



**Некоммерческое  
акционерное  
общество**

**АЛМАТИНСКИЙ  
УНИВЕРСИТЕТ  
ЭНЕРГЕТИКИ И  
СВЯЗИ**

Кафедра казахского  
и русского языков

## **ПРОФЕССИОНАЛЬНЫЙ РУССКИЙ ЯЗЫК**

Методические указания и варианты выполнения семестровых работ для  
студентов специальностей  
5В100200 – Системы информационной безопасности,  
5В073100 – Информационные системы

Алматы 2016

СОСТАВИТЕЛЬ: М.К. Нурмаханова. Профессиональный русский язык: Методические указания и варианты выполнения семестровых работ для студентов специальностей 5В100200 – Системы информационной безопасности, 5В073100 – Информационные системы – Алматы: АУЭС, 2016. – 56с.

В методические указания по дисциплине «Профессиональный русский язык» включены образцы выполнения семестровой работы № 1, а также по 25 вариантов семестровой работы № 2 для специальностей 5В100200 – Системы информационной безопасности, 5В073100 – Информационные системы.

Рецензент: к.ф.н., доцент Р.А. Досмаханова

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2016 г.

© НАО «Алматинский университет энергетики и связи», 2016 г.

## Введение

Целевая аудитория методической разработки – студенты казахских групп дневного отделения бакалавриата специальностей 5В100200 – «Системы информационной безопасности», 5В070300 – «Информационные системы».

Методическая разработка состоит из 2 разделов («Семестровая работа студента № 1. Составление двуязычного словаря терминов по специальности», «Семестровая работа студента № 2. Письменный перевод текста по специальности»), каждый из которых снабжен методической преамбулой.

В разделе «Семестровая работа студента № 2. Письменный перевод текста по специальности» включены 25 вариантов для специальностей 5В100200 – «Системы информационной безопасности» и 5В070300 – «Информационные системы».

Текстовый материал отбирался из учебной и научной литературы, рекомендуемой соответствующими программами по направлению дисциплины.

## **Семестровая работа студента № 1. Составление двуязычного словаря терминов по специальности**

Тема: составление двуязычного словаря терминов по специальности.

Цель: развить навыки работы с учебной или специальной литературой на русском языке; пополнить словарный запас новыми для студента терминами и терминосочетаниями; расширить представление о терминологических словарях по специальности; уметь оформлять работу в соответствии с предъявляемыми требованиями.

Задание: составить двуязычный словарь терминов и терминосочетаний по специальности в объеме 30-35 единиц.

Ход выполнения работы:

1) Подобрать казахские аналоги терминам и терминосочетаниям из учебной или специальной литературы по специальности в объеме 30-35 термоединиц.

2) Используя терминологические толковые словари, дать толкование русским и их казахским аналогам на русском и казахском языках.

В конце работы указать список использованных источников (учебники или специальную литературу, двуязычные словари, методическую литературу и т.д.), оформленный в соответствии с предъявляемыми требованиями.

### **Образец выполнения семестровой работы № 1**

Текст №1

#### **Основные понятия, термины и определения**

Широко распространенное в настоящее время понятие – информационная безопасность – подчеркивает важность информации в современном обществе и характеризует тот факт, что информационный ресурс является сегодня таким же богатством, как полезные ископаемые, производственные и людские ресурсы и также как они подлежат защите от различного рода посягательств, злоупотреблений и преступлений.

Под *информационной безопасностью* будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

*Субъект* - это активный компонент информационной системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.

*Объект* - пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.

В качестве объектов, подлежащих защите в интересах обеспечения безопасности субъектов информационных отношений, необходимо рассматривать:

- информацию и информационные ресурсы;
- носители информации;
- процессы обработки информации.

Осведомленность конечного пользователя о мерах безопасности должна проявляться в умении различать четыре уровня защиты компьютерных и информационных ресурсов:

а) *предотвращение* – доступ к информации и технологии имеет только авторизованный персонал;

б) *обнаружение* – раннее обнаружение преступлений и злоупотреблений, даже в случае обхода механизмов защиты;

в) *ограничение* – уменьшение размера потерь, если преступление имело место несмотря на предпринятые меры по его предотвращению;

г) *восстановление* – обеспечение эффективного восстановления информации при наличии документированных и проверенных планов проведения этой операции.

*Атака* на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы. Таким образом, атака - это реализация угрозы безопасности. Противодействие угрозам безопасности является целью защиты систем обработки информации. *Безопасная* или *защищенная система* - это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности. *Комплекс средств защиты* представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности КС. Комплекс создается и поддерживается в соответствии с принятой в данной организации политикой безопасности. *Политика безопасности* - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты КС от заданного множества угроз безопасности.

## Образец оформления СРС № 1

Термины, выписанные из текста №1 и толкование на двух языках

Термины и терминосочетания на русском языке с толкованием	Термины и терминосочетания на казахском языке с толкованием
<i>Информационная безопасность</i> - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или	Ақпараттық қауіпсіздік – инфрақұрылыммен жұмыс жасайтын және ақпарат иесіне немесе пайдаланушыларына қолайсыздық әрекеттерден, табиғи немесе жасанды түрдегі

искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.	кездейсоқ немесе арнайы зиян келтіруден ақпараттың қорғалуы.
<i>Субъект</i> - это активный компонент информационной системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.	<i>Субъект</i> – ақпараттық жүйенің белсенді компоненті (құраушы), бұл объектіден субъектіге ақпараттың өтіп кетуінің немесе жүйе өзгеруінің себебі болуы мүмкін.
<i>Объект</i> - пассивный компонент системы, хранящий, принимающий или передающий информацию.	<i>Объект</i> (нысан) – ақпаратты қабылдайтын, сақтайтын немесе тарататын жүйенің белсенді емес құраушысы.
<i>Атака</i> на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.	Компьютер жүйесіне <i>шабуыл</i> – зиянкестің жасайтын әрекеті, ол жүйенің қандай да бір осалдығын іздеп және соны пайдалануға негізделеді.
<i>Безопасная</i> или <i>защищенная система</i> - это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.	<i>Қауіпсіз</i> немесе <i>қорғалған жүйе</i> – қауіпсіздік қатерлеріне тиімді және қолайлы қарсы тұратын қорғаныстық құралдары бар жүйе.
<i>Комплекс средств защиты</i> представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности КС.	<i>Қорғаныс құралдарының кешені</i> – КЖ ақпараттық қауіпсіздігін қамтуға құрылған және пайдаланылатын программалық және техникалық құралдардың жиынтығы.
<i>Политика безопасности</i> - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты КС от заданного множества угроз безопасности.	<i>Қауіпсіздік саясаты</i> – КЖ қауіпсіздік қатерлерден қорғайтын құралдардың жұмыстарын реттейтін тәжірибелік ұсынымдардың, ережелер мен нормалардың жиынтығы.
<i>Предотвращение</i> – доступ к информации и технологии имеет только авторизованный персонал.	<i>Сақтап қалу (болдырмау)</i> – тек ақпаратқа және технологияға тіркелген қызметкер ғана қатынай алады.
<i>Обнаружение</i> – раннее обнаружение преступлений и злоупотреблений, даже в случае обхода механизмов защиты.	<i>Тауып алу</i> – қорғаныс механизмдерін айналып өтетін жағдай туғанда, қылмыстар мен теріс пайдаланушыларды алдын ала тауып алу.
<i>Ограничение</i> - уменьшение размера	<i>Шектеу</i> – егер қылмыс, оны

потерь, если преступление имело место несмотря на предпринятые меры по его предотвращению.	болдырмауға жасалған шараларға қарамастан болса, соның шығын мөлшерлерін азайту.
<i>Восстановление</i> – обеспечение эффективного восстановления информации при наличии документированных и проверенных планов проведения этой операции.	<i>Қалпына келтіру</i> – операция өткізудің құжаттандырылған және тексерілген жоспарымен ақпаратты тиімді қалпына келтіруді қамтамасыз ету.

*Следует привлечь еще несколько текстов, чтобы набрать 30-35 терминов согласно заданию СРС.*

### **Рекомендуемая литература для СРС № 1**

- 1 Акулиничев Ю. П., Дроздова В.И. Теория информации: Учебное пособие. - Томск: ТМЦДО, 2005. – 108 с.
- 2 Букейханова Р.К., Чумбалова Г.М. Обучение перевода на казахский язык научно-технических текстов. - Алматы: АУЭС, 2007. – 50 с.
- 3 Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 586 с.
- 4 Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации: Учебное пособие. – М.: Горячая линия. – Телеком, 2014. – 442 с.
- 5 Кудряшов Б.Д. Теория информации: Учебник для вузов. – СПб.: Изд. Дом Питер, 2009.- 460 с.
- 6 Куралбаев З.К. Основы информационных систем. Конспект лекций. – Алматы: АИЭС, 2009. – 80 с.
- 7 Новиков В.К. Организационно-правовые основы информационной безопасности: Учебное пособие. – М.: Горячая линия – Телеком, 2015. – 176 с.
- 8 Нурмаханова М.К. Профессиональный русский язык. Методические указания для студентов специальности 5В100200. – Алматы: АУЭС, 2015. – 49 с.
- 9 Панарин И.Н. Информационная война, PR и мировая политика. Курс лекций. – М.: Горячая линия – Телеком, 2015. - 352 с.
- 10 Перепелкин Д.А. Схемотехника усилительных устройств: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 238 с.
- 11 Панин В.В. Основы теории информации. – М.: Бином. Лаборатория знаний, 2009. – 270 с.
- 12 Сатимова Е.Г. Операционные системы. LINUX. Решения задач структурной и функциональной организации: Учебное пособие. – Алматы: АУЭС, 2009. – 120 с.

## Словари

1 Берикулы А., Шайхин Б.М. и др. Казахско-русский, русско-казахский терминологический словарь. Электроника, радиотехника и связь. – Алматы: Рауан, 2000. – 236 с.

2 Политехнический словарь./ Гл. ред. Акад. А. Ю. Ишлинский. – М.: Советская энциклопедия, 1980. – 656 с.

3 Русско-казахско-английский политехнический словарь. Сост. М.Р.Тусипбек, А.К.Кусаинов. – Алматы: Rond&A, 2010. – 740 с.

4 Казахско-русский, русско-казахский терминологический словарь/ Под общей редакцией д.п.н., проф. А. К. Кусаинова. В 32-х томах. - Алматы: Рауан, 2000.–312 с.

5 Пчёлкина В. В., Комарова Л. Н. И др. Словарь иностранных слов.- М.: Русский язык. 1979.- 607 с.

6 Раренко М.Б. Основные понятия переводоведения. Терминологический словарь-справочник. – М.: ИНИОН РАН, 2010. – 260 с.

7 Русско-казахский словарь./ Под редакцией Н. Т. Сауранбаева и др. - Алматы: Дайк-Пресс, 2005. – 1125 с.

8 Сарыбеков М., Сыздыкназаров М. Словарь науки. Общенаучные термины и определения. Науковедческие понятия и категории: Учебное пособие. – Алматы: Триумф «Т», 2008. – 504 с.

## Семестровая работа студента № 2

Тема: письменный перевод текста по специальности.

Цель: развить умения и навыки письменного перевода научно-технических текстов.

Задание: перевести текст по специальности с русского на казахский язык.

Ход работы: основным требованием к выполнению семестровой работы № 2 является адекватный перевод научно-технического текста с русского на казахский язык. Перед началом работы над переводом необходимо полностью прочитать текст, выделить трудные для восприятия абзацы, частотные ключевые понятия и термины. При наличии нескольких вариантов перевода или неясности лексической единицы нужно использовать терминологические толковые словари. Для перевода сложного предложения необходимо разобраться в его грамматической структуре, выявить основной смысл предложения для передачи последнего в соответствии со структурой казахского предложения. Переводить текст следует по смысловым фрагментам. Такой фрагмент чаще состоит не из одного, а из нескольких предложений и редко выходит за рамки абзаца. Варианты текстов распределяются между студентами преподавателем.

*Требования к оформлению работы.*



Работа должна быть выполнена на формате А4 компьютерной версткой. Параметры оформления текста: кегль 14, шрифт Times New Roman, межстрочный интервал 1,0. Поля: левое – 2,5 см, правое – 1,8 см, нижнее – 2,5 см, верхнее – 2,0 см. Выравнивание текста на листах должно производиться по ширине строк.

## **Перечень текстов, включенных в СРС № 2, для специальности 5В100200 – Системы информационной безопасности**

### **Вариант 1**

#### **Современная ситуация в области информационной безопасности**

Последнее время сообщения об атаках на информацию, о хакерах и компьютерных взломах наполнили все средства массовой информации. Что же такое «атака на информацию»? Дать определение этому действию на самом деле очень сложно, поскольку информация, особенно в электронном виде, представлена сотнями различных видов. Информацией можно считать и отдельный файл, и базу данных, и одну запись в ней, и целиком программный комплекс. И все эти объекты могут подвергнуться и подвергаются атакам со стороны некоторой социальной группы лиц.

При хранении, поддержании и предоставлении доступа к любому информационному объекту его владелец, либо уполномоченное им лицо, накладывает явно либо самоочевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как атака на информацию.

С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде вырос в тысячи раз. И теперь скопировать за полминуты и унести дискету с файлом, содержащим план выпуска продукции, намного проще, чем копировать или переписывать кипу бумаг. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Каковы возможные последствия атак на информацию? В первую очередь, конечно, нас будут интересовать экономические потери:

1) Раскрытие коммерческой информации может привести к серьезным прямым убыткам на рынке.

2) Известие о краже большого объема информации обычно серьезно влияет на репутацию фирмы, приводя косвенно к потерям в объемах торговых операций.

3) Фирмы-конкуренты могут воспользоваться кражей информации, если та осталась незамеченной, для того чтобы полностью разорить фирму, навязывая ей фиктивные либо заведомо убыточные сделки.

4) Подмена информации как на этапе передачи, так и на этапе хранения в фирме может привести к огромным убыткам.

5) Многократные успешные атаки на фирму, предоставляющую какой-либо вид информационных услуг, снижают доверие к фирме у клиентов, что сказывается на объеме доходов.

## Вариант 2

### Категории информационной безопасности

Информация с точки зрения информационной безопасности обладает следующими категориями:

а) конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации;

б) целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения;

в) аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения;

г) апеллируемость – довольно сложная категория, но часто применяемая в электронной коммерции – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается отказываться от своих слов, подписанных им однажды.

В отношении информационных систем применяются иные категории:

1) Надежность – гарантия того, что система ведет себя в нормальном внештатном режимах так, как запланировано.

2) Точность – гарантия точного и полного выполнения всех команд.

3) Контроль доступа – гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются.

4) Контролируемость – гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса.

5) Контроль идентификации – гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает.

6) Устойчивость к умышленным сбоям – гарантия того, что при умышленном внесении ошибок в пределах нормы система будет вести себя так, как оговорено заранее.

### **Абстрактные модели защиты информации**

В 1977 г. одной из первых моделей была опубликована модель Биба (Viba). Согласно ей все субъекты и объекты предварительно разделяются по нескольким уровням доступа, а затем на их взаимодействия накладываются следующие ограничения:

а) субъект не может вызывать на исполнение субъекта с более низким уровнем доступа;

б) субъект не может модифицировать объекты с более высоким уровнем доступа.

Модель Гогена-Мезигера (Goguen-Meseguer), представленная в 1982 году, основана на теории автоматов. Согласно ей система может при каждом действии переходить из одного разрешенного состояния в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы – домены, и переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано какие операции может выполнять субъект из домена С над объектом из домена D. В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы.

Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, делает акцент на взаимодействии субъектов и потоков информации. Также как и в предыдущей модели, здесь используется машина состояний с множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Важную роль в теории защиты информации играет модель защиты Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 году и модифицированная в 1989 году. Основана данная модель на повсеместном использовании транзакций и тщательном оформлении прав доступа субъектов к объектам. В данной модели впервые исследована защищенность третьей стороны, поддерживающей всю систему безопасности. Эту роль в информационных системах обычно играет программа-супервизор. Кроме того, в модели Кларка-Вильсона транзакции впервые были построены по методу верификации, то есть идентификация субъекта производилась не только перед выполнением команды от него, но и повторно после выполнения. Это позволило снять проблему подмены автора в момент между его идентификацией и командой. Модель Кларка-Вильсона считается одной из самых совершенных в отношении поддержания целостности информационных систем.

## Вариант 4

### **Терминалы защищенной информационной системы**

Наиболее распространенным способом входа в систему при атаках на информацию остается вход через официальный login запрос системы. Вычислительная техника, которая позволяет произвести вход в систему, называется в теории информационной безопасности терминалом. Если система состоит из одного персонального компьютера, то он одновременно считается и терминалом и сервером. Доступ к терминалу может быть физическим в том случае, когда терминал – это ЭВМ с клавиатурой и дисплеем, либо удаленным – чаще всего по телефонной линии (в этом случае терминалом является модем, подключенный либо непосредственно к системе, либо к ее физическому терминалу).

При использовании терминалов с физическим доступом необходимо соблюдать следующие требования:

1) Защищенность терминала должна соответствовать защищенности помещения: терминалы без пароля могут присутствовать только в тех помещениях, куда имеют доступ лица соответствующего или более высокого уровня доступа. Отсутствие имени регистрации возможно только в том случае, если к терминалу имеет доступ только один человек, либо, если на группу лиц, имеющих к нему доступ, распространяются общие меры ответственности. Терминалы, установленные в публичных местах, должны всегда запрашивать имя регистрации и пароль.

2) Системы контроля за доступом в помещение с установленным терминалом должны работать полноценно и в соответствии с общей схемой доступа к информации.

3) В случае установки терминала в местах с широким скоплением народа клавиатура, а если необходимо, то и дисплей должны быть оборудованы устройствами, позволяющими видеть их только работающему в данный момент клиенту (непрозрачные стеклянные или пластмассовые ограждения, шторы).

## Вариант 5

### **Получение пароля на основе ошибок администратора и пользователей**

Перебор паролей по словарю являлся некоторое время одним из самых распространенных техник подбора паролей. В настоящее время, как самый малый результат пропаганды информационной безопасности, он стал сдавать свои позиции. Хотя развитие быстродействия вычислительной техники и все более сложные алгоритмы составления слов-паролей не дают «погибнуть» этому методу. Технология перебора паролей родилась в то время, когда

самым сложным паролем было слово «brilliant», а в русифицированных ЭВМ оно же, но для «хитрости», набранное в латинском режиме. В то время программа со словарем в 5000 существительных давала положительный результат в 60 % случаев. Огромное число инцидентов с взломами систем заставило пользователей добавлять к словам 1-2 цифры с конца, записывать первую или последнюю букву в верхнем регистре, это увеличило время на перебор вариантов с учетом роста быстродействия ЭВМ всего в несколько раз.

Так, в 1998 году было официально заявлено, что даже составление двух совершенно не связанных осмысленных слов не дает реальной надежности паролю. К этому времени получили широкое распространение языки составления паролей, которые записываются в абстрактной форме среднестатистическими пользователями ЭВМ.

Следующей модификацией подбора является проверка паролей, устанавливаемых в системах по умолчанию. В некоторых случаях администратор программного обеспечения, проинсталлировав или получив новый продукт от разработчика, не проверяет систему безопасности. Как следствие, пароль, установленный в фирме разработчиком по умолчанию, остается основным паролем в системе. В сети Интернет можно найти огромные списки паролей по умолчанию практически ко всем версиям программного обеспечения, если они устанавливаются на нем производителем.

## Вариант 6

### **Традиционные методы шифрования**

Традиционно людьми, больше всех нуждающимися в секретности, были военные и дипломаты. В их работе часто необходимы элементы неожиданности, а неожиданность такого рода всегда предполагает секретность. Примерно в середине XIX века для усовершенствования техники тайного письма были привлечены научные методы и способы мышления. Несмотря на это вплоть до нашего столетия способы, использованные для секретной коммуникации, продолжали оставаться процедурами, выполняемыми с помощью карандаша и бумаги. Рассмотрим некоторые традиционные методы шифрования.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра. Это самые простые и древние шифры, среди которых можно упомянуть:

- шифр перестановки «скитала»: на стержень цилиндрической формы (скиталу) наматывали спиралью полоску пергамента и писали на ней вдоль стержня несколько строк текста. Когда пергамент снимали со стержня, буквы располагались хаотично. Для расшифровки надо было знать правило шифрования и ключ в виде стержня определенного диаметра;

- шифрующие таблицы: они задавали правила перестановки букв в сообщении; в качестве ключа здесь используется: размер таблицы, слово или фраза, задающие перестановку, особенности структуры таблицы;

- одиночная перестановка по ключу: столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы;

- двойная перестановка: для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование; в качестве ключа двойной перестановки используются последовательности номеров столбцов и номеров строк исходной таблицы;

- табличная перестановка по нелинейному закону: сообщение записывается в таблицу размерности NM последовательно по строкам, а считывание происходит змейкой по спирали или по другому зигзагообразному пути;

- применение магических квадратов, то есть квадратов, в которых суммы чисел по столбцам, строкам и диагоналям равны. Текст в таблицу вписывается в соответствии с нумерацией клеток. Считалось, что эти шифртексты обладают еще и магической силой. Число магических квадратов быстро возрастает с увеличением размера квадрата.

## Вариант 7

### Узлы коммутации сетей

Узлы коммутации сетей представляют для злоумышленников:

а) как инструмент маршрутизации сетевого трафика;

б) как необходимый компонент работоспособности сети.

В отношении первой цели получение доступа к таблице маршрутизации позволяет изменить путь потока возможно конфиденциальной информации в интересующую злоумышленника сторону. Дальнейшие его действия могут быть подобны атаке на DNS-сервер. Достичь этого можно непосредственным администрированием, когда злоумышленник получил права администратора (чаще всего узнал пароль администратора или воспользовался несменным паролем по умолчанию). Получить физический доступ к устройству, управляемому через физический порт, гораздо сложно.

Возможен второй путь атаки с целью изменения таблицы маршрутизации. Он основан на динамической маршрутизации пакетов, включенной на многих узлах коммутации. В таком режиме устройство определяет наиболее оптимальный путь отправки конкретного пакета, основываясь на истории прихода определенных служебных пакетов сети – сообщений маршрутизации (протоколы ARP, RIP и другие). В этом случае при фальсификации по определенным законам нескольких подобных служебных пакетов можно добиться того, что устройство начнет отправлять пакеты по пути, интересующем злоумышленника, думая, что это и есть самый быстрый путь к пункту назначения.

При атаке класса «отказ в сервисе» злоумышленник обычно заставляет узел коммутации либо передавать сообщения по неверному пути, либо

вообще перестать передавать их. Для достижения второй цели обычно используют ошибки в программном обеспечении, запущенные на маршрутизаторе, с целью его зависания.

## Вариант 8

### **Нанотехнологии в современных электронных системах**

По своему назначению современные электронные системы охватывают широкую номенклатуру изделий, масштабы функционирования которых простираются от атомно-молекулярного уровня (нано- и микроструктуры) до планетного масштаба (телекоммуникации). Разработка и производство разнообразных миниатюрных электронных систем является одним из стратегических направлений мирового научно-технического прогресса.

Миниатюризация приводит к революционным изменениям техники, особенно в тех случаях, когда далеко не очевидным образом удается разработать и использовать технологию массового производства изделия, что позволяет существенно уменьшить его цену, повысить надежность, снизить энергопотребление и т.п. Эффективность миниатюризации наиболее ярко демонстрирует достижения микроэлектроники, компьютерной техники, телекоммуникации. Для более чем полувековой истории микроэлектроники характерны высокие темпы миниатюризации, которые описаны эмпирическими законами Мура в различных формулировках. Из наиболее распространенной формулировки следует, что плотность транзисторов в современных интегральных схемах удваивается каждые 18 месяцев. Однако в настоящее время ситуация в этой области качественно отличается от ситуации прошлого века.

В недалеком прошлом рекордные достижения миниатюризации при массовом производстве электронных систем характеризовались пространственными масштабами в сотни и десятки микрон. Сейчас же рекордные достижения миниатюризации практически достигли нанометровых пространственных масштабов, т.е. элементарных физических объектов электроники. Действительно, элементарными физическими объектами электроники являются атомы, состоящие из атомного ядра и электронов, и электромагнитное поле (фотоны). Типичные размеры атомов составляют десятые доли нанометра, а длина волны фотонов оптического электромагнитного диапазона сотни нанометров. Условно радиус электрона можно оценить величиной  $\sim 8 \cdot 10^{-6}$  нм.

Современные электронные системы имеют сложную иерархическую структуру, которые для своего функционирования реально интегрируют физико-химические явления от атомно-молекулярного уровня до макроскопического уровня. В архитектуре они неуклонно приближаются к архитектуре живых систем.

## Вариант 9

### **Вирусы и их разновидности**

Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия: портит файлы или таблицу размещения файлов на диске, засоряет оперативную память и т.д.

Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться при определенных условиях. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится и работает в обычном режиме. Таким образом, внешне работа зараженной программы выглядит как незараженной. Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное. Однако после некоторого промежутка времени на компьютере происходят сбои.

Большинство тех программ, которыми вы пользуетесь, заражены вирусом, а некоторые файлы и диски испорчены. Зараженные программы с вашего компьютера переносятся с помощью дискет или по локальной сети на компьютеры ваших коллег и друзей.

Некоторые разновидности вирусов трудно определить. Они вначале незаметно заражают большое число программ или дисков, затем причиняют серьезные повреждения, например, форматируют весь жесткий диск на компьютере.

Таким образом, если не предпринимать меры по защите компьютера от вирусов, то последствия могут быть плачевными.

## Вариант 10

### **Качество информации**

Качество информации определяется набором ее основных потребительских свойств, обеспечивающих возможность эффективного использования. Информация, как и любой материальный объект, может характеризоваться определенными показателями качества, среди которых следует назвать объективность, полноту, точность, достоверность, адекватность, доступность, актуальность и др. Объективность (субъективность) информации является понятием относительным. Это свойство проявляется во взаимодействии объективных данных, являющихся результатом регистрации объективно существующих сигналов и субъективных методов, составленных и подготовленных людьми (субъектами). Полнота (достаточность) информации также является важным ее свойством, поскольку определяет тот минимальный состав, который достаточен для принятия правильного решения или для подготовки новых



данных на основе имеющихся.

Очевидно, что как неполная, так и избыточная информация снижают эффективность принимаемых решений.

*Точность* информации характеризуется степенью близости получаемой информации к реальному состоянию объекта, процесса или явления.

*Достоверность* информации определяется ее свойством отражать реально существующие объекты с необходимой точностью. Как правило, этой цели служат вероятностные характеристики, в которых раскрывается отличие отображаемого информацией параметра от его истинного значения.

*Адекватность* информации характеризует степень ее соответствия объективной реальности.

Неадекватная информация может образовываться как на основе неполных или недостоверных данных, так и на основе полных и достоверных данных, но в случае применения к ним неадекватных методов.

*Доступность информации* обеспечивается возможностью выполнения соответствующих процедур ее получения и преобразования. Отсутствие доступа к данным или отсутствие адекватных методов их обработки приводит к одинаковому результату: информация оказывается недоступной.

*Актуальность информации* - это степень принадлежности ее текущему моменту времени. Она определяется ценностью информации в момент практического ее применения и зависит от динамики изменения ее характеристик, а также интервала времени, на котором использовалась данная информация. В заключение следует отметить, что перечисленные показатели качества информации тесно связаны и оказывают иногда друг на друга взаимное влияние.

## Вариант 11

### Основные определения

*Информационная система (ИС)* - это взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации для достижения цели управления. В современных условиях основным техническим средством обработки информации является персональный компьютер.

*Информационный процесс* - процесс взаимодействия двух и более субъектов, целью и основным содержанием которого является изменение имеющейся у них информации.

*Субъект* - активный компонент, участник процесса информационного взаимодействия, может быть пользователем (человеком), устройством или компьютерным процессом.

*Злоумышленник* - субъект, оказывающий воздействие на информационный процесс с целью вызвать его отклонение от условий нормального протекания. Злоумышленник идентифицируется набором возможностей по доступу к информационной системе, работу которой он намеревается отклонить от нормы.

Считается, что в его распоряжении всегда есть все необходимые для выполнения его задачи технические средства, созданные на данный момент.

Под *безопасность ИС* понимают ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов. Защита информации в компьютерных системах обладает рядом специфических особенностей: информация не связана с носителем; она легко и быстро копируется и передается по каналам связи.

*Угроза безопасности ИС* - возможные воздействия на ИС, которые прямо или косвенно могут нанести ущерб ее безопасности.

*Уязвимость ИС* - свойство системы (неудачное), которое делает возможным возникновение и реализацию угрозы.

*Атака на ИС* – действие, предпринимаемое злоумышленником, которое заключается в поиске той или иной уязвимости системы. Атака – это реализация угрозы безопасности.

*Безопасная или защищенная система* – это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Вариант 12

## **Материнская плата**

Материнская плата (системная плата) – устройство, предназначенное для установки процессора, оперативной памяти, плат расширения и подключения других устройств. Фактически она является «скелетом» компьютера, определяющим взаимодействие его подсистем друг с другом, а также их контакт.

Первоначально компьютер IBM PC содержал одну единственную шину, предназначенную для подключения плат расширения – шину ISA. Пропускная способность (фактически, скорость работы) этой шины вполне удовлетворяла требования того времени. Со временем появлялись программные продукты, которые требовали от компьютера все большей скорости работы. Тогда и возникла необходимость разработки более совершенного стандарта передачи данных. Материнские платы имеют следующие виды шин:

ISA – может быть 8-ми и 16-битной. Поэтому и пропускная способность будет отличаться в два раза. Применяется для устройств, не требующих высокой скорости передачи данных. Большинство разработчиков материнских плат уже отказались от использования этого морально устаревшего стандарта.

EISA – расширенный стандарт ISA с увеличенной пропускной способностью практически в 4 раза. Но из-за своей дороговизны не нашла широкого применения, несмотря на неплохие возможности автоматического конфигурирования устройств.

IEEE1394 (FireWire, iLink) – наиболее новая и самая дорогая на сегодняшний день шина. IEEE1394 характеризуется большей активностью и стабильностью чем все выше перечисленные шины. Эта шина может

использоваться для подключения жестких дисков, сканеров, сетевого оборудования, цифровых камер и других устройств требующих высокой пропускной способностью.

### Вариант 13

#### **Ресурсы информационных систем**

Цель информационной безопасности - обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму. Прежде чем определять задачи системы безопасности, необходимо провести инвентаризацию информационных ресурсов: каждый ресурс и его владелец должны быть четко идентифицированы и задокументированы. Можно привести следующие примеры ресурсов, связанных с информационными системами:

а) информационные ресурсы: базы данных и файлы данных, системная документация, руководство пользователя, учебные материалы, операционные процедуры и процедуры поддержки, планы обеспечения бесперебойной работы организации, процедуры перехода на аварийный режим;

б) программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

в) физические ресурсы: компьютеры и коммуникационное оборудование, каналы связи, магнитные носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения.

Различная информация имеет разную степень конфиденциальности и важности. Систему классификации информации по категориям секретности необходимо использовать для определения соответствующего набора уровней защиты и для уведомления пользователей о необходимости специального обращения с этой информацией. Выходные данные информационных систем, содержащие секретную информацию, должны иметь соответствующий гриф секретности. Примерами таких выходных данных являются печатные отчеты, информация, выводимая на экраны дисплеев, данные, хранимые на магнитных носителях (лентах, дисках, кассетах), электронные сообщения и передаваемые файлы. Примеры грифов: особо секретная, секретная, с ограниченным доступом, для служебного пользования, публичная.

### Вариант 14

#### **Криптография**

Пробуждение значительного интереса к криптографии и ее последующее развитие началось в 19 веке, что связано с зарождением электросвязи. В 19 столетии секретные службы большинства развитых стран стали относиться к этой дисциплине как к обязательному инструменту своей деятельности. Весь период с древних времен до 1949 года называется донаучным периодом, поскольку средства закрытия письменной информации не имели строгого

математического обоснования. Поворотным моментом, придавшим криптографии научность и выделившим ее в отдельное направление математики, явилась публикация в 1949 году статьи К.Э. Шеннона «Теория связи в секретных системах».

Фундаментальным выводом из работы Шеннона стало определение зависимости надежности алгоритма от размера и качества секретного ключа, а также от информационной избыточности исходного текста. Шеннон ввел формальное определение информации и функции ненадежности ключа как его неопределенности при заданном количестве известных битов закрытого текста. Кроме того, им было введено важное понятие расстояния единственности как минимального размера текста, для которого еще возможно однозначное раскрытие исходного текста. Было показано, что расстояние единственности прямо пропорционально длине ключа и обратно пропорционально избыточности исходного текста.

Другим фундаментальным толчком развития криптографии явилась публикация в 1976 году статьи У. Диффи и М.Е. Хеллмана «Новые направления в криптографии». В этой работе впервые было показано, что секретность передачи информации может обеспечиваться без обмена секретными ключами.

В современной криптологии принято считать, что надежность шифра определяется только секретностью используемого ключа. Это правило впервые сформулировал голландский криптограф А. Керхгофф: считается, что весь механизм шифрования, за исключением значения секретного ключа, предположительно известен противнику. Это обусловлено тем, что криптосистема обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации.

## Вариант 15

### **Комплексная система защиты информации**

Комплексная система защиты информации (КСЗИ) - это совокупность организационных и инженерных мер, программно-аппаратных средств, которые обеспечивают защиту информации во время её обработки в информационной системе.

Первая задача КСЗИ – это организационные меры, то есть выработка официальной политики предприятия в области информационной безопасности.

Вторая задача - обеспечение физической безопасности: периметр безопасности должен быть четко определен и должен соответствовать ценности защищаемых ресурсов и сервисов. В-третьих, кроме функциональных критериев, которые позволяют оценить наличие услуг безопасности в компьютерной системе, существуют критерии гарантии, которые позволяют оценить корректность реализации услуг. Критерии гарантии включают требования к архитектуре комплекса средств защиты, среды разработки, последовательности разработки, испытания комплекса средств защиты, среды функционирования и

эксплуатационной документации. В-четвертых, необходимо уметь провести оценку ущерба от реализации прогнозируемых угроз.

Применение тех или иных организационных или технических средств защиты зависит не от типа пользователя, а от стоимости информации, которую нужно защищать, то есть от потерь, которые понесёт пользователь в случае нарушения одной или нескольких функций защиты – нарушения конфиденциальности, целостности или доступности информации. Как правило, действительно, чем больше компания, тем больше у неё информации, которая носит конфиденциальный характер и потери компании в этом случае выше. Но и обычный пользователь, например, руководитель той же компании на своём домашнем компьютере может содержать информацию, компрометация которой может обойтись очень дорого. Соответственно, его компьютер должен быть защищён не хуже, чем корпоративная сеть.

## Вариант 16

### Современные симметричные криптосистемы

По мнению Шеннона в практических шифрах необходимо использовать два общих принципа: рассеивание и перемешивание.

Рассеивание представляет собой распространение влияния одного знака открытого текста на знаки шифртекста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и зашифрованного текстов. Однако шифр должен не только затруднять, но и обеспечивать лёгкость зашифрования и расшифрования при известном пользователю секретном ключе.

Распространённым способом достижения эффектов рассеивания и перемешивания является использование составного шифра, т.е. такого, который может быть реализован в виде последовательности простых шифров, каждый из которых вносит свой вклад в значительное рассеивание и перемешивание. В составных шифрах в качестве простых шифров чаще всего используются простые перестановки и подстановки (замены).

В зависимости от размера блока информации криптоалгоритмы делятся на следующие виды:

а) потоковые шифры. Единицей кодирования в потоковых шифрах является один бит. Результат кодирования не зависит от прошедшего ранее входного потока. Схема применяется в системах передачи потоков информации, то есть в тех случаях, когда передача информации начинается и заканчивается в произвольные моменты времени и может случайно прерываться. Наиболее распространёнными представителями поточных шифров являются скремблеры;

б) блочные шифры. Единицей кодирования в таких шифрах является блок из нескольких байтов. Результат кодирования зависит от всех исходных байтов этого блока. Схема применяется при пакетной передаче информации и кодировании файлов. Блочные шифры шифруют целые блоки информации (от 4 до 32 байт) как единое целое – это значительно увеличивает стойкость

преобразований к атаке полным перебором и позволяет использовать различные математические и алгоритмические преобразования

## Вариант 17

### **Локальные компьютеры**

Использование локальных компьютеров как для передачи и хранения информации, содержащей коммерческую или личную тайну, так и для работы в Internet, требует построения эффективной системы защиты. Определим, к какому уровню стека протоколов относится система сетевой безопасности.

Вероятно, какое-то одно место для нее найти сложно. Каждый уровень должен внести свой вклад. На физическом уровне с подслушиванием можно бороться за счет помещения передающих кабелей в герметичные трубы, наполненные аргоном под высоким давлением. Любая попытка просверлить трубу приведет к утечке части газа из трубы, в результате давление снизится, и это послужит сигналом тревоги. Подобная техника применяется в некоторых военных системах. На уровне передачи данных пакеты, передаваемые по двухточечной линии, могут кодироваться при передаче в линию и декодироваться при приеме.

Все детали могут быть известны только уровню передачи данных, причем более высокие уровни могут даже не догадываться о том, что там происходит. Однако такое решение перестает работать в том случае, если пакету нужно преодолеть несколько маршрутизаторов, поскольку при этом пакет придется расшифровывать на каждом маршрутизаторе, что сделает его беззащитным перед атаками внутри маршрутизатора. Кроме того, такой метод не позволит защищать отдельные сеансы (например, осуществление покупок в Интернет-магазинах). Тем не менее, этот метод, называемый шифрованием в канале связи, легко может быть добавлен к любой сети и часто бывает полезен.

На сетевом уровне могут быть установлены брандмауэры, позволяющие отвергать подозрительные пакеты, приходящие извне. К этому же уровню относится IP-защита. На транспортном уровне можно зашифровать соединения целиком, от одного конца до другого. Максимальную защиту может обеспечить только такое сквозное шифрование. Наконец, проблемы аутентификации и обеспечения строгого выполнения обязательств могут решаться только на прикладном уровне.

## Вариант 18

### **Распространенные технологии несанкционированного доступа**

Злоумышленники исключительно тщательно изучают системы безопасности перед проникновением в нее. Очень часто они находят очевидные и очень простые методы «взлома» системы, которые создатели просто «проглядели», создавая хорошую систему идентификации или шифрования. Когда речь идет о компьютерной безопасности постоянно цитируется правило: «прочность цепи не выше прочности самого слабого ее звена». Например, как бы

ни была прочна система, если пароль на доступ к ней лежит в текстовом файле в центральном каталоге или записан на экране монитора – это уже неконфиденциальная система.

Очень много примеров, когда разработчики системы защиты забывают или просто не учитывают какие-либо примитивные методы проникновения в систему. Например, при работе в сети Internet не существует надежного автоматического подтверждения того, что данный пакет пришел именно от того отправителя (IP-адреса), который заявлен в пакете. А это позволяет даже при применении самого надежного метода идентификации первого пакета подменять все остальные, заявляя, что все они пришли тоже с этого же самого IP-адреса. Все это заставляет разработчиков защищенных систем постоянно помнить о самых простых и очевидных способах проникновения в систему и предупреждать их в комплексе.

Точки входа пользователя в информационную сеть называются терминалами. В том случае, когда к ним имеют доступ несколько человек или вообще любой желающий, при их проектировании и эксплуатации необходимо тщательное соблюдение целого комплекса мер безопасности. При использовании терминалов с физическим доступом необходимо соблюдать следующие требования: защищенность терминала должна соответствовать защищенности помещения; системы контроля за доступом в помещение с установленным терминалом должны работать полноценно и в соответствии с общей схемой доступа к информации.

## Вариант 19

### **Криптография в информационном обществе**

Для обозначения всей области тайной (секретной) связи используется термин «криптология», который происходит от греческих корней: *cryptos* – тайный, *logos* – сообщение. Криптология в настоящее время является новым разделом математики, имеющим важные приложения в современных информационных технологиях и может быть разделена на два направления: криптографию и криптоанализ. Наука, которая учит как следует поступать, чтобы сохранить содержание сообщений в тайне, называется криптографией. Люди, занимающиеся криптографией – криптологи.

Своим превращением в научную дисциплину криптография обязана потребностям практики и развитию электронных информационных технологий. Специфика криптографии состоит в том, что она направлена на разработку методов, обеспечивающих стойкость к любым действиям злоумышленника, хотя на момент разработки криптосистемы нереально предусмотреть все возможные способы атаки, которые могут быть изобретены в будущем на основе новых достижений теории и технологического процесса.

Центральным является вопрос, насколько надежно решается та или иная криптографическая проблема. Ответ на этот вопрос непосредственно связан с оценкой трудоемкости каждой конкретной атаки на криптосистему. Решение

такой задачи чрезвычайно сложно и составляет самостоятельный предмет исследований, называемый криптоанализом.

Криптоанализ – наука о вскрытии шифров. Криптоаналитики – специалисты в области криптоанализа. Задача криптографа – обеспечить конфиденциальность (секретность) и аутентичность (подлинность) передаваемых сообщений. Задача криптоаналитика – «взломать» систему защиты, разработанную криптографами. Он пытается раскрыть зашифрованный текст или выдать поддельное сообщение за настоящее.

## Вариант 20

### Основные угрозы безопасности ИС

С точки зрения защиты информации, компьютерная система рассматривается как набор функциональных услуг. Каждая услуга представляет собой набор функций, которые позволяют противостоять определённому множеству угроз.

По цели воздействия различают 3 основных типа угроз безопасности ИС:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Типы угроз можно классифицировать следующим образом:

а) природного характера: стихийные бедствия (наводнения, ураганы, землетрясения, пожары);

б) технического характера: аварии, сбои и отказы оборудования, средств вычислительной техники и связи;

в) человеческий фактор: ошибки проектирования и разработки компонентов ИС; ошибки эксплуатации (пользователей, операторов, обслуживающего персонала); непреднамеренные действия пользователей и обслуживающего персонала (любопытство); преднамеренные действия нарушителей (преступников, обиженных лиц из числа персонала); развитие технологий (совершенствование технологий написания вирусов, создания средств взлома).

## Вариант 21

### Классы криптографических систем

Защита информации в компьютерных системах обладает рядом специфических особенностей, связанных с тем, что информация не является жестко связанной с носителем, может легко и быстро копироваться и передаваться по каналам связи. Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифрования. Это важное свойство функции преобразования определяет два класса криптосистем: симметричные и асимметричные криптосистемы.

Симметричным называют криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа расшифрования и наоборот. В большинстве симметричных алгоритмов



применяют всего один ключ. Такие алгоритмы называют одноключевыми или алгоритмами с секретным ключом, и требуют, чтобы отправитель сообщений и их получатель заранее условились о том, каким ключом они будут пользоваться. Надежность одноключевого алгоритма определяется выбором ключа. Симметричные алгоритмы бывают двух видов. Одни из них обрабатывают открытый текст побитно. Они называются потоковыми алгоритмами или потоковыми шифрами. Согласно другим, открытый текст разбивается на блоки, состоящие из нескольких бит. Такие алгоритмы называются блочными или блочными шифрами. В современных алгоритмах блочного шифрования обычно длина блока составляет 64 бита.

Асимметричные алгоритмы шифрования, также называемые двухключевыми или алгоритмами шифрования с открытым ключом, устроены так, что ключ, используемый для шифрования сообщений, отличается от ключа, применяемого для их расшифрования. Своё название алгоритмы с открытым ключом получили благодаря тому, что ключ шифрования не надо держать в тайне. Ключ шифрования обычно называют открытым ключом, а ключ расшифрования – секретным ключом.

Вариант 22

## Принтеры

Принтер в переводе от английского языка обозначает "печатающее устройство".

Принтер является средством предназначенный для вывода текстовой и графической информации из оперативной памяти компьютера на бумажный носитель, при этом бумага может быть как листовая, так и рулонная. Основным достоинством принтера является возможность использования большого количества шрифтов, что служит для создания достаточно сложных документов.

Для работы на принтере пользователь должен выбрать необходимый ему шрифт и установить параметры печати, чтобы согласовать ширину выводимого документа и размеры используемой бумаги. Исходя из этого, например, матричные принтеры имеют две модификации: принтеры с узкой кареткой и принтеры с широкой кареткой.

Принтеры могут выводить графическую информацию даже в цвете. Они могут быть следующих типов: матричные, струйные, литерные, лазерные.

Матричные принтеры просты в эксплуатации, имеют наименьшую стоимость, но довольно низкую производительность и качество печати, особенно при выводе графических данных.

Струйные принтеры более дороги, чем матричные принтеры и требуют тщательного ухода. Работают они бесшумно, имеют очень много встроенных шрифтов. Одними из недостатков являются: довольно высокий расход чернил и неустойчивость к влаге печатных документов.

Лазерные принтеры обеспечивают наилучшее качество печати, используют принцип ксерографии - изображение переносится на бумагу со

специального барабана, к которому электрически притягиваются частички краски. Они обладают наилучшим качеством печати и производительностью, но более дорогие.

Плоттер (графопостроитель) также служит для вывода информации на бумажный носитель и, в основном, используется для вывода графической информации. Графопостроители широко применяются при автоматизации проектирования, когда необходимо получать чертежи разрабатываемых изделий. Плоттеры разделяют на одноцветные и цветные, а также - по качеству вывода информации на печать.

## Вариант 23

### **Классификация криптоалгоритмов**

В зависимости от наличия либо отсутствия ключа кодирующие алгоритмы делятся на тайнопись и криптографию. В зависимости от соответствия ключей шифрования и дешифрования – на симметричные и асимметричные. В зависимости от типа используемых преобразований – на подстановочные и перестановочные. В зависимости от размера шифруемого блока – на потоковые и блочные шифры.

Симметричные криптоалгоритмы выполняют преобразование небольшого (1 бит либо 32 бит-128 бит) блока данных в зависимости от ключа таким образом, что прочесть исходное сообщение можно, зная этот секретный ключ.

Симметричные криптосистемы являются полноценными программами, которые могут на основе симметричных криптоалгоритмов кодировать и декодировать файлы произвольной длины. Криптосистемы устраняют целый класс потенциальных уязвимостей систем, использующих симметричные криптоалгоритмы.

В асимметричных криптоалгоритмах для зашифровывания сообщения используется один ключ, а для расшифровки другой. Ключ шифрования известен всем, но выполняемое преобразование необратимо, поэтому зашифрованный текст никто не может прочесть, кроме получателя – именно он один знает второй (закрытый) ключ.

Асимметричные криптосистемы. Поскольку асимметричные криптоалгоритмы очень медленны, в реальных системах используются быстрые надежные симметричные криптоалгоритмы по схеме с ключом сеанса. Сам ключ сеанса кодируется асимметричным криптоалгоритмом с помощью открытого ключа получателя. Подобная система обладает всеми свойствами асимметричного криптоалгоритма и высоким быстродействием.

## Вариант 24

### Скремблеры

Скремблерами называются программные или аппаратные реализации алгоритма, позволяющего шифровать побитно непрерывные потоки информации. Сам скремблер представляет набор бит, изменяющихся на каждом шаге по определенному алгоритму. После выполнения каждого очередного шага на его выходе появляется шифрующий бит – либо 0, либо 1, который накладывается на текущий бит информационного потока операцией XOR. В последнее время сфера применения скремблирующих алгоритмов значительно сократилась. Это объясняется, в первую очередь, снижением объемов побитной последовательной передачи информации, для защиты которой были разработаны данные алгоритмы. Практически повсеместно в современных системах применяются сети с коммутацией пакетов, для поддержания конфиденциальности которой используются блочные шифры.

Суть скремблирования заключается в побитном изменении проходящего через систему потока данных. Практически единственной операцией, используемой в скремблерах является XOR – побитное исключающее. Параллельно прохождению информационного потока в скремблере по определенному правилу генерируется кодирующий поток. Как прямое, так и обратное шифрование осуществляется наложением по XOR кодирующей последовательности на исходную последовательность. Генерация кодирующей последовательности бит производится циклически из небольшого начального объема информации – ключа по следующему алгоритму: из текущего набора бит выбираются значения определенных разрядов и складываются по XOR между собой. Все разряды сдвигаются на 1 бит, а только что полученное значение (0 или 1) помещается в освободившийся самый младший разряд. Значение, находившееся в самом старшем разряде до сдвига, добавляется в кодирующую последовательность, становясь очередным ее битом.

Существенным недостатком скремблирующих алгоритмов является их нестойкость к фальсификации.

## Вариант 25

### Компьютерные вирусы

Компьютерный вирус – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированных действий на несущем компьютере.

Программные вирусы. Программные вирусы – это блоки программного кода, целенаправленно внедренные внутри других прикладных программ. По прошествии определенного времени, создав достаточное количества копий, программный вирус может перейти к разрушительным действиям – нарушению работы программ и операционной системы, удалению

информации, хранящейся на жестком диске. Этот процесс называется вирусной атакой.

Загрузочные вирусы. От программных вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей (гибких и жестких дисков). Кроме того, на включенном компьютере они могут временно располагаться в оперативной памяти.

Макровирусы. Эта особая разновидность вирусов поражает документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения так называемых макрокоманд.

## **Рекомендуемая литература для СРС № 2**

1 Букейханова Р.К., Чумбалова Г.М. Обучение перевода на казахский язык научно-технических текстов. - Алматы: АУЭС, 2007. – 50 с.

2 Кубдашева К.Б. Профессиональный русский язык: Методические указания для выполнения СРС №1 (перевод специального текста). - Алматы: АУЭС, 2013.- 32 с.

3. Нурмаханова М.К. Профессиональный русский язык. Методические указания для студентов специальности 5В100200. – Алматы: АУЭС, 2015. – 49 с.

## **Словари**

1 Бериккулы А., Шайхин Б.М. и др. Казахско-русский, русско-казахский терминологический словарь. Электроника, радиотехника и связь. – Алматы: Рауан, - 2000. – 236 с.

2 Политехнический словарь./ Гл. ред. Акад. А. Ю. Ишлинский. – М.: Советская энциклопедия, 1980. – 656 с.

3 Русско-казахско-английский политехнический словарь. Сост. М.Р.Тусипбек, А.К.Кусаинов. – Алматы: Rond&A, 2010. – 740 с.

4 Казахско-русский, русско-казахский терминологический словарь/ Под общей редакцией д.п.н., проф. А. К. Кусаинова. В 32-х томах. - Алматы: Рауан, 2000.–312 с.

5 Пчёлкина В. В., Комарова Л. Н. И др. Словарь иностранных слов.- М.: Русский язык. 1979.- 607 с.

6 Раренко М.Б. Основные понятия переводоведения. Терминологический словарь-справочник. – М.: ИНИОН РАН, 2010. – 260 с.

7 Русско-казахский словарь/ Под редакцией Н. Т. Сауранбаева и др. - Алматы: Дайк-Пресс, 2005. – 1125 с.

8 Сарыбеков М., Сыздыкназаров М. Словарь науки. Общенаучные термины и определения. Науковедческие понятия и категории: Учебное пособие. – Алматы: Триумф «Т», 2008. – 504 с.

## Образец выполнения семестровой работы № 1. Специальность 5В070300 – Информационные системы

### Текст № 1

#### Работа в системе Windows

*Программа* - полный, достаточный набор команд, выполнение которых заставляет компьютер вести себя определенным образом и за конечное число шагов решить конкретную задачу.

Без программ компьютер бесполезен. Программа на языке программирования или в машинном коде описывает действия, которые компьютер должен выполнить в виде точной и подробной последовательности команд *обработки данных*. Программа подобна рецепту: содержит список ингредиентов (так называемых переменных) и команд (инструкций), которые указывают компьютеру действия с переменными. Переменные могут представлять числа, текст, графические изображения.

*Операционные системы* Microsoft Windows версий 9x/2000/jXP используются в большинстве *персональных компьютеров* (обозначение Windows 9x соответствует версиям Windows 95 и 98). Они имеют графический *интерфейс*, поддерживают многозадачный режим, управление виртуальной памятью, к ним выпущено много прикладных программ, есть возможность подключать разнообразные периферийные устройства и работать в компьютерной сети.

Вместе с операционной системой Windows кроме собственно системных программ устанавливаются *стандартные прикладные программы* - простые программы для работы и отдыха: редактирования текста, просмотра рисунков, мультимедиа.

*Программа «Блокнот»* - простой текстовый редактор одношрифтового набора, правки и просмотра текстовых файлов в окне.

WordPad (Write) - текстовый редактор, который выполняет несложное форматирование текста, позволяет менять *шрифт* и кодировку символов (Windows или DOS), переходить к греческим и западноевропейским буквам.

Paint - графический редактор растровых (точечных) рисунков. Программа «Калькулятор» имеет графический интерфейс реального калькулятора. В обычном виде - кнопки арифметических действий, а в инженерном виде - кнопки математических функций команд.

Стандартные программы выполняют базовый набор простых работ с текстом, графикой, вычислениями; запускаются они быстрее более сложных *приложений*. Можно установить разнообразные дополнительные прикладные программы.

## Образец оформления СРС № 1

Термины, выписанные из текста №1 и толкование на двух языках

Термины и терминосочетания на русском языке с толкованием.	Термины и терминосочетания на казахском языке с толкованием.
<i>Программа</i>	<i>Программа (Бағдарлама)</i>
Полный, достаточный набор команд, выполнение которых заставляет компьютер вести себя определенным образом и за конечное число шагов решить конкретную задачу.	Компьютер өзін белгілі түрде жұмыс жасауға және соңғы әрекет мөлшерінде нақты мәселені шешуге мүмкіндік беретін командалардың жетерлік, толық жинағы.
<i>Обработка данных</i>	<i>Деректерді өңдеу</i>
Обработка хранения или манипулирование данными.	Деректерді өңдеу, сақтау және бұрмалау.
<i>Операционные системы</i>	<i>Операциялық жүйелер</i>
Собрание элементов программного, микропрограммного и аппаратного обеспечения, предназначенных для управления выполнением программ и обеспечения таких функций, как распределение ресурсов компьютера, управление заданиями, управление вводом-выводом, управление файлами.	Файлдармен жұмыс жасау, енгізу-шығаруды игеру, тапсырмаларды меңгеру, компьютер қорын үлестіру сияқты жұмыстарды қамтуға және программалардың орындалуын басқаруға арналған программалық, микропрограммалық және аппараттық қамтамасыз етудің элементтер жиынтығы.
<i>Персональный компьютер</i>	<i>Персоналды (Дербес) компьютер</i>
Представляет собой конструктивно завершенное вычислительное устройство, реализованное на базе микропроцессорного комплекта сверхбольших интегральных схем (СБИС) и оформленное в виде автономного устройства с источником питания, интерфейсом, устройством отображения информации и комплектом программного обеспечения.	Есептеуіш құрылғысының конструктивті түрі, микропроцессор базасының іске асқан интегралдың жүйесі және автономдық құрылғы ретінде қорек көзімен, интерфейспен, бағдарламамен қамтамасыз ету кешенімен байланысқан.
<i>Интерфейс</i>	<i>Интерфейс</i>
Совокупность возможностей, способов и методов одновременного действия.	Компьютерлік жүйенің құрауыштары мен қатысушыларының арасындағы өзара байланыс.
<i>Стандартные прикладные програм-</i>	<i>Стандарттық қолданбалы</i>

<i>мы</i>	<i>программалар</i>
Простые программы для работы и отдыха: редактирования текста, просмотра рисунков, мультимедиа.	Жұмыс істеуге және дем алуға арналған жеңіл программалар: мәтінді редактірлеу, сурет қарау, мультимедиа.
<i>Программа «Блокнот»</i>	«Блокнот» программасы
Простой текстовый редактор одношрифтового набора, правки и просмотра текстовых файлов в окне.	Терезедегі мәтіндік файлдарды бір шрифтпен теру, түзету және қарап шығудың қарапайым мәтіндік редакторы.
<i>Шрифт</i>	<i>Қарпін</i>
Графический рисунок начертаний букв и знаков, составляющих единую стилистическую и композиционную систему, набор символов определенного размера и рисунка.	Берілген символдар жинағының графикалық формасын сипаттайтын мәліметтер файлы.
<i>Приложение</i>	<i>Қосымша бағдарлама</i>
Программы, которые функционируют под управлением определенной ОС и позволяют пользователю обрабатывать информацию и работать в компьютерных сетях.	Пайдаланушыға белгілі операциялық жүйені басқарып, ақпаратты өндеуге және компьютерлік желілерде жұмыс жасауға мүмкіндік беретін программа (бағдарлама).

*Следует привлечь еще несколько текстов, чтобы набрать 30-35 терминов согласно заданию СРС.*

### **Рекомендуемая литература для СРС № 1**

- 1 Акулиничев Ю. П., Дроздова В.И. Теория информации: Учебное пособие. - Томск: ТМЦДО, 2005. – 108 с.
- 2 Губарев А.В. Информационное обеспечение системы менеджмента качества. - М.: Горячая линия – Телеком, 2013. – 132 с.
- 3 Кудряшов Б.Д. Теория информации: Учебник для вузов. – СПб.: Изд. Дом Питер, 2009.- 460 с.
- 4 Куралбаев З.К. Основы информационных систем. Конспект лекций. – Алматы: АИЭС, 2009.- 80 с.
- 5 Нурмаханова М.К. Профессиональный русский язык. Методические указания для студентов специальности 5В100200. – Алматы: АУЭС, 2015. – 49 с.
- 6 Перепелкин Д.А. Схемотехника усилительных устройств: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 238 с.
- 7 Сатимова Е.Г. Операционные системы. LINUX. Решения задач структурной и функциональной организации: Учебное пособие. – Алматы: АУЭС, 2009. – 120 с.

8 Степанов А. Информатика: Учебник для вузов. 4-е-издание.– М.: Высшая школа, 2004. – 688 с.

9 Шелухин О.И. Моделирование информационных систем: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2016. – 516 с.

### **Словари**

1 Бериккулы А., Шайхин Б.М. и др. Казахско-русский, русско-казахский терминологический словарь. Электроника, радиотехника и связь. – Алматы: Рауан, 2000. – 236 с.

2 Политехнический словарь/ Гл. ред. Акад. А. Ю. Ишлинский. – М.: Советская энциклопедия, 1980. – 656 с.

3 Русско-казахско-английский политехнический словарь. Сост. М.Р.Тусипбек, А.К.Кусаинов. – Алматы: Rond&A, 2010. – 740 с.

4 Казахско-русский, русско-казахский терминологический словарь/ Под общей редакцией д.п.н., проф. А. К. Кусаинова. В 32-х томах. - Алматы: Рауан, 2000.–312 с.

5 Пчёлкина В. В., Комарова Л. Н. И др. Словарь иностранных слов.- М.: Русский язык. 1979.- 607 с.

6 Раренко М.Б. Основные понятия переводоведения. Терминологический словарь-справочник. – М.: ИНИОН РАН, 2010. – 260 с.

7 Русско-казахский словарь/ Под редакцией Н. Т. Сауранбаева и др. - Алматы: Дайк-Пресс, 2005. – 1125 с.

8 Сарыбеков М., Сыздыкназаров М. Словарь науки. Общенаучные термины и определения. Науковедческие понятия и категории: Учебное пособие. – Алматы: Триумф «Т», 2008. – 504 с.

### **Семестровая работа студента № 2**

Тема: письменный перевод текста по специальности.

Цель: развить умения и навыки письменного перевода научно-технических текстов.

Задание: перевести текст по специальности с русского на казахский язык.

Ход работы: основным требованием к выполнению семестровой работы № 2 является адекватный перевод научно-технического текста с русского на казахский язык. Перед началом работы над переводом необходимо полностью прочитать текст, выделить трудные для восприятия абзацы, частотные ключевые понятия и термины. При наличии нескольких вариантов перевода или неясности лексической единицы нужно использовать терминологические толковые словари. Для перевода сложного предложения необходимо разобраться в его грамматической структуре, выявить основной смысл предложения для передачи последнего в соответствии со структурой казахского предложения. Переводить текст следует по смысловым



фрагментам. Такой фрагмент чаще состоит не из одного, а из нескольких предложений и редко выходит за рамки абзаца. Варианты текстов распределяются между студентами преподавателем.

*Требования к оформлению работы.*

Работа должна быть выполнена на формате А4 компьютерной версткой. Параметры оформления текста: кегль 14, шрифт Times New Roman, межстрочный интервал 1,0. Поля: левое – 2,5 см, правое – 1,8 см, нижнее – 2,5 см, верхнее – 2,0 см. Выравнивание текста на листах должно производиться по ширине строк.

## **Перечень текстов, включенных в СРС № 2, для специальности 5В070300 – Информационные системы**

### Вариант 1

#### **Создание сайта**

Созданием сайтов сегодня занимается каждый второй. Объявления на эту тему можно встретить на каждой стене, во всех форумах и группах социальных сетей. Программы-конструкторы сайтов типа, например, Microsoft FrontPage и Dreamweaver, существуют уже не первый десяток лет. Крупный недостаток таких программ – их нужно изучать далеко не один день, чтобы понять, как они работают. Большой минус онлайн-конструкторов – они недостаточно функциональны.

Incomedia WebSite X5 Evolution (<http://www.website5.com>) представляет собой нечто среднее между этими двумя подходами. От конструкторов взята простота работы, от Dreamweaver и прочих – гибкость настроек и возможность сделать красивый дизайн.

Основа программы – шаблоны, которые можно переделывать, некий «скелет» сайта. Шаблонов в лицензионной версии около полутора тысяч на все случаи жизни – от фотографии до интернет-магазина. Стандартно X5 предлагает пользователю пройти пять этапов создания сайта. На первом вы выбираете стиль меню, настраиваете его базовые блоки (в текстовых полях – название сайта, его URL). Потом выбираете шаблон, настраиваете его цвет и переходите к названию заголовка. На втором этапе вы создаёте карту сайта. В его структуре пишете страницы на всех уровнях с их заголовками. Созданную структуру можно модифицировать в любое время. Просмотр сайта доступен на кнопке «Тест» в правом верхнем углу.

Самое главное – это, конечно, создание веб-страниц. В отличие от FrontPage и «Блокнота», в X5 они формируются в таблице, внешне похожей на Excel. Каждая ячейка таблицы – это определенный тип данных: текст, изображения, слайд-шоу, flash-анимация и т.д. Последний этап – это экспорт сайта в Интернет или на жёсткий диск. Если у вас есть FTP-доступ, то в том же окне введите данные своего FTP-аккаунта, и сайт загрузится прямо в

указанную папку. В качестве примера посмотрите на сайт <http://steklomoi.com/> – он был создан с нуля в WebSite X5 за пару часов. Это, конечно, не работа профессиональной студии, но такой сайт может сделать любой человек без специальных знаний.

Главный недостаток WebSite X5 Evolution – то, что программа платная. Незарегистрированная версия работает 30 дней и даёт доступ к пяти шаблонам и созданию пяти страниц сайта.

## Вариант 2

### **Информация и вычислительные машины**

Совершенно новые возможности для поиска и обработки информации открыло перед людьми изобретение в середине XX в. электронных вычислительных машин – ЭВМ (за рубежом эти машины получили название компьютер). Первоначально ЭВМ создавались для автоматизации вычислений. Затем их научили записывать и хранить информацию на магнитных лентах, печатать ее на бумаге, выводить на экран ЭВМ. По мере развития они стали использоваться для создания архивов, подготовки и редактирования текстов, выполнения чертежных и графических работ, автоматизации производства и многих других видов человеческой деятельности. В 70-х годах развитие электроники послужило толчком для создания и массового производства нового вида компьютеров – персональных ЭВМ, которые сегодня широко применяются в школах, институтах, издательствах и т.п. Такие машины можно использовать для учебы, работы, игры и многих других целей.

Применение таких ЭВМ на производстве, при проектировании, в научных исследованиях и образовании может коренным образом изменить содержание деятельности и условия работы многих миллионов людей. Прежде всего ЭВМ открывают возможности для создания автоматизированных технологий производства. С их помощью можно создавать новые виды машин, приборов и устройств, управляемых с помощью ЭВМ. К началу XXI вычислительные машины на базе таких устройств сделали возможным создание «безлюдных» технологий производства. На таких «фабриках будущего» физическая работа будет выполняться роботами, а роль людей сведется к планированию производства, программированию роботов и проектированию новых изделий с помощью ЭВМ.

Применение ЭВМ во многих видах деятельности уже сейчас позволяет существенно упростить работу людей по подготовке, накоплению и переработке информации, проведению проектно-конструкторских работ и научных исследований. Электронно-вычислительные машины уже есть в школах и они будут помогать при изучении физики и математики, химии, биологии и многих других учебных предметов. Умение общаться с ЭВМ и использовать их в своей работе, также, как умение пользоваться ручкой, в ближайшие 10-15 лет, станет необходимым практически для всех и составит

основу компьютерной грамотности. Компьютерная грамотность – это умение читать и писать, считать и рисовать, а также искать информацию, применяя для этого ЭВМ.

### Вариант 3

### Алгоритм

Алгоритм – описание последовательности действий (план), строгое исполнение которых приводит к решению поставленной задачи за конечное число шагов. Человек постоянно сталкивается с понятием алгоритма в различных сферах деятельности (кулинарные книги, инструкции по использованию различных приборов, правила решения математических задач и т.д.). Обычно мы выполняем привычные действия не задумываясь, механически. Например, мы хорошо знаем, как открывать дверь ключом. Однако чтобы научить этому малыша, придётся чётко объяснить и действия, и порядок их выполнения:

- 1) Достать ключ из кармана.
- 2) Вставить ключ в замочную скважину.
- 3) Повернуть ключ два раза против часовой стрелки.
- 4) Вынуть ключ.

Если мы внимательно оглянемся вокруг, то обнаружим много алгоритмов, которые мы постоянно выполняем. Мир алгоритмов очень разнообразен. Несмотря на это, удаётся выделить общие свойства, которыми обладает любой алгоритм. Свойства алгоритмов:

- 1) Дискретность: алгоритм должен состоять из конкретных действий, следующих в определённом порядке.
- 2) Детерминированность: любое действие должно быть строго и недвусмысленно определено в каждом случае.
- 3) Конечность: каждое действие и алгоритм в целом должны иметь возможность завершения.
- 4) Массовость: один и тот же алгоритм можно использовать с разными исходными данными.
- 5) Результативность: отсутствие ошибок, алгоритм должен приводить к правильному результату для всех допустимых входных значений.

Виды алгоритмов:

- 1) Линейный алгоритм: описание действий, которые выполняются однократно в разовом порядке.
- 2) Циклический алгоритм: описание действий, которые должны повторяться указанное число раз или пока не выполнено задание.
- 3) Разветвляющийся алгоритм: алгоритм, в котором в зависимости от условия выполняется либо одна, либо другая последовательность действий.
- 4) Вспомогательный алгоритм: алгоритм, который можно использовать в других алгоритмах, указав только его имя.

Стадии создания алгоритма:

1) Алгоритм должен быть представлен в форме, понятной человеку, который его разрабатывает.

2) Алгоритм должен быть представлен в форме, понятной тому объекту (в том числе и человеку), который будет выполнять описанные в алгоритме действия.

#### Вариант 4

### Технология клиент-сервер

Характер взаимодействия компьютеров в локальной сети принято связывать с их функциональным назначением. Как и в случае прямого соединения, в рамках локальных сетей используется понятие клиент и сервер. Технология клиент-сервер — это особый способ взаимодействия компьютеров в локальной сети, при котором один из компьютеров (сервер) предоставляет свои ресурсы другому компьютеру (клиенту). В соответствии с этим различают одноранговые сети и серверные сети. При одноранговой архитектуре в сети отсутствуют выделенные серверы, каждая рабочая станция может выполнять функции клиента и сервера. В этом случае рабочая станция выделяет часть своих ресурсов в общее пользование всем рабочим станциям сети. Как правило, одноранговые сети создаются на базе одинаковых по мощности компьютеров.

Одноранговые сети являются достаточно простыми в наладке и эксплуатации. В том случае, когда сеть состоит из небольшого числа компьютеров и ее основной функцией является обмен информацией между рабочими станциями, одноранговая архитектура является наиболее приемлемым решением. Подобная сеть может быть достаточно быстро и просто реализована средствами такой популярной операционной системы как Windows 98. Наличие распределенных данных и возможность изменения своих серверных ресурсов каждой рабочей станцией усложняет защиту информации от несанкционированного доступа, что является одним из недостатков одноранговых сетей. Понимая это, разработчики начинают уделять особое внимание вопросам защиты информации в одноранговых сетях. Другим недостатком одноранговых сетей является их более низкая производительность. Это объясняется тем, что сетевые ресурсы сосредоточены на рабочих станциях, которым приходится одновременно выполнять функции клиентов и серверов. В серверных сетях осуществляется четкое разделение функций между компьютерами: одни из них постоянно являются клиентами, а другие - серверами.

## Вариант 5

### Удаление и изменение программ

Независимо от того, приобрели вы новую программу или хотите удалить старую, категория *Программы* папки *Панель управления* значительно упростит вашу жизнь. В одном из его списков, *Программы и компоненты*, перечислены все программы, установленные в Windows 7. Выберите ту из них, которую нужно изменить или удалить. Для удаления или изменения настроек, которые вызывают трудности в работе программ, выполните следующие действия:

1) В меню *Пуск* выберите команду *Панель управления*, а затем щёлкните на ссылке *Удалить программу* в категории *Программы*. В диалоговом окне *Удаление или изменение программы* даётся список всех установленных в компьютере программ с указанием их разработчика, занимаемого на диске размера, даты установки, а также номера версии. Чтобы освободить место на диске, щёлкните на заголовке столбца *Установлено* или *Размер*, чтобы найти устаревшие, занимающие много места на диске программы, которые редко используются. Затем удалите их.

2) Щёлкните на названии интересующей вас программы, а потом укажите необходимое действие: *Удалить*, *Изменить* или *Восстановить*. Кнопка *Удалить* всегда отображается в строке меню. Другие две кнопки, *Изменить* и *Восстановить*, доступны только для отдельных программ. *Удалить*. Полностью удаляет программу из компьютера.

*Изменить*. Эта кнопка позволяет изменить некоторые атрибуты программы или удалить некоторые её компоненты. *Восстановить*. Эта кнопка запускает тестирование программы и производит замену повреждённых файлов новыми.

3) В окне с запросом на подтверждение операции щёлкните на кнопке *Да*. В зависимости от выбранной кнопки Windows 7 либо удалит программу с жесткого диска, либо запустит встроенную в программу утилиту установки для изменения или восстановления. После удаления программы ею можно воспользоваться только в случае повторной установки с исходного компакт-диска. В отличие от остальных удалённых элементов удалённые программы не помещаются в папку *Корзина*. Всегда используйте апплет *Удаление или изменение программы* окна *Панель управления* ненужных программ. Простое удаление папки с программой не всегда является оптимальным решением, так как операционная система будет выводить большое количество сообщений об ошибках.

## Вариант 6

### Операционная система

Операционная система – это программное обеспечение (т.е. инструкции), которое заставляет аппаратное обеспечение (т.е. компьютер) выполнять какие-

либо действия. Linux – это операционная система, которая позволяет техническим средствам вашего компьютера превратиться в пригодную для работы машину. Операционная система взаимодействует с оборудованием и позволяет ему выполнять поставленные перед ним задачи по основам построения современных операционных систем, такие, как хранение информации в файлах, отображение информации на экране монитора, отправление данных на печать, сложение двух чисел. Операционная система служит связующим звеном между всеми действиями, которые Вы выполняете на компьютере.

UNIX - одна из самых популярных в мире операционных систем благодаря тому, что ее сопровождает и распространяет большое число компаний. Linux - свободно распространяемая версия UNIX, первоначально была разработана Линусом Торвальдсом (Linus Torvalds) (torvalds@kruuna.helsinki.fi) в Университете Хельсинки (Финляндия). Linux был создан с помощью многих UNIX-программистов и энтузиастов, тех, кто имеет достаточно навыков и способностей развивать систему. Ядро Linux не использует коды AT&T или какого-либо другого частного источника, и большинство программ Linux разработаны в рамках проекта GNU из Free Software Foundation в Cambridge, Massachusetts. В настоящее время многие компании имеют компьютерные сети, построенные на серверных ОС Linux.

Linux - это многозадачная, многопользовательская операционная система. Это означает, что много людей может одновременно использовать один компьютер, выполняя много различных задач. Это существенное отличие от MS-DOS и Windows (если это не Windows Server), где только один человек может использовать в данный момент операционную систему. В Linux пользователи должны себя идентифицировать при входе, что состоит из двух шагов: ввода имени (имя, по которому вас идентифицирует система) и входной пароль, который является вашим секретным словом для регистрации в системе. Поскольку только вы знаете пароль, никто не может войти в систему под вашим именем.

## Вариант 7

### **Создание виртуальных компьютеров**

В настоящее время все чаще администраторы используют технологию виртуальных машин. Представьте себе ситуацию, часто складывающуюся в процессе разработки программы сразу для нескольких операционных систем, или может возникнуть необходимость исследования нового, неизвестного и даже потенциально опасного программного обеспечения.

В процессе разработки стратегии миграции с одной операционной системы на другую может возникнуть необходимость проверить, как будет работать новое программное обеспечение. Создав одну виртуальную машину с нужным набором программного обеспечения, в течение нескольких минут можно растиражировать ее на все машины компьютерного класса. Ничего страшного не произойдет, если обучаемый в процессе освоения преподаваемых технологий умышленно или нечаянно разрушит подопытную среду. Для восстановления

поврежденной виртуальной машины из резервной копии понадобится всего несколько минут.

Виртуальный компьютер — специальная программа, запускаемая, например, в ОС Windows XP и моделирующая физический компьютер на основе процессора Intel x86. Это бесплатная программа, которая устанавливается также как любая другая программа Windows. Фактически, вы можете иметь на своем компьютере хоть 10 одновременно загруженных и одновременно работающих операционных систем. Основная идея проста — создать эмулятор Linux, работающий под Windows и позволяющий запускать программы этой ОС.

## Вариант 8

### Изменение интерфейса Windows 7

Одна из самых популярных категорий, *Оформление и персонализация*, даёт много возможностей изменить вид и поведение элементов интерфейса Windows 7. Открыв категорию, вы увидите семь значков, описанных ниже. *Персонализация*. Несмотря на то, что многим пользователям эта область кажется ненужной, она помогает изменять внешний вид Windows. С её помощью изменяется рисунок или фотография на рабочем столе, устанавливается заставка, меняются основные цвета окон Windows 7. Для быстрого перехода к этим настройкам правой кнопкой мыши щёлкните в свободном месте рабочего стола и в контекстном меню выберите параметр *Персонализация. Экран*.

В то время как с помощью апплета *Персонализация* можно манипулировать цветами, апплет *Экран* позволяет выполнять настройки самого монитора. Например, с помощью него можно увеличить текст, чтобы не напрягать глаза, настроить разрешение экрана, а также подключить дополнительный монитор. *Гаджеты рабочего стола*. Этот апплет управляет мини-приложениями рабочего стола, называемыми гаджетами. Для быстрого вызова апплета щёлкните правой кнопкой мыши в свободной области рабочего стола и в контекстном меню выберите параметр *Гаджеты. Панель задач и меню «Пуск»*.

Хотите добавить собственную фотографию вместо изображения в верхней части меню *Пуск* или перенастроить панель задач, прикрепленную к нижнему краю рабочего стола? Для быстрого вызова этого апплета щёлкните правой кнопкой мыши на кнопке *Пуск* и выберите параметр *Свойства. Параметры папок*. Обычно используются опытными пользователями и в основном для изменения вида и поведения папок с файлами на дисках. Для быстрого перехода в эту категорию откройте любую папку, выберите пункт меню *Упорядочить* и затем — *Параметры папок и поиска. Шрифты*. С помощью этого апплета устанавливаются, просматриваются и удаляются шрифты, применяемые в работе.

## Кодирование звуковой информации

Приемы и методы работы со звуковой информацией пришли в вычислительную технику поздно. В отличие от числовых, текстовых и графических данных, у звукозаписей не было столь длительной и проверенной истории кодирования. В итоге методы кодирования звуковой информации двоичным кодом далеки от стандартизации. Множества отдельных компаний разработали свои корпоративные стандарты.

Метод FM (Frequency Modulation) основан на том, что теоретически любой сложный звук можно разложить на последовательность простейших гармонических сигналов разных частот, каждый из которых представляет собой правильную синусоиду, а следовательно, может быть описан числовыми параметрами, то есть кодом. В природе звуковые сигналы имеют непрерывный спектр. То есть являются аналоговыми. Их разложение в гармонические ряды и представление в виде дискретных цифровых сигналов выполняют специальные устройства - аналогово-цифровые преобразователи (АЦП). Обратное преобразование для воспроизведения звука, закодированного числовым кодом, выполняют цифро-аналоговые преобразователи (ЦАП). При таких преобразованных неизбежных потерях информации, связанные с методом кодирования, качество звукозаписи обычно получается не вполне удовлетворительным и соответствует качеству звучания простейших электромузыкальных инструментов с окрасом, характерным для электронной музыки. В то же время данный метод кодирования обеспечивает весьма компактный код, и потому он нашел применение еще в те годы, когда ресурсы средств вычислительной техники были явно недостаточны.

Метод таблично - волнового (Wave – Table) синтеза лучше соответствует современному уровню развития техники. Если говорить упрощенно, то можно сказать, что где-то в заранее подготовленных таблицах хранятся образцы звуков для множества различных музыкальных инструментов. В технике такие образцы называют *сэмплами*. Числовые коды выражают тип инструмента, номер его модели, высоту тона, продолжительность и интенсивность звука, динамику его изменения, некоторые параметры среды, в которой происходит звучание, а также прочие параметры, характеризующие особенности звука. Поскольку в качестве образцов используются «реальные» звуки, то качество звука, полученного в результате синтеза, получается очень высоким и приближается к качеству звучания реальных музыкальных инструментов.



## Ссылки на ячейки

Формула может содержать ссылки, т.е. адреса ячеек, содержимое которых используется в вычислениях. Это означает, что результат вычисления формулы зависит от числа, находящегося в другой ячейке. Значение, отображаемое в ячейке с формулой, пересчитывается при изменении значения ячейки, на которую указывает ссылка. Ссылку на ячейку можно задать разными способами. Во-первых, адрес ячейки можно ввести вручную. Другой способ состоит в щелчке на нужной ячейке или выборе диапазона, адрес которого требуется ввести. Ячейка или диапазон при этом выделяются пунктирной рамкой. Можно ссылаться на ячейки, находящиеся на других листах рабочей книги, в другой рабочей книге, или на данные другого приложения. Ссылки на ячейки других рабочих книг называются внешними.

После того как формула введена в ячейку, её можно перенести, скопировать или распространить на диапазон ячеек. При перемещении формулы в новое место таблицы ссылки в формуле не изменяются, а ячейка, где раньше была формула, становится свободной. При копировании формула перемещается в другое место таблицы, ссылки изменяются, но ячейка, где раньше находилась формула, остаётся без изменения. При копировании формул возникает необходимость управлять изменением адресов ячеек или ссылок. Для этого перед символами адреса ячейки или ссылки устанавливаются символы \$. Изменяются только те атрибуты адреса ячейки, перед которыми не стоит символ \$.

Если перед всеми атрибутами адреса ячейки поставить символ \$, то при копировании формулы ссылка не изменится. Например, если в записи формулы ссылку на ячейку D7 записать в виде \$D7, то при перемещении формулы будет изменяться только номер строки 7. Запись D\$7 означает, что при перемещении будет изменяться только символ столбца «D». Если же записать адрес в виде \$D\$7, то ссылка при перемещении формулы на этот адрес не изменится, и в расчётах будут участвовать данные из ячейки D7. Если в формуле указан интервал ячеек G3:L9, то управлять можно каждым из четырёх символов: G, 3, L и 9, помещая перед ними символ \$.

Если в ссылке используются символы \$, то она называется *абсолютной*, если символов \$ в ссылке нет – *относительной*. Адреса таких ссылок называются абсолютными и относительными соответственно. Абсолютные адреса при перемещении формул не изменяются, а в относительных адресах происходит смещение на величину переноса. Для редактирования формулы следует дважды щёлкнуть на соответствующей ячейке. При этом ячейки (диапазоны), от которых зависит значение формулы, выделяются на рабочем листе цветными рамками, а сами ссылки отображаются в ячейке и в строке формул тем же цветом. Это облегчает редактирование и проверку правильности формул.

## Вариант 11

### Цифровые автоматы в схемотехнике

Автомат – это пример устройства, реакция которого зависит не только от входа, но и от того что было раньше, то есть от состояния в предыдущий момент времени.

Компьютер – пример цифрового автомата. Он обладает памятью, которая хранит его состояние. В зависимости от состояния компьютер выполняет то или иное действие. Синоним термину «цифровой автомат» - «конечный автомат». Первый термин подчеркивает, что автомат работает с цифрами, то есть конечными наборами символов, второй – что его память конечна.

Отличия цифрового автомата от конечного автомата общего вида состоят в следующем:

- он предназначен для представления чисел и выполнения операций над ними, в нем на самом первом этапе, этапе синтеза одноразрядного или многоразрядного сумматора, решается проблема гонок (порождаемых задержками);

- цифровой автомат имеет погрешность представления – погрешность, которая возникает при представлении счетных или несчетных числовых систем из-за ограниченного количества разрядов и памяти. Отличия реализованной операции от арифметической в особо важных случаях выражаются дополнительными сигналами: переполнением, сигналом "машинного нуля";

- цифровой автомат слишком сложен для автоматического синтеза.

Аппаратно реализуются, в основном, сумматоры, умножители и делители. Более сложные операции сводятся к последним, так что арифметическое устройство используется в паре с управляющим автоматом, который реализуется либо аппаратно, либо программно.

## Вариант 12

### Аналого-цифровые и цифро-аналоговые преобразователи

Цифро-аналоговые преобразователи (DAC — digital-analog converter) преобразуют цифровой сигнал в аналоговый. Две самые распространенные реализации этого вида оборудования — модуляторы-демодуляторы (модемы) и преобразователи, которые используются в АТС для каждого аналогового канала.

Модем преобразует униполярные цифровые сигналы, передаваемые компьютером, в поток аналогового сигнала. Униполярным является сигнал, в котором используется только одна полярность напряжения. Таким образом, в потоке сигнала используются либо только отрицательные, либо только положительные значения напряжения. Для передачи данных по аналоговым каналам до скорости 56 Кбит/с разработаны различные типы сжатия. При использовании подобных высокоскоростных технологий полоса пропускания ограничена из-за перекрестных наводок на стороне коммутатора телефонной станции. При передаче информации по обычным голосовым каналам с чистой скоростью 56 Кбит/с возникают проблемы, поэтому ради мирного

существования механизмов передачи голоса и данных с помощью модемов приходится вносить определенные ограничения.

Цифро-аналоговые и аналого-цифровые преобразования необходимы, так как сигнал, поступающий от компьютера, является цифровым, а линия связи — аналоговой. При использовании цифровой линии связи наподобие технологий цифровой сети с комплексным обслуживанием (Integrated Services Digital Network — ISDN) потребность в преобразовании сигнала отпадает. Единственное, что может потребоваться в таком случае — изменить формат цифрового сигнала с целью установления соответствия спецификации ISDN.

### Вариант 13

#### **Устройство компьютера**

Компьютер (англ. computer – вычислитель) представляет собой программируемое электронное устройство, способное обрабатывать данные и производить вычисления, а также выполнять другие задачи манипулирования символами. Основу компьютеров образует аппаратура (HardWare), построенная, в основном, с использованием электронных и электромеханических элементов и устройств.

Принцип действия компьютеров состоит в выполнении программ (SoftWare) – заранее заданных, четко определённых последовательностей арифметических, логических и других операций.

Состав вычислительной системы называется конфигурацией. Основу построения компьютеров сформулировал в 1945 г. американский ученый Джон фон Нейман.

Компьютер должен иметь следующие устройства:

- арифметическо - логическое устройство, выполняющее арифметические и логические операции;
- устройство управления, которое организует процесс выполнения программ;
- запоминающее устройство, или память для хранения программ и данных;
- внешние устройства для ввода-вывода информации.

### Вариант 14

#### **Роль и значение информационных революций**

В истории развития цивилизации произошло несколько информационных революций — преобразований общественных отношений из-за кардинальных изменений в сфере обработки информации. Следствием подобных преобразований являлось приобретение человеческим обществом нового качества.

Первая революция связана с изобретением письменности, что привело к гигантскому качественному и количественному скачку. Появилась возможность передачи знаний от поколения к поколениям.

Вторая (середина XVI в.) вызвана изобретением книгопечатания, которое радикально изменило индустриальное общество, культуру, организацию деятельности.

Третья (конец XIX в.) обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, позволяющие оперативно передавать и накапливать информацию в любом объеме.

Четвертая (70-е гг. XX в.) связана с изобретением микропроцессорной технологии и появлением персонального компьютера. На микропроцессорах и интегральных схемах создаются компьютеры, компьютерные сети, системы передачи данных (информационные коммуникации). Этот период характеризуют три фундаментальные инновации:

а) переход от механических и электрических средств преобразования информации к электронным;

б) миниатюризация всех узлов, устройств, приборов, машин; создание программно-управляемых устройств и процессов.

Для создания более целостного представления об этом периоде целесообразно познакомиться с справкой о смене поколений электронно-вычислительных машин (ЭВМ) и сопоставить эти сведения с этапами в области обработки и передачи информации.

## Вариант 15

### Справка о смене поколений ЭВМ

1-е поколение (начало 50-х гг.). Элементная база — электронные лампы. ЭВМ отличались большими габаритами, большим потреблением энергии, малым быстродействием, низкой надежностью, программированием в кодах.

2-е поколение (с конца 50-х гг.). Элементная база — полупроводниковые элементы. Улучшились по сравнению с ЭВМ предыдущего поколения все технические характеристики. Для программирования используются алгоритмические языки.

3-е поколение (начало 60-х гг.). Элементная база — интегральные схемы, многослойный печатный монтаж. Резкое снижение габаритов ЭВМ, повышение их надежности, увеличение производительности. Доступ с удаленных терминалов.

4-е поколение (с середины 70-х гг.). Элементная база — микропроцессоры, большие интегральные схемы. Улучшились технические характеристики. Массовый выпуск персональных компьютеров. Направления развития: мощные многопроцессорные вычислительные системы с высокой производительностью, создание дешевых микроЭВМ.

5-е поколение (с середины 80-х гг.). Началась разработка интеллектуальных компьютеров, пока не увенчавшаяся успехом. Внедрение во все сферы компьютерных сетей и их объединение, использование распределенной обработки данных, повсеместное применение компьютерных информационных технологий.

Последняя информационная революция выдвигает на первый план новую отрасль — информационную индустрию, связанную с производством технических средств, методов, технологий для производства новых знаний. Важнейшими составляющими информационной индустрии становятся все виды информационных технологий, особенно телекоммуникации. Современная информационная технология опирается на достижения в области компьютерной техники и средств связи.

## Вариант 16

### **Электронная коммерция**

С середины 90-х годов во всем мире наблюдается рост активности в области онлайн-торговли. Вслед за крупными компаниями, производящими компьютерное оборудование в сеть стали выходить торговцы традиционными товарами (книжные магазины, магазины компакт-дисков). Сейчас практически любые товары можно купить через сеть.

Электронная коммерция - это виртуальная экономическая среда в которой осуществляется электронный бизнес, электронные расчеты по средствам Интернет - банкинга и иная электронно экономическая деятельность с использованием интерактивных возможностей. Электронный бизнес – это деятельность компании, направленная на получение прибыли, которая основывается на цифровых технологиях и тех преимуществах, которые они представляют. Но также электронная коммерция включает в себя деятельность провайдеров Интернет - услуг и деятельность всех прочих экономических субъектов, которые, используя каналы Интернета, организуют свою коммерческую деятельность.

Провайдер Интернет-услуг - это коммерческая фирма, которая обеспечивает доступ в Интернет, поддерживает его за определенное вознаграждение и оказывает некоторые сопутствующие услуги по требованию клиентов. При коммерческом использовании возможностей сети различными экономическими субъектами, в структуре ЭК, как правило, выделяют несколько звеньев: реклама и представление товара; осуществление операций купли-продажи через каналы сети; послепродажные услуги клиентам; построение отношений с клиентами.

## Вариант 17

### **Свойства информации**

Информация является динамическим объектом, образующимся в момент взаимодействия объективных данных и субъективных методов. Как всякий объект, она обладает свойствами (объекты различны по своим свойствам). Можно привести немало разнообразных свойств информации. Каждая научная дисциплина рассматривает те свойства, которые ей наиболее важны. С точки зрения информатики наиболее важными представляются

следующие свойства; объективность, полнота, достоверность, адекватность, доступность и актуальность информации.

*Объективность и субъективность информации.* Понятие объективности информации является относительным. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективный элемент. Так, например, принято считать, что в результате наблюдения фотоснимка природного объекта или явления образуется более объективная информация, чем в результате наблюдения рисунка того же объекта, выполненного человеком. В ходе информационного процесса степень объективности информации всегда понижается. Это свойство учитывают, например, в правовых дисциплинах, где по-разному обрабатываются показания лиц, непосредственно наблюдавших события или получивших информацию косвенным путем (посредством умозаключений или со слов третьих лиц).

*Полнота информации.* Полнота информации во многом характеризует качество информации и определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся.

*Достоверность информации.* Данные возникают в момент регистрации сигналов, но не все сигналы являются полезными - всегда присутствует какой-то уровень посторонних сигналов, в результате чего полезные данные сопровождаются определенным уровнем информационного шума.

*Адекватность информации* – это степень соответствия реальному объективному состоянию дела.

*Доступность информации* - мера возможности получить ту или иную информацию.

*Актуальность информации* – это степень соответствия информации текущему моменту времени.

## Вариант 18

### **Устройство персонального компьютера**

Все компьютеры состоят из одинаковых основных устройств: процессора, памяти, устройства ввода и устройства вывода. Обработка информации выполняется процессором.

*Процессор* – это центральное устройство ЭВМ. Существует *внутренняя* и *внешняя* память компьютера. Внутренняя память используется для временного хранения данных и программ, внешняя – для долговременного их хранения. Память компьютера дискретна.

*Внутренняя память* компьютера предназначена для оперативной обработки данных. Она является более быстрой, чем внешняя память. Выделяют следующие виды внутренней памяти:

1) *Оперативная.* В неё помещаются программы и данные. Она обладает большим быстродействием и является энергозависимой. Обозначается RAM – Random Access Memory – память с произвольным доступом. Иначе

оперативную память называют оперативным запоминающим устройством (ОЗУ).

2) *Постоянная память* – BIOS (Basic Input-Output System). Содержит программы для управления компьютером. Обозначается ROM –Read Only Memory. Иначе постоянную память называют постоянным запоминающим устройством (ПЗУ).

3) *Внешняя память* предназначена для длительного хранения программ и данных. Это память большого объёма, но низкого быстродействия. Она представлена в основном магнитными и оптическими носителями.

В состав внешней памяти компьютера входят:

- жёсткие диски;
- гибкие диски (дискеты объёмом 1,44 Мегабайт);
- лазерные диски (компакт-диски объёмом 700 Мегабайт);
- DVD-диски (объёмом 4,7...9,4 Гигабайт);
- Flash-карты (USB flash drive объёмом до 12 Гигабайт).

Человек вводит данные в компьютер через *устройства ввода* (клавиатура, мышь, сканер, микрофон), а получает результат обработки через *устройства вывода* (монитор, принтер, акустические колонки).

*Шина* – это набор проводов, по которым происходит обмен информацией между устройствами компьютера.

Вариант 19

### **Компьютерная система. Операционная система**

Система (от греч. systema - целое, составленное из частей; объединение) - совокупность взаимосвязанных, регулярно взаимодействующих объектов, образующих определенную целостность для выполнения единой цели, каких-либо функций и задач. Системой называют иногда комплекс установленных организованных процедур (методов) для достижения определенной цели. Система выполняет свои функции с учетом внешних условий и воздействий.

*Компьютерная система* состоит из устройств (внутренних и периферийных) и программ, которые, взаимодействуя, выполняют процессы обработки информации на одном или нескольких компьютерах. Система может включать в себя различные подсистемы и входить в качестве подсистемы в более крупную систему. Часть программного обеспечения, отвечающая за готовность компьютерной системы к работе, образует в общей вычислительной системе важную подчиненную систему - операционную.

*Операционная система (ОС)* - комплекс программ, которые обеспечивают выполнение других программ, распределение ресурсов компьютерной системы, ввод, вывод, сохранение данных, управление данными, предоставление интерфейса (средство взаимодействия) с пользователем, выдача сообщения.

*Ядро операционной системы* - ее основная часть, загружающаяся в

оперативную память после включения компьютера на все время работы, управляющая всей операционной системой, памятью, выполнением прикладных программ, их взаимодействием с аппаратурой, определяет порядок и время работы различных программ с процессором, обрабатывает сбои аппаратуры и программ.

Операционная система разрабатывается под набор команд процессоров конкретного семейства. Например, операционная система Microsoft Windows XP создана для работы с процессорами корпорации Intel совместимыми с ними, имеющими одинаковый или аналогичный набор команд.

## Вариант 20

### Модем

*Модем* (модулятор-демодулятор сигналов) - устройство, позволяющее обмениваться информацией между компьютерами через телефонную сеть путем взаимного преобразования цифровой и аналоговой информации. Цифровые данные компьютера преобразуются аналоговые сигналы и передаются по телефонной линии. Принимаемые аналоговые сигналы преобразуются обратно в цифровую форму.

Модемы применяют для подключения к Интернету, установки прямого соединения с другим компьютером через телефонную сеть, отправки и приема факсов (при наличии факс-модема), входа в компьютерную сеть.

Достоинства модема: простота установки; соединение с компьютером в любой точке земного шара, где есть телефонные линии. Недостатки: скорость передачи в сотни раз меньше, чем в локальной сети; низкая защищенность от помех.

Модемы бывают внешние (отдельное устройство) и внутренние.

*Внешний модем* одним выходом подключается к компьютеру, другим к телефонной линии. *Внутренний модем* в виде схемы устанавливается в системный блок, не загромождает стол, не требует отдельный блок питания.

Модем не только передает данные, но выполняет отклик, согласование условий передачи, сжатие данных, контроль качества связи для повышения скорости передачи, модемы сжимают данные перед отправкой (почти в два раза), распаковывают после получения. Если подключиться к линии, работающей на модем, то можно услышать шип, свист.

*Скорость передачи данных модемом* измеряется в битах в секунду (бит/с). Для качественных линий связи применяются модемы на 128 Кбит/с и выше. Скорость передачи информации в телекоммуникационных сетях постоянно возрастает. В 80-х гг. прошлого века телефонные кабели передавали 1 страницу в секунду. Сегодня оптоволоконный кабель передает десятки тысяч томов в секунду.



## Вариант 21

### Оперативная память

Оперативная память – память временного хранения данных и команд, необходимых процессору для выполнения операций в текущем сеансе работы. Память отличается особо быстрым доступом к чтению и записи данных процессором или другими устройствами. Работа компьютера – это, прежде всего, работа процессора с оперативной памятью. Обычно, если термин «память» используют без уточнения какая память, то имеют в виду оперативную память, другое название: *оперативное запоминающее устройство (ОЗУ)*.

При включении компьютера в оперативную память загружаются с диска программы, данные для работы операционной системы и работы отдельных устройств, а затем прикладные программы, которые открывает пользователь, обрабатываемые документы. Оперативная память хранит данные только на время, пока компьютер включен, поэтому она *временная* (на время сеанса работы) и *энергозависимая* (пока подает энергию, источник питания). Данные в памяти утрачиваются при выключении компьютера или перезагрузке операционной системы.

Процессор выполняет вычисления по программе, размещенной в оперативной памяти, обменивается с памятью данными, отправляет данные из памяти во внешние запоминающие устройства, или сеть. Доступ к данным оперативной памяти происходит гораздо быстрее, чем к данным внешней памяти, например, жесткого диска, поэтому она и называется оперативной - быстродействующей.

## Вариант 22

### Lotus Notes

Lotus является программным обеспечением, позволяющим управлять вашей персональной информацией. Lotus Organizer имитирует работу с обычным органайзером, в котором имеются ежедневник, список дел, адресный справочник, сведения о датах и юбилеях, план мероприятий на год и блокнот. Приобретя этот пакет, вы получите великолепную электронную записную книжку, позволяющую вести рабочие планы, а также деловые и прочие заметки, еженедельник, перечень текущих дел, список адресов, календарь и расписание встреч. В настоящее время персональный информационный менеджер Lotus Organizer помогает работать более чем 35 миллионам пользователей. Вы можете достаточно быстро освоить этот пакет и в дальнейшем легко использовать его в вашей повседневной работе.

Важнейшая информация, записанная с использованием технологии Lotus Notes, доступна из любой точки без помощи портативного компьютера. Кроме того, программа lotus notes позволяет легко получать новую информацию о встречах и контактах и даже работать с электронной почтой без доступа к своему компьютеру.

Основные достоинства: удобный интерфейс пользователя; удобный способ представления информации; дружественная навигация; возможность упорядочивания информации; возможность вести планирование мероприятий, задач и звонков; функция оповещения о приближающихся событиях; связываться с намеченными мероприятиями; информацию о расходах; назначение повторяющихся событий; ведение списка дел; адресная книга с именами, адресами и телефонами; возможность вносить в блокнот текстовую или графическую информацию; графическое планирование мероприятий на год; гибкие параметры управления контактами; обширный набор средств для управления информацией; необычайно быстрый доступ к нужной информации; возможность планирования деятельности сотрудников вашей компании; возможность автоматической координации графика собственной работы или деятельности целой группы; возможность планирования и организации деловых встреч в локальной сети; возможность отслеживания входящих и исходящих сообщений; передача запросов через простые средства электронной почты, совместимые со стандартом VIM (Vendor Independent Messaging) или поддерживающим интерфейс MAPI.

## Вариант 23

### Системы управления базами данных

Важная особенность реляционной базы данных состоит в том, что единая база данных может распределяться по нескольким таблицам, между которыми могут существовать связи типа «один к одному» и «один ко многим». Этим реляционная система отличается от одноуровневой базы данных, которая размещается в одной таблице например в Excel. Реляционная база хранит данные, таким образом, что их можно добавлять и использовать независимо от других хранящихся данных.

Пользователю не обязательно знать все детали того, как физически хранится информация на компьютере (локальном или удаленном), какие поля есть в таблицах, как они связаны и будут извлекаться из базы данных. Поэтому одну и ту же базу данных можно просматривать разными способами. Вместо общения с большим количеством отдельных файлов (текстовых, табличных, графических) создается единый интерфейс, с помощью которого добавляются новые записи, редактируются или удаляются имеющиеся.

*Система управления базами данных (СУБД)* - программа, которая позволяет создавать и менять структуру базы, формы для ввода и просмотра информации, запросы для избирательного извлечения. СУБД избавляет от поиска и сбора необходимых фрагментов в различных файлах, от расчета числовых показателей вручную. По готовым формам, запросам пользователи получают информацию и печатают отчеты, даже не имея представления о том, как структурирована база данных.

Примером СУБД настольного типа является программа Microsoft Access, выполняющая операции с данными. На локальном компьютере

физически хранится и предоставляется информация, работают средства управления и организации запросов. Сфера применения. СУБД Access - малые и средние организации с интенсивным товаром и документооборотом, с такими задачами, как учет складского хозяйства, обеспечение работы магазина, ведение кадровых дел, бухгалтерии, документов. При небольшом числе пользователей с базой данных Access можно работать через сеть. Программа применима для поддержки веб-сайта в Интернете или внутренней сети.

## Вариант 24

### Сетевые информационные технологии

Компьютерные сети создаются для того, чтобы дать возможность территориально разобщенным пользователям обмениваться информацией между собой, совместно использовать одинаковые программы, общие информационные и аппаратные ресурсы.

По некоторым оценкам, более половины действующих ЭВМ подключены к сетям. Необходимость внедрения электронной почты, стремление к коллективному использованию разнообразных баз данных и аппаратных средств, потребность в проведении дискуссий и оперативных совещаний без отрыва от рабочих мест, желание повысить оперативность получения «свежей» информации подталкивает пользователей к подключению своих ЭВМ к сетям.

Сети появились в результате творческого сотрудничества специалистов вычислительной техники и техники связи.

Вычислительные сети чаще всего подразделяются на два вида: локальные и глобальные. Существуют корпоративные сети, которым одновременно присущи свойства и локальных, и глобальных сетей. Корпоративные сети доступны лишь ограниченному кругу лиц.

Локальная сеть (Local Area Network - LAN) имеет небольшую протяженность: (до 10 км), характеризуется высокой скоростью передачи информации и низким уровнем ошибок. Глобальная сеть (Wide Area Network - WAN) может охватывать значительные расстояния - десятки тысяч километров. Когда-нибудь к глобальным сетям будут подключены компьютеры, расположенные на космических станциях и на других планетах Солнечной системы.

При классификации сетей можно считать, что если организация (или предприятие) является собственником линии связи (при этом канал связи является высокоскоростным), то это локальная сеть. Если же организация арендует низкоскоростные каналы связи (например, спутниковую линию связи), то это глобальная сеть.

## Языки программирования

Язык программирования – формальная знаковая система, предназначенная для записи компьютерных программ. Язык программирования определяет набор лексических, синтаксических и семантических правил, задающих внешний вид программы и действия, которые выполнит исполнитель (компьютер) под ее управлением.

Со времени создания первых программируемых машин человечество придумало уже более восьми с половиной тысяч языков программирования.

Каждый год их число пополняется новыми. Некоторыми языками умеет пользоваться только небольшое число их собственных разработчиков, другие становятся известными миллионам людей.

Профессиональные программисты иногда применяют в своей работе более десятка разнообразных языков программирования. Создатели языков по-разному толкуют понятие «язык программирования». К наиболее распространённым утверждениям, признаваемым большинством разработчиков, относятся:

1) **Функция:** язык программирования предназначен для написания компьютерных программ, которые применяются для передачи компьютеру инструкций по выполнению того или иного вычислительного процесса и организации управления отдельными устройствами.

2) **Задача:** язык программирования отличается от естественных языков тем, что предназначен для передачи команд и данных от человека к компьютеру, в то время, как естественные языки используются для общения людей между собой. Можно сказать, что «язык программирования» – это способ передачи команд, приказов, чёткого руководства к действию; тогда как человеческие языки служат также для обмена информацией.

3) **Исполнение:** язык программирования может использовать специальные конструкции для определения и манипулирования структурами данных и управления процессом вычислений.

### Рекомендуемая литература для СРС № 2

1 Букейханова Р.К., Чумбалова Г.М. Обучение перевода на казахский язык научно-технических текстов. - Алматы: АУЭС, 2007. – 50 с.

2 Кубдашева К.Б. Профессиональный русский язык: Методические указания для выполнения СРС №1 (перевод специального текста). - Алматы: АУЭС, 2013.- 32 с.

3 Нурмаханова М.К. Профессиональный русский язык. Методические указания для студентов специальности 5В100200. – Алматы: АУЭС, 2015. – 49 с.

4 Нурмаханова М.К. Профессиональный русский язык. Методические указания и варианты выполнения семестровых работ для студентов

специальностей 5В100200 – Системы информационной безопасности, 5В070300 – Информационные системы. – Алматы: АУЭС, 2016. – 55 с.

### Список литературы

- 1 Акулиничев Ю. П., Дроздова В.И. Теория информации: Учебное пособие. - Томск: ТМЦДО, 2005. – 108 с.
- 2 Букейханова Р.К., Чумбалова Г.М. Обучение перевода на казахский язык научно-технических текстов. - Алматы: АУЭС, 2007. – 50 с.
- 3 Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации: Учебное пособие. – М.: Горячая линия. – Телеком, 2014. – 442 с.
- 4 Кудряшов Б.Д. Теория информации: Учебник для вузов. – СПб.: Изд. Дом Питер, 2009. – 460 с.
- 5 Куралбаев З.К. Основы информационных систем. Конспект лекций. – Алматы: АИЭС, 2009. – 80 с.
- 6 Нурмаханова М.К. Профессиональный русский язык. Методические указания для студентов специальности 5В100200. – Алматы: АУЭС, 2015. – 49 с.
- 7 Панин В.В. Основы теории информации. – М.: Бином. Лаборатория знаний, 2009.
- 8 Сатимова Е.Г. Операционные системы. LINUX. Решения задач структурной и функциональной организации. Учебное пособие. – Алматы: АУЭС, 2009. – 120 с.
- 9 Степанов А. Информатика: Учебник для вузов. 4-е-издание.– М.: Высшая школа, 2004. – 688 с.

### Словари

- 1 Бериккулы А., Шайхин Б.М. и др. Казахско-русский, русско-казахский терминологический словарь. Электроника, радиотехника и связь. – Алматы: Рауан, - 2000. – 236 с.
- 2 Бектаев К. Большой казахско-русский, русско-казахский словарь. – Алматы: Алтын Казына, 2001. – 704 с.
- 3 Политехнический словарь/Гл. ред. Акад. А. Ю. Ишлинский. – М.: Советская энциклопедия, 1980. – 656 с.
- 4 Казахско-русский, русско-казахский терминологический словарь/ Под общей редакцией д.п.н., проф. А. К. Кусаинова. В 32-х томах. - Алматы: Рауан, 2000.– 312 с.
- 5 Пчёлкина В. В., Комарова Л. Н. И др. Словарь иностранных слов. - М.: Русский язык. 1979.- 607 с.
- 6 Раренко М.Б. Основные понятия переводоведения. Терминологический словарь-справочник. – М.: ИНИОН РАН, 2010. – 260 с.

7 Русско-казахско-английский политехнический словарь. Сост. М.Р.Тусипбек, А.К.Кусаинов. – Алматы: Rond&A, 2010. – 740 с.

8 Сарыбеков М., Сыздыкназаров М. Словарь науки. Общенаучные термины и определения. Науковедческие понятия и категории: Учебное пособие. – Алматы: Триумф «Т», 2008. – 504 с.

9 Русско-казахский словарь/ Под редакцией Н. Т. Сауранбаева и др. - Алматы: Дайк-Пресс, 2005. – 1125 с.

10 Словарь по информатике. – Минск: Университетское, 1991. – 158 с.

## Список литературы

- 1 Акулиничев Ю. П., Дроздова В.И. Теория информации: Учебное пособие. - Томск: ТМЦДО, 2005. – 108 с.
- 2 Букейханова Р.К., Чумбалова Г.М. Обучение перевода на казахский язык научно-технических текстов. - Алматы: АУЭС, 2007. – 50 с.
- 3 Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 586 с.
- 4 Губарев А.В. Информационное обеспечение системы менеджмента качества. - М.: Горячая линия – Телеком, 2013. – 132 с.
- 5 Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации: Учебное пособие. – М.: Горячая линия. – Телеком, 2014. – 442 с.
- 6 Кудряшов Б.Д. Теория информации: Учебник для вузов. – СПб.: Изд. Дом Питер, 2009.- 460 с.
- 7 Куралбаев З.К. Основы информационных систем: Конспект лекций. – Алматы: АИЭС, 2009.- 80 с.
- 8 Новиков В.К. Организационно-правовые основы информационной безопасности: Учебное пособие. – М.: Горячая линия – Телеком, 2015. – 176 с.
- 9 Нурмаханова М.К. Профессиональный русский язык. Методические указания для студентов специальности 5В100200. – Алматы: АУЭС, 2015. – 49 с.
- 10 Панарин И.Н. Информационная война, PR и мировая политика. Курс лекций. – М.: Горячая линия – Телеком, 2015. - 352 с.
- 11 Перепелкин Д.А. Схемотехника усилительных устройств: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 238 с.
- 12 Панин В.В. Основы теории информации. – М.: Бином. Лаборатория знаний, 2009. – 360 с.
- 13 Сатимова Е.Г. Операционные системы. LINUX. Решения задач структурной и функциональной организации: Учебное пособие. – Алматы: АУЭС, 2009. -120 с.
- 14 Степанов А. Информатика: Учебник для вузов. 4-е-издание.– М.: Высшая школа, 2004. – 688 с.
- 15 Шелухин О.И. Моделирование информационных систем: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2016. – 516 с.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ  
КАЗАХСТАН

Некоммерческое акционерное общество  
«Алматинский университет энергетики и связи»

**УТВЕРЖДАЮ** \_\_\_\_\_  
Проректор по учебно- методической работе  
\_\_\_\_\_ С. В. Коньшин  
“ \_\_\_\_\_ ” \_\_\_\_\_ 2016 г.

**ПРОФЕССИОНАЛЬНЫЙ РУССКИЙ ЯЗЫК**

Методические указания и варианты выполнения семестровых работ для  
студентов специальностей 5В100200 – Системы информационной  
безопасности, 5В070300 – Информационные системы

СОГЛАСОВАНО  
Начальник УМО  
\_\_\_\_\_ М.А.Мустафин  
“ \_\_\_\_\_ ” \_\_\_\_\_ 2016 г.  
Редактор \_\_\_\_\_

Председатель по ОУМК  
“ \_\_\_\_\_ ” \_\_\_\_\_ 2016 г.  
\_\_\_\_\_ Б.К. Курпенов

Редактор  
\_\_\_\_\_ Н.М.Голева  
“ \_\_\_\_\_ ” \_\_\_\_\_ 2016 г.

Специалист  
по стандартизации  
\_\_\_\_\_ Н. К. Молдабекова  
“ \_\_\_\_\_ ” \_\_\_\_\_ 2016 г.

Рассмотрено и одобрено на  
заседании кафедры казахского и  
русского языков  
Протокол № 13 23.06.2016  
Зав.кафедрой:  
Р.К.Букейханова \_\_\_\_\_

Составитель:  
\_\_\_\_\_ М.К.Нурмаханова

Зав. кафедрой СИБ  
\_\_\_\_\_ Е.Г.Сатимова  
“ \_\_\_\_\_ ” \_\_\_\_\_ 2016 г.



Алматы, 2016

Маржан Калжановна Нурмаханова

## ПРОФЕССИОНАЛЬНЫЙ РУССКИЙ ЯЗЫК

Методические указания и варианты выполнения семестровых работ для студентов специальностей 5В100200 – Системы информационной безопасности, 5В070300 – Информационные системы

Редактор Н.М. Голева

Специалист по стандартизации Н. К. Молдабекова

Подписано в печать \_ \_ \_

Тираж экз.

Объём уч.-изд. л.

Формат 60x84 1/16

Бумага типографская №1

Заказ \_\_\_\_\_. Цена \_\_\_\_ тенге.

Копировально-множительное бюро  
некоммерческого акционерного общества  
«Алматинский университет энергетики и связи»  
050013, Алматы, Байтурсынова, 126