БПОУ ВО «Грязовецкий политехнический техникум»

Рассмотрен

цикловой комиссией по общепрофессиональным дисциплинам и профессиональным модулям отделения «Электрификация и автоматизация сельского хозяйства»

Согласовано

зам. директора по ОМР
_____ Е. А. Ткаченко
«30» августа 2017 г.

Протокол № 1 от «30» августа 2017 г.

Председатель комиссии:
_____ Т. В. Невзорова

Методические рекомендации

по организации внеаудиторной самостоятельной работы студентов по профессиональному модулю:

ПМ. 03 Эксплуатация объектов сетевой инфраструктуры

Специальность 09.02.02. Компьютерные сети

Грязовец
2017 г.

Критерии оценки результатов самостоятельной работы

Критериями оценки результатов внеаудиторной самостоятельной работы обучающихся являются:

- уровень освоения учебного материала;
- уровень умения использовать теоретические знания при выполнении практических задач;
- уровень сформированности общепрофессиональных умений;
- уровень умения активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения материала;
- уровень умения ориентироваться в потоке информации, выделять главное;
- уровень умения четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- уровень умения определить, проанализировать альтернативные возможности, варианты действий;
- уровень умения сформулировать собственную позицию, оценку и аргументировать ее.

Задания для внеаудиторной самостоятельной работы рассчитаны на 179 часов.

Перечень внеаудиторной самостоятельной работы

Перечень внеаудиторной самостоятельной работы для студентов специальности 09.02.09 Компьютерные сети представлен в таблице 2.

Таблица 2.

№ СР	Вид внеаудиторной самостоятельной работы	Количество часов на внеаудиторную самостоятельную работу (ВСР)
	МДК 03.01 Эксплуатация объектов сетевой инфраструктуры	
1	Создать сообщение на тему « Виртуальные частные сети»	6
2	Создать презентацию на тему «Адресация в IP –сетях»	4
3	Создать презентацию на тему «Взаимодействие между разнородными сетями»	6
4	Создать сообщение «Сети на основе сервера. Кластеризация сервера»	4
5	Подготовить инструкцию на тему «Настройка сети в Windows Vista»	4
6	Подготовить презентацию на тему «Операционная система UNIX»	4
7	Подготовить презентацию на тему «Операционная система Apple Talk»	4
8	Подготовить сообщение на тему «Операционная система Banyan VINES»	6
9	Составить кроссворд на тему «Доменная система имен (DNS)»	6
10	Подготовить сообщение на тему «Топология коммутации пакетов и ретрансляция кадра(Frame Relay)»	4
11	Подгтовить презентацию на тему «Современные проблемы управления ИТ- инфраструктурой»	6
12	Подготовить реферат на тему «Средства продуктов Unicenter для управления ИТ- инфраструктурой»	6

13	Подготовить сравнительную таблицу по теме «Комплекс программных продуктов Hewlet – Packard ориентированных на управление корпоративными ИТ любого масштаба»	6
14	Подготовить сообщение на тему «Основные назначения средств Microsoft Systems Management Server»	4
15	Подготовить презентацию на тему «Основные назначения средств Microsoft Operations Manager»	4
16	Составить презентацию по использованию утилиты Acronis для изучения безопасной зоны Acronis	4
17	Составить сообщение по теме «Создание контрольной точки восстановления с помощью Acronis»	4
18	Разработать презентацию "План восстановления работоспособности сети на примере одной взятой организации"	6
19	Разработать инструкцию по теме «Поиск неисправностей по принципу локализации неисправностей конкретного оборудования»	4
20	Составить сообщение на тему «Принцип работы новых контрольно-измерительных аппаратов»	3
	итого по МДК 03.01	***95***
	МДК 03.02. Безопасность функционирования информационных систем	
1	Создание презентации по теме: Понятие "информационная безопасность"	3
2	Создание сообщения по теме: Составляющие информационной безопасности	3
3	Создание кроссворда по теме: Задачи информационной безопасности общества	2
4	Создание конспекта по теме: Нормативно-правовые основы информационной безопасности в РФ	4
5	Создание презентации по теме: Ответственность за нарушения в сфере информационной безопасности	4

6	Создание сообщения по теме: Принцип иерархии: класс – семейство – компонент – элемент	3
7	Создание кроссворда по теме: Сервисы безопасности в вычислительных сетях	3
8	Создание конспекта по теме: Каналы несанкционированного доступа к информации	3
9	Создание презентации по теме: Вирусы как угроза информационной безопасности	3
10	Создание сообщения по теме: Характеристика "вирусоподобных" программ	4
11	Создание кроссворда по теме: Антивирусные программы	3
12	Создание конспекта по теме: Профилактика компьютерных вирусов	4
13	Создание презентации по теме: Обнаружение загрузочного вируса	3
14	Создание сообщения по теме: Информационная безопасность вычислительных сетей	4
15	Создание кроссворда по теме: Классификация удаленных угроз в вычислительных сетях	4
16	Создание конспекта по теме: Причины успешной реализации удаленных угроз в вычислительных сетях	4
	итого по МДК 03.02	***54***
	МДК.03.03. Эксплуатация систем IP-телефонии	
1	Создание презентации по теме: Основы VoIP. Передача речи по IP-сетям.	4
2	Создание сообщения по теме: Протоколы RTP/RTCP.	4
3	Создание кроссворда по теме: Сети и сценарии IP-телефонии.	4
		4
4	Создание конспекта по теме: Архитектура распределённого шлюза.	5
5	Создание презентации по теме: Назначение основных элементов IMS.	5
6	Создание сообщения по теме: Концепция предоставления услуг в IMS.	4
	итого по МДК 03.03	**30**
	итого по ПМ03	**179**

В соответствии с таблицей 2 самостоятельную работу, выполняемую студентами по специальности 09.02.02 Компьютерные сети по ПМ. 03. «Эксплуатация объектов сетевой инфраструктуры» можно разделить на несколько видов.

Виды самостоятельной работы студентов

Репродуктивная самостоятельная работа	Самостоятельное прочтение, просмотр, конспектирование учебной литературы, прослушивание лекций, просмотр видеоуроков, заучивание, пересказ, запоминание, Интернет-ресурсы, повторение учебного материала и др.

Познавательно-поисковая самостоятельная работа	Подготовка сообщений, докладов, выступлений на семинарских и практических занятиях, подбор литературы по дисциплинарным проблемам, написание рефератов, контрольных, курсовых работ и др.

Творческая самостоятельная работа	Написание рефератов, научных статей, участие в научно-исследовательской работе. Выполнение специальных заданий и др., участие в научной конференции.

Методические рекомендации по выполнению реферата

Внеаудиторная самостоятельная работа в форме реферата является индивидуальной самостоятельно выполненной работой студента.

Содержание реферата.

Реферат, как правило, должен содержать следующие структурные элементы:

1. титульный лист;
2. содержание;
3. введение;
4. основная часть;
5. заключение;
6. список использованных источников;
7. приложения (при необходимости).

Примерный объем в машинописных страницах составляющих реферата представлен в таблице 3.

Таблица 3. Рекомендуемый объем структурных элементов реферата

Наименование частей реферата	Количество страниц
Титульный лист	1
Содержание (с указанием страниц)	1
Введение	2
Основная часть	15-20
Заключение	1-2
Список использованных источников	1-2
Приложения	Без ограничений

В содержании приводятся наименования структурных частей реферата, глав и параграфов его основной части с указанием номера страницы, с которой начинается соответствующая часть, глава, параграф.

Во введении дается общая характеристика реферата:

– обосновывается актуальность выбранной темы;

– определяется цель работы и задачи, подлежащие решению для её достижения;

– описываются объект и предмет исследования, информационная база исследования;

– кратко характеризуется структура реферата по главам.

Основная часть должна содержать материал, необходимый для достижения поставленной цели и задач, решаемых в процессе выполнения реферата. Она включает 2-3 главы, каждая из которых, в свою очередь, делится на 2-3

параграфа. Содержание основной части должно точно соответствовать теме проекта и полностью её раскрывать. Главы и параграфы реферата должны раскрывать описание решения поставленных во введении задач. Поэтому заголовки глав и параграфов, как правило, должны соответствовать по своей сути формулировкам задач реферата. Заголовка «ОСНОВНАЯ ЧАСТЬ» в содержании реферата быть не должно.

Главы основной части реферата могут носить теоретический, методологический и аналитический характер.

Обязательным для реферата является логическая связь между главами и последовательное развитие основной темы на протяжении всей работы, самостоятельное изложение материала, аргументированность выводов. Также обязательным является наличие в основной части реферата ссылок на использованные источники.

Изложение необходимо вести от третьего лица («Автор полагает...») либо использовать безличные конструкции и неопределенно-личные предложения («На втором этапе исследуются следующие подходы…», «Проведенное исследование позволило доказать...» и т.п.).

В заключении логически последовательно излагаются выводы, к которым пришел студент в результате выполнения реферата. Заключение должно кратко характеризовать решение всех поставленных во введении задач и достижение цели реферата.

Список использованных источников является составной частью работы и отражает степень изученности рассматриваемой проблемы. Количество источников в списке определяется студентом самостоятельно, для реферата их рекомендуемое количество от 10 до 20. При этом в списке обязательно должны присутствовать источники, изданные в последние 3 года, а также ныне действующие нормативно-правовые акты, регулирующие отношения, рассматриваемые в реферате.

В приложения следует относить вспомогательный материал, который при включении в основную часть работы загромождает текст (таблицы вспомогательных данных, инструкции, методики, формы документов и т.п.).

Оформление реферата

При выполнении внеаудиторной самостоятельной работы в виде реферата необходимо соблюдать следующие требования:

- на одной стороне листа белой бумаги формата А-4
- размер шрифта-12; Times New Roman, цвет - черный
- междустрочный интервал – 1,5.
- поля на странице – размер левого поля – 2 см, правого – 1 см, верхнего – 2см, нижнего – 2см.
- отформатировано по ширине листа
- на первой странице необходимо изложить план (содержание) работы.
- в конце работы необходимо указать источники использованной литературы

Список использованных источников должен формироваться в алфавитном порядке по фамилии авторов. Литература обычно группируется в списке в такой последовательности:

1. законодательные и нормативно-методические документы и материалы;
2. специальная научная отечественная и зарубежная литература (монографии, учебники, научные статьи и т.п.);
3. статистические, инструктивные и отчетные материалы предприятий, организаций и учреждений.

Включенная в список литература нумеруется сплошным порядком от первого до последнего названия.

По каждому литературному источнику указывается: автор (или группа авторов), полное название книги или статьи, место и наименование издательства (для книг и брошюр), год издания; для журнальных статей указывается наименование журнала, год выпуска и номер. По сборникам трудов (статей) указывается автор статьи, ее название и далее название книги (сборника) и ее выходные данные.

Приложения следует оформлять как продолжение реферата на его последующих страницах.

Каждое приложение должно начинаться с новой страницы. Вверху страницы справа указывается слово «Приложение» и его номер. Приложение должно иметь заголовок, который располагается по центру листа отдельной строкой и печатается прописными буквами.

Приложения следует нумеровать порядковой нумерацией арабскими цифрами.

На все приложения в тексте работы должны быть ссылки. Располагать приложения следует в порядке появления ссылок на них в тексте.

Критерии оценки реферата

Срок сдачи готового реферата определяется утвержденным графиком.

В случае отрицательного заключения преподавателя студент обязан доработать или переработать реферат. Срок доработки реферата устанавливается руководителем с учетом сущности замечаний и объема необходимой доработки.

Реферат оценивается по системе:

Оценка «отлично» выставляется за реферат, который носит исследовательский характер, содержит грамотно изложенный материал, с соответствующими обоснованными выводами.

Оценка «хорошо» выставляется за грамотно выполненный во всех отношениях реферат при наличии небольших недочетов в его содержании или оформлении.

Оценка «удовлетворительно» выставляется за реферат, который удовлетворяет всем предъявляемым требованиям, но отличается поверхностью, в нем просматривается непоследовательность изложения материала, представлены необоснованные выводы.

Оценка «неудовлетворительно» выставляется за реферат, который не носит исследовательского характера, не содержит анализа источников и подходов по выбранной теме, выводы носят декларативный характер.

Студенты, не представивший в установленный срок готовый реферат по дисциплине учебного плана или представивший реферат, который был оценен на «неудовлетворительно», считается имеющим академическую задолженность и не допускается к сдаче экзамена по данной дисциплине (МДК).

Методические рекомендации по подготовке сообщения

Регламент устного публичного выступления – не более 10 минут.

Искусство устного выступления состоит не только в отличном знании предмета речи, но и в умении преподнести свои мысли и убеждения правильно и упорядоченно, красноречиво и увлекательно.

Любое устное выступление должно удовлетворять трем основным критериям, которые в конечном итоге и приводят к успеху: это критерий правильности, т.е. соответствия языковым нормам, критерий смысловой адекватности, т.е. соответствия содержания выступления реальности, и критерий эффективности, т.е. соответствия достигнутых результатов поставленной цели.

Работу по подготовке устного выступления можно разделить на два основных этапа: докоммуникативный этап (подготовка выступления) и коммуникативный этап (взаимодействие с аудиторией).

Работа по подготовке устного выступления начинается с формулировки темы. Лучше всего тему сформулировать таким образом, чтобы ее первое слово обозначало наименование полученного в ходе выполнения проекта научного результата («Модель развития…», «Система управления…», и пр.). Тема выступления не должна быть перегруженной, нельзя «объять необъятное», охват большого количества вопросов приведет к их беглому перечислению, к декларативности вместо глубокого анализа. Неудачные формулировки – слишком длинные или слишком краткие и общие, очень банальные и скучные, не содержащие проблемы, оторванные от дальнейшего текста и т.д.

Само выступление должно состоять из трех частей – вступления (10—15% общего времени), основной части (60—70%) и заключения (20—25%).

Вступление включает в себя представление авторов (фамилия, имя отчество, при необходимости место учебы, статус), название доклада, расшифровку подзаголовка с целью точного определения содержания выступления, четкое определение стержневой идеи. Стержневая идея сообщения понимается как основной тезис, ключевое положение. Стержневая идея дает возможность задать определенную тональность выступлению. Сформулировать основной тезис означает ответить на вопрос, зачем говорить (цель) и о чем говорить (средства достижения цели).

Требования к основному тезису выступления:

– фраза должна утверждать главную мысль и соответствовать цели выступления;

– суждение должно быть кратким, ясным, легко удерживаться в кратковременной памяти;

– мысль должна пониматься однозначно, не заключать в себе противоречия.

В речи может быть несколько стержневых идей, но не более трех.

Самая частая ошибка в начале речи – либо извиняться, либо заявлять о своей неопытности. Результатом вступления должны быть заинтересованность

слушателей (студентов и преподавателя), внимание и расположенность к презентатору и будущей теме.

К аргументации в пользу стержневой идеи проекта можно привлекать фото-, видеофрагметы, аудиозаписи, фактологический материал. Цифровые данные для облегчения восприятия лучше демонстрировать посредством таблиц и графиков, а не злоупотреблять их зачитыванием. Лучше всего, когда в устном выступлении количество цифрового материала ограничено, на него лучше ссылаться, а не приводить полностью, так как обилие цифр скорее утомляет слушателей, нежели вызывает интерес.

План развития основной части должен быть ясным. Должно быть отобрано оптимальное количество фактов и необходимых примеров.

В научном выступлении принято такое употребление форм слов: чаще используются глаголы настоящего времени во «вневременном» значении, возвратные и безличные глаголы, преобладание форм 3-го лица глагола, форм несовершенного вида, используются неопределенно-личные предложения. Перед тем как использовать в своей презентации корпоративный и специализированный жаргон или термины, Вы должны быть уверены, что аудитория поймет, о чем вы говорите.

Если использование специальных терминов и слов, которые часть аудитории может не понять, необходимо, то постарайтесь дать краткую характеристику каждому из них, когда употребляете их в процессе презентации впервые.

Самые частые ошибки в основной части доклада – выход за пределы рассматриваемых вопросов, перекрывание пунктов плана, усложнение отдельных положений речи, а также перегрузка текста теоретическими рассуждениями, обилие затронутых вопросов (декларативность, бездоказательность), отсутствие связи между частями выступления, несоразмерность частей выступления (затянутое вступление, скомканность основных положений, заключения).

В заключении необходимо сформулировать выводы, которые следуют из основной идеи (идей) выступления. Правильно построенное заключение способствует хорошему впечатлению от выступления в целом. В заключении имеет смысл повторить стержневую идею и, кроме того, вновь (в кратком виде) вернуться к тем моментам основной части, которые вызвали интерес слушателей. Закончить выступление можно решительным заявлением. Вступление и заключение требуют обязательной подготовки, их труднее всего создавать на ходу. Психологи доказали, что лучше всего запоминается сказанное в начале и в конце сообщения («закон края»), поэтому вступление должно привлечь внимание слушателей, заинтересовать их, подготовить к восприятию темы, ввести в нее (не вступление важно само по себе, а его соотнесение с остальными частями), а заключение должно обобщить в сжатом виде все сказанное, усилить и сгустить основную мысль, оно должно быть таким, «чтобы слушатели почувствовали, что дальше говорить нечего» (А.Ф. Кони).

В ключевых высказываниях следует использовать фразы, программирующие заинтересованность. Вот некоторые обороты, способствующие повышению интереса:

- «Это Вам позволит…»
- «Благодаря этому вы получите…»
- «Это позволит избежать…»
- «Это повышает Ваши…»
- «Это дает Вам дополнительно…»
- «Это делает вас…»
- «За счет этого вы можете…»

После подготовки текста / плана выступления полезно проконтролировать себя вопросами:

- Вызывает ли мое выступление интерес?
- Достаточно ли я знаю по данному вопросу, и имеется ли у меня достаточно данных?
- Смогу ли я закончить выступление в отведенное время?
- Соответствует ли мое выступление уровню моих знаний и опыту?

При подготовке к выступлению необходимо выбрать способ выступления: устное изложение с опорой на конспект (опорой могут также служить заранее подготовленные слайды) или чтение подготовленного текста. Отмечу, однако, что чтение заранее написанного текста значительно уменьшает влияние выступления на аудиторию. Запоминание написанного текста заметно сковывает выступающего и привязывает к заранее составленному плану, не давая возможности откликаться на реакцию аудитории.

Общеизвестно, что бесстрастная и вялая речь не вызывает отклика у слушателей, какой бы интересной и важной темы она ни касалась. И наоборот, иной раз даже не совсем складное выступление может затронуть аудиторию, если оратор говорит об актуальной проблеме, если аудитория чувствует компетентность выступающего. Яркая, энергичная речь, отражающая увлеченность оратора, его уверенность, обладает значительной внушающей силой.

Кроме того, установлено, что короткие фразы легче воспринимаются на слух, чем длинные. Лишь половина взрослых людей в состоянии понять фразу, содержащую более тринадцати слов. А третья часть всех людей, слушая четырнадцатое и последующие слова одного предложения, вообще забывают его начало. Необходимо избегать сложных предложений, причастных и деепричастных оборотов. Излагая сложный вопрос, нужно постараться передать информацию по частям.

Пауза в устной речи выполняет ту же роль, что знаки препинания в письменной. После сложных выводов или длинных предложений необходимо сделать паузу, чтобы слушатели могли вдуматься в сказанное или правильно понять сделанные выводы. Если выступающий хочет, чтобы его понимали, то не следует говорить без паузы дольше, чем пять с половиной секунд (!).

Особое место в подготовке сообщения занимает обращение к аудитории.

Известно, что обращение к собеседнику по имени создает более доверительный контекст деловой беседы. При публичном выступлении также можно использовать подобные приемы. Так, косвенными обращениями могут служить такие выражения, как «Как Вам известно», «Уверен, что Вас это не оставит равнодушными». Подобные доводы к аудитории – это своеобразные высказывания, подсознательно воздействующие на волю и интересы слушателей. Выступающий показывает, что слушатели интересны ему, а это самый простой путь достижения взаимопонимания.

Во время выступления важно постоянно контролировать реакцию слушателей. Внимательность и наблюдательность в сочетании с опытом позволяют оратору уловить настроение публики. Возможно, рассмотрение некоторых вопросов придется сократить или вовсе отказаться от них. Часто удачная шутка может разрядить атмосферу.

После выступления нужно быть готовым к ответам на возникшие у аудитории вопросы.

Методические рекомендации по составлению конспекта.

Конспект – краткое изложение существенного содержания чего-либо.

Для того чтобы написать конспект:

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 выразить мысль 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.

Методические рекомендации по выполнению сравнительного анализа

Одной из форм самостоятельной работы студентов является проведение сравнительного анализа по исследованному материалу изучаемого МДК.

Преподавателем прилагается методика формирования сравнительного анализа. Данный метод определяется как частично поисковый, т.е. часть материала по проведению анализа определяется преподавателем, а другая часть материала подбирается самим студентом.

Студент, применяя рекомендации, рассматривает выявленный научно-практический и учебный материал с позиции анализа для формирования своей внеаудиторной работы. Кроме этого данный метод является репродуктивным, т.е. способствующим формированию монологического высказывания студента, определяющего основные моменты, принципы и способы, послужившие основанием для формирования анализа, а в дальнейшем для его представления или защиты.

Зачастую сравнительный анализ выполняется в виде таблицы (сравнительной таблицы).

Самостоятельно и индивидуально каждый из студентов выявляет на основе анализа теоретического материала необходимые и достаточные для заполнения сравнительной таблицы сведения.

Педагогическая ценность подобной работы студентов заключается в обеспечении развития мышления, самостоятельности и активности студента, при максимальной индивидуализации задания, с учетом психофизиологических особенностей студентов. Работа каждого из студентов оценивается преподавателем с позиции логического и образного мышления.

При проведении сравнительного анализа студент для осуществления самостоятельной работы имеет только объекты сравнения, а выявление сходства и различия определяется им самим. Используя учебно-практическое пособие по дисциплине, МДК (если такое имеется), литературу, рекомендованную преподавателем, студент выявляет характерные признаки, черты или виды, дающие возможность рассмотреть объекты как схожие с одной стороны, и различные, с другой.

Метод сравнительного анализа используется в качестве выполнения самостоятельной работы и заполнение тезисных таблиц.

Тезисные таблицы предпочтительны по той причине, что они не только дают впоследствии возможность восстановить содержание и главные моменты изучаемого учебного материала, выделить в нем главное, но также обеспечивают возможность определения их взаимосвязи друг с другом, или сравнения. При этом главные моменты усваиваются намного быстрее, нежели в конспектах. Кроме того, при желании эти главные моменты могут быть поставлены в виде ключевых вопросов для развёрнутого ответа на них своими словами. Наконец, тезисная таблица – самая простая в составлении, что немаловажно в условиях дефицита времени для полных записей студентами.

Завершение выполнения сравнительного анализа рассматривается преподавателем как контроль полученных студентом знаний. Для получения оценки преподавателем определяются соответствующие критерии:

- выполнение работы на уровне распознавания – знакомство: низкое
- качество;
- выполнение работы на уровне запоминания (чтение, пересказ, воспроизведение изученного материала через схему, таблицу, но в полной мере не может воспользоваться результатами своей работы): удовлетворительное качество;
- выполнение работы на уровне понимания, т. е. студент, используя краткую запись в схеме или таблице способен осуществить процесс нахождения существенных исследуемых объектов, выделение из всей массы несущественного и случайного, установления сходства и различий - в конечном итоге сопоставление полученной информации с имеющимися знаниями: хорошее качество;
- использование полученных знаний при выполнении иных заданий по теме, решение типовых практических задач или тестов, творческое применение полученных знаний: отличное качество.

Методические рекомендации по подготовке презентации

Компьютерную презентацию, сопровождающую выступление докладчика, удобнее всего подготовить в программе MS Power Point. Презентация как документ представляет собой последовательность сменяющих друг друга слайдов – то есть электронных страничек, занимающих весь экран монитора (без присутствия панелей программы). Чаще всего демонстрация презентации проецируется на большом экране, реже – раздается собравшимся как печатный материал. Количество слайдов адекватно содержанию и продолжительности выступления (например, для 5-минутного выступления рекомендуется использовать не более 10 слайдов).

На первом слайде обязательно представляется тема выступления и сведения об авторах. Следующие слайды можно подготовить, используя две различные стратегии их подготовки:

1 стратегия: на слайды выносится опорный конспект выступления и ключевые слова с тем, чтобы пользоваться ими как планом для выступления. В этом случае к слайдам предъявляются следующие требования:

- объем текста на слайде – не больше 7 строк;
- маркированный/нумерованный список содержит не более 7 элементов;
- отсутствуют знаки пунктуации в конце строк в маркированных и нумерованных списках;
- значимая информация выделяется с помощью цвета, кегля, эффектов анимации.

Особо внимательно необходимо проверить текст на отсутствие ошибок и опечаток. Основная ошибка при выборе данной стратегии состоит в том, что выступающие заменяют свою речь чтением текста со слайдов.

2 стратегия: на слайды помещается фактический материал (таблицы, графики, фотографии и пр.), который является уместным и достаточным средством наглядности, помогает в раскрытии стержневой идеи выступления. В этом случае к слайдам предъявляются следующие требования:

- выбранные средства визуализации информации (таблицы, схемы, графики и т. д.) соответствуют содержанию;
- использованы иллюстрации хорошего качества (высокого разрешения), с четким изображением (как правило, никто из присутствующих не заинтересован вчитываться в текст на ваших слайдах и всматриваться в мелкие иллюстрации);

Максимальное количество графической информации на одном слайде – 2 рисунка (фотографии, схемы и т.д.) с текстовыми комментариями (не более 2 строк к каждому). Наиболее важная информация должна располагаться в центре экрана.

Основная ошибка при выборе данной стратегии – «соревнование» со своим иллюстративным материалов (аудитории не предоставляется достаточно времени, чтобы воспринять материал на слайдах). Обычный слайд, без эффектов анимации должен демонстрироваться на экране не менее 10—15

секунд. За меньшее время присутствующие не успеет осознать содержание слайда. Если какая-то картинка появилась на 5 секунд, а потом тут же сменилась другой, то аудитория будет считать, что докладчик ее подгоняет. Обратного (позитивного) эффекта можно достигнуть, если докладчик пролистывает множество слайдов со сложными таблицами и диаграммами, говоря при этом «Вот тут приведен разного рода *вспомогательный* материал, но я его хочу пропустить, чтобы не перегружать выступление подробностями». Правда, такой прием делать в *начале* и в *конце* презентации – рискованно, оптимальный вариант – в середине выступления.

Если на слайде приводится сложная диаграмма, ее необходимо предварить вводными словами (например, «На этой диаграмме приводится то-то и то-то, зеленым отмечены показатели А, синим – показатели Б»), с тем, чтобы дать время аудитории на ее рассмотрение, а только затем приступать к ее обсуждению. Каждый слайд, в среднем должен находиться на экране не меньше 40 – 60 секунд (без учета времени на случайно возникшее обсуждение). В связи с этим лучше настроить презентацию не на автоматический показ, а на смену слайдов самим докладчиком.

Особо тщательно необходимо отнестись к *оформлению презентации*. Для всех слайдов презентации по возможности необходимо использовать один и тот же шаблон оформления, кегль – для заголовков – не меньше 24 пунктов, для информации – для информации не менее 18. В презентациях не принято ставить переносы в словах.

Подумайте, не отвлекайте ли вы слушателей своей же презентацией? Яркие краски, сложные цветные построения, излишняя анимация, выпрыгивающий текст или иллюстрация – не самое лучшее дополнение к научному докладу. Также нежелательны звуковые эффекты в ходе демонстрации презентации. Наилучшими являются контрастные цвета фона и текста (белый фон – черный текст; темно-синий фон – светло-желтый текст и т. д.). Лучше не смешивать разные типы шрифтов в одной презентации. Рекомендуется не злоупотреблять прописными буквами (они читаются хуже).

Неконтрастные слайды будут смотреться тусклыми и невыразительными, особенно в светлых аудиториях. Для лучшей ориентации в презентации по ходу выступления лучше пронумеровать слайды. Желательно, чтобы на слайдах оставались поля, не менее 1 см с каждой стороны. Вспомогательная информация (управляющие кнопки) не должны преобладать над основной информацией (текстом, иллюстрациями). Использовать встроенные эффекты анимации можно только, когда без этого не обойтись (например, последовательное появление элементов диаграммы). Для акцентирования внимания на какой-то конкретной информации слайда можно воспользоваться лазерной указкой.

Диаграммы готовятся с использованием мастера диаграмм табличного процессора MS Excel. Для ввода числовых данных используется числовой формат с разделителем групп разрядов. Если данные (подписи данных) являются дробными числами, то число отображаемых десятичных знаков должно быть одинаково для всей группы этих данных (всего ряда подписей

данных). Данные и подписи не должны накладываться друг на друга и сливаться с графическими элементами диаграммы. Структурные диаграммы готовятся при помощи стандартных средств рисования пакета MSOffice. Если при форматировании слайда есть необходимость пропорционально уменьшить размер диаграммы, то размер шрифтов реквизитов должен быть увеличен с таким расчетом, чтобы реальное отображение объектов диаграммы соответствовало значениям, указанным в таблице. В таблицах не должно быть более 4 строк и 4 столбцов — в противном случае данные в таблице будет просто невозможно увидеть. Ячейки с названиями строк и столбцов и наиболее значимые данные рекомендуется выделять цветом.

Табличная информация вставляется в материалы как таблица текстового процессора MSWord или табличного процессора MS Excel. При вставке таблицы как объекта и пропорциональном изменении ее размера реальный отображаемый размер шрифта должен быть не менее 18 pt. Таблицы и диаграммы размещаются на светлом или белом фоне.

Если Вы предпочитаете воспользоваться помощью оператора (что тоже возможно), а не листать слайды самостоятельно, очень полезно предусмотреть ссылки на слайды в тексте доклада («Следующий слайд, пожалуйста...»).

Заключительный слайд презентации, содержащий текст «Спасибо за внимание» или «Конец», вряд ли приемлем для презентации, сопровождающей публичное выступление, поскольку завершение показа слайдов еще не является завершением выступления. Кроме того, такие слайды, так же как и слайд «Вопросы?», дублируют устное сообщение. Оптимальным вариантом представляется повторение первого слайда в конце презентации, поскольку это дает возможность еще раз напомнить слушателям тему выступления и имя докладчика и либо перейти к вопросам, либо завершить выступление.

Для показа файл презентации необходимо сохранить в формате «Демонстрация Power Point» (Файл — Сохранить как — Тип файла — Демонстрация Power Point). В этом случае презентация автоматически открывается в режиме полноэкранного показа (slideshow) и слушатели избавлены как от вида рабочего окна программы Power Point, так и от потерь времени в начале показа презентации.

После подготовки презентации полезно проконтролировать себя вопросами:

- удалось ли достичь конечной цели презентации (что удалось определить, объяснить, предложить или продемонстрировать с помощью нее?);
- к каким особенностям объекта презентации удалось привлечь внимание аудитории?
- не отвлекает ли созданная презентация от устного выступления?
- После подготовки презентации необходима репетиция выступления.

Критерии оценки презентации

Критерии оценки	Содержание оценки
Содержательный критерий	правильный выбор темы, знание предмета и свободное владение текстом, грамотное использование научной терминологии, импровизация, речевой этикет
Логический критерий	стройное логико-композиционное построение речи, доказательность, аргументированность
Речевой критерий	использование языковых (метафоры, фразеологизмы, пословицы, поговорки и т.д.) и неязыковых (поза, манеры и пр.) средств выразительности; фонетическая организация речи, правильность ударения, четкая дикция, логические ударения и пр.
Психологический критерий	взаимодействие с аудиторией (прямая и обратная связь), знание и учет законов восприятия речи, использование различных приемов привлечения и активизации внимания
Критерий соблюдения дизайн-эргономических требований к компьютерной презентации	соблюдены требования к первому и последним слайдам, прослеживается обоснованная последовательность слайдов и информации на слайдах, необходимое и достаточное количество фото- и видеоматериалов, учет особенностей восприятия графической (иллюстративной) информации, корректное сочетание фона и графики, дизайн презентации не противоречит ее содержанию, грамотное соотнесение устного выступления и компьютерного сопровождения, общее впечатление от мультимедийной презентации

Методические рекомендации по подготовке кроссворда

КРОССВОРД – игра-задача, в которой фигура из рядов пустых клеток заполняется перекрещивающимися словами со значениями, заданными по условиям игры. Для составления кроссворда по заданной теме нужно найти информацию с разных источников (сеть Internet, энциклопедии, практические пособия, учебная литература), изучить ее и составить в рукописном варианте или пользуясь одним из программных средств: Microsoft Word, Microsoft Excel. Кроссворд составляется индивидуально. Работа должна быть представлена на бумаге формата А4 в печатном (компьютерном) или рукописном варианте. Выполненную работу сдать к указанному сроку.

Правила при составлении кроссвордов

1. Не допускается наличие "плашек" (незаполненных клеток) в сетке кроссворда.
2. Не допускаются случайные буквосочетания и пересечения.
3. Загаданные слова должны быть именами существительными в именительном падеже единственного числа.
4. Двухбуквенные слова должны иметь два пересечения.
5. Трехбуквенные слова должны иметь не менее двух пересечений.
6. Не допускаются аббревиатуры, сокращения.
7. Не рекомендуется большое количество двухбуквенных слов.
8. Все тексты должны быть написаны разборчиво, желательно отпечатаны.
9. На каждом листе должна быть фамилия автора, а также название данного кроссворда.

Требования к оформлению кроссворда:

Рисунок кроссворда должен быть четким.

1. Сетка кроссворда должна быть пустой только с цифрами позиций слов-ответов.

2. Ответы на кроссворд публикуются на отдельном листе. Ответы предназначены для проверки правильности решения кроссворда и дают возможность ознакомиться с правильными ответами на нерешенные позиции условий.

3. Объем работы: 4 листа, нумерация страниц – снизу, справа;

1 лист – титульный,
2 лист – сетка кроссворда (без ответов),
3 лист – вопросы,
4 лист – ответы и используемые источники.

Создание кроссворда в MS Word.

1. Создание сетки графическим методом; при этом все элементы должны быть сгруппированы.

2. Создание сетки табличным методом; при этом границы ненужных ячеек стираются.

3. Номера либо вставляют непосредственно в ячейки, либо записывают рядом с соответствующими ячейками.

4. Задания к кроссворду могут быть расположены обычным способом или оформлены в виде выносок к соответствующим клеткам.

5. Задания к кроссворду должны быть грамотно сформулированы.

6. Кроссворд на странице должен быть наглядно оформлен и правильно расположен.

Создание кроссворда в Microsoft Excel.

1. Сетка кроссворда создается путем обозначения границ ячеек и настройки их ширины и высоты таким образом, чтобы они получились квадратными.

2. Задания к кроссворду могут быть расположены обычным образом или оформлены в виде примечаний к ячейкам, в которых находится нумерация.

3. Проверка правильности разгадывания кроссворда может быть осуществлена с помощью условного форматирования (например, если в ячейку введена правильная цифра, то ячейка заливается определенным цветом).

4. Задания к кроссворду должны быть грамотно сформулированы.

5. Кроссворд на рабочем листе должен быть наглядно оформлен и правильно расположен.

6. Наличие проверки правильности решения кроссворда.

Планирование деятельности по составлению кроссворда.

1. Определить, с какой целью составляется кроссворд.
2. Просмотреть и изучить лексико-грамматический материал по теме в учебнике.
3. Просмотреть и выбрать вид кроссворда.
4. Продумать составные части кроссворда.
5. Изучить дополнительный материал по теме.
6. Продумать критерии оценивания.
7. Составить список слов раздельно по направлениям.
8. Написать условия (текст) кроссворда.
9. Проверить орфографию текста, соответствие нумерации.
10. Проанализировать составленный кроссворд согласно критериям оценивания.
11. Оформить готовый кроссворд.
12. Продумать защиту проекта-кроссворда

Тематика и задания самостоятельной работы

МДК 03.01 Эксплуатация объектов сетевой инфраструктуры

Виртуальные частные сети
(подготовка сообщения)

План:

1. Уровни VPN
2. Структура VPN
3. Классификация VPN
4. Примеры VPN

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
3. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
4. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
5. https://ru.wikipedia.org
6. http://rus-linux.net
7. http://www.ietf.org/rfc/rfc2764.txt
8. http://www.nestor.minsk.by/sr/2005/03/050315.html

Адресация в IP –сетях
(мультимедийная презентация)

План:

1. Задачи IP-адресации
2. Структура IP-адреса
3. Части IP-адреса
4. Взаимодействие IP-адресов и масок подсети
5. Типы IP-адресов

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.

3. http://habrahabr.ru
4. http://rfc2.ru
5. http://www.ip-ping.ru/

Взаимодействие между разнородными сетями
(мультимедийная презентация)

План:

1. Понятие основного шлюза
2. Границы сети и пространство адресов
3. Присвоение адресов
4. Преобразование сетевых адресов

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. https://ru.wikipedia.org
4. http://ubuntu.ru
5. http://habrahabr.ru
6. http://rus-linux.net
7. http://www.linuxsecurity.com
8. http://www.softpile.ru/TCPIP4.html

Сети на основе сервера. Кластеризация сервера
(подготовка сообщения)

План:

1. Понятие сети на основе сервера
2. Вычислительные кластеры
3. Кластер серверов
4. Самые высокопроизводительные кластеры
5. Программные средства для межсерверного взаимодействия

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.

4. Компьютерные сети. Сертификация Network. Учебный курс/Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
5. https://ru.wikipedia.org
6. http://ubuntu.ru
7. http://habrahabr.ru
8. http://rus-linux.net
9. http://www.linuxsecurity.com
10. http://www.softpile.ru/TCPIP4.html

Настройка сети в Windows Vista
(подготовка инструкции)

План:

1. Составить инструкцию по изменению имени рабочей группы
2. Составить инструкцию по предоставлению общего доступа
3. Составить инструкцию по назначению ip адресов

Форма контроля:

- проверка инструкции в тетради;
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
4. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
5. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
6. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
7. Компьютерные сети. Сертификация Network. Учебный курс/Пер. англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
8. https://ru.wikipedia.org
9. http://ubuntu.ru
10. http://habrahabr.ru
11. http://rus-linux.net
12. http://www.linuxsecurity.com
13. http://www.softpile.ru/TCPIP4.html
14. http://www.microsoft.com/

Операционная система UNIX
(мультимедийная презентация)

План:

1. История развития Unix
2. Особенности ОС Unix
3. Архитектурные особенности ОС Unix
4. Стандартные команды ОС Unix

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
2. Робачевский А. М., Немнюгин С. А., Стесик О. Л. Операционная система UNIX. — 2-е изд. — СПб.: БХВ-Петербург, 2010.
3. Роберт Шимонски. Освой самостоятельно Unix. 10 минут на урок = Sams Teach Yourself Unix in 10 Minutes. — М.: «Вильямс», 2006.
4. Эрик С. Реймонд. Искусство программирования для Unix = Art of Unix Programming. — М.: «Вильямс», 2005.
5. Роббинс А. Unix. Справочник. Пер. с англ. 4-е издание. — "КУДИЦ-ПРЕСС", 2007.
6. http://ubuntu.ru
7. http://habrahabr.ru
8. http://rus-linux.net
9. http://www.linuxsecurity.com
10. http://www.softpile.ru/TCPIP4.html

Apple Talk
(мультимедийная презентация)

План:

1. Основы технологии
2. Доступ к среде
3. Сетевой уровень
4. Транспортный уровень

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. https://ru.wikipedia.org
3. http://citforum.ru/nets/ito/16.shtml

Операционная система Banyan VINES
(подготовка сообщения)

План:

1. Основы технологии
2. Доступ к среде
3. Протокол VIP
4. Протокол RTR
5. Протокол разрешения адресов ARP
6. Протокол ICP

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. https://ru.wikipedia.org
4. http://citforum.ru/nets/ito/21.shtml
5. http://www.osp.ru/nets/1997/08/142728/
6. http://v-ps.ru/it/studying/os-net/glava_45.htm

Доменная система имен (DNS)
(подготовка кроссворда)

План:

1. изучить информацию по теме
2. создать графическую структуру, вопросы и ответы к ним

Форма контроля:

- защита кроссворда на учебном занятии,

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. https://ru.wikipedia.org
5. http://habrahabr.ru
6. http://rfc2.ru

Топология коммутации пакетов и ретрансляция кадра (Frame Relay)
(подготовка сообщения)

План:

1. Формат кадра

2. Виртуальные каналы
3. CIR и EIR

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Хендерсон Л., Дженкинс Т. Frame Relay. Межсетевое взаимодействие. – М.: Горячая Линия – Телеком, 2002
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
3. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
4. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
5. https://ru.wikipedia.org

Современные проблемы управления ИТ- инфраструктурой (мультимедийная презентация)

План:

1. Бесперебойная работа
2. Масштабируемость
3. Безопасность
4. Уровень сервиса
5. Прозрачность и управляемость
6. Адекватная стоимость владения

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
5. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
6. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
7. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
8. https://ru.wikipedia.org

9. http://habrahabr.ru
10. http://ntv.ifmo.ru/file/article/17.pdf

Средства продуктов Unicenter для управления ИТ- инфраструктурой (подготовка реферата)

Цели:

- получить более глубокие знания по данной теме;
- закрепить навыки пользования дополнительной литературой;
- научиться составлять и оформлять рефераты.

Порядок выполнения работы

1. Изучить дополнительную литературу по данной теме.
2. Изучить правила выполнения реферативных работ.
3. Подготовить реферат
4. Оформить реферат в соответствии со всеми требованиями и сдать для проверки в установленные сроки.

Контрольные вопросы:

1. Подчинение Internet
2. Повышение качества работы сервисной службы
3. Обеспечение безопасности предприятия
4. Обеспечение интеллектуального управления сетями
5. Простота управления настольными системами и серверами
6. Системные агенты
7. Управление приложениями
8. Защита данных от аварийных ситуаций
9. Поддержка популярных СУБД
10. Достижение максимальной эффективности работы

Форма контроля:

- проверка рефератов;
- заслушивание лучших рефератов на занятии;

Литература и интернет ресурс:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
5. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
6. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002

7. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
8. http://habrahabr.ru
9. http://www.interface.ru/home.asp?artId=4589
10.http://ru.wikipedia.org

«Комплекс программных продуктов Hewlet – Packard ориентированных на управление корпоративными ИТ любого масштаба (подготовка сравнительной таблицы)

План:

1. Ознакомиться с комплексом программных продуктов HP для управления IT
2. Заполнить таблицу

Отрасль	Обзор	Продукты	Решения	Ресурсы

Форма контроля:

- проверка тетради;

Литература и интернет ресурс:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
5. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
6. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
7. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
8. http://ru.wikipedia.org/
9. http://h17007.www1.hp.com/ru/ru/products/index.aspx

Основные назначения средств Microsoft Systems Management Server
(подготовка сообщения)

План:

1. История версий
2. System Center Configuration Manager
3. Configuration Manager Service Pack 1
4. Configuration Manager R2
5. Архитектура System Center Configuration Manager

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
5. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
6. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
7. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
8.https://ru.wikipedia.org
9. http://www.microsoft.com/ru-ru/server-cloud/products/system-center-2012-r2-configuration-manager/default.aspx

Основные назначения средств Microsoft Operations Manager
(мультимедийная презентация)

План:

1. Обзор программы
2. Архитектура программы
3. Версии продукта

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
5. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
6. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
7. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
8. https://ru.wikipedia.org
9. http://technet.microsoft.com/en-us/library/hh205987.aspx

Использование утилиты Acronis для изучения безопасной зоны Acronis (мультимедийная презентация)

План:

1. Обзор продуктов компании Acronis
2. Описание зоны безопасности Acronis
3. Создание безопасной зоны Acronis
4. Удаление безопасной зоны Acronis
5. Активация функции восстановление при загрузке
6. Просмотр и редактирование зоны безопасности Acronis

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. http://www.timosh.ru/safety-zone-acronis-.html
3. http://www.acronis.com/ru-ru/support/documentation/ABR11/index.html#14080.html
4. https://ru.wikipedia.org
5. http://ubuntu.ru
6. http://habrahabr.ru

Создание контрольной точки восстановления с помощью Acronis
(подготовка сообщения)

План:

1. Обзор программы Acronis True Image Home
2. Создание образа диска (контрольная точка)
3. Восстановление образа диска (контрольной точки)
4. Восстановление образа на компьютерах с разным аппаратным обеспечением

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологиии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. http://www.acronis.com/ru-ru/support/documentation/ATI2015/index.html#16986.html
3. https://ru.wikipedia.org
4. http://ubuntu.ru
5. http://habrahabr.ru

План восстановления работоспособности сети на примере одной взятой организации
(мультимедийная презентация)

План:

1. Выбор организации для восстановления (образовательная, коммерческая, политическая, оборонная)
2. Разработка плана восстановления организации
3. Использование модели OSI для восстановления работоспособности
4. Методика устранения неисправностей
5. Инструменты для восстановления неисправности

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. — М: Радио и связь, 2002.
5. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.

6. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
7. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
8. Роббинс А. Unix. Справочник. Пер. с англ. 4-е издание. — "КУДИЦ-ПРЕСС", 2007.
9. https://ru.wikipedia.org
10. http://ubuntu.ru
11. http://habrahabr.ru
12. http://rus-linux.net
13. http://www.linuxsecurity.com
14. http://www.softpile.ru/TCPIP4.html

Поиск неисправностей по принципу локализации неисправностей конкретного оборудования
(подготовка инструкции)

План:

1. Подготовить инструкцию по поиску неисправностей 1 и 2 уровня модели OSI
2. Подготовить инструкцию по устранению неполадок оборудования в процессе загрузки
3. Подготовить инструкцию по диагностике ошибок кабелей и портов
4. Подготовить инструкцию по поиску неисправных соединений LAN
5. Подготовить инструкцию по поиск неисправных соединений WAN
6. Подготовить инструкцию по поиск неисправностей на уровне 3

Форма контроля:

- проверка инструкции в тетради;
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Виснадул Б.Н. Основы компьютерных сетей: учебное пособие. – М.: ИД Форум: Инфра – М, 2007.
3. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
4. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
5. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
6. Робачевский А. М., Немнюгин С. А., Стесик О. Л. Операционная система UNIX. — 2-е изд. — СПб.: БХВ-Петербург, 2010.

7. Роберт Шимонски. Освой самостоятельно Unix. 10 минут на урок = Sams Teach Yourself Unix in 10 Minutes. — М.: «Вильямс», 2006.
8. Эрик С. Реймонд. Искусство программирования для Unix = Art of Unix Programming. — М.: «Вильямс», 2005.
9. Роббинс А. Unix. Справочник. Пер. с англ. 4-е издание. — "КУДИЦ-ПРЕСС", 2007.
10. https://ru.wikipedia.org
11. http://ubuntu.ru
12. http://habrahabr.ru
13. http://rus-linux.net

Принцип работы новых контрольно-измерительных аппаратов (подготовка сообщения)

План:

1. Обзор новейших контрольно-измерительных аппаратов компьютерных сетей
2. Принцип работы кабельных тестеров
3. Принцип работы кабельных сертификаторов
4. Принцип работы мультиметров

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. - 4 - е изд. - СПб.: Питер, 2011.
2. Кульгин М. Технологии корпоративных сетей. Энциклопедия. — СПб.: Питер, 2000.
3. Компьютерные сети. Сертификация Network. Учебный курс/Пер.с англ. — М.: Издательско-торговый дом «Русская Редакция», 2002
4. Эви Немет, Гарт Снайдер, Трент Хейн, Бэн Уэйли. Unix и Linux: руководство системного администратора, 4-е издание = Unix and Linux System Administration Handbook, 4ed. — М.: «Вильямс», 2011.
5. https://ru.wikipedia.org
6. http://ubuntu.ru
7. http://habrahabr.ru
8. http://rus-linux.net
9. http://citforum.ru/nets/optimize/locnop_07.shtml

МДК 03.02. Безопасность функционирования информационных систем

Понятие "информационная безопасность" (ИБ)
(подготовка презентации)

План:

1. Исторические аспекты возникновения ИБ
2. Стандартизированные определения
3. Признаки понятия
4. Объем понятия ИБ
5. Нормативные документы в области ИБ

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002.
2. Галатенко В. А. Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий, 2006.
3. Гафнер В.В. Информационная безопасность: учеб. пособие. – Ростов на Дону: Феникс, 2010.
4. https://ru.wikipedia.org
5. http://habrahabr.ru

Составляющие информационной безопасности
(подготовка сообщения)

План:

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008
2. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
3. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
4. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000.

5. https://ru.wikipedia.org
6. http://habrahabr.ru

Задачи информационной безопасности общества (подготовка кроссворда)

План:

1. изучить информацию по теме
    1. секретность (privacy, confidentiality, secrecy);
    2. целостность (data integrity);
    3. идентификация (identification);
    4. аутентификация (data origin, authentication);
    5. уполномочивание (authorization);
    6. контроль доступа (access control);
    7. право собственности (ownership);
    8. сертификация (certification); О подпись (signature);
    9. неотказуемость (non-repudiation);
    10. датирование (time stamping);
    11. расписка в получении (receipt);
    12. аннулирование (annul);
    13. анонимность (anonymity);
    14. свидетельствование (witnessing);
    15. подтверждение (confirmation);
    16. ратификация (validation).
2. создать графическую структуру, вопросы и ответы к ним

Форма контроля:

- защита кроссворда на учебном занятии,

Литература и интернет ресурсы:

1. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002.
2. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
3. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000.
4. Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации. (Гриф УМО по классическому университетскому образованию). Изд.2 М.: Книжный дом «ЛИБРОКОМ», 2013.
5. Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.
6. https://ru.wikipedia.org
7. http://www.des-crypto.ru/itsecur/quest/

Нормативно-правовые основы информационной безопасности в РФ
(подготовка конспекта)

План:

1. Состояние нормативного правового обеспечения Информационной Безопасности
2. Нормативно правовое регулирование направлений Информационной Безопасности
3. Основные направления совершенствования нормативного правового обеспечения Информационной Безопасности РФ

Форма контроля:

- проверка конспекта
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000.
2. Малюк А.А. Теория защиты информации. — М.: Горячая линия - Телеком, 2012.
3. Жданов О. Н., Чалкин В. А. Эллиптические кривые: Основы теории и криптографические приложения. М.: Книжный дом «ЛИБРОКОМ», 2013.
4. Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации. (Гриф УМО по классическому университетскому образованию). Изд.2 М.: Книжный дом «ЛИБРОКОМ», 2013.
5. https://ru.wikipedia.org
6. http://www.des-crypto.ru
7. http://asher.ru/security/book/its

Ответственность за нарушения в сфере информационной безопасности
(подготовка презентации)

План:

1. Неправомерный доступ к компьютерной информации (ст. 272)
2. Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273)
3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274)

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
2. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.

3. Борисов М. А. Особенности защиты персональных данных в трудовых отношениях. (Гриф УМО по дополнительному профессиональному образованию) М.: Книжный дом «ЛИБРОКОМ», 2013.
4. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). №2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014.
5. https://ru.wikipedia.org
6. http://avoidance.ru/articles/osnovy-obespechenija-informacionnoj-bezopasnosti/99-otvetstvennost-za-prestuplenija-v-oblasti-informatsionnyh-tehnologij.html

Принцип иерархии: класс – семейство – компонент – элемент (подготовка сообщения)

План:

1. Понятие критериев ИБ
2. Предложения безопасности
3. Требования к безопасности
4. Угрозы безопасности
5. Иерархия класс-семейство-компонент-элемент

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
2. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000.
3. Малюк А.А. Теория защиты информации. — М.:Горячая линия - Телеком, 2012.
4. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008.
5. Петренко С. А., Курбатов В. А. Политики информационной безопасности.
6. http://www.intuit.ru/studies/courses/30/30/lecture/937?page=2

Сервисы безопасности в вычислительных сетях (подготовка кроссворда)

План:

1. изучить информацию по теме
2. создать графическую структуру, вопросы и ответы к ним

Форма контроля:

- защита кроссворда на учебном занятии,

Литература и интернет ресурсы:

1. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
2. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
3. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004.
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
6. Борисов М. А. Особенности защиты персональных данных в трудовых отношениях. (Гриф УМО по дополнительному профессиональному образованию) М.: Книжный дом «ЛИБРОКОМ», 2013.
7. https://ru.wikipedia.org
8. http://habrahabr.ru
9. http://www.des-crypto.ru

Каналы несанкционированного доступа к информации (подготовка конспекта)

План:

1. Установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации;
2. Организация физического проникновения к носителям конфиденциальной информации;
3. Подключение к средствам отображение, хранения, обработки, воспроизведения и передачи информации средствам связи;
4. Прослушивание речевой конфиденциальной информации;
5. Визуальный съем конфиденциальной информации;
6. Перехват электромагнитных излучений;
7. Исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации;
8. Изучение доступных источников информации;

Форма контроля:

- проверка конспекта
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008

2. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
3. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008.
4. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006.
5. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004.
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
7. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
8. Применко Э. А. Алгебраические основы криптографии. №9. Изд. стереотип. М.: Книжный дом «ЛИБРОКОМ», 2014.
9. Гуров С. И. Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. Изд.2. М.: Книжный дом «ЛИБРОКОМ», 2013.
10. Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.
11. https://ru.wikipedia.org
12. http://www.life-prog.ru/1_6615_kanali-nesanktsionirovannogo-dostupa-k-informatsii.html

Вирусы как угроза информационной безопасности (подготовка презентации)

План:

1. Классификация компьютерных вирусов
   1.1. Загрузочные вирусы
   1.2. Файловые вирусы
   1.3. Сетевые вирусы
   1.4. Макро-вирусы
   1.5. Резидентные вирусы
   1.6. Нерезидентные вирусы

Форма контроля:

- защита презентации на учебном занятии

Литература и интернет ресурсы:

1. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
2. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.

4. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
5. https://ru.wikipedia.org
6. http://habrahabr.ru

Характеристика "вирусоподобных" программ
(подготовка сообщения)

План:

1. Виды вирусоподобных программ
2. Характеристика вирусоподобных программ
3. Утилиты скрытого администрирования

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Касперски К. Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006.
2. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
3. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
6. Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.
7. https://ru.wikipedia.org
8. http://habrahabr.ru

Антивирусные программы
(подготовка кроссворда)

План:

1. изучить информацию по теме
   1.1. Целевые платформы антивирусного ПО
   1.2. Классификация антивирусных продуктов
   1.3. Специальные антивирусы
   1.4. Лжеантивирусы
   1.5. Работа антивируса
   1.6. База антивирусов
2. создать графическую структуру, вопросы и ответы к ним

Форма контроля:

- защита кроссворда на учебном занятии,

Литература и интернет ресурсы:

1. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005.
2. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
3. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
6. Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.
7. https://ru.wikipedia.org
8. http://habrahabr.ru

Профилактика компьютерных вирусов (подготовка конспекта)

План:

1. Резервное копирование
2. Переход на защищенные операционные системы
3. Уменьшение привилегий пользователя
4. Сокращение избыточной функциональности программ
5. Методика обнаружения и удаления вирусов

Форма контроля:

- проверка конспекта
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005.
2. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
3. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
6. Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.
7. https://ru.wikipedia.org
8. http://habrahabr.ru

Обнаружение загрузочного вируса
(подготовка презентации)

План:

1. Мониторинг изменения файлов
2. Контроль за обращением к файлам
3. Контроль за состоянием системы
4. Обнаружение загрузочных вирусов в BIOS

Форма контроля:

- защита презентации на учебном занятии,

Литература и интернет ресурсы:

1. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005.
2. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
3. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
6. Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Книжный дом «ЛИБРОКОМ», 2014.
7. https://ru.wikipedia.org
8. http://habrahabr.ru

Информационная безопасность вычислительных сетей
(подготовка сообщения)

План:

1. Современные механизмы и средства защиты корпоративных сетей
2. Уязвимости протоколов и служб
3. Реализация атак в сетях TCP/IP
4. Протоколы IPSec, SSL, SSH

Форма контроля:

- защита сообщения на учебном занятии

Литература и интернет ресурсы:

1. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
2. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
3. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004.

4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009.
6. Борисов М. А. Особенности защиты персональных данных в трудовых отношениях. (Гриф УМО по дополнительному профессиональному образованию) М.: Книжный дом «ЛИБРОКОМ», 2013.
7. https://ru.wikipedia.org
8. http://habrahabr.ru
9. http://www.des-crypto.ru

Классификация удаленных угроз в вычислительных сетях (подготовка кроссворда)

План:

1. изучить информацию по теме
2. создать графическую структуру, вопросы и ответы к ним

Форма контроля:

- защита кроссворда на учебном занятии,

Литература и интернет ресурсы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
2. Описание протоколов SSL/TLS // 3. — ООО "КРИПТО-ПРО"., 2002.
3. Семенов Ю.А. Протокол SSL. Безопасный уровень соединителей. — 2000.
4. E. Rescorla The Transport Layer Security (TLS) Protocol Version 1.2 // 1-st. — RTFM, Inc., August 2008.
5. P. Karlton The Secure Sockets Layer (SSL) Protocol Version 3.0 // 1-st. — RTFM, Inc., August 2011.
6. T. Dierks The Secure Sockets Layer (SSL) // 1-st. — RTFM, Inc., August 2008.
7. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005.
8. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
9. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
10. https://ru.wikipedia.org
11. http://ubuntu.ru
12. http://habrahabr.ru
13. http://rus-linux.net
14. http://www.linuxsecurity.com

Причины успешной реализации удаленных угроз в вычислительных сетях (подготовка конспекта)

План:

1. Обзор сетевых угроз
2. Недостаточная аутентификация
3. Недостаточна авторизация
4. Подмена содержания
5. Выполнение кода
6. Разглашение информации
7. Логический атаки
8. DDoS атаки

Форма контроля:

- проверка конспекта
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
2. Описание протоколов SSL/TLS // 3. — ООО "КРИПТО-ПРО"., 2002.
3. Семенов Ю.А. Протокол SSL. Безопасный уровень соединителей. — 2000.
4. E. Rescorla The Transport Layer Security (TLS) Protocol Version 1.2 // 1-st. — RTFM, Inc., August 2008.
5. P. Karlton The Secure Sockets Layer (SSL) Protocol Version 3.0 // 1-st. — RTFM, Inc., August 2011.
6. T. Dierks The Secure Sockets Layer (SSL) // 1-st. — RTFM, Inc., August 2008.
7. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005.
8. Колесниченко Д.Н. Анонимность и безопасность в интернете. Справочный материал. - СПб.: Питер, 2014.
9. Столлингс В. Основы защиты сетей. Приложения и стандарты = Network Security Essentials. Applications and Standards. — М.: «Вильямс», 2002.
10. https://ru.wikipedia.org
11. http://ubuntu.ru
12. http://habrahabr.ru
13. http://rus-linux.net
14. http://www.linuxsecurity.com

МДК 03.03 Эксплуатация систем IP-телефонии

Тема 3.1. Восстановление поврежденных файлов

Создание презентации по теме: Основы VoIP. Передача речи по IP-сетям.
(подготовка презентации)

План:

1. Описание
2. Алгоритм работы
3.
4. Сообщение об ошибках

Форма контроля:

- защита презентации на учебном занятии,

Литература и интернет ресурсы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
2. http://ubuntu.ru
3. http://habrahabr.ru
4. http://rus-linux.net/MyLDP/file-sys/vosstanovlenie-failov-v-Linux.html
5. http://www.linuxsecurity.com

Протоколы RTP/RTCP
(подготовка сообщения)

План:

1. Установка и запуск*
   1.1. Установка и запуск*
   1.2. Системные требования
   1.3. Активация
   1.4. Настройки
   1.5. Проблемы и ограничения
   1.6. Обновления, скачивание лиц. копий

Форма контроля:

- защита сообщения на учебном занятии,

Литература и интернет ресурсы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
2. http://ubuntu.ru
3. http://habrahabr.ru
4. http://rus-linux.net
5. http://dmde.ru/manual.html
6. http://www.linuxsecurity.com

Сети и сценарии IP-телефонии
(подготовка кроссворда)

План:

1. изучить информацию по теме
2. создать графическую структуру, вопросы и ответы к ним

Форма контроля:

- защита кроссворда на учебном занятии

Литература и интернет ресурсы:

7. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
8. http://ubuntu.ru
9. https://ru.wikipedia.org/wiki/Dvdisaster
10. http://habrahabr.ru
11. http://rus-linux.net
12. http://www.linuxsecurity.com

Архитектура распределённого шлюза
(подготовка конспекта)

План:

1. установка
2. описание
3. опции
4. фильтры
5. пример восстановления файлов

Форма контроля:

- проверка конспекта
- заслушивание и обсуждение вопросов в аудитории на занятии;

Литература и интернет ресурсы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
2. http://ubuntu.ru
3. https://ru.wikipedia.org/wiki/Dvdisaster
4. http://habrahabr.ru
5. http://rus-linux.net
6. http://www.linuxsecurity.com

Назначение основных элементов IMS
(подготовка презентации)

План:

1. установка
2. описание
3. опции
4. фильтры
5. пример восстановления файлов

Форма контроля:

- защита презентации на учебном занятии,

Литература и интернет ресурсы:

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
2. http://ubuntu.ru
3. https://ru.wikipedia.org/wiki/Dvdisaster
4. http://habrahabr.ru
5. http://rus-linux.net
6. http://www.linuxsecurity.com
7. http://projects.izzysoft.de/trac/ext3undel/wiki/ext3undel

Концепция предоставления услуг в IMS
(подготовка сообщения)

План:

1. установка
2. описание
3. пример восстановления файлов

Форма контроля:

- защита сообщения на учебном занятии,

Литература и интернет ресурсы:

8. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. – 4-е изд . – СПб. : Питер, 2011.
9. http://www.giis.co.in/
10. http://ubuntu.ru
11. https://ru.wikipedia.org/wiki/Dvdisaster
12. http://habrahabr.ru
13. http://rus-linux.net
14. http://www.linuxsecurity.com

Основные источники:

1. Назаров А. В. Эксплуатация объектов сетевой инфраструктуры : учебник для студ. учреждений сред. проф. образования / А. В. Назаров, В. П. Мельников, А. И. Куприянов, А. Н. Енгалычев; под ред. А. В. Назарова. — М. : Издательский центр «Академия», 2014. — 368 с.
2. А.В. Кузин, Компьютерные сети: Учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2011.
3. Олифер В.Г. , Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-ое. – СПб.: Питер. 2010
4. Домарев В. В. Защита информации и безопасность компьютерных систем / В.В. Домарев. - К.: Издательство "ДиаСофт", 2010.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф., «Защита информации в компьютерных системах и сетях/Под ред. В.Ф. Шаньгина. – 4-е изд., перераб. И доп. – М.: радио и связь, 2010.
6. Колисниченко Д. Linux. От новичка к профессионалу. С-Пб.: БХВ-Петербург, 2011

Дополнительные источники:

1. Максимов Н. В., Попов И. И. Компьютерные сети: Учебное пособие. – М.: Форум, 2010. – 464 с
2. Самойленко В.В. Локальные сети. Полное руководство. — К., 2002.
3. Гук М. Аппаратные средства локальных сетей. Энциклопедия. — Пи тер, 2000.
4. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. — СПб.: Питер, 2006
5. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие. Издательство «Форум». – М., 2011. – 432
6. Пескова С. А., Кузин А. В., Волков А. Н. Сети и телекоммуникации: учебное пособие. – М.: Издательский центр «Академия», 2009. – 352
7. Электронный учебник Современные компьютерные сети. [Электронный ресурс] /http://depositfiles.com/files/fbcf8p1zz

Основные нормативные источники:

1. **ГОСТ Р 34.11-95**. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хеширования.
2. **ГОСТ Р. 50922-96**. Защита информации. Основные термины и определения.
3. **ГОСТ Р 52069.0-2003.** Государственный стандарт Российской Федерации. Защита информации. Система стандартов. Основные положения. SAFETY OF INFORMATION. SYSTEM OF STANDARDS. BASIC PRINCIPLES.

4. **ГОСТ Р ИСО/МЭК 15408-1-2002.** Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

Интернет-ресурсы:

1. http://zenway.ru/page/safecopy
1. http://www.tux.org/pub/people/kent-robotti/looplinux/rip/
1. http://www.r-tt.com/ru/data_recovery_linux/
1. http://manpages.ylsoftware.com/ru/parted.8.html
1. http://ru.wikipedia.org/
2. http://support.microsoft.com/KB/100108
3. http://www.linux.com/
1. http://www.network.xsp.ru/3_5.php
2. http://help.ubuntu.ru/
3. http://rfc2.ru/
1. http://www.inssl.com/about-ssl-protocol.html
2. http://habrahabr.ru
3. http://ru.hostings.info/ssl.html
10. http://www.networkcenter.info/calcs/cidrcalc