступа по умолчанию для пользователей, права которых не ука- заны. Например, в ОС Unix все субъекты-пользователи разделены на три группы (владелец, группа и остальные), и для членов каждой группы контролируются операции чтения, записи и исполнения (rwx). В итоге имеем ACL — 9-битный код, который является атрибутом разнообразных объектов Unix. Мандаты возможностей. Как отмечалось выше, если матрицу доступа хранить по строкам, т. е. если каждый субъект хранит список объектов и для каждого объекта — список допустимых операций, то такой способ хранения называется «мандаты возможностей» или «перечни возможностей» (capability list). Каждый пользователь обладает несколькими мандатами и может иметь право передавать их другим. Мандаты могут быть рассеяны по системе и вследствие этого представлять большую угрозу для безопасности, чем списки контроля доступа. Их хранение должно быть тщательно продумано. Избирательное разграничение доступа — наиболее распространенный способ разграничения доступа. Это обусловлено сравнительной простотой его реализации и необременительностью правил такого разграничения доступа для пользователей. Главное достоинство избирательного разграничения доступа — гибкость; основные недостатки — рассредоточенность управления и сложность централизованного контроля. Вместе с тем, защищенность ОС, подсистема защиты которой реализует только избирательное разграничение доступа, в некоторых случаях может оказаться недостаточной. В частности, в США запрещено хранить информацию, содержащую государственную тайну, в компьютерных системах, поддерживающих только избирательное разграничение доступа. Расширением модели избирательного разграничения доступа является изолированная (или замкнутая) программная среда. При использовании изолированной программной среды права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту. Можно, например, разрешить обращаться к файлам с расширением .doc только программам Word, Word Viewer и WPview. Изолированная программная среда существенно повышает защищенность операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы. Кроме того, при использовании данной модели повышается защищенность целостности данных, хранящихся в системе. Полномочное разграничение доступа с контролем информационных потоков Полномочное, или мандатное, разграничение доступа (mandatory access control) обычно применяется в

совокупности с избирательным разграничением доступа. Рассмотрим именно такой случай. Правила разграничения доступа в данной модели формулируются следующим образом.

1. Для любого объекта ОС существует владелец.

2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

3. Для каждой четверки субъект—объект—метод—процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Вместе с тем, в каждый момент времени возможность доступа определена однозначно. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.

4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.

5. В множестве объектов выделяется множество объектов полномочного разграничения доступа. Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен. Если объект не является объектом полномочного разграничения доступа или если объект несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа.

6. Каждый субъект доступа имеет уровень допуска. Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.

7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если: • объект является объектом полномочного разграничения доступа;

• гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему;

• субъект открывает объект в режиме, допускающем чтение информации. Это правило называют правилом NRU (Not Read Up — не читать выше).

8. Каждый процесс ОС имеет уровень конфиденциальности, равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования.

Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.

9. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

• объект является объектом полномочного разграничения доступа;

• гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему;

• субъект собирается записывать в объект информацию, Это правило предотвращает утечку секретной информации; его называют правилом NWD (Not Write Down — не записывать ниже).

10. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:

• имеет доступ к объекту согласно правилу 7;

• обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

Аппаратура и материалы Для выполнения лабораторной работы необходим персональный компьютер со следующими характеристиками: процессор Intel Pentium-сов–месстимый с тактовой частотой 800 МГц и выше, оперативная память – не менее 512 Мбайт, свободное дисковое пространство – не менее 2 Гбайт, устройство для чтения компакт-дисков, монитор типа Super VGA (число цветов от 256) с диагональю не менее 15″. Программное обеспечение – операционная система Windows XP с пакетом обновлений SP2 и выше, ассемблер MASM версии 6.14 и выше, дизассемблер IDA Pro Free версии 4.9 и выше. Указания по технике безопасности Техника безопасности при выполнении лабораторной работы совпадает с общепринятой для пользователей персональных компьютеров, самостоятельно не производить ремонт персонального компьютера, установку и удаление программного обеспечения; в случае неисправности персонального компьютера сообщить об этом обслуживающему персоналу лаборатории (оператору, администратору); соблюдать правила техники безопасности при работе с электрооборудованием; не касаться электрических розеток металлическими предметами; рабочее место пользователя персонального компьютера должно содержаться в чистоте; не разрешается возле персонального компьютера принимать пищу, напитки.

Практическая работа 5: Изучение базовых команд ОС Linux

Цель: Первичное знакомство с командным интерпретатором. Изучение базовых команд операционной системы Linux.

Теоретическая часть:

Среди всех элементов операционной системы Linux самым важным, является командная строка (Терминал). Оболочка во многом определяет богатые возможности и гибкость операционной системы Linux. С помощью командной строки можно выполнять действия, которые были бы немыслимы при работе с графическим пользовательским интерфейсом. Независимо от того, KDE или GNOME, оказывается, что многие действия гораздо быстрее и эффективнее выполнить, пользуясь только командной строкой. Освоение Linux стоит начинать с изучения средств командной оболочки.

Файлы и ничего кроме файлов

Все, с чем Вы встретитесь в операционной системе Linux, - это файлы. Абсолютно все! Очевидно, что текстовый документ - это файл. Изображения, аудиоданные в формате MP3 и видеофрагменты - это несомненно файлы. Каталоги - это тоже файлы, содержащие информацию о других файлах. Дисковые устройства - это большие файлы. Сетевые соединения тоже файлы. Даже исполняемый процесс - это файл. С точки зрения операционной системы Linux файл представляет собой поток битов или байтов. Система не интересуется тем, что означает каждый байт. Это забота конкретных программ, выполняющихся в операционной системе Linux. Для операционной системы Linux и документ, и сетевое соединение всего лишь файлы. Как обрабатывать текстовый документ, знает редактор, а сетевое приложение умеет работать с сетевым соединением.

В отличие от Windows и MacOS в операционной системе Linux имена файлов чувствительны к регистру символов. В частности, Вы можете встретить в одном каталоге все три файла которые приведены ниже в качестве примера:

Sit.txt
sIt.txt
SIT.txt

С точки зрения файловой операционной системы Linux - это различные имена файлов. Если вы попытаетесь создать файлы с этими же именами в Windows или MacOS, то вероятнее всего попытка увенчается провалом, и система предложит Вам выбрать другое имя для файла.

Чувствительность к регистру символов также означает, что при вводе команд они должны в точности совпадать с именами файлов, поддерживающих их. Так, например, удаляя файл с помощью команды rm, нельзя вводить RM, Rm или rM. Надо также следить за написанием имен, задаваемых в качестве параметров. Если вы захотите удалить файл «SIT.txt», а укажете имя Sit.txt, вы лишитесь совсем не того файла, с которым предполагали расстаться.

Предупреждение

Список специальных символов которые не рекомендуется использовать в названиях файлов.

```
/   - Нельзя использовать ни при каких обстоятельствах
\   - Должен быть предварен таким же символом. Применять не рекомендуется
-   - Нельзя использовать в начале имени файла или каталога
[]  - Каждый из этих символов должен быть предварен обратной косой чертой. Применять не рекомендуется
{}  - Каждый из этих символов должен быть предварен обратной косой чертой. Применять не рекомендуется
*   - Должен быть предварен обратной косой чертой. Применять не рекомендуется
?   - Должен быть предварен обратной косой чертой. Применять не рекомендуется
'   - Должен быть предварен обратной косой чертой. Применять не рекомендуется
"   - Должен быть предварен обратной косой чертой. Применять не рекомендуется
```

Групповые операции:

Предположим, что в одном из каталогов на вашем компьютере содержатся сто файлов с изображениями и два текстовых файла. Ваша задача удалить все файлы с изображениями за исключением двух текстовых файлов. Удалять файлы по одному - это утомительное занятие. В операционных системах Linux для автоматизации данного процесса можно применять символы групповых операций. Групповые операции задаются посредством звездочки (*), знака вопроса (?) и квадратных скобок ([ ]).

Пример использования групповых операций:

Групповая операция с применение » * » - отмечает любое (в том числе нулевое) количество любых символов.

```
rm sit1*.*      Удаляться файлы : sit1.txt, sit1.jpg, sit11.jpg, sit123123.txt
rm sit*.jpg     Удаляться файлы : sit1.jpg, sit11.jpg
rm *txt         Удаляться файлы : sit1.txt, sit123123.txt
rm sit*         Удаляться файлы : sit1.txt, sit1.jpg, sit11.jpg, sit123123.txt
rm *            Удалятся все файлы в каталоге
```

Групповая операция с применение » ? «. Символ » ? » - соответствует одному произвольному символу.

```
rm sit1?.jpg    Удалится файл : sit11.jpg, но не sit1.txt, sit1.jpg, sit123123.txt
rm sit?.jpg             Удалится файл : sit1.jpg, но не sit1.txt, sit11.jpg, sit123123.txt
rm sit?.*               Удаляться файлы : sit1.txt, sit1.jpg, но не sit11.jpg, sit123123.txt
```

Групповая операция с применением » [] «. Квадратные скобки позволяют задавать один символ из числа заключенных в скобки, принадлежащий определенному диапазону.

```
rm sit[0-1].txt        Удалится файл :  sit1.txt, но не sit1.jpg, sit11.jpg, sit123123.txt
rm sit1[0-2].jpg       Удалится файл :  sit11.jpg, но не sit1.txt, sit1.jpg, sit123123.txt
```

Практическая работа 6 Настройка ОС Linux

Введение

ОС Linux - это многопользовательская, многозадачная, многотерминальная операционная система (ОС) из семейства UNIX, под управлением которой могут одновременно выполняться несколько задач. Она предназначена для работы на серверах и рабочих станциях, обеспечивает подключение дополнительных терминалов и допускает этом режиме использование графических оболочек.

UNIX-серверы предназначены для хранения и обработки больших объемов информации. Особенно эффективно использование UNIX-серверов при распределенной обработке данных. Для этого разработаны системы распределенных вычислений в соответствии со стандартом CORBA. К таким системам относятся системы управления базами данных (СУБД типа Oracle, Informix), файл-серверы, FTP-серверы, WWW-серверы и др., которые поддерживаются ОС Linux. В распределенных системах информация может находиться на различных рабочих станциях, различных дисках, программные модули могут функционировать на различных компьютерах, но система работает таким образом, что это составляет единое целое. При обработке больших объемов информации используется технология клиент - сервер, при которой пользователь работает только с той информацией, которая ему необходима. Развитием технологии клиент - сервер является технология интеллектуальных агентов.

ОС Linux является сетевой операционной системой для 32-х или 64-х разрядных платформ. Она обеспечивает маштабируемость в диапазоне от игровыхприставок (Sony Play Station) до кластерных серверов Internet. ОС Linux не связана с конкретной моделью компьютеров. Её ядро реализовано на языке высокого уровня (языке СИ), что позволяет достаточно легко переносить эту систему с одной платформы на другую. Системараспространяется по лицензии GNU либо подобным свободным лицензиям, обеспечивается как коммерческое, так и свободное сопровождение через Internet.Поставка исходных модулей системы обеспечивает возможность адаптации прикладных программ в случае перехода на другую платформу и дает возможность контроля кодов, реализующих несанкционированный доступ. В разработке системы приняло участие большое количество специалистов, зарегистрировавших свои авторские права, что дает гарантии ее немонополизации.

Подключение персональных компьютеров (ПК) в вычислительную сеть с UNIX - серверами может осуществляться по протоколу TCP/IP, при этом пользователи получают следующие возможности:

1) использование UNIX-сервера, как файл - сервера;
2) эмуляция на ПК удаленного терминала (режим TELNET);
3) организация системы клиент - сервер (рабочая станция формирует SQL - запросы, сервер их обрабатывает);
4) непосредственный обмен файлами между ПК по протоколу FTP;
5) организация распределенных вычислений по стандарту CORBA.

Все действия в ОС UNIX оформлены как процессы. Процесс представляет собой совокупность выполнения программ или одну выполняемую программу, которые вызываются при исполнении системной команды. Процесс может породить один или

несколько других процессов, которые могут выполняться параллельно. ОС Linux поддерживает многопроцессорную архитектуру для параллельного выполнения процессов.

Теоретическая часть

Система включает следующие основные компоненты.

Ядро. Выполняет функции управления памятью, процессорами.
Осуществляет диспетчеризацию выполнения всех программ и обслуживание внешних устройств. Все действия, связанные с вводом/выводом и выполнениемсистемных операций, выполняются с помощью системных вызовов. Системныевызовы реализуют программный интерфейс между программами и ядром.
Имеется возможность динамического конфигурирования ядра.

Диспетчер процессов Init. Активизирует процессы, необходимые длянормальной работы системы и производит их начальную инициализацию.
Обеспечивает завершение работы системы, организует сеансы работыпользователей, в том числе, для удаленных терминалов.

Интерпретатор команд Shell. Анализирует команды, вводимые с терминала либо из командного файла, и передает их для выполнения в ядро системы. Команды обычно имеют аргументы и параметры, которые обеспечивают модернизацию выполняемых действий. Shell является также языком программирования, на котором можно создавать командные файлы (shell-файлы). При входе в ОС пользователь получает копию интерпретатора shell в качестве родительского процесса. Далее, после ввода команды пользователем создается порожденный процесс, называемый процессом-потомком. Т.е. после запуска ОС каждый новый процесс функционирует только как процесс - потомок уже существующего процесса. В ОС Linux имеется возможность динамического порождения и управления процессами.

Shell - интерпретатор в соответствии с требованиями стандарта POSIX поддерживает графический экранный интерфейс, реализованный средствами языка программирования Tcl/Tk.
Обязательным в системе является интерпретатор Bash, полностью соответствующий стандарту POSIX. В качестве Shell может быть использованаоболочка **mc** с интерфейсом, подобным Norton Commander.

Сетевой графический интерфейс X-сервер (X-Windows). Обеспечиваетподдержку графических оболочек.

Графические оболочки KDE, Gnome. Отличительными свойствами KDE являются: минимальные требования к аппаратуре, высокая надежность, интернационализация. Базовые библиотеки KDE (qt, kde-libs) признаны одними из

лучших продуктов по созданию графического интерфейса, обеспечивают простое написание программ с использованием передовых технологий. Gnome имеет развитые графические возможности, но более требователен к аппаратным средствам.

Сетевая поддержка NFS, SMB, TCP/IP. NFS - программный комплекс PC-NFS (Network File System) для выполнения сетевых функций. PC-NFS ориентирован для конкретной ОС персонального компьютера (PC) и включает драйверы для работы в сети и дополнительные утилиты. SMB - сетевая файловая система, совместимая с Windows NT. TCP/IP - протокол контроля передачи данных (Transfer Control Protocol/Internet Protocol). Сеть по протоколам TCP/IP является неотъемлемой частью ОС семейства UNIX. Поддерживаются любые сети, от локальных до Internet, с использованием только встроенных сетевых средств.

Инструментальные средства программирования. Основой средств программирования является компилятор GCC или его экспериментальные версииEGCS и PGCC для языков C и C++; модули поддержки других языков программирования (Obective

С, Фортран, Паскаль, Modula-3, Ада, Java и др.); интегрированные среды и средства визуального проектирования: Kdevelop, Xwpe;средства адаптации привязки программ.

Регистрация пользователя в системе

Для входа пользователя с терминала в многопользовательскую операционную систему LINUX необходимо зарегистрироваться в качествепользователя. Для этого нужно после сообщения

Login:

ввести системное имя пользователя, например, "student". Если имя задано верно,выводится запрос на ввод пароля:

Password:

Наберите пароль "student" и нажмите клавишу *Enter*.

Если имя или пароль указаны неверно, сообщение *login* повторяется. Значение пароля проверяется в системном файле *password*, где приводятся и другие сведения о пользователях. После правильного ответа появляется приветствие LINUX и приглашение:
student@linux:>

Вы получили доступ к ресурсам ОС LINUX.

Выход из системы

exit - окончание сеанса пользователя.

Выполнение простых команд

Формат команд в ОС LINUX следующий:

имя команды [аргументы] [параметры] [метасимволы]

Имя команды может содержать любое допустимое имя файла; аргументы - одна или несколько букв со знаком минус (-); параметры - передаваемые значениядля обработки; метасимволы интерпретируются как специальные операции. В квадратных скобках указываются необязательные части команд.

Введите команду **echo**, которая выдает на экран свои аргументы:

echo good morning

и нажмите клавишу *Enter*. На экране появится приветствие "*good morning*" – аргумент команды **echo.** Командный интерпретатор *shell* вызвал команду **echo**, реализованную в виде программы на языке СИ, и передал ей аргументы. После этого интерпретатор команд вывел знак-приглашение. Синтаксис команды **echo**:

echo [-n] [arg1] [arg2] [arg3]...

Команда помещает в стандартный вывод свои аргументы, разделенные пробелами и завершаемые символом перевода строки. При наличии флага *-n* символ перевода строки исключается.

who [am i] - получение информации о работающих пользователях.

В квадратных скобках указываются аргументы команды, которые можно опустить. Ответ представляется в виде таблицы, которая содержит следующуюинформацию:

- идентификатор пользователя;
- идентификатор терминала;
- дата подключения;
- время подключения.

cal [[месяц]год] - календарь; если календарь не помещается на одном экране, то используется команда **cal год | more** и клавишей пробела производитсяпостраничный вывод информации.

man <название команды> - вызов электронного справочника об указанной команде. Выход из справочника - нажатие клавиши Q.

Команда **man man** составит информацию о том, как пользоваться справочником.

>имя файла - перенаправление стандартного вывода, соответствующего терминалу пользователя.

cat <имя файла> - вывод содержимого файла на экран. Команда **cat > text.1** создает новый файл с именем text.1, который можно заполнить символьными строками, вводя их с клавиатуры. Нажатие клавиши *Enter* создаетновую строку. Завершение ввода - нажатие *Ctrl - d*. Команда **cat text.1 >**
text.2 пересылает содержимое файла text.1 в файл text.2. Слияние файловосуществляется командой **cat text.1 text.2 > text.3**.
ls [-alrstu] [имя] - вывод содержимого каталога на экран. Если аргумент неуказан, выдается содержимое текущего каталога.
Аргументы команды:
-a - выводит список всех файлов и каталогов, в том числе и скрытых;
-l - выводит список файлов в расширенном формате, показывая тип каждогоэлемента, полномочия, владельца, размер и дату последней модификации;

- r - выводит список в порядке, обратном заданному;
- s - выводит размеры каждого файла;
- t - перечисляет файлы и каталоги в соответствии с датой их последнеймодификации;
- u - перечисляет файлы и каталоги в порядке, обратном их последнеймодификации.

rm <имя файла> - удаление файла (файлов). Команда **rm text.1 text.2 text.3** удаляет файлы text.1, text.2, text.3. Другие варианты этой команды - **rm text.**
[123] или rm text.[1-3].
wc [имя файла] - вывод числа строк, слов и символов в файле

Порядок выполнения работы

1. Ознакомиться с теоретической частью к лабораторной работе.
2. Зарегистрироваться в системе LINUX.
3. Определить день недели, в который Вы родились.
4. Получить подробную информацию обо всех активных процессах.
5. Используя редактор VI (см. приложение), создать два текстовых файла (срасширением TXT) и командой CAT просмотреть их на экране.
6. Получить информацию о работающих пользователях, подсчитать ихколичество и запомнить в файле.
7. Объединить текстовые файлы в единый файл и посмотреть его на экране.
8. Посмотреть приоритет своего процесса и уменьшить скорость еговыполнение за счет повышения номера приоритета.
9. Используя редактор VI, написать программу на языке СИ и запустить еена трансляцию в фоновом режиме.
10. Показать преподавателю исходный текст программы на языке СИ,текстовый файл, файл с сохранением количества пользователей.
11. Продемонстрировать выполнение СИ - программы.
12. Удалить свои файлы и выйти из системы.

Контрольные вопросы

1. Перечислите основные функции и назначение многопользовательской многозадачной операционной системы LINUX и ее отличительные особенностиот однопрограммной системы DOS.
2. Какое назначение имеет ядро системы и интерпретатор команд?
3. В чем заключается понятие "процесс" и какие операции можно выполнить над процессами?
4. Как задаются и выполняются простые и сложные команды?

5. Какие функции выполняет командный интерпретатор *Shell*?

Практическая работа 7. Работа с файлами в Linux

ОС Linux - это многопользовательская, многозадачная, многотерминальная операционная система (ОС) из семейства UNIX, под управлением которой могут одновременно выполняться несколько задач. Она предназначена для работы на серверах и рабочих станциях, обеспечивает подключение дополнительных терминалов и допускает этом режиме использование графических оболочек.

UNIX-серверы предназначены для хранения и обработки больших объемов информации. Особенно эффективно использование UNIX-серверов при распределенной обработке данных. Для этого разработаны системы распределенных вычислений в соответствии со стандартом CORBA. К таким системам относятся системы управления базами данных (СУБД типа Oracle, Informix), файл-серверы, FTP-серверы, WWW-серверы и др., которые поддерживаются ОС Linux. В распределенных системах информация может находиться на различных рабочих станциях, различных дисках, программные модули могут функционировать на различных компьютерах, но система работает таким образом, что это составляет единое целое. При обработке больших объемов информации используется технология клиент - сервер, при которой пользователь работает только с той информацией, которая ему необходима. Развитием технологии клиент - сервер является технология интеллектуальных агентов.

ОС Linux является сетевой операционной системой для 32-х или 64-х разрядных платформ. Она обеспечивает маштабируемость в диапазоне от игровыхприставок (Sony Play Station) до кластерных серверов Internet. ОС Linux не связана с конкретной моделью компьютеров. Её ядро реализовано на языке высокого уровня (языке СИ), что позволяет достаточно легко переносить эту систему с одной платформы на другую. Системараспространяется по лицензии GNU либо подобным свободным лицензиям, обеспечивается как коммерческое, так и свободное сопровождение через Internet.Поставка исходных модулей системы обеспечивает возможность адаптации прикладных программ в случае перехода на другую платформу и дает возможность контроля кодов, реализующих несанкционированный доступ. В разработке системы приняло участие большое количество специалистов, зарегистрировавших свои авторские права, что дает гарантии ее немонополизации.

Подключение персональных компьютеров (ПК) в вычислительную сеть с UNIX - серверами может осуществляться по протоколу TCP/IP, при этом пользователи получают следующие возможности:

6) использование UNIX-сервера, как файл - сервера;
7) эмуляция на ПК удаленного терминала (режим TELNET);
8) организация системы клиент - сервер (рабочая станция формирует SQL - запросы, сервер их обрабатывает);
9) непосредственный обмен файлами между ПК по протоколу FTP;
10) организация распределенных вычислений по стандарту CORBA.

Все действия в ОС UNIX оформлены как процессы. Процесс представляетсобой совокупность выполняемых программ или одну выполняемую программу,которые вызываются при исполнении системной команды. Процесс может породить один или несколько других процессов, которые могут выполняться параллельно. ОС Linux поддерживает многопроцессорную архитектуру для параллельного выполнения процессов.

Система включает следующие основные компоненты.

Ядро. Выполняет функции управления памятью, процессорами.
Осуществляет диспетчеризацию выполнения всех программ и обслуживание внешних устройств. Все действия, связанные с вводом/выводом и выполнениемсистемных операций, выполняются с помощью системных вызовов. Системныевызовы реализуют программный интерфейс между программами и ядром.
Имеется возможность динамического конфигурирования ядра.

Диспетчер процессов Init. Активизирует процессы, необходимые длянормальной работы системы и производит их начальную инициализацию.
Обеспечивает завершение работы системы, организует сеансы работыпользователей, в том числе, для удаленных терминалов.

Интерпретатор команд Shell. Анализирует команды, вводимые с терминала либо из командного файла, и передает их для выполнения в ядро системы. Команды обычно имеют аргументы и параметры, которые обеспечивают модернизацию выполняемых действий. Shell является также языком программирования, на котором можно создавать командные файлы (shell-файлы). При входе в ОС пользователь получает копию интерпретатора shell в качестве родительского процесса. Далее, после ввода команды пользователем создается порожденный процесс, называемый процессом-потомком. Т.е. после запуска ОС каждый новый процесс функционирует только как процесс - потомок уже существующего процесса. В ОС Linux имеется возможность динамического порождения и управления процессами.
Shell - интерпретатор в соответствии с требованиями стандарта POSIXподдерживает графический экранный интерфейс, реализованный средствами языка программирования Tcl/Tk.
Обязательным в системе является интерпретатор Bash, полностью соответствующий стандарту POSIX. В качестве Shell может быть использованаоболочка **mc** с интерфейсом, подобным Norton Commander.

Сетевой графический интерфейс X-сервер (X-Windows). Обеспечиваетподдержку графических оболочек.

Графические оболочки KDE, Gnome. Отличительными свойствами KDE являются: минимальные требования к аппаратуре, высокая надежность, интернационализация. Базовые библиотеки KDE (qt, kde-libs) признаны одними из

лучших продуктов по созданию графического интерфейса, обеспечивают простое написание программ с использованием передовых технологий. Gnome имеет развитые графические возможности, но более требователен к аппаратным средствам.

Сетевая поддержка NFS, SMB, TCP/IP. NFS - программный комплекс PC-NFS (Network File System) для выполнения сетевых функций. PC-NFS ориентирован для конкретной ОС персонального компьютера (PC) и включает драйверы для работы в сети и дополнительные утилиты. SMB - сетевая файловая система, совместимая с Windows NT. TCP/IP - протокол контроля передачи данных (Transfer Control Protocol/Internet Protocol). Сеть по протоколам TCP/IP является неотъемлемой частью ОС семейства UNIX. Поддерживаются любые сети, от локальных до Internet, с использованием только встроенных сетевых средств.

Инструментальные средства программирования. Основой средств программирования является компилятор GCC или его экспериментальные версииEGCS и PGCC для языков C и C++; модули поддержки других языков программирования (Obective C, Фортран, Паскаль, Modula-3, Ада, Java и др.); интегрированные среды и средства визуального проектирования: Kdevelop, Xwpe;средства адаптации привязки программ.

Регистрация пользователя в системе

Для входа пользователя с терминала в многопользовательскую операционную систему LINUX необходимо зарегистрироваться в качествепользователя. Для этого нужно после

сообщения
Login:
ввести системное имя пользователя, например, "student". Если имя задано верно,выводится запрос на ввод пароля:
Password:
Наберите пароль "student" и нажмите клавишу *Enter*.
Если имя или пароль указаны неверно, сообщение *login* повторяется. Значение пароля проверяется в системном файле *password*, где приводятся и другие сведения о пользователях. После правильного ответа появляется приветствие LINUX и приглашение:
student@linux:>

Вы получили доступ к ресурсам ОС LINUX.

Выход из системы

exit - окончание сеанса пользователя.

Выполнение простых команд

Формат команд в ОС LINUX следующий:

имя команды [аргументы] [параметры] [метасимволы]

Имя команды может содержать любое допустимое имя файла; аргументы - одна или несколько букв со знаком минус (-); параметры - передаваемые значениядля обработки; метасимволы интерпретируются как специальные операции. В квадратных скобках указываются необязательные части команд.

Введите команду **echo**, которая выдает на экран свои аргументы:

echo good morning

и нажмите клавишу *Enter*. На экране появится приветствие "*good morning*" – аргумент команды **echo.** Командный интерпретатор *shell* вызвал команду **echo**, реализованную в виде программы на языке СИ, и передал ей аргументы. После этого интерпретатор команд вывел знак-приглашение. Синтаксис команды **echo**:

echo [-n] [arg1] [arg2] [arg3]...

Команда помещает в стандартный вывод свои аргументы, разделенные пробелами и завершаемые символом перевода строки. При наличии флага *-n* символ перевода строки исключается.

who [am i] - получение информации о работающих пользователях.

В квадратных скобках указываются аргументы команды, которые можно опустить. Ответ представляется в виде таблицы, которая содержит следующуюинформацию:

- идентификатор пользователя;
- идентификатор терминала;
- дата подключения;
- время подключения.

cal [[месяц]год] - календарь; если календарь не помещается на одном экране, то используется команда **cal год | more** и клавишей пробела производитсяпостраничный вывод информации.

man <название команды> - вызов электронного справочника об указанной команде. Выход из справочника - нажатие клавиши Q.

Команда **man man** сообщает информацию о том, как пользоваться справочником.

tty - сообщение имени специального файла стандартного вывода, соответствующего терминалу пользователя.

cat <имя файла> - вывод содержимого файла на экран. Команда **cat > text.1** создает новый файл с именем text.1, который можно заполнить символьными строками, вводя их с клавиатуры. Новая строка создается нажатием *Ctrl* + *a*. Команда **cat text.1 >**

text.2 пересылает содержимое файла text.1 в файл text.2. Слияние файловосуществляется командой **cat text.1 text.2 > text.3**.

ls [-alrstu] [имя] - вывод содержимого каталога на экран. Если аргумент неуказан, выдается содержимое текущего каталога.

Аргументы команды:

-a - выводит список всех файлов и каталогов, в том числе и скрытых;

-l - выводит список файлов в расширенном формате, показывая тип каждогоэлемента, полномочия, владельца, размер и дату последней модификации;

- r - выводит список в порядке, обратном заданному;
- s - выводит размеры каждого файла;
- t - перечисляет файлы и каталоги в соответствии с датой их последнеймодификации;
- u - перечисляет файлы и каталоги в порядке, обратном их последнеймодификации.

rm <имя файла> - удаление файла (файлов). Команда **rm text.1 text.2 text.3** удаляет файлы text.1, text.2, text.3. Другие варианты этой команды - **rm text.**
[123] или rm text.[1-3].

wc [имя файла] - вывод числа строк, слов и символов в файле

Порядок выполнения работы

13. Ознакомиться с теоретической частью к лабораторной работе.
14. Зарегистрироваться в системе LINUX.
15. Определить день недели, в который Вы родились.
16. Получить подробную информацию обо всех активных процессах.
17. Используя редактор VI (см. приложение), создать два текстовых файла (срасширением TXT) и командой CAT просмотреть их на экране.
18. Получить информацию о работающих пользователях, подсчитать ихколичество и запомнить в файле.
19. Объединить текстовые файлы в единый файл и посмотреть его на экране.
20. Посмотреть приоритет своего процесса и уменьшить скорость еговыполнение за счет повышения номера приоритета.
21. Используя редактор VI, написать программу на языке СИ и запустить еена трансляцию в фоновом режиме.
22. Показать преподавателю исходный текст программы на языке СИ,текстовый файл, файл с сохранением количества пользователей.
23. Продемонстрировать выполнение СИ - программы.
24. Удалить свои файлы и выйти из системы.

Практическая работа 8 Работа с файлами в Linux

Операционная система UNIX представляет собой ядро многопользовательской операционной системы с разделением времени. Она дает пользователям возможность запускать свои программы, управляет периферийными устройствами и обеспечивает работу файловой системы.

Работу операционной системы UNIX можно представить в виде функционирования множества взаимосвязанных процессов. При загрузке системы сначала запускается ядро (процесс 0), которое в свою очередь запускаеткомандный интерпретатор shell (процесс 1). Взаимодействие пользователя с системой UNIX происходит в интерактивном режиме посредством командного языка. Оболочка операционной системы shell интерпретирует вводимые команды, запускает соответствующие программы (процессы), формирует и выводит ответные сообщения.

Важной составной частью UNIX является файловая система, которая является сложной многопользовательской системой, так как в основе этой системы лежала операционная система MULTICS. Файловая система имеет иерархическую структуру, образующую дерево каталогов и файлов. Дерево начинается в корневом каталоге, с добавлением связей, формирующих направленный ациклический граф. Имена файлов могут содержать до 14 символов, включающихв себя любые символы ASCII, кроме косой черты (использовавшейся в качестве разделителя компонентов пути) и символа NUL (использовавшегося для дополнения имен короче 14 символов). Символ NUL обозначается байтом 0.

Рис. 5. Пример *i-mого* узла

Корневой каталог обозначается символом «/», путь по дереву каталогов состоит из имен каталогов, разделенных символом «/», например: /usrlinclude/sys. В каждый момент времени с любым процессом связан некоторый текущий каталог, то есть местоположение пользователя в иерархической файловой системе. Каталог UNIX содержит по одной записи для каждого

файла этого каталога. Каждая каталоговая запись проста, так как в системе UNIX используется схема i-узлов (рис.5.). Каталоговая запись состоит всего из двух полей: имени файла (14 байт) и номера i-узла для этого файла (рис.6.).

Каждый файл операционной системы UNIX может быть однозначно определен некоторой структурой данных, называемой описателем файла (дескриптором). Он содержит всю информацию о файле: тип файла, режим доступа, идентификатор владельца, размер, адрес файла, даты последнего доступаи последней модификации, дату создания и пр.

Обращение к файлу происходит по имени. Путь к файлу от корневого каталога называется полным именем файла. Если обращение к файлу начинается с символа

«/», то считается, что указано полное имя файла и его поиск начинается с корневого каталога, в любом другом случае поиск файла начинается с текущего каталога. У любого файла может быть несколько имен. Фактически имя файла является ссылкой на файл, специфицированный номером описателя.

Номер i-узла	Имя файла

Рис.6. Каталоговая запись файловой системы *UNUX V7*

I-узлы системы UNIX (рис.7.) содержат атрибуты: размер файла, три указателявремени (создания, последнего доступа и последнего изменения), идентификатор владельца, номер группы, информацию о защите и счетчик каталоговых записей, указывающих на данный i-узел. При добавлении новой связи к i-узлу счетчик в i- узле увеличивается на единицу. При удалении связи счетчик в i-узле уменьшаетсяна единицу. Когда значение счетчика достигает нуля, i-узел освобождается, а блоки диска, которые занимал файл, возвращаются в список свободных блокДля учета дисковых блоков файла используется обобщение схемы, позволяющее работать с очень большими файлами. Первые 10 дисковых адресов хранятся в самом i-узле. Для небольших файлов необходимая информация содержится прямо в i-узле, считываемом с диска при открытии файла. Для файловбольшего размера один из адресов в i-узле представляет собой адрес блока диска, называемого одинарным косвенным блоком. Этот блок содержит дополнительные дисковые адреса. Если и этого недостаточно используется другой адрес в i-узле, называемый двойным косвенным блоком и содержащий адрес блока, в котором хранятся адреса однократных косвенных блоков. Если и этого мало, используется тройной косвенный блок.

При открытии файла файловая система по имени файла находит его блоки на диске. Вначале файловая система открывает корневой каталог, i-узел которого располагается в фиксированном месте диска. По этому i-узлу система определяет положение корневого каталога, который может находиться в любом месте диска, например, в блоке 1. Затем файловая система считывает корневой каталог и ищетв нем первый компонент пути, чтобы определить номер i-узла файла. По этому i- узлу файловая система находит следующий каталог и находит в нем следующий компонент и т.д. Относительные пути файлов обрабатываются так же как и абсолютные, с той разницей, что алгоритм начинает работу не с корневого, а с рабочего каталога.

Работа пользователя в системе начинается с того, что активизируется сервер терминального доступа getty (программа, организующая диалог работы с пользователем в многопользовательской операционной системе), который запускает программу login, запрашивающую у пользователя имя и пароль.

Далее происходит проверка аутентичности пользователя (подлинности регистрации пользователя в системе) в соответствии с той информацией, которая хранится в файле /etc/passwd. В этом файле хранятся записи, содержащие:

- зашифрованный пароль;
- идентификатор пользователя;
- идентификатор группы;
- информация о минимальном сроке действия пароля;
- общая информация о пользователе;
- начальный каталог пользователя;
- регистрационный shell пользователя.

Если пользователь зарегистрирован в системе и ввел правильный пароль, loginзапускает программу, указанную в /etc/passwd – регистрационный shell пользователя.

Пользователь системы – это объект, обладающий определенными правами, определяющими возможность запуска программ на выполнение, а также владениефайлами. Единственный пользователь системы, обладающий неограниченными правами – это суперпользователь или администратор системы.

Система идентифицирует пользователей по идентификатору пользователя (UID – User Identifier). Каждый пользователь является членом одной или нескольких групп – списка пользователей, имеющих сходные задачи. Каждая группа имеет свой уникальный идентификатор группы (GID – Group Identifier) Принадлежность группе определяет совокупность прав, которыми обладают члены данной группы.

Права пользователя UNIX – это права на работу с файлами. Файлы имеют двух владельцев: пользователя (user owner) и группу (group owner). Соответственно, атрибуты защиты файлов определяют права пользователя- владельца файла, права члена группы-владельца (g) и права всех остальных (o). В каждый момент времени с любым пользователем связан текущий каталог, то есть местоположение пользователя в иерархической файловой системе.

Всякий файл операционной системы UNIX в соответствии с его типом может быть отнесен к одной из следующих групп: обычные файлы, каталоги, специальные файлы и каналы.

Обычный файл представляет собой последовательность байтов. Никаких ограничений на файл системой не накладывается, и никакого смысла не приписывается его содержимому: смысл байтов зависит исключительно от программ, обрабатывающих файл.

Каталог – это файл особого типа, отличающийся от обычного файла наличием структуры и ограничением по записи: осуществить запись в каталог может толькоядро операционной системы UNIX. Каталог устанавливает соответствие между файлами (номерами описателей) и их локальными именами.

Специальный файл – это файл, поставленный в соответствие некоторому внешнему устройству и имеющий специальную структуру. Его нельзяиспользовать для хранения данных как обычный файл или каталог, но над ним можно производить те же операции, что и над любым другим. При этом ввод/вывод информации в этот файл будет соответствовать вводу с внешнего устройства или выводу на него.

Канал – это программное средство, связывающее процессы операционной системы UNIX буферами ядра. Например, запуск процессов в виде

процесс_1|процесс_2 означает, что стандартный вывод процесса_1 будет замкнут на стандартный ввод процесса_2. При этом сначала создается канал, а потом на выполнение

одновременно запускаются оба процесса, и общее время их выполнения определяется более медленным процессом.

Практическая работа 9

Работа с реестром Windows

Теоретические сведения.

Реестр - это ерархическая централизованная база данных, используемая в ОС Microsoft Windows для хранения сведений, необходимых для настройки операционной системы для работы с пользователями, программными продуктами и устройствами.

В реестре хранятся данные, которые необходимы для правильного функционирования Windows. К ним относятся профили всех пользователей, сведения об установленном программном обеспечении и типах документов, которые могут быть созданы каждой программой, информация о свойствах папок и значках приложений, а также установленном оборудовании и используемых портах.

Системный реестр заменяет собой большинство текстовых INI-файлов, которые использовались в Windows 3.x, а также файлы конфигурации MS-DOS, такие как Autoexec.bat и Config.sys. Версии реестра для разных версий операционных систем семейства Windows имеют определенные различия.

Куст реестра - это группа разделов, подразделов и параметров реестра с набором вспомогательных файлов, содержащих резервные копии этих данных. Вспомогательные файлы для всех кустов за исключением HKEY_CURRENT_USER хранятся в системах Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 и Windows Vista в папке %SystemRoot%\ System32\Config. Вспомогательные файлы для куста HKEY_CURRENT_USER хранятся в папке %SystemRoot%\Profiles\Имя_пользователя. Расширения имен файлов в этих папках указывают на тип содержащихся в них данных. Отсутствие расширения также иногда может указывать на тип содержащихся в файле данных.

HKEY_LOCAL_MACHINE\SAM Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\SystemSystem, System.alt, System.log,
System.sav
HKEY_CURRENT_CONFIG System, System.alt, System.log,
System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT Default, Default.log, Default.sav

В Windows 98 файлы реестра называются User.dat и System.dat. В Windows Millennium Edition — Classes.dat, User.dat и System.dat.

Примечание. Средства безопасности в Windows NT, Windows 2000, Windows XP, Windows Server 2003 и Windows Vista позволяют администратору контролировать доступ к разделам реестра.

Следующая таблица содержит перечень и краткое описание стандартных разделов. Максимальная длина имени раздела составляет 255 символов.

Папка/стандартный раздел
Описание
HKEY_CURRENT_USER Данный раздел является корневым для данных конфигурации пользователя, вошедшего в систему в настоящий момент. Здесь хранятся папки пользователя, цвета экрана и параметры панели управления. Эти сведения сопоставляются профилю пользователя. Вместо полного имени раздела иногда

HKEY_USERS Данный раздел содержит все активные загруженные профили пользователей компьютера.

Контрольные вопросы:

1) Перечислить системные процессы Windows.
2) Дать определения драйвера устройства в различных контекстах.
3) Пояснить принцип функционирования уровня абстрагирования от оборудования.
4) Перечислить основные компоненты исполнительной системы Windows.
5) Дать определения подсистемам Windows.
6) Перечислить возможные места хранения назначенных политик безопасности
7) Отобразить переменные среды в Windows двумя способами: из командной оболочки и окна свойств системы
8) Задать переменную среды с различными вариантами динамически формируемых значений.

Практическая работа 10

Работа в командной строке

Операционная система Microsoft Windows XP в бета версиях, известная как Microsoft Codename Whistler, является продолжением линейки Windows NT. Это полностью 32 разрядная операционная система с приоритетной многозадачностью. В ее основе лежат базовые принципы:

- совместимость – поддержка файловых систем FAT 16, FAT32 и NTFS, поддержка приложений написанных под DOS, Windows 9x, Windows NT, а также некоторых приложений под OS/2 и POSIX;
- переносимость – реализация поддержки процессоров разных архитектур;
- реализация системы безопасности на уровне пользователей.

Первоначально Microsoft планировала разработку двух независимых операционных систем - Neptun (эта система должна была стать продолжением Windows 9x) и Odyssey (должна была стать продолжением линейки Windows NT). Однако впоследствии планы корпорации изменились и обе разработки были объединены в один проект Windows XP – операционную систему с полностью переработанным интерфейсом, новыми возможностями и более высоким уровнем обеспечения безопасности.

Все операционные системы, как современные, так и давно уже неиспользуемые, имеют одну общую черту – хранение информации в операционных системах осуществляется подсистемой, называемой файловой системой.

Файловая система – это набор спецификаций и соответствующее им программное обеспечение, которое отвечает за создание, удаление, организацию, чтение, запись, модификацию и перемещение файлов информации, а также за управление доступом к файлам и за управление ресурсами, которые используются файлами. Файловая система определяет способ организации данных на диске и принципы хранения данных на физическом носителе. Например, как должны сохраняться данные файла, какая информация (например, имя, дата создания и т.п.) о файле должна храниться и каким образом. Формат хранения данных определяет основные характеристики файловой системы.

Информация на магнитных дисках размещается и передается блоками. Каждый блок называется сектором и располагается на концентрических дорожках поверхности диска. Группа дорожек одного радиуса, расположенных на поверхностях магнитных дисков, образуют цилиндры. Каждый сектор состоит из поля данных и поля служебной информации, ограничивающей и идентифицирующей его. Размер сектора (объем поля данных) устанавливается контроллером или драйвером. Физический адрес сектора на диске определяется спомощью трех «координат»:

- номер цилиндра;
- номер рабочей поверхности диска;
- номер сектора на дорожке.

Обмен информацией между оперативно запоминающим устройством и дисками физически осуществляется только секторами. Диск может быть разбит нанесколько разделов, которые могут использоваться как одной операционной системой, так и несколькими. На каждом разделе может быть организована своя файловая система. Для организации хотя бы одной файловой системы должен быть определен, по крайней мере, один раздел. Разделы могут быть двух типов:

- первичный раздел
- расширенный раздел

Максимальное число первичных разделов – четыре, но обязательно должен быть хотя бы один. Если первичных разделов больше одного, то один должен быть активным, в нем находится загрузчик операционной системы. На одном диске может быть только один расширенный раздел, который в свою очередь может содержать большое количество подразделов – логических дисков.

Операционная система Windows XP поддерживает работу со следующими файловыми системами:

- FAT (File Allocation Table) – файловая система, разработанная для MS-DOS и являющаяся основной для Windows 3.x и 9x. Windows XP и Windows Server 2003 поддерживают три разновидности FAT: FAT12, FAT16 и FAT32. Первые двеобеспечивают совместимость со старыми операционными системами Microsoft. Кроме того, FAT12 используется как формат хранения данных на гибких дисках. FAT 32 – модифицированная версия FAT, используемая в Windows 95 OSR2, Windows 98 и Windows Millennium.
- NTFS (Windows NT file system) – файловая система, разработанная специально для Windows NT и унаследованная Windows 2000, Windows XP, Windows 2003.
- CDFS (Compact Disk File System) – файловая система компакт-дисков.
- UDF (Universal Disk Format) – универсальный формат дисков, используемый современными магнитооптическими накопителями и технологией DVD.
- DFS (Distributed File System) – распределенная файловая система.

Возможность поддержки различных файловых систем в линейке современных операционных систем семейства Windows заложена в архитектуре системы ввода-вывода, которая отвечает за обработку запросов ввода-вывода и выполняет следующие задачи:

- обеспечение работы сверхпроизводительных операций ввода-вывода;
- возможность использования асинхронного ввода-вывода;
- поддержка нескольких файловых систем;
- модульная архитектура, с возможностью добавления новых файловых системи устройств;
- предоставление расширенных возможностей, например, кэширования;
- защита совместно используемых ресурсов.

Список зарегистрированных файловых систем можно посмотреть с помощью утилиты WinObj. У каждой системы есть свои полезные свойства, но возможности защиты и аудита различны. На выбор файловой системы оказывают влияние следующие факторы: цель, для которой предполагается использовать компьютер, аппаратная платформа, количество жестких дисков и их объем, требования к безопасности, используемые в системе приложения.

Вопросы по разделу^

1. Дайте определение термину «файловая система».
2. Определите назначение файловой системы.
3. Объясните, каким образом размещается и передается информация намагнитных дисках.
4. Дайте определение термину «сектор» и поясните из каких элементов он состоит.
5. Дайте определение термину «цилиндр».
6. Как определяется физический адрес сектора?
7. Как осуществляется обмен между ОЗУ и дисками?
8. Определите типы разделов и их использование.
9. С какими файловыми системами поддерживает работу операционная система Windows XP?

10. В каком элементе архитектуры операционной системы Windows XPреализуется возможность поддержки различных файловых систем?

Практическая работа 11

Пакетные файлы

Организация пакетных файлов и сценариев в ОС Windows

Пакетный файл – *это неформатированный текстовый файл ASCII, содержащий одну или несколько команд ОС.* Имена пакетных файлов имеют расширения **.cmd** или **.bat**. **ОС** при работе с пакетным файлом последовательно обрабатывает его команды после ввода его имени в строке командной оболочки или запуска из другой программы. **Сценарий** – это программа, состоящая из набора инструкций для работы приложения или служебной утилиты. Сценарий – разновидность пакетного файла.Инструкции в сценариях обычно выражаются с использованием правил и синтаксиса соответствующего приложения или служебной утилиты в сочетании с простыми управляющими операторами, такими как операторы циклов и условныеоператоры.

Пакетные файлы и сценарии часто называют командными файлами, содержащими любые команды. Некоторые команды, такие как **For, Goto** и **If**, позволяют выполнять обработку условий в пакетных файлах. Другие команды позволяют управлять вводом и выводом, а также запускать другие пакетные файлы.

При организации пакетных файлов и сценариев применяют **переменные**, задающие поведение командной оболочки или ОС и **пакетные параметры** командного интерпретатора, которые используются в пакетном файле дляполучения информации о настройках среды. Поведение среды командной оболочки или всей ОС задают с помощью двухтипов переменных среды: **системных** и **локальных.**

- **Системные переменные** *определяют поведение глобальной среды ОС.*
- **Локальные переменные** *определяют поведение среды в конкретном экземпляре командного интерпретатора Cmd.exe.*

Системные переменные среды задаются заранее в ОС Windows XP и доступны для всех ее процессов. Только пользователи с привилегиями администратора могут изменять эти переменные. **Локальные переменные** среды доступны в случае, когда пользователь, для которого они были созданы, входит в систему. В частности, локальные переменные реестра **HKEY_CURRENT_USER** подходят только для текущего пользователя, но определяют поведение глобальной среды ОС. В следующем списке представлены различные типы переменных в порядке убывания их приоритета:

1. встроенные системные переменные,
2. системные переменные реестра **HKEY_LOCAL_MACHINE**,
3. локальные переменные реестра **HKEY_CURRENT_USER**,
4. все переменные среды и пути, указанные файле **Autoexec.bat**,
5. все переменные среды и пути, указанные в сценарии входа в систему, еслион имеется,
6. переменные, используемые интерактивно в пакетном файле или сценарии. Чтобы иметь возможность подставить значение в переменную среды изкомандной строки или в пакетном файле (сценарии), следует заключить имя соответствующей переменной в символы процентов (%), например **Set MyPath=%CD%.** Символы процентов указывают на то, что командный интерпретатор должен обратиться к значению переменной безпосредственного выполнения и сравнения.Командный интерпретатор Cmd.exe может декорировать переменными с %0 по %9. При использовании пакетных параметров переменная %0 заменяется именем пакетного файла, а переменные с %1 по %9 — на

соответствующие аргументы командной строки. Для доступа к переменным больше %9 необходимо воспользоваться командой Shift. Параметр %* ссылается на все аргументы, которые передаются пакетному файлу, за исключением %0. В качестве примера, рассмотрим копирование содержимого из каталога 1 (*Folder1*) в каталог 2 (*Folder2*), где параметр %1 заменяется значением *Folder1*, а параметр %2 соответственно значением *Folder2*. В пакетном файле **Mybatch.bat** следует ввести следующую строку: **Xcopy %1*.* %2**

Используйте пакетный файл **Mybatch.bat** следующим образом:

Mybatch.bat *C:\folder1 D:\folder2*

Результат будет таким же, как и при записи в пакетный файл строки:

Xcopy *C:\folder1*.* D:\folder2*

С пакетными параметрами можно также использовать модификаторы. **Модификаторы** *используют информацию о текущем диске и каталоге как часть или полное имя файла (каталога)*. Синтаксис модификатора: *%~xy*, где *x* — символьное сокращение действия, определяемое модификатором, *y* — идентификатор переменной (в диапазоне от 1до 9).

В табл. 1 и 2 описаны модификаторы, выполняемые ими действия, и даны возможные комбинации модификаторов и квалификаторов для получения более сложных результатов. В этих таблицах %1 и переменную среды PATH можно заменить другими значениями пакетных параметров.

Таблица 1. Модификаторы и выполняемые ими действия

№	**Модификатор**	**Описание**
п.п.		
1	%~1	расширение %1 и удаление любых кавычек (" ")
2	%~f1	замена %1 полным путем
3	%~d1	замена %1 именем диска
4	%~p1	замена %1 путем
5	%~n1	замена %1 именем файла
6	%~x1	замена %1 расширением имени файла
7	%~s1	замена путем, содержащим только короткие имена
8	%~a1	Замена %1 атрибутами файла
9	%~t1	замена %1 датой и временем модификации файла
10	%~z1	замена %1 размером файла

11	%~$PATH:1	поиск в каталогах, перечисленных в переменной среды PATH, замена %1 полным именем первого найденного файла. Если переменная среды не определена или поиск не обнаружил файлов, модификатор выдает пустую строку.

Таблица 2. Комбинации модификаторов и квалификаторов

№ п.п.	Модификатор	Описание
1	%~dp1	замена %1 именем диска и путем
2		%~nx1 замена %1 именем файла и расширением
3	%~dp$PATH:1	поиск в каталогах, перечисленных в переменной средыPATH, и замена %1 именем диска и путем к первому найденному файлу.
4	%~ftza1	замена %1 строкой, аналогичной результату работы команды Dir

Еще один модификатор, являющийся уникальным, имеет вид %*. Он представляет все аргументы, переданные пакетному файлу. Этот модификатор не используется в комбинации с модификатором %~. Конвейеры команд и «каналы», рассмотренные в предыдущих лабораторных работах (Часть I, Приложения 1 и 2) являются инструментами для расширения функционала пакетных файлов и сценариев при их построении и организации. **Сервер сценариев ОС Windows XP** *позволяет быстро запустить пакетныйфайл или сценарий, имя которого введено в командной строке оболочки.*
Сервер сценариев

- служит контроллером средств обработки сценариев в ОС Windows XP;
- не требует много памяти;
- является идеальным средством, как для интерактивных, так и для пакетных сценариев.

Существуют две версии сервера сценариев, доступных в окне командноойоболочки:

- **Wscript.exe** — позволяет задавать параметры выполнения сценариев в окне свойств;
- **Cscript.exe** — позволяет задавать параметры выполнения сценариев с помощью ключей командной строки.

Для разработки сценариев **ОС Windows XP** следует использовать редакторы сценариев **JScript** или **VBScript** (в составе **Visual Basic ScriptingEdition**). Призапуске сценария из командной строки сервер сценария читает и передает содержимое указанного файла зарегистрированному обработчику сценариев. Для определения языка сценария используется расширение имени файла(**.vbs** для **VBScript**, **.js** для **JScript**). Благодаря этому, разработчик сценария не обязан знать точные программные идентификаторы

(**ProgID**) различных обработчиков сценариев. Сопоставление расширения имени файла сценария спрограммным идентификатором и запуск конкретного обработчика сценариев осуществляется непосредственно сервером сценариев **ОС Windows XP**. Простейшим сценарием, не требующим применения среды Visual Basic, является сценарий входа в систему, представляющий собой файл, связываемый с одной или несколькими учетными записями пользователей. Обычно сценарий входа является пакетным файлом, который автоматически выполняется при каждом входе пользователя в систему. Сценарии входа используются для настройки рабочей среды пользователя при входе и позволяют администратору задавать основные параметры рабочей среды пользователя без непосредственного его участия.

Поскольку пакетные файлы могут включать в себя любые команды, их конвейеры «каналы», при большом количестве условий и циклов последствиянекорректной работы пакетного файла могут быть непредсказуемыми для ОС, и возможно как следствие разрушительными. Поэтому для организации пакетного файла разработчику необходимо четко представлять себе, что именно и каким образом должно происходить в системе при работе этого файла, какая последовательность действий реализуется в результате выполнения задуманного сценария и как на эти действия реагирует ОС. Помимо рассмотренных в предыдущих лабораторных работах команд, которые могут быть использованы при организации пакетного файла, существует ряд дополнительных, функционал которых напоминает операторы языков программирования высокого уровня. К их числу относятся: **At, Call, Doskey, Echo, Endlocal, For, Goto, If, Pause, Rem, Set, Setlocal и Shift**. В настоящей лабораторной работе предполагается ознакомление с основными командами, используемыми в качестве инструментов организации пакетных файлов, создание командного файла в формате ASCII, реализующего определенный сценарий работы системы, а также оценка возможности использования его в качестве сценария входа в систему. Лабораторная работа выполняется на виртуальной машине в среде ОС Windows XP.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

5.1.1. Перечень основной литературы:

4 Воронцова, В. Л. Лекции по системному и прикладному программному обеспечению: Учебное пособие / В. Л. Воронцова, И. А. Журавлева; Ставроп. гос. ун-т. – Ставрополь: СГУ, 2004. – 208 с. – Библиогр: с. 205-206

5 Защита информации в операционных системах: лабораторные работы: учеб.- метод. пособие / М. В. Романкова / сост.: И. В. Зайцева / Федеральное агентство по образованиюСтавроп. гос. ун-т. – Ставрополь : Изд-во СГУ, 2008. – 99 с. – Библиогр.: с. 96-97

6 Программно-аппаратные средства обеспечения информационной безопасности: учеб.пособие / сост. В. И. Петренко, Н. В. Куклева ; Федер. агентство по образованию,Ставроп. гос. ун-т, Ч. 2, Защита в операционных системах. – Ставрополь: Изд-во СГУ,2007. – 154 с. – Библиогр: с. 154

5.1.2. Перечень дополнительной литературы:

3 Безручко, В. Т. Практикум по курсу "Информатика". Работа в Windows, Word, Excel [Учеб.пособие для вузов*]. – М.: Финансы и статистика, 2004. – 272с.: ил. – Библиогр.: 265. – ISBN 5-279-02436-8

4 Грищенко, Ю.Б. Операционные системы: в 2-х ч. / Ю.Б. Грищенко; Федеральное агентст по образованию, Томский межвузовский центр дистанционного образования (ТУСУРКафедра автоматизации обработки информации (АОИ). Томск: Томскийгосударственный университет систем управления и радиоэлектроники, 2009. – Ч. 2. – 2 с.– Режим доступа: по подписке. – URL: http://biblioclub.ru/index.ph page=book&id=208655

5.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации по выполнению практических работ по дисциплине «Защищенные локальные вычислительные сети».

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине «Защищенные локальные вычислительные сети».

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Цифровая грамотность и обработка данных»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению курсовой работы
по дисциплине «**ЗАЩИЩЕННЫЕ ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ**»
для студентов направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2022

ВВЕДЕНИЕ

Методические указания содержат формулировку задания к курсовой работе, общие требования к написанию и оформлению курсовой работы, индивидуальные задания к курсовой работе по темам дисциплины, теоретический материал по основным разделам дисциплины. Выбор варианта курсовой работы проводится по последней цифре зачетной книжки.

Методические указания посвящены курсу «Защищенные локальные вычислительные сети». Курсовая работа по изучаемой имеет своей целью систематизацию, закрепление и расширение приобретённых по данной дисциплине теоретических знаний, а также проверку умения студентов самостоятельно использовать приобретенные ими знания в практических приложениях при решении конкретных задач.

Дисциплина «Защищенные локальные вычислительные сети» имеет целью раскрыть содержание основных понятий и формальных моделей обеспечения безопасности компьютерных систем (моделей компьютерной безопасности).

Задачи дисциплины – дать основы:

• исходных понятий и формализации в сфере компьютерной безопасности;

• представления, анализа и обоснования моделей, методов и механизмов обеспечения безопасности компьютерных систем;

• методологии схемно-технических и программно-алгоритмических решений, используемыхв компьютерных системах защиты информации.В отличие от корпоративных сетей, подключенных к Internet, где обычные средства безопасности в большой степени решают проблемы защиты внутренних сегментов сети от злоумышленников, распределенные корпоративные информационные системы, системы электронной коммерции и предоставления услуг пользователям Internet предъявляют повышенные требования в плане обеспечения информационной безопасности.

Межсетевые экраны, системы обнаружения атак, сканеры для выявления уязвимостей в узлах сети, операционных систем и СУБД, фильтры пакетов данных на маршрутизаторах - достаточно ли всего этого мощного арсенала (так называемого «жесткого периметра») для обеспечения безопасности критически важных информационных систем, работающих в Internet и Intranet. Практика и накопленный к настоящему времени опыт показывают - чаще всего нет.

Концепция «Защищенные локальные вычислительные сети» включает ряд законодательных инициатив, научных, технических и технологических решений, готовность государственных организаций и компаний использовать их для того, чтобы люди, используя устройства на базе компьютеров и программного обеспечения, чувствовали себя так же комфортно и безопасно.

Наличие и полнота политики безопасности - набор внешних и корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и определяющих, как организация собирает, обрабатывает, распространяет и защищает информацию. В частности, стандарты и правила определяют, в каких случаях и каким образом пользователь имеет право оперировать с определенными наборами данных. В политике сформулированы права и ответственности пользователей и персонала отделов ИБ. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения. Чем больше информационная система и чем больше она имеет "входов" и «выходов» (распределенная система), тем «строже», детализированнее и многообразнее должна быть политика безопасности.

1. Цель и задачи изучения дисциплины

Целью освоения дисциплины «Защищенные локальные вычислительные сети» является формирование набора профессиональных компетенций будущего магистра по направлению подготовки 10.03.01 «Информационная безопасность» для решения прикладных задач управления проектами.

Задачи освоения дисциплины: защита информации в операционных системах, защита информации в компьютерных сетях, защита информации в системах управления базами данных.

2. Формулировка задания к КУРСОВОМУ ПРОЕКТУ

В курсовой работе в соответствии с полученным вариантом необходимо выполнить этап концептуального проектирования системы информационной безопасности: материалы исследования, разработки, анализа различных методов, методик, способов, алгоритмов в области обработки и защиты информации

2.1 Варианты курсовой работы

1. Отделение коммерческого банка.
2. Поликлиника.
3. Университет.
4. Офис страховой компании.
5. Интернет-магазин.
6. Офис адвоката.
7. Агентство недвижимости.
8. Туристическое агентство.
9. Издательство.
10. Отделение налоговой службы.
11. Гостиница.
12. Железнодорожная касса.
13. Офис нотариуса.
14. Администрация завода.
15. Администрация города.

2.2 Рекомендуемое содержание

1. Титульный лист

2. Задание на курсовую работу.

3. Отзыв.

4. Содержание (автоматически собираемое).

5. Введение.

6. Три основных раздела, предусмотренные заданием: 1. Обследование существующей инфраструктуры предприятия; 2. Предпроектное обследование информационной безопасности предприятия; 3. Проектирование системы информационной безопасности предприятия.

7. Заключение.

8. Список использованных источников (допускается: список литературы, библиографический список).

9. Приложения.

2.3 Комментарии к содержанию курсовой работы

Курсовая работа должна состоять не менее чем из 25 листов (без приложений). Не следует делать его более 40 листов с приложениями. Отклонения объема от нормы не является принципиальным, но может вызвать замечания.

Титульный лист (приложение А) является первым листом курсовой работы. Он должен быть оформлен на бланке университета или по той же форме как распечатка с ПК.

Задание на курсовую работу (приложение Б):

- заполняется в соответствии с приказами и календарным планом выполнения курсовой работы;

- тема работы;

- цель работы;

- задачи;

- перечень подлежащих к разработке вопросов;

- исходные данные;

- список рекомендуемой литературы;

- контрольные сроки представления отдельных разделов курсовой работы;

- срок защиты студентом курсовой работы;

- даты выдачи и утверждения задания – первый день курсового проектирования.

Отзыв руководителя на курсовую работу должен содержать:

- оценку актуальности курсовой работы;

- краткое содержание основных глав курсовой работы;

- оценку соответствия выводов, сделанных в Заключении поставленным целям.

Кроме того, рецензент выставляет заслуживающую на его взгляд оценку рецензируемой им работе.

Содержание должно быть авто-собираемыми включать в себя введение, наименования всех разделов, подразделов и пунктов (если последние имеют наименования) с указанием номеров страниц, с которых начинаются эти элементы пояснительной записки.

Введение

Данный пункт должен содержать:

- развернутую оценку современного состояния решаемой задачи;

- актуальность и новизну темы;

- постановку задачи исследования с указанием цели и используемых методов и средств;

- исходные данные для исследования;

- планируемые результаты.

Объем введения 2-3 страницы.

Основные разделы. Наименования и содержание основных разделов пояснительной записки определяется заданием на курсовую работу.

Первый раздел (Обследование существующей инфраструктуры и определение исходных данных для проектирования системы ИБ) обычно носит постановочный характер. Здесь рассматриваются: организационная структура предприятия. состав и назначение аппаратных и программных средств, основные цели защиты информации на предприятии, перечень конфиденциальной информации и информации, составляющей коммерческую тайну. Раскрываются недостатки в системе информационной безопасности, и формулируется задача исследования. При необходимости раздел может содержать описание используемых аппаратных или программных средств, математического аппарата и т.п.

Второй раздел (Предпроектное обследование информационной безопасности предприятия (или одного из его отделов)) содержит: классификацию угроз безопасности информации; разработку концепции ИБ; анализ рисков; определение класса защищенности системы и показателей защищенности от несанкционированного доступа. Необходимо произвести анализ последних достижений в данной конкретной области знаний (научные статьи, разработки, патенты и т.д.) Особое внимание следует уделить иллюстрации полученных результатов с помощью таблиц, графиков, диаграмм и т.п..

Третий раздел (Проектирование системы информационной безопасности предприятия) содержит: рекомендации по разработке концепции информационной безопасности предприятия (или одного из его отделов); разработку политики ИБ и выбор решений по обеспечению политики ИБ; создание системы информационной безопасности; техническое задание на проектирование системы информационной безопасности.

Заключение должно содержать краткие выводы по результатам решения поставленных в курсовой работе задач.

Здесь необходимо отметить преимущества и недостатки разработки (исследования), вопросы реализации и использования проектных предложений, охарактеризовать перспективы дальнейшего развития работ в этой области. Объем заключения обычно не превышает одной или двух страницы.

Список использованных источников должен содержать сведения обо всех источниках, использованных при выполнении дипломного проекта. В список следует включать только те наименования, с которыми есть возможность ознакомиться лично. На все источники, приведенные в списке должны быть ссылки в тексте. На источники, содержащие общие сведения по теме проекта (работы),ссылки делают обычно во введении. Источники нумеруются в порядке появления ссылок в тексте. При ссылке на тот или иной источник информации и оформлении его библиографического описания необходимо руководствоваться ГОСТ 7.1 – 84.

Требования к оригинальности основного текста. Основной текст курсовой работы в обязательном порядке проверяется системой «Антиплагиат» на оригинальность. Для магистров оригинальность текста должна быть не ниже 70%. На все заимствования из патентов, научной или учебной литературы должны быть ссылки непосредственно по месту их появления в тексте курсовой работы

3. Общие требования к написанию и оформлению работы

3.1 Требования к оформлению

Курсовой проект выполняется в электронном виде, сдается в распечатанном и электронном виде (цифровая копия на CD/CDRW носителе). На конверте к CD/CDRW необходимо указать название дисциплины, ФИО студента, факультет, номер группы, шифр зачетной книжки, тему курсового проекта, список всех созданных в ходе выполнения задания файлов.

Приведенный в конце методических указаний список литературы может использоваться студентами при выполнении курсовой работы.

Обязательное выполнение требований вуза к оформлению отчетных работ. Объем работы составляет не менее чем из 25 листов (без приложений) и более 40 листов с приложениями. Работа выполняется на компьютере.

3.2. Выполнение курсовой работы

Сроки сдачи курсовой работы регламентированы в соответствии с требованиями вуза. Пояснительная записка к курсовому проекту с цифровыми материалами к курсовому проекту должны быть сданы за 2 недели до сессии на проверку

3.3 Защита курсовой работы

Защита курсовой работы проходит на последнем занятии. Необходимо подготовить доклад, в котором коротко (3-5 минут) рассказано об основных результатах выполнения курсового проекта. Далее выступающему студенту задаются вопросы. По результатам выступления выносится решение о возможности получения положительной оценки.

4. Индивидуальные задания к курсовой работе

Тема 1.	Защитные механизмы ОС
	В соответствии с указанной предметной областью и классом разрабатываемой информационной системы разработать методы и средства построения систем информационной безопасности и провести анализ механизмов защиты.
Базовый уровень	1. Парольная аутентификация в операционных системах семейства Windows и UNIX. 2. Управление доступом в операционных системах семейства Windows и UNIX. 3. Технические меры защиты от сетевых атак. 4. Механизмы реализации атак в сетях TCP/IP. 5. Средства защиты локальных сетей при подключении к Интернет. 6. Межсетевые экраны (МЭ) – основные возможности, схемы развертывания МЭ и построение правил фильтрации. 7. Системы обнаружения вторжений (СОВ). 8. Угрозы безопасности и многоуровневая защита БД. 9. Политика и модели безопасности в СУБД. 10. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД.
Повышенный уровень	1. Дискреционное и мандатное управление доступом. Контроль информационных потоков в операционных системах семейства Windows и UNIX. 2. Использование протокола PPTP для организации виртуальных частных сетей. 3. Разработка защищенных сетевых приложений. 4. Организация туннелирования на различных уровнях модели ISO/OSI. 5. Средства обнаружения уязвимостей сетевых служб. 6. Системы виртуальных ловушек (HoneyPot иPaddedCell). 7. Угрозы конфиденциальности СУБД и способы противодействия. 8. Основные механизмы управления СУБД (транзакция, блокировки, ссылочная целостность, правила – триггеры). 9. Мониторинг серверов СУБД. 10.Криптографические методы защиты баз данных.
Тема 3.	Угрозы сетевой безопасности и сетевые атаки

	В соответствии с указанной предметной областью и классом разрабатываемой информационной системы разработать и проанализировать имеющиеся средства защиты от утечек по сетям.
Базовый уровень	1. Парольная аутентификация в операционных системах семейства Windows и UNIX. 2. Управление доступом в операционных системах семейства Windows и UNIX. 3. Технические меры защиты от сетевых атак. 4. Механизмы реализации атак в сетях TCP/IP. 5. Средства защиты локальных сетей при подключении к Интернет. 6. Межсетевые экраны (МЭ) – основные возможности, схемы развертывания МЭ и построение правил фильтрации. 7. Системы обнаружения вторжений (СОВ). 8. Угрозы безопасности и многоуровневая защита БД. 9. Политика и модели безопасности в СУБД. 10. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД.
Повышенный уровень	1. Дискреционное и мандатное управление доступом. Контроль информационных потоков в операционных системах семейства Windows и UNIX. 2. Использование протокола PPTP для организации виртуальных частных сетей. 3. Разработка защищенных сетевых приложений. 4. Организация туннелирования на различных уровнях модели ISO/OSI. 5. Средства обнаружения уязвимостей сетевых служб. 6. Системы виртуальных ловушек (HoneyPot иPaddedCell). 7. Угрозы конфиденциальности СУБД и способы противодействия. 8. Основные механизмы управления СУБД (транзакция, блокировки, ссылочная целостность, правила – триггеры). 9. Мониторинг серверов СУБД. 10.Криптографические методы защиты баз данных.
Тема 4.	Обеспечение информационной безопасности в вычислительных сетях
	В соответствии с указанной предметной областью и классом разрабатываемой информационной системы создать защищенную среду информационного обмена, реализующей правила и политику безопасности.
Базовый уровень	1. Парольная аутентификация в операционных системах семейства Windows и UNIX. 2. Управление доступом в операционных системах семейства Windows и UNIX. 3. Технические меры защиты от сетевых атак. 4. Механизмы реализации атак в сетях TCP/IP. 5. Средства защиты локальных сетей при подключении к Интернет. 6. Межсетевые экраны (МЭ) – основные возможности, схемы развертывания МЭ и построение правил фильтрации. 7. Системы обнаружения вторжений (СОВ). 8. Угрозы безопасности и многоуровневая защита БД. 9. Политика и модели безопасности в СУБД. 10. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД.

Повышенный уровень	1. Дискреционное и мандатное управление доступом. Контроль информационных потоков в операционных системах семейства Windows и UNIX. 2. Использование протокола PPTP для организации виртуальных частных сетей. 3. Разработка защищенных сетевых приложений. 4. Организация туннелирования на различных уровнях модели ISO/OSI. 5. Средства обнаружения уязвимостей сетевых служб. 6. Системы виртуальных ловушек (HoneyPot иPaddedCell). 7. Угрозы конфиденциальности СУБД и способы противодействия. 8. Основные механизмы управления СУБД (транзакция, блокировки, ссылочная целостность, правила – триггеры). 9. Мониторинг серверов СУБД. 10.Криптографические методы защиты баз данных.
Тема 6.	Обеспечение конфиденциальности, целостности и высокой готовности СУБД.
	В соответствии с указанной предметной областью и классом разрабатываемой информационной системы описать систему отвечающую параметрам конфиденциальности, целостности и высокой готовности СУБД.
Базовый уровень	1. Парольная аутентификация в операционных системах семейства Windows и UNIX. 2. Управление доступом в операционных системах семейства Windows и UNIX. 3. Технические меры защиты от сетевых атак. 4. Механизмы реализации атак в сетях TCP/IP. 5. Средства защиты локальных сетей при подключении к Интернет. 6. Межсетевые экраны (МЭ) – основные возможности, схемы развертывания МЭ и построение правил фильтрации. 7. Системы обнаружения вторжений (СОВ). 8. Угрозы безопасности и многоуровневая защита БД. 9. Политика и модели безопасности в СУБД. 10. Механизмы обеспечения конфиденциальности, целостности и высокой готовности СУБД.
Повышенный уровень	1. Дискреционное и мандатное управление доступом. Контроль информационных потоков в операционных системах семейства Windows и UNIX. 2. Использование протокола PPTP для организации виртуальных частных сетей. 3. Разработка защищенных сетевых приложений. 4. Организация туннелирования на различных уровнях модели ISO/OSI. 5. Средства обнаружения уязвимостей сетевых служб. 6. Системы виртуальных ловушек (HoneyPot иPaddedCell). 7. Угрозы конфиденциальности СУБД и способы противодействия. 8. Основные механизмы управления СУБД (транзакция, блокировки, ссылочная целостность, правила – триггеры). 9. Мониторинг серверов СУБД. 10.Криптографические методы защиты баз данных.

5.2 Правила оформления курсовой работы

1. Курсовая работа должна быть напечатана на стандартном листе писчей бумаги в формате А4. Поля должны оставаться по всем четырём сторонам печатного листа: левое поле - 35 мм, правое -не менее 10 мм, верхнее и нижнее - не менее 20 мм, количество знаков на странице - примерно 2000. Красная строка – 1,25, межстрочный интервал – 1,15. Каждая новая глава начинается с новой страницы; это же правило относится к другим основным структурным частям работы (введению, заключению, списку литературы, приложениям и т. д.). Страницы с рисунками и приложениями должны быть пронумерованы сквозной нумерацией в рамках раздела. Первой страницей является титульный лист.
2. Титульный лист оформляется по установленному образцу.
3. После титульного листа помещается оглавление с указанием номеров страниц. Оглавление оформляется по установленному образцу.
4. Последняя страница работы подписывается студентом.
5. Курсовая работа должна быть «переплетена» и вставлена в скоросшиватель с прозрачной пластиковой обложкой.

Правила написания буквенных аббревиатур

В тексте курсовой работы, кроме общепринятых буквенных аббревиатур, используются вводимые их авторами буквенные аббревиатуры, сокращённо обозначающие какие-либо понятия из соответствующих областей знания. При этом первое упоминание таких аббревиатур указывается в круглых скобках после полного наименования, в дальнейшем они употребляются в тексте без расшифровки. Если число сокращений превышает десять, то составляется список принятых сокращений, который помещается перед списком литературы.

Правила представления формул, написания символов

Формулы обычно располагают отдельными строками посередине листа или внутри текстовых строк. В тексте рекомендуется помещать формулы короткие, простые, не имеющие самостоятельного значения и не пронумерованные. Наиболее важные формулы, а также длинные и громоздкие формулы, содержащие знаки суммирования, произведения, дифференцирования, интегрирования, располагают на отдельных строках.

Для экономии места несколько коротких однотипных формул, выделенных из текста, можно помещать на одной строке, а не одну под другой.

Нумеровать следует наиболее важные формулы, на которые имеются ссылки в последующем тексте. Порядковые номера формул обозначают арабскими цифрами в круглых скобках у правого края страницы.

Правила оформления таблиц, рисунков, графиков

Таблицы и рисунки должны иметь названия и порядковую нумерацию (например, табл. 1.1, рис. 3.2). Нумерация таблиц и рисунков должна быть сквозной для каждого раздела текста курсового проекта. Порядковый номер таблицы проставляется в правом верхнем углу перед её названием (с выравниванием текста по правой стороне). В каждой таблице следует указывать единицы измерения показателей, и период времени, к которому относятся данные. Если единица измерения в таблице является общей для всех числовых табличных данных, то её приводят в заголовке таблицы после её названия. Пример оформления таблиц представлен ниже.

Таблица 1.1 – Административные участки и УППг. Ессентуки

Административный участок/ УПП	Территория обслуживания	Адрес
Административный участок №1 и УПП	ул. Шевченко, Харьковская, Совхозная, Дружбы, Киевская, Дзержинского, Возрождения, поселок «Северный», Просторная, Виноградная,	г. Ессентуки ул. Энгельса №23 тел. 6-74-72

	Сосновая, Ореховая, Розовая, Тополиная, Яблоневая, Бульварная, проезд Горный, Осиновый, Радужный.	
Административный участок №2/УПП№ 1	Ул. Пушкина № 1-54 «А», Запорожская, Пригородная, А.Сергеева № 75-113, Маркова от № 65-95, Буачидзе № 1-43, Попова № 1-5, П. Шейна № 1-59, ул. С.Разина№ 1-31.	г. Ессентуки ул. Энгельса №23 тел. 6-74-72

Порядковый номер рисунка и его название проставляются под рисунком (с выравниванием текста по центру). Пример оформления рисунков представлен ниже.

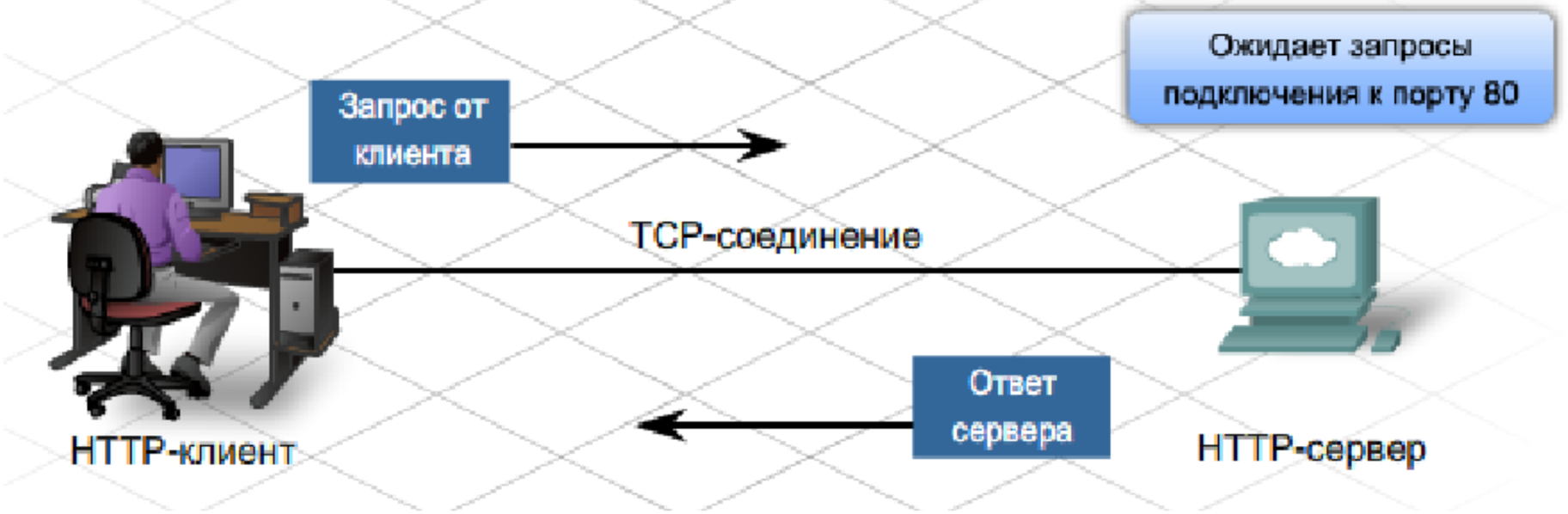

Рис. 2.1. Определение правил передачи через запрос

При построении графиков по осям координат откладываются соответствующие показатели, буквенные обозначения которых выносятся на концы координатных осей, фиксируемые стрелками. При необходимости вдоль координатных осей делаются поясняющие надписи.

При использовании в работе материалов, заимствованных из литературных источников, цитировании различных авторов, необходимо делать соответствующие ссылки, а в конце работы помещать список использованной литературы. Не только цитаты, но и произвольное изложение заимствованных из литературы принципиальных положений, включается в курсовую работу со ссылкой на источник. Наличие в тексте курсовой работы ссылок, пусть даже многочисленных, подчеркивает научную добросовестность автора.

Правила оформления списка использованной литературы

Использованные литературные источники должны быть перечислены в следующем порядке:

монографическая и учебная литература;

периодическая литература - статьи из журналов и газет;

законодательные и инструктивные материалы;

статистические сборники и другие, используемые в работе отчётные и учётные материалы;

интернет источники.

При составлении списка использованной литературы указываются все реквизиты книги: фамилия и инициалы автора, название книги, место издания, название издательства. Для статей, опубликованных в периодической печати, следует указывать наименование издания, номер, год, а также занимаемые станицы (от и до). Литературные источники должны быть расположены в алфавитном порядке по фамилиям авторов.В случае, если количество авторов более трех – по названию книги, остальные материалы в хронологическом порядке. Сначала должны быть указаны источники на русском языке, затем – на иностранном.

Если в курсовой работе была аппаратная разработка, то чертежи схем должны выноситься на плакаты и подшиваться в приложение. В тексте документа на все приложения должны быть даны ссылки. Степень обязательности приложений при ссылках не указывается. Приложения располагают в порядке ссылок на них в тексте документа.

Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова «Приложение» и его обозначения.

Приложение должно иметь заголовок, который записывают симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ь, Ы, Ъ. После слова «Приложение» следует буква, обозначающая его последовательность, например, «Приложение А».

При необходимости текст приложения может быть разбит на разделы, подразделы, пункты и подпункты, которые следует нумеровать в пределах каждого приложения в соответствии с требованиями для основной части записки. Формулы, рисунки и таблицы, включенные в приложения, нумеруются в пределах каждого приложения и содержат в начале своего номера букву «П». Пакеты программной документации, приводимой в приложениях к пояснительной записке, должны оформляться в соответствии с требованиями ЕСПД.

Оформление пояснительной записки осуществляется в соответствии с Методическими указаниями по оформлению отчетов по практике, рефератов, курсовых и дипломных работ/проектов (изд. СКФУ-2015).

5.3 Примеры библиографического описания использованных источников:

Книги

Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн.1. – М.: Энергоатомиздат, 2014. – 400 с.

Статьи

Левкин В.В., Малюк А.А., Петров В.А., Прелов А.В. Проблемы автоматизированной разработки технического задания на проектирование системы защиты информации//Безопасность информационных технологий. – 2015. – №11. – С.40-44.

Нормативно-технические документы

ГОСТ 12.1.003–83. Шум. Общие требования безопасности = NoiseGeneralsafetyrequirements. – Переизд. Апр. 1982 с изм. 1. – Взамен ГОСТ 12.1.003–68; Введ. 01.01.77 до 01.07.84. – М.: Изд-во стандартов, 1982. 9 с.: ил. – (Система стандартов безопасности труда). УДК 534.845.46. Группа Т58. (47) СССР.

Патентные документы

А. с. 1688260 СССР, МПК 5G06F15/36. Устройство для анализа альтернативных решений/М.Д. Скубилин, А.В. Письменов. – № 4454992/24; Заявлено 05.07.88; Опубл. 30.10.91. Бюл. № 40.

Пат. 2130641 РФ, МПК 6G06F 13/00. Способ и устройство защиты информации от несанкционированного доступа/В.И. Божич, М.Д. Скубилин, О.Б. Спиридонов (РФ). – № 98116168/09; Заявлено 24.08.98; Опубл. 20.05.99. Бюл. № 14.

5.4 Теоретические сведения

Для выполнения курсового проекта следует изучить теоретический материал.

5.4.4 Этапы построения системы безопасности ИС

Концепция информационной безопасности определяет этапы построения системы информационной безопасности в соответствии со стандартизованным жизненным циклом

ИС: аудит безопасности (обследование) существующей системы защиты ИС, анализ рисков, формирование требований и выработка первоочередных мер защиты, проектирование, внедрение и аттестация, сопровождение системы. Рассмотрим кратко содержание отдельных этапов.

Аудит безопасности. Аудит безопасности может включать по крайней мере четыре различных группы работ.

К первой группе относятся так называемые "тестовые взломы" ИС. Эти тесты применяются, как правило, на начальных стадиях обследования защищенности ИС. Причина малой эффективности "тестовых взломов" скрывается в самой постановке задачи. Действительно, основной задачей "взломщика" является обнаружение нескольких уязвимостей и их использование для доступа в систему. Если тест оказался успешным, то, предотвратив потенциальное развитие возможных сценариев "взлома", работу надо начинать сначала и искать следующие. Неуспех "взлома" может означать в равной мере как защищенность системы, так и недостаточность тестов.

Вторая группа - экспресс-обследование. В рамках этой, обычно непродолжительной, работы оценивается общее состояние механизмов безопасности в обследуемой ИС на основе стандартизованных проверок. Экспресс-обследование обычно проводится в случае, когда необходимо определить приоритетные направления, позволяющие обеспечить минимальный уровень защиты информационных ресурсов. Основу для него составляют списки контрольных вопросов, заполняемые как в результате интервьюирования, так и в результате тестовой работы автоматизированных сканеров защищенности.

Третья группа работ по аудиту - аттестация систем на соответствие требованиям защищенности информационных ресурсов. При этом происходит формальная проверка набора требований как организационного, так и технического аспектов, рассматриваются полнота и достаточность реализации механизмов безопасности. Типовая методика анализа защищенности корпоративной информационной системы состоит в совокупности следующих методов:

– изучение исходных данных по структуре, архитектуре, инфраструктуре и конфигурации ИС на момент обследования;

– предварительная оценка рисков, связанных с осуществлением угроз безопасности в отношении технических и информационных ресурсов;

– анализ механизмов безопасности организационного уровня, политики безопасности, стандартов и организационно-распорядительной документации по

обеспечению режима ИБ и оценка их соответствия требованиям существующих стандартов и нормативных документов, а также их адекватности существующим рискам;

– анализ конфигурационных файлов маршрутизаторов и Proxy-серверов, почтовых и DNS-серверов (Domain Name System), шлюзов виртуальных частных сетей (VPN), других критических элементов сетевой инфраструктуры;

– сканирование внешних сетевых адресов локальной сети;

– сканирование ресурсов локальной сети изнутри;

– анализ конфигурации серверов и рабочих станций при помощи специализированных программных агентов.

Перечисленные технические методы предполагают применение как активного, так и пассивного тестирования системы защиты. Активное тестирование заключается в моделировании действий потенциального злоумышленника; пассивное тестирование предполагает анализ конфигурации операционной системы и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную или с использованием специализированных программных средств.

При анализе конфигурации средств защиты для внешнего периметра локальной сети и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты:

– настройка правил разграничения доступа (фильтрация сетевых пакетов);

– используемые схемы и настройка параметров аутентификации;

– настройка параметров системы регистрации событий;

– использование механизмов, обеспечивающих сокрытие топологии защищаемой сети (например, трансляция сетевых адресов);

– настройка механизмов оповещения об атаках и реагирования;

– наличие и работоспособность средств контроля целостности;

– версии используемого программного обеспечения и установленные обновления.

Анализ конфигурации предполагает проверку правильности установки сотен различных параметров. Для автоматизации этого процесса могут использоваться специализированные программные средства анализа защищенности, выбор которых в настоящее время достаточно широк.

Один из современных и быстро развивающихся методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем - использование технологии динамически загружаемых программных агентов. На каждую из контролируемых систем устанавливается программный агент, который выполняет соответствующие

настройки программного обеспечения, проверяет их правильность, контролирует целостность файлов, своевременность установки обновлений, а также решает другие задачи по контролю защищенности ИС. Управление агентами осуществляет по сети программа-менеджер. Такие менеджеры, являющиеся центральными компонентами подобных систем, посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все полученные от агентов данные в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, осуществлять ранжирование уязвимостей и т. п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход, например, использован при построении комплексной системы управления безопасностью организации ESM (производитель - компания Symantec Enterprise Security Manager).

Четвертая группа - предпроектное обследование - самый трудоемкий вариант аудита. Такой аудит предполагает анализ организационной структуры предприятия в приложении к информационным ресурсам, правила доступа сотрудников к тем или иным приложениям. Затем выполняется анализ самих приложений. После этого должны учитываться конкретные службы доступа с одного уровня на другой, а также службы, необходимые для информационного обмена. Затем картина дополняется встроенными механизмами безопасности, что в сочетании с оценками потерь в случае нарушения ИБ дает основания для ранжирования рисков, существующих в ИС, и выработки адекватных контрмер. Успешное проведение предпроектного обследования, последующего анализа рисков и формирования требований определяют, насколько принятые меры будут адекватны угрозам, эффективны и экономически оправданы.

Проектирование системы. В настоящее время сложились два подхода к построению системы ИБ - продуктовый и проектный. В рамках продуктового подхода выбирается набор средств физической, технической и программной защиты (готовое решение), анализируются их функции, а на основе анализа функций определяется политика доступа в рабочие и технологические помещения, к информационным ресурсам. Можно поступать наоборот: вначале прорабатывается политика доступа, на основе которой определяются функции, необходимые для ее реализации, и производится выбор средств и продуктов, обеспечивающих выполнение этих функций. Выбор методов зависит от конкретных условий деятельности организации, ее местонахождения, расположения помещений, состава подсистем ИС, совокупности решаемых задач, требований к системе защиты и т. д.

Продуктовый подход более дешев с точки зрения затрат на проектирование. Кроме того, в некоторых случаях он является единственно возможным в условиях дефицита решений или жестких требований нормативных документов на государственном уровне (например, для криптографической защиты в сетях специального назначения и правительственных телефонных сетях применяется только такой подход). Проектный подход заведомо более полон, и решения, построенные на его основе, более оптимизированы и проще аттестуемы. Проектный подход предпочтительнее и при создании больших гетерогенных распределенных систем, поскольку в отличие от продуктового подхода он не связан изначально с той или иной платформой. Кроме того, он обеспечивает более «долгоживущие» решения, поскольку допускает проведение замены продуктов и решений без изменения политики доступа. А это, в свою очередь, обеспечивает хороший показатель возврата инвестиций (ROI) при развитии ИС и системы ИБ.

Объекты или приложения? При проектировании архитектуры системы информационной безопасности применяются объектный, прикладной или смешанный подходы.

Объектный подход строит защиту информации на основании физической структуры того или иного объекта (здания, подразделения, предприятия). Применение объектного подхода предполагает использование набора универсальных решений для обеспечения механизмов безопасности, поддерживающих однородный набор организационных мер. Классическим примером такого подхода является построение защищенных инфраструктур внешнего информационного обмена, локальной сети, системы телекоммуникаций и т. д. К недостаткам объектного подхода относятся очевидная неполнота его универсальных механизмов, особенно для организаций с большим набором сложно связанных между собой приложений.

Прикладной подход «привязывает» механизмы безопасности к конкретному приложению. Пример прикладного подхода - защита подсистемы либо отдельных зон автоматизации (бухгалтерия, склад, кадры, проектное бюро, аналитический отдел, отделы маркетинга и продаж и т. д.). При большей полноте защитных мер такого подхода у него имеются и недостатки, а именно: необходимо увязывать различные по функциональным возможностям средства безопасности с целью минимизации затрат на администрирование и эксплуатацию, а также с необходимостью задействовать уже существующие средства защиты информации для сохранения инвестиций.

Возможна комбинация двух описанных подходов. В смешанном подходе информационная система представляется как совокупность объектов, для каждого из

которых применен объектный подход, а для совокупности взаимосвязанных объектов - прикладной. Такая методика оказывается более трудоемкой на стадии проектирования, однако часто дает хорошую экономию средств при внедрении, эксплуатации и сопровождении системы защиты информации.

Службы и механизмы безопасности. Стратегию защиты можно реализовать двумя методами - ресурсным и сервисным. Первый метод рассматривает ИС как набор ресурсов, которые «привязываются» к конкретным компонентам системы ИБ. Это метод хорош для небольших ИС с ограниченным набором задач. При расширении круга задач и разрастании ИС приходится во многом дублировать элементы защиты для однотипных ресурсов, а это часто приводит к неоправданным затратам. Сервисный подход трактует ИС как набор служб, программных и телекоммуникационных сервисов для оказания услуг пользователям. В этом случае один и тот же элемент защиты можно использовать для различных сервисов, построенных на одном и том же программном обеспечении или техническом устройстве. Сегодня сервисный подход представляется предпочтительным, поскольку он предполагает строгий функциональный анализ существующих многочисленных служб, обеспечивающих функционирование ИС, и позволяет исключить широкий класс угроз при помощи отказа от «лишних» служб и оптимизации работы оставшихся, делая структуру системы ИБ логически обоснованной. Именно сервисный подход лежит в основе современных стандартов по безопасности, в частности ISO 15408.

Внедрение и аттестация. Этап внедрения включает целый комплекс последовательно проводимых мероприятий, включая установку и конфигурирование средств защиты, обучение персонала работе со средствами защиты, проведение предварительных испытаний и сдачу в опытную эксплуатацию. Опытная эксплуатация позволяет выявить и устранить возможные недостатки функционирования подсистемы информационной безопасности, прежде чем запустить систему в «боевой» режим. Если в процессе опытной эксплуатации выявлены факты некорректной работы компонентов, проводится корректировка настроек средств защиты, режимов их функционирования и т. п. По результатам опытной эксплуатации проводится внесение корректировок (при необходимости) и уточнение настроек средств защиты. Далее следует проведение приемо-сдаточных испытаний, ввод в штатную эксплуатацию и оказание технической поддержки и сопровождения.

Подтверждение функциональной полноты системы безопасности и обеспечения требуемого уровня защищенности ИС обеспечивается проведением аттестации системы ИБ соответствующим аккредитованным центром Гостехкомиссии или зарубежной

независимой лаборатории. Аттестация предусматривает комплексную проверку защищаемого объекта в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности. Аттестация проводится в соответствии со схемой, составляемой на подготовительном этапе исходя из следующего перечня работ:

– анализ исходных данных, предварительное ознакомление с аттестуемым объектом информатизации;

– экспертное обследование объекта информатизации и анализ документации по защите информации на предмет соответствия требованиям;

– испытания отдельных средств и систем защиты информации на аттестуемом объекте с помощью специальной контрольной аппаратуры и тестовых средств;

– испытания отдельных средств и систем защиты информации в испытательных центрах (лабораториях);

– комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и аттестационных испытаний и утверждение заключения по результатам аттестации объекта информатизации.

По результатам испытаний готовится отчетная документация, проводится оценка результатов испытаний и выдается аттестат соответствия установленного образца. Его наличие дает право обработки информации со степенью конфиденциальности и на период времени, которые установленны в аттестате.

Техническая поддержка и сопровождение. Для поддержания работоспособности подсистемы информационной безопасности и бесперебойного выполнения ею своих функций необходимо предусмотреть комплекс мероприятий по технической поддержке и сопровождению программного и аппаратного обеспечения подсистемы информационной безопасности, включая текущее администрирование, работы, проводимые в экстренных случаях, а также периодически проводимые профилактические работы. Данный комплекс мероприятий включает в себя:

– администрирование штатных средств защиты и их техническое обслуживание;

– контроль состояния системы, профилактическое обследование конфигурации, выявление потенциальных проблем;

– мониторинг и установка выпускаемых обновлений и программных коррекций средств защиты, а также используемых операционных систем, СУБД и приложений;

– регулярный поиск и анализ уязвимостей в защищаемой системе с использованием специальных средств сканирования;

– диагностику неисправностей и проведение восстановительных работ при возникновении аварийных и нештатных ситуаций;

– периодическое тестирование системы ИБ и оценку эффективности защиты.

Техническая поддержка и сопровождение системы ИБ требует наличия у обслуживающего персонала определенных знаний и навыков и может осуществляться как штатными сотрудниками организации - владельца ИС, ответственными за информационную безопасность, так и сотрудниками специализированных организаций.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

6.1.1. Перечень основной литературы

1. Горев А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс]: учебно-практическое пособие/ Горев А.И., Симаков А.А.— Электрон. текстовые данные.— Омск: Омская академия МВД России, 2016.— 88 с.— Режим доступа: http://www.iprbookshop.ru/72856.html

2. Технологии защиты информации в компьютерных сетях [Электронный ресурс]/ Н.А. Руденков [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 368 с.— Режим доступа: http://www.iprbookshop.ru/73732.html.

6.1.2. Перечень дополнительной литературы

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.

2. Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ Креопалов В.В.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 с.— Режим доступа: http://www.iprbookshop.ru/10871.html.

6.2. Законы Российской Федерации в области защиты информации (защиты государственной тайны)

1. ФЗ РФ «Об информации, информационных технологиях и о защите информации».

2. ФЗ РФ «О коммерческой тайне» (в редакции Федерального закона от 02.02.2006 № 19-ФЗ).

3. ФЗ РФ «О персональных данных» от 27.07.2006 № 152ФЗ.

4. ФЗ РФ от 23 сентября 1992 г. N 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных».

5. Закон РФ от 19 февраля 1993г. N 4524-1 «О федеральных органах правительственной связи и информации» (с изменениями от 24 декабря 1993 года, по состоянию на 1 апреля 1994 года).

6. Закон РФ от 10 июня 1993 года N 5151-1 «О сертификации продуктов и услуг».

7. Закон РФ от 10 июня 1993 года N 5154-1 «О стандартизации».

8. Закон РФ от 01 июля 1993 г. N 5306-1 «О внесении изменений и дополнений в Закон Российской Федерации «О федеральных органах государственной безопасности».

9. Закон РФ от 20 января 1995 года N 15-ФЗ «О связи».

6.3. ГОСТы в области защиты информации (защиты государственной тайны):

1. ГОСТ Р 34.10-94«Информационная технология криптографическая защита информации процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

2. ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»

3. ГОСТ Р 50862-96 «Сейфы и хранилища ценностей. Требования и методы испытаний на устойчивость к взлому и огнестойкость».

6.4. Указы Президента РФ в области защиты информации (защиты государственной тайны)

1. Указ Президента РФ от 7 октября 1993г. N 1607 «О государственной политике в области охраны авторского права и смежных прав».

2. Указ Президента РФ от 31 декабря 1993г. N 2334 «О дополнительных гарантиях прав граждан на информацию».

3. Указ Президента РФ от 20 января 1994г. N 170 «Об основах государственной политики в сфере информатизации».

4. Указ Президента РФ от 3 апреля 1995 г. N 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

5. Указ Президента РФ от 3 июля 1995 г. N 662 «О мерах по формированию общероссийской телекоммуникационной системы и обеспечению прав собственников при хранении ценных бумаг и расчетах на фондовом рынке Российской Федерации».

6. Указ Президента РФ от 30 ноября 1995г. N 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».

7. Указ Президента РФ от 26 августа 1996г. N 1268 «О контроле за экспортом из Российской Федерации товаров и технологий двойного назначения».

8. Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента РФ от 30 мая 1997 года N 226-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

6.5. Постановления Правительства РФ в области защиты информации (защиты государственной тайны)

1. Постановление Правительства РФ от 24 декабря 1994 г. N 1418 «О лицензировании отдельных видов деятельности» (с изменениями от 5 мая, 3 июня, 7 августа,12 октября 1995г.).

2. Постановление Правительства РФ от 15 апреля 1995 года N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и(или) оказанием услуг по защите государственной тайны».

3. Постановление Правительства РФ от 26 июня 1995 г. N 608 «О сертификации средств защиты информации».

4. Постановление Правительства РФ от 04 сентября 1995г. N 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

5. Постановление Правительства РФ от 17 ноября 2007 г. № 781 об Утверждении «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

6.6.Нормативные документы в области защиты информации от несанкционированного доступа

1. Защита от несанкционированного доступа к информации. Термины и определения. ГОСТЕХКОМИССИЯ РОССИИ.

2. Постановление правительства РФ от 30 апреля 1997 г. N 513 «О внесении дополнения в Положение о лицензировании».

3. Положение «О порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

4. Нормативные документы в области защиты информации от несанкционированного доступа.

6.7. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Защищенные локальные вычислительные сети».
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Защищенные локальные вычислительные сети
3. Методические указания по выполнению курсовых работ по дисциплине «Защищенные локальные вычислительные сети».

6.8. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. https://rocit.ru – Региональный общественный центр интернет-технологий.

2. http://цифроваяграмотность.рф – Сайт проекта «Цифровая грамотность РФ».

3. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий.

4. http://window.edu.ru – образовательные ресурсы ведущих вузов.

5. http://www.consultant.ru/ - сайт правовой поддержки.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 12000002A633E3D113AD425FB50002000002A6
Владелец: Шебзухова Татьяна Александровна

Действителен: с 20.08.2021 по 20.08.2022