МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ

Санкт-Петербургский университет ГПС МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева

Т.Н. Антошина, А.А. Воронцова, А.А. Кабанов

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Учебное пособие для самостоятельной работы и самоконтроля знаний обучающихся

Санкт-Петербург
2024

УДК 004.2
ББК 16.2
А72

А72 Т.Н. Антошина, А.А. Воронцова, А.А. Кабанов
Информационные технологии. Учебное пособие для самостоятельной работы и самоконтроля знаний обучающихся. — СПб.: С.-Петерб. ун-т ГПС МЧС России, 2024. – 100 с.
ISBN 978-5-907883-11-6

Учебно-методическое пособие разработано в соответствии с программой учебного курса «Информационные технологии» с целью углубления изучения профессионально значимых тем — «Работа с ресурсами информационно-вычислительных сетей» и «Защита информации при применении современных информационных технологий».

Пособие содержит вводные тесты для самоконтроля исходного (школьного) уровня знаний, а также систематизированный теоретический и практический материал.

Каждая тема включает в себя: краткие сведения из теории с выделением ключевых понятий; примеры решения практических задач; задачи для самостоятельного изучения, а также тесты для самоконтроля знаний.

В содержание учебного пособия включены качественные практические задачи по темам «Работа с ресурсами информационно-вычислительных сетей» и «Защита ин-формации при применении современных информационных технологий», так же объединенные тесты, которые позволят обучающемуся определить уровень овладения учебным материалом по данным темам.

Разработанное пособие рекомендуется обучающимся для самостоятельной подготовки к лабораторным, практическим занятиям, а также к зачетам и экзаменам по дисциплине «Информационные технологии».

УДК 004.2
ББК 16.2

ISBN 978-5-907883-11-6

СОДЕРЖАНИЕ

1. ТЕСТОВЫЕ ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОГО КОНТРОЛЯ ЗНАНИЙ ПО ТЕМАМ «РАБОТА С РЕСУРСАМИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ» И «ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

(в объёме курса информатики средней школы)

Уважаемые обучающиеся! В первом разделе Вам предлагается самостоятельно оценить личный уровень освоения знаний курса информационных технологий средней школы по темам:

1. Основные термины, определения и классификация вычислительных сетей;
2. Топологии построения локальных вычислительных сетей;
3. Понятийный аппарат информационной безопасности;
4. Методы и средства защиты информации.

Самоконтроль знаний по указанным темам предлагается провести с помощью разработанных вариантов тематических тестовых заданий. В каждой теме тестовые задания сгруппированы в вариант по 12 заданий приблизительно одинаковой сложности.

Каждое задание вариантов представляет собой несложную теоретическую задачу, для решения которой, в первую очередь, требуются:

умение внимательно и грамотно читать задачу (анализ исходной информации);

умение использовать понятийный аппарат курса информационные технологии для решения задачи.

Каждое задание в варианте должно быть выполнено приблизительно за 5 минут, а каждый вариант в целом примерно за 45 минут.

Полученные ответы Вы можете сравнить с вариантами ответов, которые приводятся на странице в конце пособия.

Если Ваши результаты Вас не удовлетворяют, то Вы должны подумать, к каким темам дисциплины «Информационные технологии» средней школы Вам следует вернуться и более глубоко проработать понятийный аппарат. Желаем успехов!

2. ВАРИАНТЫ ТЕМАТИЧЕСКИХ ТЕСТОВЫХ ЗАДАНИЙ

2.1. Основные термины, определения и классификация вычислительных сетей

1. Маршрутизатор – устройство, соединяющее различные:
1) Компьютерные сети;
2) По архитектуре компьютеры;
3) Маршруты передачи адресов для e-mail;
4) 1 и 2 правильные ответы;
5) Нет правильного ответа.

2. Что представляет собой сервер?
1) Сетевая программа, предназначенная для организации информационного обмена между пользователями;
2) Компьютер, выполняющий функции по обслуживанию работы пользователей, к которому подключаются остальные компьютеры;
3) Компьютер, подключенный в компьютерную сеть;
4) Протокол передачи данных;
5) Нет правильного ответа.

3. Какие из утверждений являются правильными?
1) Интернет — самый массовый и наиболее оперативно обновляемый источник информации;
2) Интернет — среда для получения файлов и программ;
3) Интернет — средство для локальной работы;
4) Интернет — средство общения и коммуникаций;
5) Нет правильного ответа.

4. Архитектура компьютера – это:
1) Техническое описание деталей устройств компьютера;
2) Описание устройств для ввода-вывода информации;
3) Его устройство и принципы взаимодействия его основных элементов;
4) Описание устройства и принципов работы компьютера, достаточное для понимания пользователя;
5) Нет правильного ответа.

5. IP адрес – это…

1) Логический адрес компьютера;
2) Физический адрес компьютера;
3) Имя компьютера в сети;
4) Логический и физический адрес компьютера;
5) Нет верного варианта ответа.

6. Repeater – это…

1) Устройство, усиливающие электрические сигналы и обеспечивающие сохранение их формы и амплитуды при передаче на большие расстояния;
2) Устройство, передающее пакеты данных на все свои порты;
3) Программа для передачи данных локальной сети;
4) Устройство, к которому подключается монитор;
5) Нет правильного ответа.

7. Какой модели данных не существует?

1) Иерархическая;
2) Функциональная;
3) Сетевая;
4) Реляционная;
5) Логическая.

8. Протокол – это:

1) Устройство для преобразования информации;
2) Линия связи, соединяющая компьютеры в сеть;
3) Специальная программа, помогающая пользователю найти нужную информацию в сети;
4) Специальное техническое соглашения для работы в сети;
5) Устройство для передачи данных.

9. WWW.yandex.ru – это

1) Браузер;
2) Поисковая система;
3) Домашняя страница;
4) Почта;
5) Язык гипертекстовой разметки.

10. Гипертекст — это:

1) Способ организации текстовой информации, внутри которой установлены смысловые связи между ее различными фрагментами;
2) Обычный, но очень большой по объему текст;
3) Текст, который набран шрифтом большого размера;
4) Распределенная совокупность баз данных, содержащих тексты;
5) Очень ценный текст.

11. Электронная почта (e-mail) позволяет передавать:

1) Исключительно текстовые сообщения;
2) Исполняемые программы;
3) Сообщения и приложенные файлы;
4) WWW-страницы;
5) Исключительно базы данных.

12. Телеконференция — это:

1) Обмен письмами в глобальных сетях;
2) Информационная система в гиперсвязях;
3) Служба приема и передачи файлов любого формата;
4) Процесс создания, приема и передачи WEB-страниц;
5) Система обмена информацией между абонентами компьютерной сети.

2.2 Топология построения локальных вычислительных сетей.

1. Компьютерная глобальная сеть мирового уровня является:

1) E-mail;
2) Интернет;
3) WWW;
4) Яндекс;
5) HTML.

2 Основными видами компьютерных сетей являются сети:

1) Локальные;
2) Региональные;
3) Социальные;
4) Глобальные;
5) Корпоративные.

3. Локальная компьютерная сеть – сеть, состоящая из компьютеров, связываемых в рамках:

1) WWW;
2) Одного учреждения;
3) Одной города, района;
4) Одного региона;
5) Одного дома.

4. Сеть, разрабатываемая в рамках одного учреждения, предприятия – сеть:

1) Локальная;
2) Глобальная;
3) Интранет;
4) Региональная;
5) Корпоративные.

5. Каналами связи в компьютерных сетях являются все перечисленное в списке:

1) Спутниковая связь, солнечные лучи;
2) Спутниковая связь, оптоволоконные кабели, телефонные сети, радиорелейная связь;
3) Спутниковая связь, ультрафиолет, контактно-релейная связь;
4) Инфракрасные лучи;
5) Магнитные поля, телефон.

6. Ethernet поддерживает топологию:

1) Кольцевую;
2) Шинную;
3) Звезда;
4) Ячеистая;
5) Смешанная;

7. В модели OSI первым уровнем является:

1) Канальный;
2) Сетевой;
3) Физический;
4) Сеансовый;
5) Транспортный.

8. Какой компонент обеспечивает резервное питание компьютерной системы в течение короткого периода времени?

1) CPU;
2) Модем;
3) Сетевой фильтр;
4) Источник бесперебойного питания;
5) Концентратор.

9. По какому протоколу передаются веб – страницы?

1) HTML;
2) POP3;
3) SMPT;
4) FTP;
5) HTTP.

10. Пропускная способность канала передачи информации измеряется в:

1 Мбит;
2) Мбайт/с;
3) Бит/с;
4) Кбайт;
5) Тбайт.

11. Локальные компьютерные сети это?

1) Сеть, к которой подключены все компьютеры страны;
2) Сеть, к которой подключены все компьютеры одного населённого пункта;
3) Сеть, к которой подключены все компьютеры;
4) Сеть, к которой подключены все компьютеры, находящиеся в одном здании;
5) Нет правильного ответа.

12. В компьютерной сети Интернет транспортный протокол TCP обеспечивает:

1) Передачу почтовых сообщений;
2) Способ передачи информации по заданному адресу;
3) Передачу информации по заданному адресу;
4) Получение почтовых сообщений;
5) Нет правильного ответа.

2.3 Понятийный аппарат информационной безопасности

1. Виды информационной безопасности:

1) Персональная;
2) Корпоративная;
3) Государственная;
4) Клиентская;
5) Серверная.

2. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

1) Целостность;
2) Доступность;
3) Актуальность;
4) Объективностью;
5) Доступность.

3. Защита информации – это:

1) Распространять государственную тайну и конфиденциальность документированной информации;
2) Непрерывный процесс построения, поддержки нормального функционирования и совершенствования системы защиты информации;
3) Распространять личную тайну и конфиденциальность персональных данных;
4) Распространять утечку, хищение, искажение, подделки информации;
5) Нет правильного ответа.

4. Определение «компьютерный вирус» – это:

1) Размножающаяся программа, которая может находиться в выполняемых файлах;
2) Размножающаяся программа, которая может находиться в загрузочных записях;
3) Размножающаяся программа, которая может находиться в макросах;
4) Размножающаяся программа, которая может находиться в выполняемых файлах, загрузочных записях и макросах;
5) Нет правильного ответа.

5. Сведения (сообщения, данные) независимо от формы их представления:

1) Информация;
2) Информационные технологии;
3) Информационная система;
4) Информационно-телекоммуникационная сеть;
5) Обладатель информации.

6. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:

1) Информация;
2) Информационные технологии;
3) Информационная система;
4) Информационно-телекоммуникационная сеть;
5) Обладатель информации.

7. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:

1) Источник информации;
2) Потребитель информации;
3) Уничтожитель информации;
4) Носитель информации;
5) Обладатель информации.

8. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

1) Токен;
2) Password;
3) Пароль;
4) Login;
5) Смарт – карта.

9. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

1) Идентификация;
2) Аутентификация;
3) Авторизация;
4) Экспертиза;
5) Шифрование.

10. Несанкционированный доступ к информации это:

1) Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально;
2) Работа на чужом компьютере без разрешения его владельца;
3) Вход на компьютер с использованием данных другого пользователя;
4) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей;
5) Доступ к СУБД под запрещенным именем пользователя.

11. «Персональные данные» это:

1) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;
2) Фамилия, имя, отчество физического лица;
3) Год, месяц, дата и место рождения, адрес физического лица;
4) Адрес проживания физического лица;
5) Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна».

12. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:

1) Идентификация;
2) Аутентификация;
3) Стратификация;
4) Регистрация;
5) Авторизация.

2.4 Методы и средства защиты информации

1. Каналы утечки информации из компьютерных систем

1) Телефон;
2) Интернет;
3) Радио;
4) Письма;
5) Нет правильного ответа.

2. Очень сложные пароли гарантируют 100% защиту?

1) Нет;
2) Да, если после работы полностью очищать куки и не хранить пароль на компьютере;
3) Да, если пароль не сохранен на компьютере;
4) Да, если пароль более 10 символов;
5) Да, если в пароли использовать разный регистр символов.

3. Какие вирусы активизируются после включения операционной системы?

1) Снифферы;
2) Троянский конь;
3) Загрузочные;
4) Черви;
5) Логические бомбы.

4. Представляют ли угрозу вирусы для крупных компаний?

1) Нет;
2) Да, представляют;
3) Скорее нет. В крупных компаниях развита система безопасности;
4) Если компания обладает сотрудниками, занимающимися безопасностью сети, вирусы не могут нанести такому предприятию вреда;
5) Нет правильного ответа.

5. Самый лучший способ хранения паролей в информационной системе?

1) Хранить только с включенным брандмауэром;
2) Вообще не сохранять;
3) Архивирование;
4) Хеширование;
5) Записывать пароль в блокнот.

6. Самая массовая угроза компьютерной безопасности, это:

1) Спам;
2) Трояны;
3) Черви;
4) Шпионские программы;
5) Все перечисленное.

7. Если компьютер работает в нормальном режиме, означает ли это, что он не заражен?

1) Если не изменилась скорость работы, компьютер чист;
2) Да;
3) Если антивирус ничего не показывает, то компьютер чист;
4) Если антивирус ничего не показывает, то компьютер все равно может быть заражен;
5) Нет.

8. Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?

1) Включить брандмауэр;
2) Установить новое программное обеспечение;
3) Таких гарантий нет;
4) Посещать только сайты известных брендов;
5) Постоянно менять пароли.

9. Что необходимо выполнять для контроля безопасности электронной почты?

1) Часто сменять пароли;
2) Проверять страницу посещения;
3) Регистрировать почтовый ящик только в известных системах;
4) Использовать сложные пароли;
5) Поставить антивирусное программное обеспечение.

10. Можно ли хранить важную информацию на жестком диске компьютера, в том числе пароли?

1) Да, если это мой личный компьютер;
2) Да;
3) Нет;
4) Да, если компьютер не подключен к интернету;
5) Нет правильного ответа.

11. Если, не нажимая на иконки просто просмотреть подозрительный сайт, ничего не произойдет. Вы согласны?

1) Нет. Заражение может произойти даже если вы просто посмотрели информацию с экрана, при этом ничего не нажимая «+»;
2) Да, простой просмотр не наносит никакого вреда;
3) Да, заражение происходит только после кликов, чем запускается вирусная программа;
4) Нет, ничего не произойдет;
5) Нет правильного ответа.

12. Обеспечивает ли форматирование жесткого диска полное избавление от вирусов?

1) Обеспечивает полностью;
2) Обеспечивает если выполнено быстрое форматирование;
3) Нет;
4) Обеспечивает при низкоуровневом форматировании;
5) Нет правильного ответа.

3. РАБОТА С РЕСУРСАМИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

3.1. Основные термины и определения

Сеть – это совокупность объектов, образуемых устройствами передачи и обработки данных.

Международная организация по стандартизации (International Organization for Standardization, ISO) определила компьютерную сеть как последовательную биториентированную передачу информации между связанными друг с другом независимыми устройствами. В общем случае различают два понятия сети: коммуникационная сеть и информационная сеть (см. рис. 1).

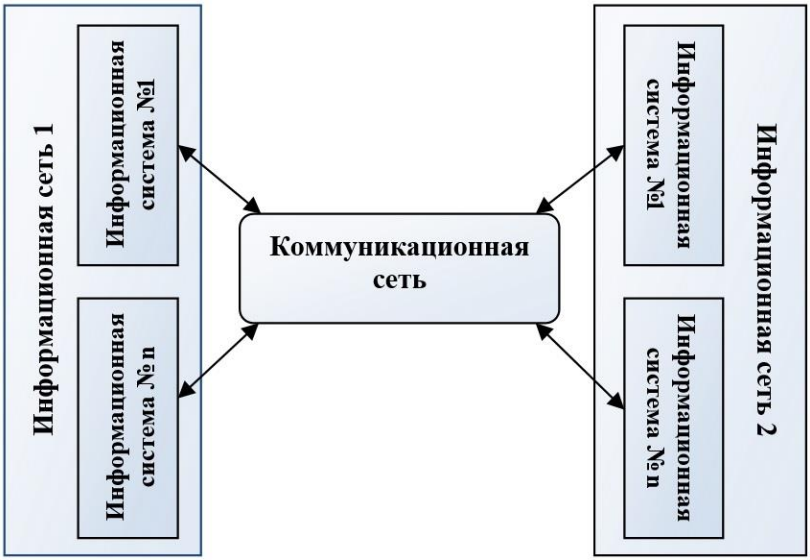


Рис. 1. Информационные и коммуникационные сети

Коммуникационная сеть — система, состоящая из объектов, осуществляющих функции генерации, преобразования, хранения и потребления продукта, называемых пунктами (узлами) сети, и линий

передачи (связей, коммуникаций, соединений), осуществляющих передачу продукта между пунктами.

Информационная сеть — коммуникационная сеть, в которой продуктом генерирования, переработки, хранения и использования является информация.

Глобальная вычислительная сеть объединяет множество локальных сетей и сотни тысяч — миллионы разнотипных ЭВМ по всему миру, физическая линия связи — оптоволоконный кабель или космическая радиолиния связи (не только).

Локальная вычислительная сеть (ЛВС) — система связи отдельно расположенных ЭВМ на относительно небольшом расстоянии (обычно в пределах помещении и/или этажа здания); обычно объединяет до нескольких десятков (чаще однотипных) компьютеров, физическая линия связи — «витая пара» или коаксиальный кабель. В последнее время для связи между узлами все чаще используются беспроводные технологии стандартов 802.11.

Корпоративная вычислительная сеть — локальная вычислительная сеть (крупной) организации, работающая на протоколах Интернет (стек TCP/IP) и использующая сервисы Интернет. При непосредственном подключении к глобальной сети — еще и телекоммуникационную среду Интернета.

Вычислительная сеть — это совокупность компьютеров, соединенных между собой с помощью каналов связи в единую систему и использующих общие ресурсы.

Региональная сеть — это вычислительная сеть, которая связывает абонентов, расположенных на значительном расстоянии друг от друга (десятки - сотни километров).

Рабочая группа (workgroup) — набор компьютеров, объединенных для удобства при просмотре сетевых ресурсов одним именем.

Домен (domain) — определенная администратором сети совокупность компьютеров, использующих общую базу данных и систему защиты; каждый домен имеет уникальное имя.

Узел (host) — подключенное к сети устройство (обычно компьютер), идентифицируемое собственным адресом (например, в сети Internet host-адресом является уникальное 32-разрядное двоичное число. (Это в IPv4. Ipv6 иначе)

Трафик (traffic) — поток сообщений в разделяемой среде передачи данных, часто используется для грубой оценки уровня использования передающей среды (тяжелый, средний, легкий трафик).

Маршрутизация — процесс определения (оптимального) пути доступа к объектам (компьютерам) сети.

Пакет, кадр, сообщение, датаграмма — единица передаваемой по сети информации, определенное количество байт, сгруппированное вместе и посылаемое одновременно. То или иное наименование применяется в контексте описания различных уровней сетевого взаимодействия.

Сетевая архитектура — концепция, представляющая логическую, функциональную и физическую организацию технических и программных средств сети и определяющая основные элементы информационной сети, характер и топологию взаимодействия этих элементов.

Протокол — это набор семантических и синтаксических правил, определяющий поведение функциональных блоков сети при передаче данных. Другими словами, протокол — это совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и правильную интерпретацию данных всеми участниками процесса информационного обмена.

Программное обеспечение компьютерных сетей — комплекс программ, поддерживающий функции обмена информацией между отдельно расположенными ЭВМ. В настоящее время программное обеспечение компьютерных сетей обычно является (иногда опционально устанавливаемой) составной часть операционных систем.

Сервер — это компьютер, выделенный для обработки запросов от всех подсоединенных рабочих станций, предоставляющий доступ к общим сетевым ресурсам (базам данных, библиотекам программ, принтерам, факсам и т. д.).

В зависимости от разделяемых ресурсов серверы делятся на:

- ✓ Файл-сервер (дисковая память);
- ✓ Факс-сервер;
- ✓ Сервер приложений;
- ✓ Почтовый сервер (для организации почтовой связи) и др.

Рабочая станция (клиент) — это компьютер, с помощью которого пользователь получает доступ ко всем ресурсам сети.

Компьютер, подключенный к вычислительной сети, может быть либо рабочей станцией, либо сервером, в зависимости от выполняемых им функций.

В компьютерных сетях могут быть реализованы два способа обработки данных:

- ✓ Централизованная (центральная ЭВМ или Host-компьютер, все запросы идут к ней, и обработка ведется на ней);

- ✓ Распределенная "клиент-серверная" (клиентская часть программы делает запрос серверу, на нем производится обработка запроса и передача ответа клиенту).

Такое разделение в сети на клиента и сервер позволяет эффективно использовать технологию «клиент/сервер». В этом случае приложение делится на две части: клиентскую и серверную. Один или несколько мощных компьютеров сети конфигурируются как серверы приложений, на них выполняются серверные части приложений. Клиентские части выполняются на рабочих станциях, именно на них формируются запросы к серверам приложений и обрабатываются полученные результаты (см. таблицу 1).

Таблица 1.

Одноранговые ЛВС	Сети по типу «клиент-сервер»
✓ Пользователи сети имеют доступ к файлам, находящимся на дисковых накопителях других пользователей. ✓ Производительность падает при расширении сети свыше 10-20 узлов. ✓ Некоторые сети используют не стандартные средства Ethernet, а свои собственные аппаратные средства, что затрудняет межсетевые преобразования и расширение (наращивание) сети. ✓ Инсталляция (установка) отличается простотой, однако управление большой сетью может оказаться весьма затруднительным.	✓ Файлы общего пользования хранятся централизованно, что уменьшает вероятность их разрушения. ✓ Производительность, как правило, выше благодаря наличию выделенных серверов. ✓ Стандарты на аппаратные средства упрощают наращивание (расширение) сетей и реализацию межсетевых преобразований. ✓ Инсталляция и управление довольно трудоемки и сложны, однако для этих целей созданы достаточно совершенные инструментальные средства

3.2. Физические основы построения ЛВС.

Для объединения локальных вычислительных сетей применяются следующие устройства:

Сетевой концентратор или хаб (от англ. *hub* — центр) — устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа *витая пара*.

Хаб – это повторитель. Всё что к нему подключено – будет повторяться. На хаб даётся один IP адрес и поэтому всё связано.

Свитч пришёл на смену хабу и исправляет недостатки предшественника.

Маршрутизатор – (проф. жарг. ра́утер, ру́тер или ро́утер) специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

Роутер – его часто ещё называют маршрутизатором. Почему? Да потому что он является связующим звеном между двумя различными сетями и передает данные, основываясь на определенном маршруте, указанном в его таблице маршрутизации. Если выражаться очень просто, то роутер является посредником между Вашей сетью и выходом в интернет. Роутер исправляет все ошибки предшественников и именно поэтому в наше время он наиболее популярен. Особенно если учесть тот факт, что зачастую роутеры снабжаются Wi-Fi антеннами для передачи интернета на беспроводные устройства, а также имеют возможность подключать USB модемы.

Повторитель (репитер, от англ. repeater) — сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения и его расширения за пределы одного сегмента или для организации двух ветвей, путём повторения электрического сигнала «один в один».

Mesh-системы — обеспечивают более высокую скорость, широкое покрытие и надёжное соединение для устройств, подключённых к сети. В то время как обычные роутеры раздают Wi-Fi из одной точки, у систем Mesh Wi-Fi их несколько.

Mesh Wi-Fi — это домашняя Wi-Fi система, созданная для устранения зон со слабым сигналом и обеспечения непрерывного покрытия Wi-Fi во всём доме.

Мост — устройство, выполняющее функции повторителя для тех сигналов (сообщений), адреса которых удовлетворяют заранее наложенным ограничениям. Одной из проблем больших сетей является напряженный сетевой трафик (поток сообщений в сети). Эта проблема может решаться следующим образом. Компьютерная сеть делится на сегменты. Передача сообщений из сегмента в сегмент осуществляется только целенаправленно, если абонент одного сегмента передает сообщение абоненту другого сегмента. Мост является устройством,

ограничивающим движение по сети и не позволяющим сообщениям попадать из одной сети в другую без подтверждения права на переход.

Шлюз — специальный аппаратно-программный комплекс, предназначенный для обеспечения совместимости между сетями, использующими различные протоколы взаимодействия. Шлюз преобразует форму представления и форматы данных при передаче их из одного сегмента в другой. Он не зависит от используемой передающей среды, но зависит от используемых протоколов обмена данными. Обычно шлюз выполняет преобразования между протоколами.

3.3. Топология построения локальных вычислительных сетей.

К ***локальным*** компьютерным сетям (ЛВС или LAN – *Local Area Net Work*) относятся сети, узлы которых располагаются на небольшом расстоянии друг от друга, обычно не дальше нескольких сотен метров. Основным назначением ЛВС является предоставление информационных, вычислительных и технических ресурсов подключенным к сети пользователям.

ЛВС имеют характерные отличительные черты, позволяющие их выделить в отдельный класс компьютерных сетей:

1. Компактное территориальное расположение узлов сети. Расстояние между узлами сети обычно не превышает нескольких сот метров (LAN и корпоративные сети);
2. В качестве среды передачи данных используется кабельная система;
3. В качестве узлов сети часто используются персональные компьютеры;
4. Методы доступа, топологии, компоненты ЛВС разнообразны, имеют высокую степень совместимости и гибкости применения, что позволяет разрабатывать сети любой сложности и архитектуры.

Под ***архитектурой сети*** понимается вариант сети с конкретными *компонентами* сети (компьютеры, данные, программы, сетевое оборудование, различные устройства внешней памяти, принтеры, сканеры и другие устройства), *топологией* построения и *технологией* функционирования сети.

Под ***топологией*** вычислительной сети понимается изображение сети в виде графа, вершинами которого соответствуют компьютеры сети, отдельные виды сетевого оборудования, а ребрам – физические связи между ними. Также под ***топологией*** понимают, различные

способы конфигурации соединения кабелей для объединения компьютеров в ЛВС.

Существуют три основные *базовые топологии*:

- ✓ Звезда (Star);
- ✓ Кольцо (Ring);
- ✓ Шина (Bus), или общая.

Наряду с перечисленными топологиями компьютерных сетей на практике применяются и различные виды *комбинированных топологий*, которые получаются в результате комбинаций базовых топологий, это:

- ✓ Полносвязная;
- ✓ Ячеистая;
- ✓ Иерархическая;
- ✓ Смешанная.

Выбор топологии существенно влияет на многие характеристики сети. На рисунке 2 представлены базовые топологии сетей.

В топологии «Звезда» (см. рис. 2, *а*) один узел является центральным. Он соединен линиями связи со всеми остальными узлами сети. Благодаря этому связь любой рабочей станции с центральным узлом независима от связей остальных станций.

Основным преимуществом топологии «Звезда» является обеспечение работоспособности сети при выходе из строя отдельных рабочих станций и их соединений. В сетях с такой топологией проще обнаружить и устранить неисправности, связанные с работой отдельных узлов сети и линий передачи, наращивать масштаб сети за счет добавления новых компьютеров и менять их местонахождение.

Топология «Звезда» является наиболее быстродействующей, поскольку передача данных между рабочими станциями проходит через центральный узел по отдельным линиям. К недостаткам топологии следует отнести большой расход кабеля. Большинство сетей, использующих кабель типа «витая пара», монтируются по топологии «Звезда».

«Кольцевая» топология (рис. 2, *б*) представляет собой непрерывную магистраль для передачи данных, не имеющую логической начальной или конечной точек. Каждый компьютер является частью кольца и, получая данные, адресованные другому компьютеру, пересылает их по назначению. При такой топологии просто можно сделать кольцевой запрос на все станции. Однако продолжительность передачи информации увеличивается пропорционально количеству рабочих станций, входящих в сеть. Ограничения на протяженность сети не существует при условии соблюдения разрешенного расстояния между двумя соседними узлами. Основная проблема использования кольцевой

топологии состоит в том, что каждая рабочая станция должна активно участвовать в пересылке информации и в случае выхода из стоя хотя бы одной из них вся сеть становится неработоспособной. При этом неисправности линий связи легко локализуются и устраняются. Сети, сконструированные на основе топологии «Кольцо», могут использовать различные типы кабеля. Например, сети *Token Ring* используют витую пару, в то время как *FDDI-сети* реализуют топологию «кольцо» с помощью оптоволоконных кабелей.

Шинная топология (рис. 2, *в*) представляет собой наиболее простой способ установки сети. Она требует меньше оборудования, кабелей, времени на настройку, чем другие топологии. Физическая среда передачи состоит из единственного кабеля, который называется общей шиной, к которой подключаются все компьютеры сети. Недостатками являются подключение небольшого числа рабочих станций (не более 30) и полное прекращение работы сети при повреждении общего кабеля. Шинную архитектуру использует большая часть сетей, построенных на коаксиальных кабелях, таких, как сети *Ethernet*.

Рис. 2. Базовые топологии сетей:
***а* – звезда; *б* – кольцо; *в* – общая шина**

Наряду с описанными базовыми топологиями, на практике применяются различные их комбинации. Это связано с тем, что «созданная на определенном этапе развития системы ЛВС с течением времени перестает удовлетворять потребности всех пользователей, и тогда встает проблема расширения ее функциональных возможностей». Проблема расширения конфигурации сети может быть решена как в пределах ограниченного пространства, так и с выходом во внешнюю среду.

Виды комбинированных топологий представлены на рисунке 3.

В **полносвязной топологии** (рис. 3, *а*) используется связь между узлами по принципу «каждый с каждым». Данная топология характерна для глобальных сетей.

Ячеистая топология (рис. 3, *б*) предполагает, что любой узел сети располагает не менее чем двумя физическими связями с другими узлами. Данная топология применяется в неблагоприятных условиях

агрессивной окружающей среды при недостаточно большой вероятности разрыва сетевых соединений. Если одна из связей доступа к узлу будет нарушена, то всегда в качестве альтернативной связи будет существовать еще одна.

Иерархическая топология (рис. 3, *в*) используется в сетях, где существует жесткое распределение рабочих станций по уровням иерархии. При этом каждый узел более нижнего уровня имеет только одну линию связи с узлом более высокого уровня.

Смешанная топология (рис.3, *г*) в большинстве случаев образуется при объединении между собой ранее существовавших отдельные сетей с разными топологиями или в результате наращивания сети. «Так как к одному концентратору можно подключить неограниченное число хостов, смешанная топология находит широкое применение в крупных локальных сетях, связывающих сотни компьютеров».

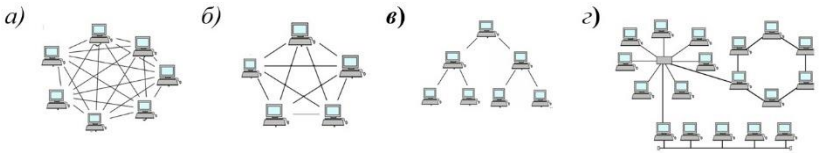


Рис. 3. Комбинированные топологии компьютерных сетей: *а* – полносвязная; *б* – ячеистая; *в* – иерархическая; *г* – смешанная

При построении архитектуры ЛВС следует учитывать существующие зависимости между используемыми технологиями работы, топологиями сети и кабельной системой. Возможные сочетания этих элементов архитектуры определены соответствующими стандартами и спецификациями.

Отметим, что основными методами доступа при построении современных ЛВС являются высокоскоростные технологии Ethernet, которые называются соответственно *Fast Ethernet* (скорость передачи – 100 Мбит/с) и *Gigabit Ethernet* (скорость передачи – 1Гбит/с).

Технологии *Arcnet* (скорость передачи – 2,5 Мбит/с) и *Token Ring* (скорость передачи – 4 Мбит/с или 16 Мбит/с) в настоящее время практически не используются из-за низкой производительности. Таким образом, технологии *Fast Ethernet* и *Gigabit Ethernet* являются основными технологиями построения ЛВС. Несмотря на то, что эти технологии являются прямыми преемниками *Ethernet*, у них отсутствуют многие недостатки, присущие прежней технологии.

Преодоление недостатков технологии *Fast Ethernet* и *Gigabit Ethernet* стало возможным благодаря реализации шиной топологии построения сети *Ethernet* в виде физической «звезды», а также использования витой пары и волоконно-оптического кабеля в качестве среды передачи. При такой архитектуре каждый луч «звезды» функционирует как отдельная логическая шина, но без концевых терминаторов. Один конец шины заканчивается на сетевом устройстве, к примеру, коммутаторе, другой – на узле сети. При этом общая шина выполняет роль высокоскоростной магистрали, соединяющей коммутаторы различных сегментов сети.

3.4. Оборудование ЛВС

Оборудование ЛВС может быть активным или пассивным. К пассивным элементам относятся кабель, короб, коммутационные устройства такие как шкафы, Patch-panel, розетки, коммутационные шнуры.

К активному оборудованию ЛВС относятся сетевые адаптеры, выполняющие функцию присоединения пользователя к ЛВС, поддерживающими обмен данными между ПК и средой передачи данных ЛВС. Кроме этого, сетевой адаптер выполняет роль временного хранилища данных, буферизацию.

Сетевые карты можно разделить на два типа: адаптеры для клиентских компьютеров и адаптеры для серверов.

Медиа конвертер — прибор, как правило, с двумя портами, обычно используемый для преобразования среды передачи данных (коаксиал-витая пара, витая пара-оптоволокно)

Активное оборудование мосты, маршрутизаторы и шлюзы в локальной вычислительной сети используют специализированное программное обеспечение.

При выборе лучшей передающей среды для ЛВС следует учитывать следующие факторы: скорость передачи данных, возможность применения в конкретных сетевых архитектурах, расстояние между соседними сетевыми устройствами, устойчивость к помехам от внешних источников, стоимость кабеля, сложность установки и модернизации.

В ЛВС применяют три типа кабеля: кабели на основе скрученных пар медных *проводов (витая пара), коаксиальные* кабели, *волоконно-оптические* кабели.

Витая пара существует в экранированном варианте, когда пара медных проводов заключается в изоляционный экран, и неэкранированном без изоляционной обертки. Скручивание проводов, а также наличие

изоляционного экрана снижают влияние внешних помех на полезные сигналы, передаваемые по кабелю. Все кабели типа витой пары имеют 4 пары скрученных проводов и делятся на 5 категорий, каждая из которых характеризуется определенной совокупностью электромагнитных характеристик (5-я категория позволяет передавать данные со скоростью до 1 Гбит/с).

Коаксиальный кабель состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существуют два типа коаксиального кабеля, толстый коаксиальный кабель и тонкий.

Толстый коаксиальный кабель достигает в диаметре 10 мм (скорость передачи данных не превышает 10 Мбит/с), тонкий – 5 мм (достигает 100 Мбит/с). Поэтому *тонкий* коаксиальный кабель используется при прокладке ЛВС в агрессивной внешней среде с высоким уровнем воздействия радио- и электромагнитных волн.

Волоконно-оптический кабель состоит из одной или нескольких стеклянных или пластиковых жил (световодов), по которым распространяются световые сигналы. Жилы покрыты защитной поливинилхлоридной оболочкой. Этот тип кабеля обеспечивает наивысшую скорость передачи данных до 100 Гбит/с. По волоконно-оптическому кабелю можно одновременно передавать по нескольку световых волн. Волоконно-оптический кабель применяется в ЛВС в качестве магистральных каналов передачи данных благодаря высокой скорости передачи и малого затухания сигнала. К достоинствам волоконно-оптического кабеля следует также отнести сложность получения несанкционированного доступа к данным во время передачи и невосприимчивость кабеля к радио- и электромагнитным помехам. Недостатками являются его высокие стоимость и хрупкость, сложность монтажа, а также высокие требования к квалификации обслуживающего персонала.

3.5. Модель взаимосвязи открытых систем OSI

Модель OSI была предложена Международной организацией стандартов ISO (International Standards Organization) в 1984 году. С тех пор ее используют (более или менее строго) все производители сетевых продуктов. Как и любая универсальная модель, OSI довольно громоздка, избыточна, и не слишком гибка. Поэтому реальные сетевые средства, предлагаемые различными фирмами, не обязательно придерживаются принятого разделения функций. Однако знакомство с моделью OSI позволяет лучше понять, что же происходит в сети (см. таб.2).

В модели OSI семь уровней взаимодействия: прикладной, представительный сеансовый, транспортный, сетевой, канальный и физический. Модель не включает средства взаимодействия приложений конечных пользователей, к тому же, приложение может взять на себя функции некоторых верхних уровней модели.

Таблица 2. Уровни модели OSI

Уровень OSI	Название уровня OSI	Назначение
7	Прикладной	Обеспечивает прикладным процессам пользователя средства доступа к сетевым ресурсам; является интерфейсом между программами пользователя и сетью. Имеет интерфейс с пользователем
6	Представления	Устанавливает стандартные способы представления данных, которые удобны для всех взаимодействующих объектов прикладного уровня. Имеет интерфейс с прикладными программами
5	Сеансовый	Обеспечивает средства, необходимые сетевым объектам для организации, синхронизации и административного управления обменом данных между ними
4	Транспортный	Обеспечивает надежную, экономичную и «прозрачную» передачу данных между взаимодействующими объектами сеансового уровня
3	Сетевой	Обеспечивает маршрутизацию передачи данных в сети, устанавливает логический канал между объектами для реализации протоколов транспортного уровня
2	Канальный	Обеспечивает непосредственную связь объектов сетевого уровня, функциональные и процедурные средства ее поддержки для эффективной реализации протоколов сетевого уровня
1	Физический	Формирует физическую среду передачи данных, устанавливает соединения объектов сети с этой средой

Прикладной уровень *(application) – управляет* запуском программ пользователя, их выполнением, вводом-выводом данных, управлением терминалами, административным управлением сетью. На этом уровне обеспечивается предоставление пользователям различных услуг, связанных с запуском его программ. На этом уровне функционируют технологии, являющиеся как бы надстройкой над передачей данных.

Уровень представления *(presentation)* — интерпретация и преобразование передаваемых в сети данных к виду, удобному для прикладных процессов. На практике многие функции этого уровня задействованы на прикладном уровне, поэтому протоколы уровня представлений не получили развития и во многих сетях практически не используются.

Сеансовый уровень *(session)* — организация и проведение сеансов связи между прикладными процессами (инициализация и поддержание сеанса между абонентами сети, управление очередностью и режимами передачи данных). Многие функции этого уровня в части установления соединения и поддержания упорядоченного обмена данными на практике реализуются на транспортном уровне, поэтому протоколы сеансового уровня имеют ограниченное применение.

Транспортный уровень *(transport)* — управление сегментированием данных и транспортировкой данных от источника к потребителю (т.е. обмен управляющей информацией и установление между абонентами логического канала, обеспечение качества передачи данных). Протоколы транспортного уровня развиты очень широко и интенсивно используются на практике. Большое внимание на этом уровне уделено контролю достоверности передаваемой информации.

Сетевой уровень *(network)* — управление логическим каналом передачи данных в сети (адресация и маршрутизация данных). Каждый пользователь сети обязательно использует протоколы этого уровня и имеет свой уникальный сетевой адрес, используемый протоколами сетевого уровня. На этом уровне выполняется структуризация данных — разбивка их на пакеты и присвоение пакетам сетевых адресов.

Канальный уровень *(data — reference)* — формирование и управление физическим каналом передачи данных между объектами сетевого уровня (установление, поддержание и разъединение логических каналов), обеспечение "прозрачности" физических соединений, контроля и исправления ошибок передачи.

Физический уровень *(physical)* — установление, поддержание и расторжение соединений с физическим каналом сети. Управление выполняется на уровне *битов* цифровых (импульсы, их амплитуда, форма) и аналоговых (амплитуда, частота, фаза непрерывного сигнала).

Блоки информации, передаваемые между уровнями, имеют стандартный формат: заголовок (header), служебная информация, данные, концевик. Каждый уровень при передаче блока информации нижестоящему уровню снабжает его своим заголовком. Заголовок вышестоящего уровня воспринимается нижестоящим как передаваемые данные.

Средства каждого уровня отрабатывают протокол своего уровня и интерфейсы с соседними уровнями.

Указанные уровни управления можно по разным признакам объединять в группы:

– Уровни 1, 2 и частично 3 реализуются в большей части за счет аппаратных средств; верхние уровни с 4 по 7 и частично 3 обеспечиваются программными средствами;
– Уровни 1 и 2 ответственны за физические соединения; уровни 3-6 заняты организацией передачи, передачей и преобразованием информации в понятную для абонентской аппаратуры форму; уровень 7 обеспечивает выполнение прикладных программ пользователя.

3.6. Основы гипертекстовой разметки

Hyper Text Markup Language (HTML) – язык разметки гипертекста.

Гипертекст - информационная структура, позволяющая устанавливать смысловые связи между элементами текста на экране компьютера таким образом, чтобы можно было легко осуществлять переходы от одного элемента к другому. На практике в гипертексте некоторые слова выделяют путем подчеркивания или окрашивания в другой цвет (гиперссылки). Выделение слова говорит о наличии связи этого слова с некоторым документом, в котором тема, связанная с выделенным словом, рассматривается более подробно.

Отдельный документ, выполненный в формате HTML, называется:

– HTML-документом;
– Web-документом;
– Web-страницей.

Такие страницы как правило имеют расширение html или htm.

URL-адрес ресурса образуется объединением доменного имени компьютера, на котором он хранится, и пути поиска (пути доступа), который ведет от корневого каталога жесткого диска этого компьютера через все вложенные каталоги к файлу, представляющему ресурс.

Типичный URL для WWW имеет вид:

http://www.название.домен/имя файла

Здесь название – это часть адреса, который часто употребляется для обозначения владельца сайта, а домен – обозначение крупного «раздела» Интернета: страны (ru), области деятельности (com) и т.д.

Например, адрес гипертекстового файла справочно-поисковой системе «Яндекс» в Интернете:

https://ya.ru/

Элемент – конструкция языка HTML. Это контейнер, содержащий данные и позволяющий отформатировать из определенным образом. Любая Web-страница представляет собой набор элементов. Одна из основных идей гипертекста возможность вложения элементов.

Тег – начальный или конечный маркеры элемента. Теги определяют границы действия элементов и отделяют элементы друг от друга. В тексте Web-страницы теги заключаются в угловые скобки, а конечный тег всегда снабжается косой чертой.

Задание 1. Рассмотреть структуру Web-документа.

<HTML>	Обозначение html документа
<HEAD>	Содержит служебную информацию. Здесь подключаются стили, указывается заголовок страницы, подключаются мета теги. Начало Области.
<TITLE>Структура Web-страницы</title>	Заголовок HTML-документа, отображаемый в верхней части строки заголовка браузера
<META>	Тег <meta> определяет данные (они называются ещё метатеги), которые используются для хранения информации, предназначенной для браузеров и поисковых систем.
<META name="Author" content="Ivan Petrov ">	Имя автора Web-страницы.
<META name="Keywords" content="WWW, HTML, document, страничка, структура">	Мета-тег, содержащий список ключевых слов, соответствующих странице сайта
</head>	Конец области заголовка Web-страницы.

<BODY bgcolor="blue">	Устанавливает цвет фона веб-страницы. Можно использовать этот атрибут совместно с background, подобрав цвет фона близкий к фоновому рисунку
<H> Здесь расположен заголовок вашей странички </h>	HTML предлагает шесть заголовков разного уровня, которые показывают относительную важность секции, расположенной после заголовка. Так, элемент <h1> представляет собой наиболее важный заголовок первого уровня, а <h6> служит для обозначения заголовка шестого уровня и является наименее значительным
<P> Здесь расположен текст первого абзаца вашей странички	Тег определяет текстовый абзац. Элемент является блочным, всегда начинается с новой строки, абзацы текста идущие друг за другом разделяются между собой отбивкой. Величиной отбивки можно управлять с помощью стилей. Если закрывающего тега нет, считается, что конец абзаца совпадает с началом следующего абзаца или другого блочного элемента.
<P> Здесь расположен текст второго абзаца вашей странички	
</body>	Конец содержимого Web-страницы.
</html>	Конец HTML-документа.

Задание 2. Самостоятельно рассмотреть правила форматированиz текста

Элемент	Тег	Атрибуты	Пример
Абзац	<P>	<P align="left"> - выравнивание текста по левому краю экрана. <P align="center> - выравнивание текста по центру экрана. <P align="right"> - выравнивание текста по правому краю экрана. <P align="justify"> Выравнивание по ширине, что означает одновременное выравнивание по левому и правому краю.	<P align="center"> Текст этого абзаца выровнен по центру экрана
Принудительный переход на новую строку	 		Перенос строк текста в HTML А. Блок Осенний вечер так печален; Смежает очи тающий закат Леса в безмолвии холодном спят Над тусклым золотом прогалин.
Выделение текста полужирным шрифтом	<B>		Тег задаёт жирное начертание шрифта. Допустимо использовать этот элемент совместно с другими, которые определяют начертание текста.
Выделение текста курсивом	<I>		Тег устанавливает курсивное начертание шрифта.

Определение типа, размера и цвета шрифта.	<FONT> 	<FONT size=4> - абсолютный размер шрифта (возможные значения от 1 до 7). <FONT color="red"> - цвет шрифта <FONT face=" Times New Roman "> - определение определенного шрифта. <FONT size=3 color="blue" face=" Times New Roman "> - все атрибуты могут быть использованы совместно внутри данного тега.	<FONT size=1> Шрифт номер 1 <FONT size=2> Шрифт номер 2 <FONT size=3> Шрифт номер 3 <FONT size=4> Шрифт номер 4 <FONT size=5> Шрифт номер 5 <FONT size=6> Шрифт номер 6 <FONT size=7> Шрифт номер 7 <FONT color="red"> Шрифт синего цвета <FONT face=" Times New Roman " size=3 color="blue" > Шрифт arial размером 3, цвет синий.
Маркированный список	<UL> <LI> <LI> <LI> 		<UL> <LI> Первый пункт списка; <LI> Второй пункт списка; <LI> Третий пункт списка.
Нумерованный список	<OL> <LI> <LI> <LI> 		<OL> <LI> Первый пункт списка; <LI> Второй пункт списка; <LI> Третий пункт списка.

Задание 3. Самостоятельно рассмотреть управление цветом

Кодирование цвета используется для раскрашивания шрифтов, горизонтальных линий, фона и других элементов страницы. Цвета обозначаются английскими названиями или числовыми шестнадцатеричными кодами.

Стандартные цвета

Аквамарин		aqua	#00FFFF
Белый		white	#FFFFFF
Желтый		yellow	#FFFF00
Зеленый		green	#008000
Золотистый		gold	#FFD700
Индиго		indigo	#4B0080
Каштановый		maroon	#800000
Красный		red	#FF0000
Оливковый		oliv	#808000
Пурпурный		purple	#800080
Светло-зеленый		lime	#00FF00
Серебристый		silver	#C0C0C0
Серый		gray	#808080
Сизый		teal	#008080
Синий		blue	#0000FF
Ультрамарин		navy	#000080
Фиолетовый		violet	#EE80EE
Фуксиновый		fuchsia	#FF00FF
Черный		black	#000000

Градации красного

Код	Цвет	Код	Цвет
#010000		#800000	
#100000		#900000	
#200000		#A00000	
#300000		#B00000	
#400000		#C00000	
#500000		#D00000	
#600000		#E00000	
#700000		#FF0000	

Градации зеленого

Код	Цвет	Код	Цвет
#000100		#008000	
#001000		#009000	
#002000		#00A000	
#003000		#00B000	
#004000		#00C000	
#005000		#00D000	
#006000		#00E000	
#007000		#00FF00	

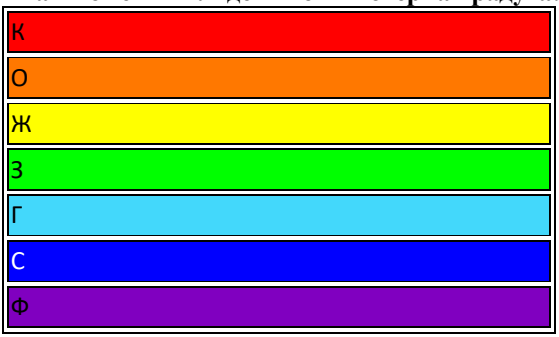
Градации синего

Код	Цвет	Код	Цвет
#000001		#000080	
#000010		#000090	
#000020		#0000A0	
#000030		#0000B0	
#000040		#0000C0	
#000050		#0000D0	
#000060		#0000E0	
#000070		#0000FF	

Градации оранжевого цвета

Код	Цвет
#FFB000	1
#FFA800	2
#FFA000	3
#FF9800	4
#FF9000	5
#FF8800	6
#FF8000	7
#FF7800	8
#FF7000	9
#FF6800	10
#FF6000	11
#FF5800	12

А так может выглядеть компьютерная радуга:



3.7. Примеры решения практических задач

Задание 1. Моя первая Web-страница

1. Откройте текстовый редактор «Notepad++» — бесплатный редактор исходного кода и универсальный помощник веб-дизайнеров и программистов.

2. Наберите в нем структуру HTML-документа:

```
<HTML>
<HEAD>
<TITLE>.....</title>
</head>
<BODY>
.....
</body>
</html>
```

3. Сохраните файл как main_page1.html в ***папке под названием «Моя первая Web-страница»***

4. Зайдите в свою папку и откройте созданный файл. Вы увидите, как выглядит созданный вами файл в окне браузера.

5. Закройте браузер.

6. Вернитесь к сохраненному файлу в «Notepad++».

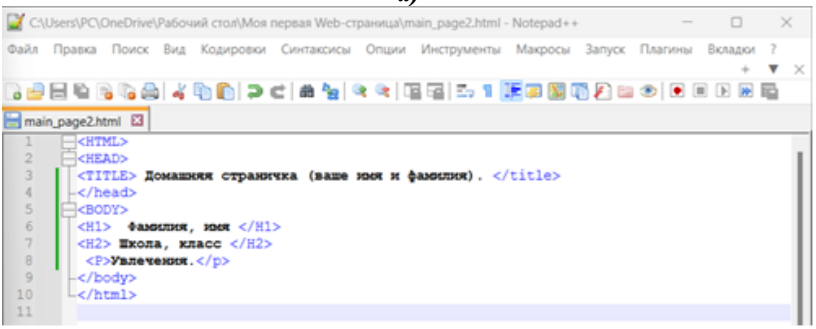
7. Внесите в него следующие изменения: пусть это будет ваша первая страничка. Укажите в ней ваши фамилию, имя, школу, класс, увлечения. Используйте для этого форматирование заголовков и абзацев.

8. В строке <TITLE> укажите: «Домашняя страничка (ваше имя и фамилия)»

9. Сохраните файл как main_page2.html.

10. Просмотрите результат в браузере, при необходимости отредактируйте файл при помощи «Notepad++» (см. рис.4 a,b):

a)



b)

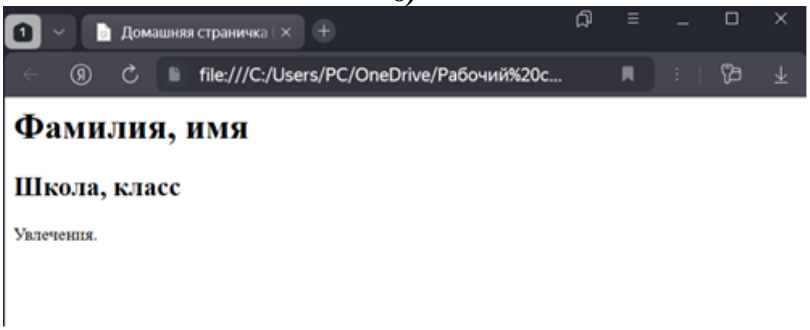


Рис. 4. Результат кода страницы и результат страницы в браузере a,b

<u>Задание 2.</u> Самостоятельно рассмотреть использование цвета при оформлении страницы.

Цвет **шрифта** можно задать с помощью атрибута **color** в теге <FONT>, например (см. рис.5 a,b):

<FONT color="#00D000"> Зеленый текст

<FONT color="aqua"> Аквамариновый текст

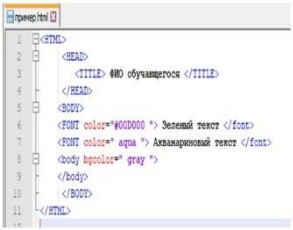
Для задания цвета фона документа (страницы) используется атрибут bgcolor:< body bgcolor="gray">

Код:

```
<HTML>
  <HEAD>
```

```
      <TITLE> ФИО обучающегося </TITLE>
    </HEAD>
   <BODY>
            <FONT color="#00D000 "> Зеленый текст </font>
            <FONT color=" aqua "> Аквамариновый текст </font>
            <body bgcolor=" gray ">
            </body>
    </BODY>
</HTML>
```

a)



b)

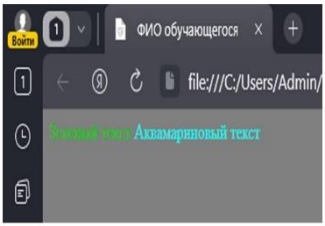


Рис. 5. *a, b.* Пример работы с текстом

Сохраните файл как main_page3.html.

<u>Задание 3.</u> Использование цвета при оформлении страницы.

1. Откройте файл «main_page1.html» при помощи «Notepad++».
2. Самостоятельно подберите цвет для текста в вашей странице и задайте цвет фона вашей страницы.
3. Сохраните файл как «main_page4.html».

3.8. Практические задачи для самостоятельного решения

<u>Задание 1.</u> Создание простейшей WEB - страницы

ТЕХНОЛОГИЯ РАБОТЫ

1. Запустите текстовый редактор «Notepad++»
2. Введите следующий документ (см. рис.6 a,b):

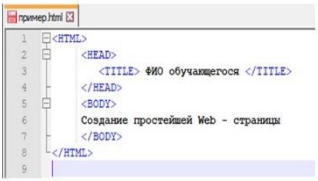
```
<HTML>
   <HEAD>
     <TITLE> ФИО обучающегося </TITLE>
   </HEAD>
   <BODY>
```

Создание простейшей Web - страницы
</BODY>
</HTML>

3. Сохраните этот документ под именем «original.html»
4. Запустите браузер.
5. Дайте команду Файл - Открыть. Щелкните на кнопке Обзор и откройте файл «original.html»
6. Посмотрите, как отображается этот файл – простейший корректный документ HTML. Где отображается содержимое документа BODY
7. Закройте программу.

Примечание: При использовании тега TITLE содержание заголовка документа отображается в верхней строке рабочего поля браузера.

a)



b)

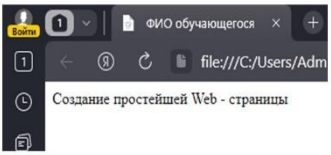


Рис. 6. *a, b.* Создание WEB – страницы

Задание 2. Изучение приемов форматирования абзацев

В большинстве документов основными функциональными элементами являются заголовки и абзацы. Язык HTML поддерживает шесть уровней заголовков. Они создаются при помощи парных тегов от <H1> до <H6>. При отображении Web - документа на экране компьютера эти элементы показываются при помощи шрифтов разного размера.

Обычные абзацы задаются с помощью парного тега <P>. Язык HTML не содержит средств для создания абзацного отступа (красной строки), поэтому при отображении на экране компьютера абзацы разделяются пустой строкой. Закрывающий тег </P> рассматривается как необязательный. Подразумевается, что он стоит перед тегом, который задает начало очередного абзаца документа. Например:

<H1> Заголовок</H1>
<P>Первый абзац<P>Второй абзац
<H2> Заголовок второго уровня</H2> (см. рис.7 a,b):

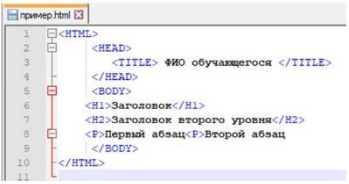
В качестве ограничителя абзацев может также использоваться горизонтальная линейка. Этот элемент задается непарным тегом <HR>.

При отображении документа на экране линейка разделяет части текста друг от друга.

Код:

```
<HTML>
   <HEAD>
     <TITLE> ФИО обучающегося </TITLE>
   </HEAD>
   <BODY>
          <H1>Заголовок</H1>
          <H2>Заголовок второго уровня</H2>
          <P>Первый абзац<P>Второй абзац
   </BODY>
</HTML>
```

a)



b)

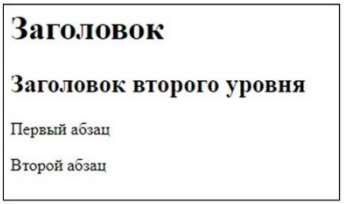


Рис. 7. *a, b.* Пример форматирования абзацев

ТЕХНОЛОГИЯ РАБОТЫ

1. Откройте документ «original.html», в программе «Notepad++»
2. Между тегами <TITLE> и </TITLE> наберите Задание 2
3. Удалите весь текст, находящийся между тегами <BODY> и </BODY>. Текст, который будет вводится в последующих пунктах этого задания, необходимо поместить после тега <BODY>, а его конкретное содержание может быть любым
4. Введите заголовок первого уровня, заключив его между тегами <H1> и </H1>, например «**Топология построения локальных вычислительных сетей**»
5. Введите заголовок второго уровня, заключив его между тегами <H2> и </H2>,

Например:

1. Общая характеристика топологий компьютерных сетей (см. рис.2 *a, b*):

Введите отдельный абзац текста, например

Существуют три основные базовые топологии:

- Звезда (Star);

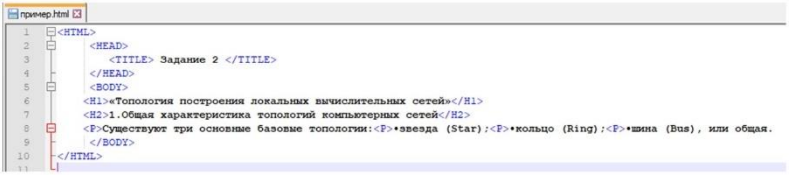
- Кольцо (Ring);
- Шина (Bus), или общая.

начав его с тега <P>. Пробелы и символы перевода строки можно использовать внутри абзаца произвольно

Код:

```
<HTML>
   <HEAD>
     <TITLE> Задание 2 </TITLE>
   </HEAD>
   <BODY>
            <H1>«Топология построения локальных вычислительных сетей»</H1>
            <H2>1.Общая характеристика топологий компьютерных сетей</H2>
            <P>Существуют три основные базовые топологии:<P>•звезда (Star);<P>•кольцо (Ring);<P>•шина (Bus), или общая.
   </BODY>
</HTML>
```

a)



b)

Рис. 8. *a, b.* Пример маркированного списка

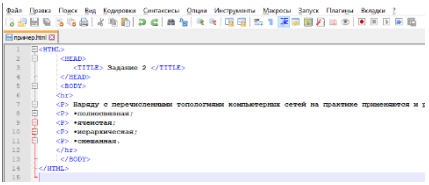
6. Введите тип горизонтальной линейки <HR> (см. рис.9 a, b):

Введите еще один абзац текста, начав его с тега <P>, например:

Наряду с перечисленными топологиями компьютерных сетей на практике применяются и различные виды комбинированных топологий, которые получаются в результате комбинаций базовых топологий, это:

- Полносвязная;
- Ячеистая;
- Иерархическая;
- Смешанная.

a)



b)

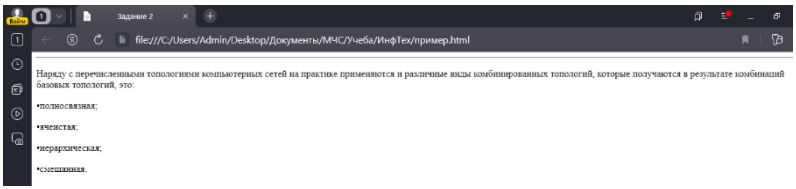


Рис. 9. *a, b.* Комбинированные топологии

7. Сохраните этот документ под именем «list.html».
8. Запустите программу браузера и откройте файл «list.html».
9. Посмотрите, как отображается этот файл.

Закройте программу

Задание 3. Создание гиперссылок

Гипертекстовая ссылка является фрагментом текста документа и поэтому задается текстовым элементом, определяемым при помощи парного тега <A>. Этот элемент содержит обязательный атрибут, который не может быть опущен. В данном случае обязательным является атрибут HREF= (знак равенства показывает, что необходимо задать значение этого атрибута). В качестве значения атрибута используется адрес URL документа, на который указывает ссылка. Она может указывать на произвольный документ, располагающийся на любом общедоступном узле сети (Web -узел). Например, открывающий тег ссылки может иметь вид <A HREF=http://otvet-akab.ru/index/zavtra_ehkzamen/0-9>.

ТЕХНОЛОГИЯ РАБОТЫ

1. Откройте файл «original.html» в программе «Notepad++»
2. Удалите весь текст, находящийся между тегами <BODY> и </BODY>. Текст, который будет вводится в последующих пунктах этого упражнения, необходимо поместить после тега <BODY>
3. Введите фразу: Текст до ссылки (см. рис.10 a,b):
4. Введите тег <A HREF="original.html">
5. Введите фразу: Ссылка
6. Введите закрывающийся тег </A>
7. Введите фразу: Текст после ссылки
8. Сохраните документ под именем «reference.html».
9. Запустите программу браузера.
10. Выполните команду Файл - Открыть. Щелкните по кнопке Обзор и откройте файл «reference.html»
11. Убедитесь в том, что текст между тегами <A> и </A> выделен как ссылка
12. Щелкните по ссылке и убедитесь, что при этом загружается документ, на который указывает ссылка
13. Щелкните по кнопке Назад на панели инструментов, чтобы вернуться к предыдущей странице. Убедитесь, что ссылка теперь считается просмотренной и отображается другим цветом.
14.

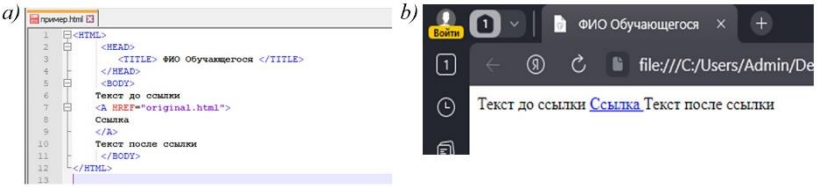


Рис. 10. *a, b.* Пример гиперссылок

Задание 4. Создание изображения и использование его на Web странице

Графические иллюстрации в большинстве случаев являются неотъемлемой частью Web - документов. Сегодня графические элементы Web страниц используют два основных формата - JPEG и JPEG. Все графические браузеры, предназначенные для отображения Web - страниц на экране компьютера, способны распознавать и отображать файлы этих форматов. Для вставки рисунка используется текстовый элемент, задаваемый непарным тегом <IMG>. Тег <IMG> должен

содержать обязательный атрибут SRQ=, задающий адрес URL файла с изображением. <IMG SRC="picture1.jpeg"

При отображении рисунка браузер по умолчанию использует его реальные размеры. Если рисунок необходимо отмасштабировать, применяют атрибуты WIDTH= и HEIGHT=, задающие ширину и высоту рисунка в пикселях.

Для изображения, которое действительно включено в строку, можно задать режим взаимодействия с текстом с помощью атрибута ALIGN=.

Этот атрибут может принимать три значения:

– если задано ALIGN="BOTTOM", то нижняя граница изображения совмещается с основанием текстовой строки;
– если задано ALIGN="MIDDLE», то середина изображения совмещается с серединой текстовой строки;
– если задано ALIGN="TOP», то верхняя граница изображения выравнивается по верхнему обрезу текстовой строки;
– если ALIGN="LEFT", то изображение размещается у левого края страницы, а текст справа от него;
– если ALIGN="RIGHT", то изображение размещается у правого края страницы, а текст слева от него.

ТЕХНОЛОГИЯ РАБОТЫ

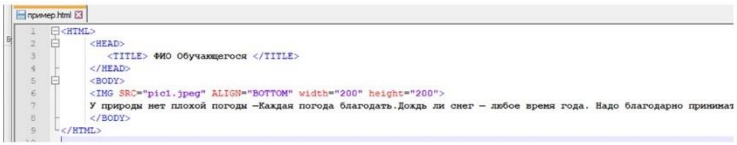
1. Откройте программу Paint. Задайте размеры рисунка, например 200x200 точек
2. Выберите красный цвет переднего плана и зеленый цвет фона. Залейте рисунок фоновым цветом
3. Инструментом Кисть, нанесите произвольный красный рисунок на зеленый фон
4. Сохраните рисунок по именем pic1.jpeg
5. Закройте программу Paint
6. Запустите программу «Notepad++»
7. Откройте файл «original.html».
8. Удалите весь текст, находящийся между тегами <BODY> и </BODY>. Текст, который будет вводится в последующих пунктах этого задания, необходимо поместить после тега <BODY>
9. Введите произвольный текст (протяженностью 4-5 строк) и установите текстовый курсор в его начало
10. Введите тег <IMG SRC="pic1.jpeg" ALIGN="BOTTOM" width="200" height="200"> (см. рис.11 a, b):
11. Сохраните документ под именем «picture.html»

12. Запустите программу браузера.
13. Задайте команду Файл - Открыть. Щелкните по кнопке Обзор и откройте файл «picture.html».
14. Вернитесь в программу «Notepad++» и измените значение атрибута ALIGN="TOP". Сохраните файл под прежним именем
15. Вернитесь в браузер и щелкните по кнопке «Обновить» на панели инструментов. Посмотрите, как изменился вид страницы при изменении атрибутов
16. Вернитесь в программу «Notepad++» и измените значение атрибута: ALIGN="LEFT"> Сохраните файл под прежним именем
17. Вернитесь в браузер и щелкните по кнопке Обновить на панели инструментов. Посмотрите, как изменился вид страницы при изменении атрибутов
18. Вернитесь в программу «Notepad++» и добавьте в тег <IMG> атрибуты: HSPACE=40 VSPACE=20. Сохраните файл под прежним именем
19. Вернитесь в программу «Notepad++» и измените имя рисунка: SRC="pic2.jpeg". Сохраните файл под прежним именем
20. Вернитесь в браузер и щелкните по кнопке Обновить. Посмотрите, как изменился вид страницы при изменении атрибутов

Код:

```
<HTML>
  <HEAD>
    <TITLE> ФИО Обучающегося </TITLE>
  </HEAD>
  <BODY>
        <IMG SRC="pic1.jpeg" ALIGN="BOTTOM" width="200" height="200">
        У природы нет плохой погоды — Каждая погода благодать. Дождь ли снег — любое время года. Надо благодарно принимать
  </BODY>
</HTML>
```

a)



b)

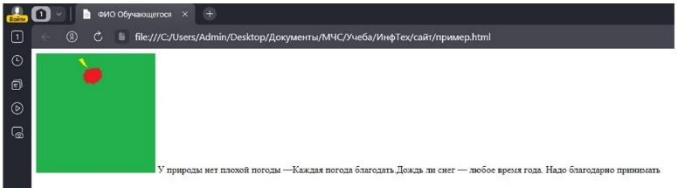


Рис. 11. *a, b.* Пример изображения его на Web странице

Задание 5. Создание таблиц и фреймов в HTML – формате

Приемы создания списков

Упорядоченные (нумерованные) и неупорядоченные (маркированные) списки оформляются одинаково. Они создаются при помощи парных тегов <OL> для упорядоченного списка и <UL> для неупорядоченного. Эти списки могут содержать только элементы списка, определяемые парным тегом <LI>. Закрывающийся тег </LI> можно опускать. Список определений задается парным тегом <DL>. Он содержит элементы двух типов: определяемые термины (парный тег <DT> и определение (парный тег <DD>. Такой список может быть сформирован следующим образом:

<DL>
<DT>Поршень
<DD>Сплошной цилиндр или диск, который плотно заходит внутрь полого цилиндра
</DL>

ТЕХНОЛОГИЯ РАБОТЫ

1. Откройте документ «original.html» в программе «Notepad++»
2. Удалите весь текст, находящийся между тегами <BODY> И </BODY>. Текст, который будет вводится в последующих пунктах этого упражнения, необходимо поместить после тега <BODY>.
3. Вставьте в документ тег <OL TYPE="I">, который начинает упорядоченный (нумерованный) список (см. рис.12. a,b)
4. Вставьте в документ элементы списка, предваряя каждый из них тегом <LI>, например:
   <LI> Компьютер;

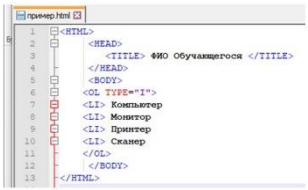
<LI> Монитор;
<LI> Принтер;
<LI> Сканер.

5. Завершите список при помощи тега </OL>
6. Сохраните полученный документ под именем «checklist.html».
7. Запустите браузер.
8. Задайте команду Файл - Открыть. Щелкните по кнопке Обзор и откройте файл «checklist.html».
9. Изучите, как упорядоченный список отображается в браузере.

Код:

```
<HTML>
  <HEAD>
    <TITLE> ФИО Обучающегося </TITLE>
  </HEAD>
  <BODY>
   <OL TYPE="I">
   <LI> Компьютер;
   <LI> Монитор;
   <LI> Принтер;
   <LI> Сканер.
   </OL>
  </BODY>
</HTML>
```

a)



b)

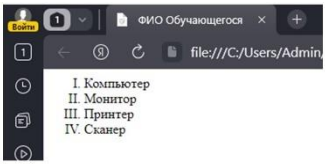


Рис. 12. *a, b.* Пример таблиц и фреймов в HTML

10. Вернитесь в программу «Notepad++» и установите текстовый курсор после окончания введенного списка
11. Вставьте в документ тег <UL TYPE="SQUARE">, который начинает неупорядоченный (маркированный) список (см рис.13 a,b)
12. Вставьте в документ элементы списка, предваряя каждый из них тегом <LI>, например:

<LI> Word;
<LI> Excel;
<LI> Access.

13. Завершите список при помощи тега </UL>.Сохраните документ под тем же именем
14. Вернитесь в браузер и щелкните по кнопке Обновить на панели инструментов. Посмотрите, как изменился вид страницы, обратив внимание на способ маркировки, заданный при помощи атрибута TYPE=

Код:

```
<HTML>
   <HEAD>
     <TITLE> ФИО Обучающегося </TITLE>
   </HEAD>
   <BODY>
    <UL TYPE="SQUARE">
    <LI> Word
    <LI> Excel
    <LI> Access
    </UL>
   </BODY>
</HTML>
```

a)

b)

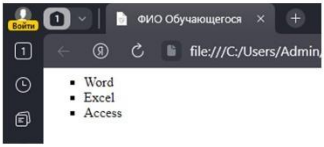


Рис. 13. *a, b*. Пример таблиц и фреймов в HTML

15. Вернитесь в программу «Notepad++» и установите текстовый курсор после окончания введенного списка
16. Вставьте в документ тег <DL>, который начинает список определений
17. Вставьте в список определяемое слово, предваряя соответствующий абзац тегом <DT>, например *Производительность процессора*
18. Вставьте в список соответствующее определение, предваряя его тегом <DD>, например: *это интегральная характеристика, зависящая от частоты процессора, его разрядности и особенностей архитектуры*
19. Завершите список при помощи тега </DL>. Сохраните документ под тем же именем

20. Вернитесь в браузер и щелкните по кнопке Обновить на панели инструментов. Посмотрите, как выглядит при отображении Web - страницы список определений (см. рис. 14):

Код:

```
<HTML>
  <HEAD>
    <TITLE> ФИО Обучающегося </TITLE>
  </HEAD>
  <BODY>
   <DL>
   <DT> Производительность процессора
   <DD> Это интегральная характеристика, зависящая от частоты процессора, его разрядности и особенностей архитектуры
    </DL>
     </BODY>
</HTML>
```

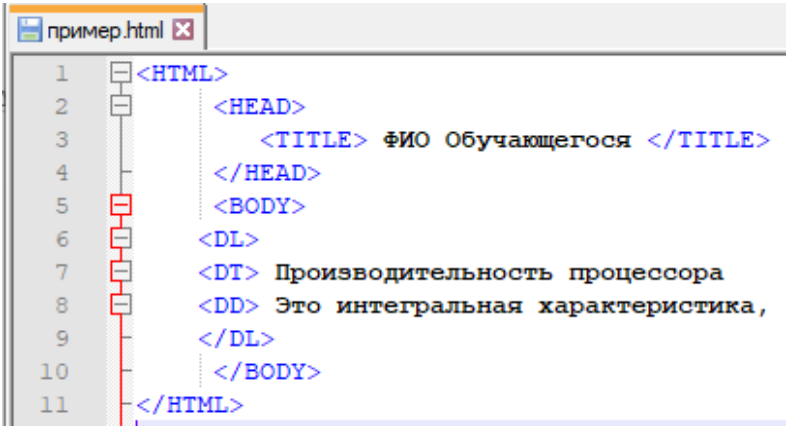


Рис. 14. Пример таблиц и фреймов в HTML

Задание 6. Создание таблиц

Таблицы в языке HTML задаются при помощи парного тега <TABLE>. Она может содержать заголовок таблицы, определяемый парным тегом <CAPTION> и строк таблицы, задаваемых при помощи парных тегов <TR>. Каждая строка таблицы содержит ячейки таблицы, которые могут относится к двум разным типам. Ячейки в заголовках столбцов и строк задают парным тегом <TH>, а обычные ячейки - парным тегом <TD>. Закрывающиеся теги </TH> и </TD> можно опускать.

Например: "пустая" таблица с двумя строками и двумя столбцами может быть задана следующим образом:

```
<TABLE>
<CAPTION>Пустая таблица</CAPTION>
<TR><TD><TD>
<TR><TD><TD>
</TABLE>
```

ТЕХНОЛОГИЯ РАБОТЫ

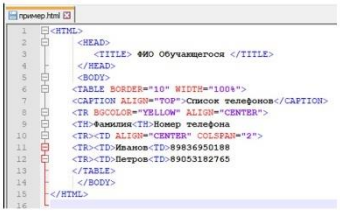
1. Откройте документ «original.html» в программе «Notepad++»
2. Удалите весь текст, находящийся между тегами <BODY> и </BODY>. Текст, который будет вводится в последующих пунктах этого задания, необходимо поместить после тега <BODY>. В данном задании используется список номеров телефонов
3. Введите тег <TABLE BORDER="10" WIDTH="100%"> (см рис. 15)
4. Введите строку <CAPTION ALIGN="TOP"> Список телефонов</CAPTION>
5. Первая строка таблицы должна содержать заголовки столбцов. Определите ее следующим образом:
   <TR BGCOLOR="YELLOW" ALIGN="CENTER">
   <TH>Фамилия<TH>Номер телефона
6. Определите последующие строки таблицы, предваряя каждую из них тегом <TR> и помещая содержимое каждой ячейки после тега <TD>
7. Последнюю строку таблицы задайте следующим образом:
   <TR><TD ALIGN="CENTER" COLSPAN="2">На первом этаже здания имеется бесплатный телефон
8. Таблица состоит из 5 строк (5 фамилий и 5 номеров телефона)
9. Завершите таблицу тегом </TABLE>
10. Сохраните документ под именем «table.html».
11. Запустите браузер Откройте файл «table.html».
12. Изучите, как отображается в программе таблица
13. Закройте программу

Код:

```
<HTML>
  <HEAD>  <TITLE> ФИО Обучающегося </TITLE>  </HEAD>
  <BODY>
   <TABLE BORDER="10" WIDTH="100%">
   <CAPTION ALIGN="TOP">Список телефонов</CAPTION>
   <TR BGCOLOR="YELLOW" ALIGN="CENTER">
   <TH>Фамилия<TH>Номер телефона
```

```
<TR><TD ALIGN="CENTER" COLSPAN="2">
<TR><TD>Иванов<TD>89836950188
<TR><TD>Петров<TD>89053182765
</TABLE>
 </BODY>
</HTML>
```

a)



b)

Список телефонов

Фамилия	Номер телефона
Иванов	89836950188
Петров	89053182765

Рис. 15. *a, b.* Пример создания таблиц

Задание 7. Создание описания фреймов

Язык HTML позволяет в рамках одной Web страницы отобразить несколько документов. Для этого страница должна быть разбита на несколько областей - фреймов. Тело документа заменяется описанием фреймов, задаваемых первым тегом <FRAMESET>. Открывающий тег <FRAMESET> должен содержать обязательный атрибут COLS= или ROWS=, определяющий способ разбиения окна. В первом случае окно разбивается вертикальными линиями, во втором - горизонтальными. Если заданы оба атрибута задается сетка фреймов. Значение любого из этих атрибутов — это перечисленные через запятую размеры отдельных фреймов.

ТЕХНОЛОГИЯ РАБОТЫ

1. Запустите программу «Notepad++»
2. Введите следующий документ:

```
<HTML>
<HEAD> <TITLE>Описание фреймов</TITLE> </HEAD>
<FRAMESET ROWS="60%,*">
    <FRAME SRC="table.html">
    <FRAMESET COLS="35%,65%"NORESIZE>
        <FRAME SRC="original.html">
```

```
        <FRAME SRC="reference.html">
    <FRAMESET>
    </HTML>
```

3. Сохраните этот документ под именем «frames.html».
4. Запустите браузер.
5. Откройте документ «frames.html».
6. Изучите его структуру.
7. Закройте документ.

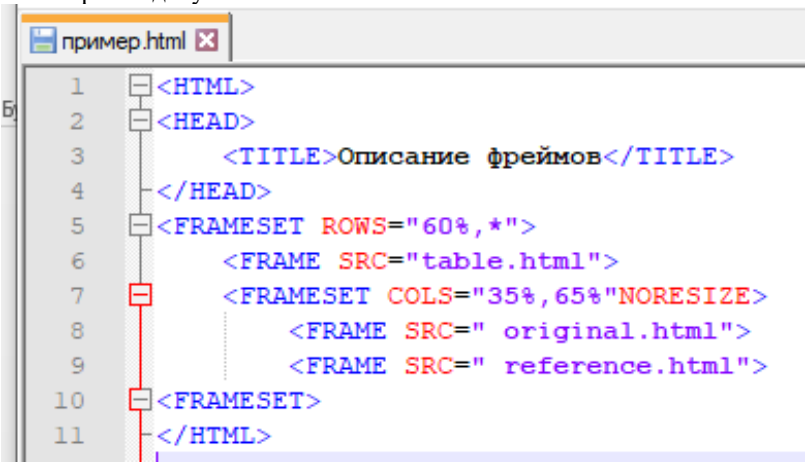


Рис. 16. Пример создания и описания фреймов

3.9. Тесты для самоконтроля знаний по теме «Работа с ресурсами информационно-вычислительных сетей»

1. … – это комплекс аппаратных и программных средств, позволяющих компьютерам обмениваться данными:

1) Интерфейс;
2) Компьютерная сеть;
3) Магистраль;
4) Адаптеры;
5) Все ответы правильные.

2. Как называется группа компьютеров, связанных каналами передачи информации и находящихся в пределах территории, ограниченной небольшими размерами:

1) Глобальной компьютерной сетью;
2) Информационной системой с гиперсвязями;
3) Локальной компьютерной сетью;
4) Электронной почтой;
5) Региональной компьютерной сетью.

3. Глобальная компьютерная сеть — это:

1) Совокупность локальных сетей и компьютеров, расположенных на больших расстояниях и соединенные в единую систему;
2) Информационная система с гиперсвязями;
3) Множество компьютеров, связанных каналами передачи информации и находящихся в пределах одного помещения, здания;
4) Система обмена информацией на определенную тему;
5) Нет правильного ответа.

4. Как называется обмен информацией между компьютерными сетями, в которых действуют разные стандарты представления информации (сетевые протоколы), осуществляется с использованием:

1) Магистралей;
2) Хост-компьютеров;
3) Электронной почты;
4) Шлюзов;
5) Файл-серверов.

5. Как называется топология локальной компьютерной сети, в которой все рабочие станции соединены непосредственно с сервером, называется:

1) Кольцевой;
2) Звезда;
3) Шинной;
4) Древовидной;
5) Сетевой.

6. Протокол маршрутизации (IP) обеспечивает:

1) Доставку информации от компьютера-отправителя к компьютеру-получателю;
2) Интерпретацию данных и подготовку их для пользовательского уровня;
3) Сохранение механических, функциональных параметров физической связи в компьютерной сети;
4) Управление аппаратурой передачи данных и каналов связи;
5) Разбиение файлов на IP-пакеты в процессе передачи и сборку файлов в процессе получения.

7.Компьютер, подключенный к Интернет, обязательно имеет:

1) IP-адрес;
2) Web-страницу;
3) Домашнюю web-страницу;
4) Доменное имя;
5) URL-адрес.

8. Модем обеспечивает:

1) Преобразование двоичного кода в аналоговый сигнал и обратно;
2) Преобразование двоичного кода в аналоговый сигнал;
3) Преобразование аналогового сигнала в двоичный код;
4) Усиление аналогового сигнала;
5) Ослабление аналогового сигнала.

9. Телеконференция — это:

1) Обмен письмами в глобальных сетях;
2) Информационная система в гиперсвязях;
3) Система обмена информацией между абонентами компьютерной сети;
4) Служба приема и передачи файлов любого формата;
5) Процесс создания, приема и передачи web-страниц.

10. Web – страницы имеют расширение:

1) *.htm;
2) *.txt;
3) *.web;
4) *.exe;
5) *.www.

11. HTML (HYPER TEXT MARKUP LANGUAGE) является:

1) Язык разметки web-страниц;
2) Системой программирования;
3) Текстовым редактором;
4) Системой управления базами данных;
5) Экспертной системой.

12. Служба FTP в Интернете предназначена:

1) Для создания, приема и передачи web-страниц;
2) Для обеспечения функционирования электронной почты;
3) Для обеспечения работы телеконференций;
4) Для приема и передачи файлов любого формата;
5) Для удаленного управления техническими системами.

13. Компьютер, предоставляющий свои ресурсы в пользование другим компьютерам при совместной работе, называется:

1) Адаптером;
2) Коммутатором;
3) Станцией;
4) Сервером;
5) Клиент-сервером.

14. Теоретически модем, передающий информацию со скорость 57600 бит/с, может передать 2 страницы текста (3600 байт) в течении:

1) 0.5 ч;
2) 0.5 мин;
3) 0.5 с;
4) 3 мин 26 с.

15.Топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу – это:

1) Кольцо;
2) Шина;
3) Звезда;
4) Ячеистая;
5) Смешанная.

16. Сеть, объединяющая несколько компьютеров и позволяет использовать ресурсы компьютеров и подключённых к сети периферийных устройств, называется:

1) Замкнутая;
2) Региональная;
3) Локальная;
4) Корпоративная;
5) Глобальная.

3.10 Ответ на тест для самоконтроля знаний по теме «Работа с ресурсами информационно-вычислительных сетей»

КЛЮЧ

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	3	4	4	2	1	1	1	1	1	1	3	2	1	3	3

3.11 Ключевые понятия и термины

OSI	Модель взаимосвязи открытых систем
ЛВС (LAN)	Локальная вычислительная сеть
ЭВМ	Электронно-вычислительная машина
TCP/IP	Сетевая модель передачи данных, представленных в цифровом виде
USB	Последовательный интерфейс для подключения периферийных устройств к вычислительной технике
Wi-Fi	Технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11. Логотип Wi-Fi является торговой маркой Wi-Fi Alliance.
HTML	Язык разметки гипертекста

4. ЗАЩИТА ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

4.1. Краткие сведения из теории

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности.

Информационная безопасность – это:

- ✓ Состояние объекта, когда ему путем воздействия на его информационную сферу не может быть нанесен существенный ущерб или вред;
- ✓ Свойство объекта, характеризующее его способность не наносить существенного ущерба какому-либо объекту путем оказания воздействия на информационную сферу этого объекта.

Информационная угроза – угроза объекту путем оказания воздействия на его информационную сферу:

- ✓ Намерение нанести (причинить) объекту существенный ущерб путем оказания воздействия на его информационную сферу;
- ✓ Информационная опасность, реализация которой становится весьма вероятной;
- ✓ Фактор или совокупность факторов, создающих информационную опасность объекту; такими факторами могут быть действия, поведение объектов, природные явления и т. д.

Информационная безопасность личности – это состояние человека, в котором его личности не может быть нанесен существенный ущерб путем оказания воздействия на окружающее информационное пространство.

Информационная безопасность общества – это состояние общества, в котором ему не может быть нанесен существенный ущерб путем воздействия на его информационную сферу.

Информационная безопасность государства – это состояние государства, в котором ему не может быть нанесен существенный ущерб путем оказания воздействия на его информационную сферу. Обеспечение информационной безопасности государства неразрывно связано с обеспечением национальной безопасности.

Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Субъекты информационных отношений – государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица),

отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

Доступность информации – свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Конфиденциальность информации – субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней. Объективные предпосылки подобного ограничения доступности информации заключены в необходимости защиты законных интересов некоторых субъектов информационных отношений.

Другими словами, можно сказать, ***что конфиденциальность информации –*** это решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней.

Безопасность информации (данных) (англ. information (data) security) — состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (при применении информационных технологий) (англ. IT security) — состояние защищённости информации (данных), обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы — состояние защищённости автоматизированной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

Доступ к информации – ознакомление с информацией (копирование, тиражирование), ее модификация (корректировка) или уничтожение (удаление).

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Доступ к ресурсу – получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

Несанкционированный доступ (НСД) – доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Правовые меры защиты информации – действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Морально-этические меры защиты информации – традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как традиционно сложившиеся (например, общепризнанные нормы честности, патриотизма и т.п.), так и специально разработанные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Организационные (административные) меры защиты – это меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Физические меры защиты – это разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам АС и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации.

Технические (аппаратно-программные) средства защиты – различные электронные устройства и специальные программы, входящие в состав, АС, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам,

регистрацию событий, криптографическое закрытие информации и т.д.).

4.2 Место и роль информационной безопасности в системе национальной безопасности России

В современных общественно-политических условиях, характеризующихся высоким уровнем технологизации всех сторон жизни, обеспечение информационной безопасности страны является весьма важной задачей, определяющей ее национальную безопасность в целом. Действенная политика в области информационной безопасности невозможна без соответствующего нормативно-правового регулирования.

Все множество документов этой сферы можно представить в виде нескольких групп (рис.17)

Рис. 17 Группы документов в области информационной безопасности

К первой группе относятся Законы Российской Федерации, такие как:

- «О Государственной тайне» №5151-1 от 21 июля 1993 г. (с посл. изм. от 08.08.2024 N 249-ФЗ);
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (СЗ РФ, 2006, № 31, ст. 3448; с посл. изм. от 08.08.2024 № 303 ФЗ);
- Федеральный закон от 22 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации" (СЗ РФ. 2004, N 43, ст. 4169; с посл. изм. от 25.12.2023 N 635-ФЗ);

- Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" (Собрание законодательства РФ, 2011, N 15, ст. 2036; с посл. изм. от 04.08.2023 N 457-ФЗ).

Вторую группу документов составляют Указы Президента Российской Федерации. В их число входят:

- Указ Президента РФ “Об утверждении Перечня сведений конфиденциального характера” от 06.03.1997 N 188 (с посл. изм. от 13.07.2015 N 357);
- Указ Президента РФ “Об утверждении перечня сведений, отнесенных к государственной тайне” от 30.11.1995 N 1203 (ред. от 11.04.2024);
- Указ Президента РФ “О Стратегии национальной безопасности Российской Федерации” от 02.07.2021 N 400;
- Указ Президента РФ “Об утверждении Положения о персональных данных государственного гражданского служащего Российской Феде-рации и ведении его личного дела” от 30.05.2005 N 609 (ред. от 10.10.2024);
- Указ Президента РФ “О Стратегии развития информационного общества в РФ на 2017 — 2030 годы” от 09.05.2017 N 203.

Третья группа документов состоит из Постановлений Правительства Российской Федерации. Ее образуют:

- Постановление Правительства РФ от 22 сентября 2009 г. N 754 "Об утверждении Положения о системе межведомственного электронного документооборота" (Собрание законодательства РФ, 2009, N 39, ст. 4614; 2019, N 12, ст. 1314);
- Постановление Правительства РФ "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012 N 1119.
- Постановление Правительства РФ "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом “О персональных данных" от 21.03.2012 N 211 (ред. от 15.04.2019);
- Постановление Правительства РФ "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных" от 13.02.2019 N 146;
- Постановление Правительства РФ "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных" от 06.07.2008 N 512;

- Постановление Правительства РФ "О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию" от 04.03.2010 N 125 (ред. от 10.02.2014);
- Постановление Правительства РФ "О лицензировании деятельности по технической защите конфиденциальной информации" от 03.02.2012 N 79 (ред. от 03.02.2023).

Четвертая группа документов представлена Решениями Государственной технической комиссии (Гостехкомиссии) при Президенте Российской Федерации – основного исполнительного органа в области защиты информации. В эту группу входят:

- Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 04.06.1999 № 114;
- Руководящий документ Гостехкомиссии России «Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам» Гостехкомиссия России, от 01.01.1998 г.;
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № 187.

В пятой группе представлены следующие Руководящие и Нормативно-методические документы Гостехкомиссии Российской Федерации:

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 14.02.2008;
- Сборник нормативно-методических документов ФСТЭК России «Базовая модель и методика определения угроз безопасности информации в ключевых системах информационной инфраструктуры» в составе: Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждена Заместителем директора ФСТЭК России 18.05.2008; Методика определения актуальных угроз безопасности информации в ключевых системах

информационной инфраструктуры утверждена Заместителем директора ФСТЭК России 18.05.2008;

- Информационное сообщение ФСТЭК России от 20.11.2012 № 240/22/4669 Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных.

Шестая группа документов образована Государственными Стандартами Российской Федерации:

- ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». Дата введения 01.09.2014;
- ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». Дата введения 30 июня 2000 г. 175-ст.;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создании автоматизированных систем». Дата введения 01.01.1990;
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». Дата введения 01.01.1993;
- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации». Дата введения 01.01.1996.

4.3. Правовое регулирование в области информационной безопасности

Преступления в области компьютерной информации впервые включены в Уголовный Кодекс Российской Федерации, вступивший в действие 1 января 1997 года. Поэтому необходимо определить основные понятия, используемые в данном разделе.

Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, – наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет.

Примечания.

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации

средств защиты компьютерной информации, – наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, – наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их

наступления, – наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

4.4. Сущность и организация криптографической защиты информации

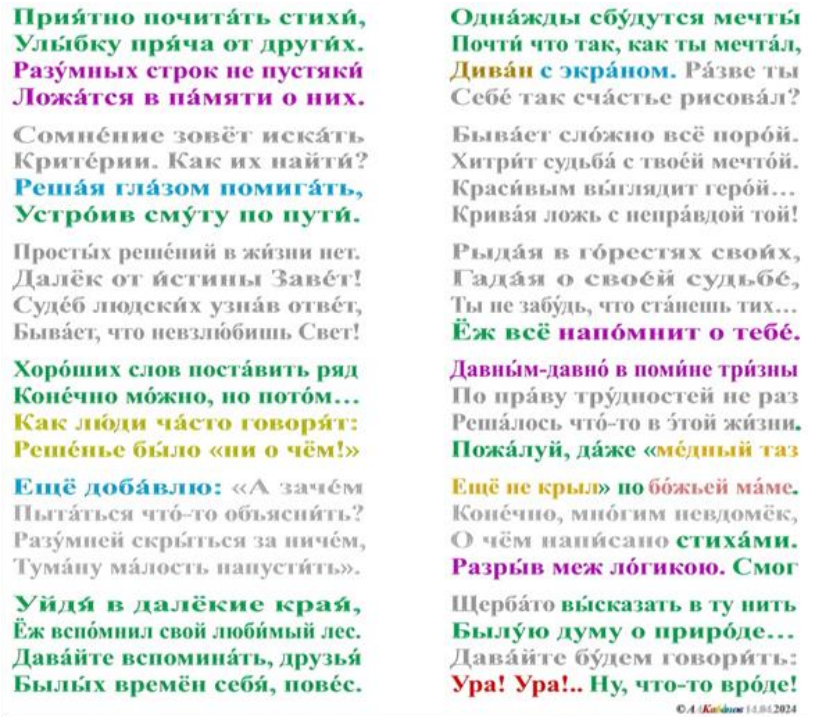
Проблемой защиты информации при ее передаче между абонентами люди занимаются на протяжении всей своей истории. Человечеством изобретено множество способов, позволяющих в той или иной мере скрыть смысл передаваемых сообщений от противника. На практике выработалось несколько групп методов защиты секретных посланий. Назовем некоторые из них, применяющиеся так же давно, как и криптографические.

Первым способом является физическая защита материального носителя информации от противника. В качестве носителя данных может выступать бумага, компьютерный носитель. Для реализации этого способа необходим надежный канал связи, недоступный для перехвата.

Второй способ защиты информации, известный с давних времен –*стеганографическая защита* информации. Этот способ защиты основан на попытке скрыть от противника сам факт наличия интересующей его информации. При стеганографическом методе защиты от противника прячут физический носитель данных или маскируют секретные сообщения среди открытой, несекретной информации. К таким способам относят, например, «запрятывание» микрофотографии с тайной информацией в несекретном месте: под маркой на почтовом конверте, под обложкой книги и т.д.

Одним из примеров применения стеганографии можно назвать стихотворение одного из авторов данного пособия. Стихотворение называется «Закавыка» https://stihi.ru/2024/04/15/96

Портал «Стихи.ру» предназначен для неограниченного круга лиц. Ежедневное количество посетителей – 200000. На это стихотворение примерно за пол года написано 5 рецензий, и только в одной из них есть догадка: «…Подача странная, вроде слова знакомые, а читается, как шифровка Алекса Юстасу….». А ведь это – криптографически зашифрованный «акростих», в котором первые буквы каждой строки имеют некоторое содержание:



Приятно почитать стихи,
Улыбку прячa от другиx.
Разумных строк не пустяки
Ложатся в памяти о них.

Сомнение зовёт искать
Критерии. Как их найти?
Решая глазом помигать,
Устроив смуту по пути.

Простых решений в жизни нет.
Далёк от истины Завет!
Судеб людскиx узнав ответ,
Бывает, что невзлюбишь Свет!

Хороших слов поставить ряд
Конечно можно, но потом…
Как люди часто говорят:
Решенье было «ни о чём!»

Ещё добавлю: «А зачем
Пытаться что-то объяснить?
Разумней скрыться за ничем,
Туману малость напустить».

Уйдя в далёкие края,
Ёж вспомнил свой любимый лес.
Давайте вспоминать, друзья
Былых времён себя, повес.

Однажды сбудутся мечты
Почти что так, как ты мечтал,
Диван с экраном. Разве ты
Себе так счастье рисовал?

Бывает сложно всё порой.
Хитрит судьба с твоей мечтой.
Красивым выглядит герой…
Кривая ложь с неправдой той!

Рыдая в горестях своиx,
Гадая о своей судьбе,
Ты не забудь, что станешь тиx…
Ёж всё напомнит о тебе.

Давным-давно в помине тризны
По праву трудностей не раз
Решалось что-то в этой жизни.
Пожалуй, даже «медный таз

Ещё не крыл» по божьей маме.
Конечно, многим невдомёк,
О чём написано стихами.
Разрыв меж логикою. Смог

Щербато высказать в ту нить
Былую думу о природе…
Давайте будем говорить:
Ура! Ура!.. Ну, что-то вроде!

© А. Кайдаков 14.04.2024

«ПУРЛСКРУПДСБХЛЛРЕПРТУЁДБОПДСБХККРГТЁДПРПЕКОРЩБДТ»
«ОТ КРИПТОГРАФИИ ДО СТЕГАНОГРАФИИ ВСЕГО ОДИН ШАГ.»

Криптография заключается всего лишь в сдвиге каждой буквы на 1 вправо (при расшифровке – влево). Пробелы между словами заменены на букву «П», а точка – на букву «Т».

Третий способ защиты информации – наиболее надежный и распространенный в наши дни – *криптографический*. Этот метод защиты информации предполагает преобразование информации для сокрытия ее смысла от противника.

Криптография в переводе с греческого означает «тайнопись» – изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия.

В настоящее время *криптография* занимается поиском и исследованием математических методов преобразования информации.

Наряду с криптографией развивается и совершенствуется **криптоанализ** – наука о преодолении криптографической защиты

информации. Криптоаналитики исследуют возможности расшифровывания информации без знания ключей.

В настоящее время *криптография* прочно вошла в нашу жизнь. Перечислим лишь некоторые сферы применения криптографии в современном информатизированном обществе:

- Шифрование данных при передаче по открытым каналам связи (например, при совершении покупки в Интернете сведения о сделке, такие как адрес, телефон, номер кредитной карты, обычно зашифровываются в целях безопасности);
- Обслуживание банковских пластиковых карт;
- Хранение и обработка паролей пользователей в сети;
- Сдача бухгалтерских и иных отчетов через удаленные каналы связи;
- Банковское обслуживание предприятий через локальную или глобальную сеть;
- Безопасное от несанкционированного доступа хранение данных на жестком диске компьютера (в операционной системе Windows даже имеется специальный термин – шифрованная файловая система (EFS)).

Основные определения

Шифр – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

Символ – это любой знак, в том числе буква, цифра или знак препинания.

Ключ – *информация*, необходимая для шифрования и расшифрования сообщений.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

Все методы преобразования информации с целью защиты от несанкционированного доступа делятся на две большие группы: методы шифрования *с закрытым ключом* и методы шифрования *с открытым ключом*.

Шифрование с закрытым ключом (*шифрование* с секретным ключом или *симметричное шифрование*) используется человеком уже довольно долгое время. Для шифрования и расшифрования данных в этих методах используется один и тот же *ключ*, который обе стороны стараются хранить в секрете от противника.

Шифрование с открытым ключом (*асимметричное шифрование*) стало использоваться для криптографического закрытия

информации лишь во второй половине XX века. В эту группу относятся методы шифрования, в которых для шифрования и расшифрования данных используются два разных ключа. При этом один из ключей (открытый *ключ*) может передаваться *по* открытому (незащищенному) каналу связи.

Электронной (цифровой) подписью называется обычно присоединяемый к сообщению *блок данных*, полученный с использованием криптографического преобразования. *Электронная подпись* позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптографическая система защиты информации – система защиты информации, в которой используются криптографические методы для шифрования данных.

Не для всех алгоритмов шифрования перечисленные требования выполняются полностью. В частности, требование отсутствия слабых ключей (ключей, которые позволяют злоумышленнику легче вскрыть зашифрованное сообщение) не выполняется для некоторых «старых» блочных шифров. Однако все вновь разрабатываемые системы шифрования удовлетворяют перечисленным требованиям.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

- ✓ Достаточная криптостойкость (надежность закрытия данных);
- ✓ Простота процедур шифрования и расшифрования;
- ✓ Незначительная избыточность информации за счет шифрования;
- ✓ Нечувствительность к небольшим ошибкам шифрования и др.

В той или иной мере этим требованиям отвечают:

- ✓ Шифры перестановок:
- ✓ Шифры замены;
- ✓ Шифры гаммирования;
- ✓ Шифры, основанные на аналитических преобразованиях шифруемых данных.

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

*Шифрование заменой (*подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены.

Шифрование гаммированием заключается в том, что символы шифруемою текста складываются с символами некоторой случайной последовательности, именуемой гаммой шифра. Стойкость шифрования определяется в основном длиной (периодом) неповторяющейся части гаммы шифра. Поскольку с помощью ЭВМ можно генерировать практически бесконечную гамму шифра, то данный способ является одним из основных для шифрования информации в автоматизированных системах.

Шифрование аналитическим преобразованием заключается в том, что шифруемый текст преобразуется по некоторому аналитическому правилу (формуле).

1. В пятом веке до н.э. правители Спарты имели хорошо отработанную систему секретной военной связи и шифровали свои донесения с помощью **скитала**, первое криптографическое устройство, реализующее метод простых перестановок.

Шифрование заключалось в следующем. На стержень цилиндрической формы (скитала) наматывалась лента по спирали, виток к витку и на ней писалось послание вдоль стержня (Рис. 18).

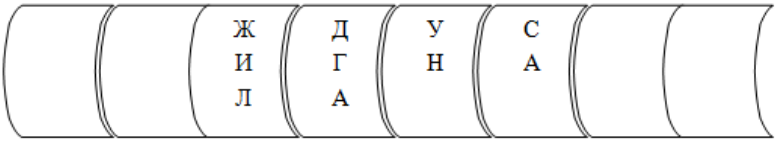


Рис. 18. Скитала.

После чего лента разматывалась и получался текст (Рис.19).

ЖИЛДГАУНСА

Рис. 19. Зашифрованный текст.

Получатель сообщения наматывал ленту на такой же стержень и расшифровывал сообщение.

2. Шифрующие таблицы

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. Наряду с традиционными применениями криптографии и политике, дипломатии и военном деле появляются и

другие задачи – защита интеллектуальной собственности от преследований инквизиции или заимствований злоумышленников. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые, в сущности, задают правила перестановки букв и сообщении.

В качестве ключа в шифрующих таблицах используются:

- ✓ Размер таблицы;
- ✓ Слово или фраза, задающие перестановку;
- ✓ Особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром Скитала. Например, сообщение:

НАСТУПАЕМ ВСЕ ВМЕСТЕ СЕДЬМОГО В ПОЛНОЧЬ

записывается в таблицу поочередно по столбцам. Результат заполнения табл. из 5 строк и 7 столбцов показан на рис. 20.

Н	П	С	С	Д	О	Н
А	А	Е	Т	Ь	В	О
С	Е	В	Е	М	П	Ч
Т	М	М	С	О	О	Ь
У	В	Е	Е	Г	Л	*

Рис. 20. Заполнение таблицы из 5 строк и 7 столбцов.

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение:

НПССДОН ААЕТЬВО СЕВЕМПЧ ТММСООЬ УВЕЕГЛ*

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи не смыслового текста. При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово: ВСТРЕЧА, а текст сообщения возьмем из предыдущего примера. На рис. 21 показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая таблица - заполнению после перестановки.

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были пронумерованы слева направо. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого правой таблицы по строкам и записи шифр-текста группами по пять букв получим шифрованное сообщение: НПССДОН ААЕТЬВО СЕВЕМПЧ ТММСООЬ УВЕЕГЛ*

В	С	Т	Р	Е	Ч	А
2	5	6	4	3	7	1
Н	П	С	С	Д	О	Н
А	А	Е	Т	Ь	В	О
С	Е	В	Е	М	П	Ч
Т	М	М	С	О	О	Ь
У	В	Е	Е	Г	Л	*

До перестановки

А	В	Е	Р	С	Т	Ч
1	2	3	4	5	6	7
Н	Н	Д	С	П	С	О
О	А	Ь	Т	А	Е	В
Ч	С	М	Е	Е	В	П
Ь	Т	О	С	М	М	О
*	У	Г	Е	В	Е	Л

После перестановки

Рис. 21. Таблицы, заполненные ключевым словом и текстом сообщения.

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

1. В средние века для шифрования перестановкой применялись и магические квадраты. Магическими квадратами называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью магических квадратов шифртексты охраняет не только ключ, но и магическая сила. Пример магического квадрата и его заполнен сообщением: ПРИЛЕТАЮ ДЕВЯТОГО

(показан на рис. 22)

Шифртекст, получаемый при считывании содержимого второй таблицы по строкам, имеет вполне загадочный вид: ОИРТЕЕВЮДТАЯЛГОП

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	Т
Е	Е	В	Ю
Д	Т	А	Я
Л	Г	О	П

Рис. 22 Пример магического квадрата 4×4 и его заполнения сообщением ПРИЛЕТАЮ ДЕВЯТОГО.

Число магических квадратов быстро возрастает с увеличением размера квадрата Существует только один магический квадрат размером 3×3 (если не учитывать его повороты). Количество магических квадратов 4×4составляет уже 880, а количество магических квадратов 5×5- около 250000.

Магические квадраты средних и больших размеров могли служить хорошей базой для обеспечения нужд шифрования того времени, поскольку практически нереально выполнить вручную перебор всех вариантов для такою шифра.

4.5 Сокращения

АС	Автоматизированные системы
НСД	Несанкционированный доступ
РД	Руководящий документ
СЗИ	Система защиты информации
СЗИ НСД	Система защиты информации от несанкционированного доступа

4.6. Примеры решения практических задач

Задание 1.

Зашифровать фразы с использованием шифрующей таблицы методом простой перестановки. Размер таблицы подобрать самостоятельно.

«Криптографическая стойкость»

«Системы управления базой данных»

Задание 2.

Выполнить шифрование методом одиночной перестановки по ключу.

А. Фраза: «Основные понятия баз данных». Ключ: «График».

Таблицу составить самостоятельно.

Б. Фраза: «Средства для работы с векторной графикой».

Подобрать ключ и таблицу самостоятельно.

Задание 3.

А. Зашифровать фразу: «Защита информации» с помощью магического квадрата 4x4.

Б. Зашифровать слово «Испытание» с помощью магического квадрата 3x3.

В. Зашифровать фразу: «Внутренняя схема базы данных» с помощью магического квадрата 5x5. Компьютерные системы

2	7	6
9	5	1
4	3	8

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

11	9	22	5	18
19	12	10	23	1
2	20	13	6	24
25	3	16	14	7
8	21	4	17	15

Рис. 24. Примеры магических квадратов на 9, 16 и 25.

4.7. Задачи для самостоятельного решения по теме «Защита информации при применении современных информационных технологий»

Задание 1.

Используя ключ, расшифровать послание:

А. Шифротекст имеет вид:
ИРОНФМЯИАЦАНЕУТТКИИФА*ИЦИ
Ключевое слово АРХИВ

Б. Шифротекст имеет вид:
БАИТПРЕССЬЬНЗНТКЮЫООЕОТХПСММЕС
Ключевое слово: ДОСТУП

Задание 2.

Выполнить дешифрование фраз, зашифрованных с использованием шифрующей таблицы методом простой перестановки.

А. «ДОНЬАКФАОВООБИОЦСЕСБОИРИТРТРТНМИ»
Размер таблицы 4х8 (4 столбца и 8 строк)

Б. «ОИОМРЯЩНАРЗНЕИПИФЦГАНРЯОТОИАЦЫОТЗЕРИНИЕПИАИМ.»
Размер таблицы 5х9

Задание 3.

А. Зашифровать фразу: «Сертификат защиты» с помощью магического квадрата 4х4.

Б. Зашифровать слово «Тип записи» с помощью магического квадрата 3х3.

В. Зашифровать фразу: «Предписание на эксплуатацию» с помощью магического квадрата 5х5.

4.8. Тесты для самоконтроля знаний по теме «Защита информации при применении современных информационных технологий»

1. Какие средства применяются при технической защите информации

1) Технические;
2) Программные;
3) Программно-аппаратные;
4) Криптографические;
5) Нет правильного ответа.

2. Что такое сжатие информации?

1) Процесс преобразования хранящейся в файле, к виду, при котором уменьшается избыточность в ее представлении и соответственно требуется меньший объем памяти;
2) Хранения информации;
3) Хэширование информации;
4) Стенографическое внедрении защищаемой информации;
5) Криптографическое преобразование информации.

3. Назовите все основные подсистемы, которые реализуются в рамках системы защиты информации от несанкционированного доступа?

1) Управления доступом;
2) Регистрации и учета;
3) Криптографическая;
4) Обеспечения целостности;
5) Нет правильного ответа.

4.Какие элементы включены в официальное понятие информационные технологии?

1) Актуальные угрозы информации;
2) Сбор, хранение, уничтожение;
3) Методы поиска, сбора, хранения, обработки, предоставления, распространения информации, способы осуществления таких процессов и методов;
4) Процессы;
5) Все ответы верные.

5. Показатели качества доступа в Интернет:
1) Время входа в систему;
2) Достигнутая скорость передачи данных;
3) Коэффициент неуспешных передач;
4) Коэффициент успешных входов в систему;
5) Задержка (время передачи в одну сторону).

6. Оператор информационной системы – это:
1) Физическое лицо, осуществляющие деятельность по эксплуатации информационной системы;
2) Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;
3) Юридическое лицо, осуществляющие обработку информации, содержащейся в базах данных информационной системы;
4) Федеральный орган исполнительной власти или гражданин;
5) Все ответ верные.

7. Что в переводе с греческого языка означает слово «криптография»?
1) Преобразование;
2) Расшифровка;
3) Шифр;
4) Тайнопись;
5) Все ответы верны.

8. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
1) Шифр Маркова;
2) Шифр Цезаря;
3) Шифр Энигма;
4) Шифр Бэбиджа;
5) Шифр Скитала.

9. Когда в криптографии стало использоваться асимметричное шифрование?

1) В первой половине XIX;
2) Во второй половине XIX;
3) В первой половине XX;
4) Во второй половине XX;
5) Использовался еще до н.э.

10. Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты?

1) Алгоритм;
2) Шифр;
3) Ключ;
4) Протокол;
5) Метод;

11. Что в криптографии называют открытым текстом?

1) Исходное сообщение (сообщение до шифрования);
2) Открытый ключ шифрования;
3) Сообщение, получение после преобразования с использованием любого шифра;
4) Электронную цифровую подпись;
5) Закрытый ключ шифрования.

12. Гарантирование невозможности несанкционированного изменения информации – это:

1) Обеспечение конфиденциальности;
2) Обеспечение целостности;
3) Обеспечение аутентификации;
4) Обеспечение шифрования;
5) Все ответы верные.

13. Под конфиденциальностью понимают (выберите продолжение)

1) Решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, имеющих права доступа к ней;
2) Решение проблемы защиты информации от ее изменения со стороны лиц, не имеющих права доступа к ней;
3) Решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней;
4) Решение проблемы запуска программ со стороны лиц, не имеющих права доступа к ним;
5) Разрешение пользоваться информацией только одному лицу.

14. Под целостностью понимают (выберите продолжение)

1) Гарантирование невозможности несанкционированного изменения объема информации;
2) Гарантирование невозможности несанкционированного изменения информации;
3) Гарантирование невозможности несанкционированного изменения порядка следования информации;
4) Гарантирование невозможности несанкционированного изменения переносов в текстовой информации;
5) Нет правильного ответа.

15. Выберите правильное определение термина «криптография»

1) Криптография – это наука о преодолении криптографической защиты информации;
2) Криптография – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи;
3) Криптография изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия;
4) Криптография изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации;
5) Все ответы верные.

16. Выберите правильное определение термина «криптоанализ»

1) Криптоанализ – это наука о преодолении криптографической защиты информации;
2) Криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи;
3) Криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия;
4) Криптоанализ изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации;
5) Все ответы верные.

17. Какая наука разрабатывает методы «вскрытия» шифров?

1) Криптография;
2) Криптоанализ;
3) Теория чисел;
4) Тайнопись;
5) Линейная алгебра.

18. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования:

1) 1;
2) 2;
3) 3;
4) 4;
5) 5.

19. Сколько ключей используется в системах с открытым ключом?

1) 1;
2) 2;
3) 3;
4) 4;
5) 5.

20. Сколько существует способов гаммирования?

1) 1;
2) 2;
3) 3;
4) 4;
5) 5.

21. Деяния, предусмотренные частями первой или второй ст. 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения?

1) До 100 тыс. рублей;
2) До 300 тыс. рублей;
3) До 200 тыс. рублей;
4) До 500 тыс. рублей;
5) До 400 тыс. рублей.

22. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации наказывается ограничение свободы?

1) До 1 года;
2) До 2-х лет;
3) До 3-х лет;
4) До 4-х лет;
5) До 5-ти лет.

23. Деяние, предусмотренное частью первой ст.274 УК РФ, если оно повлекло тяжкие последствия или создало угрозу их наступления наказывается принудительными работами на срок?

1) До 1 года;
2) До 2-х лет;
3) До 3-х лет;
4) До 4-х лет;
5) До 5-ти лет.

24. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, наказывается исправительными работами на срок?

1) До 1 года;
2) До 18 месяцев;
3) До 2-х лет;
4) До 6 месяцев;
5) До 3-х лет.

25. Деяния, предусмотренные частями первой, второй или третьей ст. 272 УК РФ, если они повлекли тяжкие последствия или создали угрозу их наступления

1) Наказываются лишением свободы на срок до двух лет;
2) Наказываются лишением свободы на срок до трех лет;
3) Наказываются лишением свободы на срок до пяти лет;
4) Наказываются лишением свободы на срок до четырех лет;
5) Наказываются лишением свободы на срок до семи лет.

5. ОТВЕТЫ НА КОНТРОЛЬНЫЕ ЗАДАНИЯ

5.1 Ответы на тесты для самоконтроля знаний в объеме программы средней школы

Основные термины, определения и классификация вычислительных сетей

№ теста	1	2	3	4	5	6	7	8	9	10	11	12
№ ответа	1	2	1,2,4	3	1	1	2	4	2	1	3	5

Топология построения локальных вычислительных сетей.

№ теста	1	2	3	4	5	6	7	8	9	10	11	12
№ ответа	2	1,2,4	2	1	2	2	3	4	5	3	4	1, 3-4

Понятийный аппарат информационной безопасности

№ теста	1	2	3	4	5	6	7	8	9	10	11	12
№ ответа	1-3	1	2	4	1	2	5	4	5	1	1	2

Методы и средства защиты информации

№ теста	1	2	3	4	5	6	7	8	9	10	11	12
№ ответа	2	1	3	2	4	5	5	3	1-5	3	1	4

5.2. Ответы на примеры решения практических задач по теме «Защита информации при применении современных информационных технологий»

Задание 1.

Зашифровать фразы с использованием шифрующей таблицы методом простой перестановки. Размер таблицы подобрать самостоятельно.

А. «Криптографическая стойкость»

к	р	и	п	т	о	г
р	а	ф	и	ч	е	с
к	а	я	с	т	о	й
к	о	с	т	ь	*	*

КРККРААОИФЯСПИСТТЧТЬОЕО*ГСЙ*

Б. «Системы управления базой данных»

с	е	п	л	я	о	н
и	м	р	е	б	й	н
с	ы	а	н	а	д	ы
т	у	в	и	з	а	х

СЕПЛЯОНИМРЕБЙНСЫАНАДЫТУВИЗАХ

Задание 2.

Выполнить шифрование методом одиночной перестановки по ключу.

А. Фраза: «Основные понятия баз данных». Ключ: «График».

Таблицу составить самостоятельно.

Г	**Р**	**А**	**Ф**	**И**	**К**
2	***5***	***1***	***6***	***3***	***4***
о	в	п	т	а	н
с	н	о	и	з	н
н	ы	н	я	д	ы
о	е	я	б	а	х

1.	**2.**	**3.**	**4.**	**5.**	**6.**
А	***Г***	***И***	***К***	***Р***	***Ф***
п	о	а	н	в	т
о	с	з	н	н	и
н	н	д	ы	ы	я
я	о	а	х	е	б

ПОАНВТОСЗННИННДЫЫЯЯОАХЕБ

Б. Фраза: «Средства для работы с векторной графикой».

Подобрать ключ и таблицу самостоятельно.

Л	**О**	**Г**	**И**	**Н**
3	***5***	***1***	***2***	***4***
с	а	о	т	р
р	д	т	о	а
е	л	ы	р	ф
д	я	с	н	и
с	р	в	о	к
т	а	е	й	о
в	б	к	г	й

1	**2**	**3**	**4**	**5**
Г	***И***	***Л***	***Н***	***О***
о	т	с	р	а
т	о	р	а	д
ы	р	е	ф	л
с	н	д	и	я
в	о	с	к	р
е	й	т	о	а
к	г	в	й	б

ОТСРАТОРАДЫРЕФЛСНДИЯВОСКРЕЙТОАКГВЙБ

Задание 3.

А. Зашифровать фразу: «Защита информации» с помощью магического квадрата 4х4.

И	Щ	А	А
Т	О	Р	Н
Ф	А	И	М
И	И	Ц	З

Б. Зашифровать слово «Испытание» с помощью магического квадрата 3х3.

С	Н	А
Е	Т	И
Ы	П	И

В. Зашифровать фразу: «Внутренняя схема базы данных» с помощью магического квадрата 5х5. Компьютерные системы

С	Я	Н	Р	З
Ы	Х	Я	Н	В
Н	Д	Е	Е	Ы
Х	У	Б	М	Н
Н	А	Т	А	А

5.3 Ответы на задачи для самостоятельного решения по теме «Защита информации при применении современных информационных технологий»

Задание 1.

Используя ключ, расшифровать послание:

А. Шифротекст имеет вид:

ИРОНФМЯИАЦАНЕУТТКИИФА*ИЦИ

Ключевое слово АРХИВ

1	2	3	4	5
А	***В***	***И***	***Р***	***Х***
И	Р	О	Н	Ф
М	Я	И	А	Ц
А	Н	Е	У	Т
Т	К	И	И	Ф
А	*	И	Ц	И

А	Р	Х	И	В
1	***4***	***5***	***3***	***2***
И	Н	Ф	О	Р
М	А	Ц	И	Я
А	У	Т	Е	Н
Т	И	Ф	И	К
А	Ц	И	И	*

ИНФОРМАЦИЯ АУТЕНТИФИКАЦИИ

Б. БАИТПРЕССЬЬНЗНТКЮЫООЕОТХПСММЕС

Ключевое слово: ДОСТУП

1	2	3	4	5	6
Д	***О***	***П***	***С***	***Т***	***У***
Б	А	И	Т	П	Р
Е	С	С	Ь	Ь	Н
З	Н	Т	К	Ю	Ы
О	О	Е	О	Т	Х
П	С	М	М	Е	С

Д	**О**	**С**	**Т**	**У**	**П**
1	***2***	***4***	***5***	***5***	***3***
Б	А	Т	П	Р	И
Е	С	Ь	Ь	Н	С
З	Н	К	Ю	Ы	Т
О	О	О	Т	Х	Е
П	С	М	Е	С	М

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Задание 2.

Выполнить дешифрование фраз, зашифрованных с использованием шифрующей таблицы методом простой перестановки.

А. «ДОНЬАКФАОВООБИОЦСЕСБОИРИТРТРТНМИ»

Размер таблицы 4х8 (4 столбца и 8 строк)

Д	О	С	Т
О	В	Е	Р
Н	О	С	Т
Ь	О	Б	Р
А	Б	О	Т
К	И	И	Н
Ф	О	Р	М
А	Ц	И	И

ДОСТОВЕРНОСТЬ ОБРАБОТКИ ИНФОРМАЦИИ

Б. «ОИОМРЯЩНАРЗНЕИПИФЦГАНРЯОТОИАЦЫОТЗЕРИНИЕПИАИМ.»

Размер таблицы 5х9

О	Р	Г	А	Н
И	З	А	Ц	И
О	Н	Н	Ы	Е
М	Е	Р	О	П
Р	И	Я	Т	И
Я	П	О	З	А
Щ	И	Т	Е	И
Н	Ф	О	Р	М
А	Ц	И	И	.

ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Задание 3.

А. Зашифровать фразу: «Сертификат защиты» с помощью магического квадрата 4х4.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Б. Зашифровать слово «Тип записи» с помощью магического квадрата 3х3.

2	7	6
9	5	1
4	3	8

В. Зашифровать фразу: «Предписание на эксплуатацию» с помощью магического квадрата 5х5.

11	9	22	5	18
19	12	10	23	1
2	20	13	6	24
25	3	16	14	7
8	21	4	17	15

5.4. Ответы на тест для самоконтроля знаний по теме «Защита информации при применении современных информационных технологий»

№ теста	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
№ ответа	1,2, 3	1	1,2, 3,4	3,4	1,2, 3, 4,5	2	4	2	4	2	11	2
№ теста	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
№ ответа	3	2	3	1	2	1	2	2	4	4	5	1
№ теста	**25**											
№ ответа	**5**											

СПИСОК ЛИТЕРАТУРЫ

1. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. — Екатеринбург: Изд-во Урал. ун-та, 2019. — 204 с. ISBN 978-5-7996-2677-8.
2. Галас, В.П. Вычислительные системы, сети и телекоммуникации: учебник. В 2 ч. Ч. 2/ Сети и телекоммуникации / В.П. Галас; Владим. гос. ун-т им. А.Г. и Н.Г. Столетовых. – Владимир: Изд-во ВлГУ, 2017. − 284 с. – ISBN 978-5-9984-0817-5 (ч. 2). – ISBN 978-5-9984-0731-4.
3. Галатенко В.А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий. – https://intuit.ru/, 2008. – 208 с.
4. Гришин В.Н. Информационные технологии в профессиональной деятельности: Учебник / В.Н. Гришин, Е.Е. Панфилова. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. – 416 с.
5. Гильфанов К.Х. Информационные сети и телекоммуникации: учебное пособие. К.Х. Гильфанов. – Казань: Казан. гос. энерг. ун-т, 2014 – 364 с.
6. Карпов А.В. Введение в криптографию: Учебное пособие. / А.В. Карпов, Р.А. Ишмуратов. – Казань: Казан. ун-т, 2024 – 128 с.
7. Максимов А.В., Матвеев А.В., Уткин О.В. Информационные технологии в техносферной безопасности. Компьютерный практикум: Учебное пособие/ Под общей ред. Э.Н. Чижикова – СПб.: Санкт-Петербургский университет ГПС МЧС России, 2019. – 175 с.
8. Метельков А.Н., Уткин О.В. Организационно-правовые и технические основы защиты конфиденциальной информации в МЧС России: учебное пособие / Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Санкт-Петербургский университет ГПС МЧС России имени Е. Н. Зиничева. – СПб.: Санкт-Петербургский ун-т ГПС МЧС России, 2022. – 215 с.: ил. – Библиогр.: с. 206-212 (79 назв.). – 500 экз. - ISBN 978-5-907724-00-6.
9. Урбанович П.П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 2. Криптографические и стенографические методы защиты информации: учеб.-метод. пособие для студ. вузов / П. П. Урбанович, Н. П. Шутько. – Минск: БГТУ, 2020 – 226 с.

ИНФОРМАЦИОННАЯ СПРАВКА

Старейшее учебное заведение пожарно-технического профиля России образовано 18 октября 1906 года, когда на основании решения Городской Думы Санкт-Петербурга были открыты Курсы пожарных техников. Наряду с подготовкой пожарных специалистов, учебному заведению вменялось в обязанность заниматься обобщением и систематизацией пожарно-технических знаний, оформлением их в отдельные учебные дисциплины. Именно здесь были созданы первые отечественные учебники, по которым обучались все пожарные специалисты страны.

В последующем учебное заведение преобразовывалось и меняло своё название 25 апреля 2022 года в соответствии с Указом Президента Российской Федерации В.В. Путина Санкт-Петербургскому университету ГПС МЧС России присвоено почётное наименование «имени Героя Российской Федерации генерала армии Е.Н. Зиничева».

Учебным заведением за вековую историю подготовлено несколько десятков тысяч специалистов, которых всегда отличали не только высокие профессиональные знания, но и беспредельная преданность профессии пожарного и верность присяге. Свидетельство тому – целый ряд сотрудников и выпускников ВУЗа, награждённых высшими наградами страны, среди них: кавалеры Георгиевского креста, четыре Героя Советского Союза и Герой России. Далеко не случаен тот факт, что среди руководящего состава пожарной охраны страны всегда было много выпускников учебного заведения.

Сегодня федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева» – современный научно-образовательный комплекс, интегрированный в российское и мировое научно-образовательное пространство. Учебный процесс осуществляется по 891 дисциплине на 28 кафедрах. Университет осуществляет подготовку по разным формам обучения: очной, заочной и заочной с применением дистанционных технологий по программам среднего, высшего образования, а также подготовку специалистов высшей квалификации, переподготовку и повышение квалификации специалистов МЧС России.

Начальник университета – генерал-лейтенант внутренней службы доктор технических наук, доцент Гавкалюк Богдан Васильевич.

Подготовка реализуется по 21 образовательной программе высшего образования, что является наибольшим количеством реализуемых программ среди образовательных организаций высшего образования МЧС России, и 83 программам дополнительного профессионального образования и профессионального обучения.

По программам специалитета в университете можно пройти обучение по таким направлениям подготовки, как: «Пожарная безопасность», «Горное дело», «Психология служебной деятельности», «Экономическая безопасность», «Правовое обеспечение национальной безопасности», «Судебная экспертиза». По программам бакалавриата – «Техносферная безопасность», «Системный анализ и управление», «Психология», «Управление персоналом», «Государственное и муниципальное управление», «Юриспруденция». По программам магистратуры – «Техносферная безопасность», «Системный анализ и управление», «Государственное и муниципальное управление», «Юриспруденция».

Широта научных интересов, высокий профессионализм, большой опыт научно-педагогической деятельности, владение современными методами научных исследований позволяют коллективу университета преумножать научный и научно-педагогический потенциал вуза, обеспечивать непрерывность и преемственность образовательного процесса.

Укомплектованность научно-педагогическим составом, имеющим учёные степени и звания, составляет более 70 %, что позволяет университету занимать лидирующие позиции среди учебных заведений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. Сегодня в университете свои знания и огромный опыт передают: 56 докторов наук, 267 кандидатов наук, 46 профессоров, 150 доцентов.

В составе университета:

– 28 кафедр;

– Институт безопасности жизнедеятельности;

– Институт заочного и дистанционного обучения;

– Институт нравственно-патриотического и эстетического развития;

– Институт профессиональной подготовки;

– Институт развития;

– Научно-исследовательский институт перспективных исследований и инновационных технологий в области безопасности жизнедеятельности;

– Дальневосточная пожарно-спасательная академия – филиал университета (ДВПСА);

– 5 факультетов: факультет инженерно-технический, факультет экономики и права, факультет подготовки кадров высшей квалификации, факультет пожарной безопасности (подразделение ДВПСА), факультет дополнительного профессионального образования (подразделение ДВПСА).

Институт безопасности жизнедеятельности осуществляет образовательную деятельность по программам высшего образования по договорам об оказании платных образовательных услуг.

Приоритетным направлением в работе Института заочного и дистанционного обучения является подготовка кадров начальствующего состава для замещения соответствующих должностей в подразделениях МЧС России. Нарастающая сложность и комплексность современных задач заметно повышают требования к организации образовательного процесса.

Сегодня университет реализует программы обучения с применением технологий дистанционного обучения.

Институт развития реализует дополнительные профессиональные программы по повышению квалификации и профессиональной переподготовке в рамках выполнения государственного заказа МЧС России для совершенствования и развития системы кадрового обеспечения, а также на договорной основе.

Научно-исследовательский институт перспективных исследований и инновационных технологий в области безопасности жизнедеятельности осуществляет: реализацию государственной научно-технической политики, изучение и решение научно-технических проблем, информационного и методического обеспечения в области пожарной безопасности. Основные направления деятельности научно-исследовательского института: организационное и научно-методическое руководство судебно-экспертными учреждениями федеральной противопожарной службы МЧС России; сертификация продукции в области пожарной безопасности; проведение испытаний и разработка научно-технической продукции в области пожарной безопасности; проведение расчётов пожарного риска и расчётов динамики пожара с использованием компьютерных программ.

Институт активно участвует в разработке новых и совершенствовании существующих инструментальных методов и технических средств исследования и экспертизы пожаров, производстве судебных пожарно-технических экспертиз и исследованиях в области экспертизы пожаров, выполнении поисковых научно-исследовательских работ прикладного характера, выполнении поисковых научно-исследовательских работ по обеспечению безопасности в Арктическом регионе и проведении сертификационных испытаний, апробировании методик по стандартам ISO, EN и резолюциям IMO.

Университет имеет представительства в городах: Выборг (Ленинградская область), Вытегра, Горячий Ключ (Краснодарский край), Мурманск, Петрозаводск, Пятигорск, Севастополь, Стрежевой, Сыктывкар, Тюмень, Уфа; представительства университета за рубежом: г. Алма-Ата (Республика Казахстан), г. Баку (Азербайджанская Республика), г. Ниш (Сербия).

На базе Санкт-Петербургского университета Государственной противопожарной службы МЧС России 1 июля 2013 года открыт Кадетский пожарно-спасательный корпус. Он осуществляет подготовку кадетов по общеобразовательным программам среднего общего образования с учётом дополнительных образовательных программ. Основные особенности деятельности корпуса – интеллектуальное, культурное, физическое и духовно-нравственное развитие кадет, их адаптация к жизни в обществе, создание основы для подготовки несовершеннолетних граждан к служению Отечеству на поприще государственной гражданской, военной, правоохранительной и муниципальной службы.

Общее количество обучающихся в университете по всем специальностям, направлениям подготовки, среднему общему образованию составляет более 7 000 человек. Ежегодный выпуск составляет более 1 100 специалистов.

В университете действует два диссертационных совета по защите диссертаций на соискание учёной степени доктора и кандидата наук по техническим и экономическим наукам. Университет издаёт 7 научных журналов, публикуются материалы ряда международных и всероссийских научных мероприятий, сборники научных трудов профессорско-преподавательского состава университета.

Издания университета соответствуют требованиям законодательства Российской Федерации и включены в электронную базу Научной электронной библиотеки для определения Российского индекса научного цитирования, а также имеют международный индекс (ISSN). Научно-аналитический журнал «Проблемы управления рисками в

техносфере» и электронный «Научно-аналитический журнал «Вестник Санкт-Петербургского университета ГПС МЧС России» включены в утверждённый решением Высшей аттестационной комиссии «Перечень рецензируемых научных журналов, в которых публикуются основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук».

Ежегодно университет проводит научно-практические конференции различного уровня: Всероссийскую научно-практическую конференцию «Сервис безопасности в России: опыт, проблемы и перспективы», Международную научно-практическую конференцию «Подготовка кадров в системе предупреждения и ликвидации последствий чрезвычайных ситуаций».

Университет ежегодно принимает участие в выставках, организованных МЧС России и другими ведомствами и организациями. Традиционно большим интересом пользуется выставочная экспозиция университета на Международном салоне средств обеспечения безопасности «Комплексная безопасность», Петербургском международном экономическом форуме, Международном форуме «Арктика: настоящее и будущее».

Международная деятельность вуза направлена на всестороннюю интеграцию университета в международное образовательное пространство. Университет, осуществляя образовательную деятельность, обладает широкой локализацией на территории Российской Федерации, государств-участников Содружества Независимых Государств и других стран.

Большой интерес к обучению в университете проявляется со стороны иностранных граждан. В университете обучаются иностранные курсанты из числа сотрудников Государственной противопожарной службы МЧС Кыргызской Республики и Комитета по чрезвычайным ситуациям МВД Республики Казахстан. Только в период с 2016 по 2021 год в университете прошли обучение по программам дополнительного профессионального образования 712 иностранных граждан, завершили обучение по программам высшего образования 468 иностранных граждан.

В соответствии с двусторонними соглашениями университет осуществляет обучение по программам повышения квалификации. Регулярно проходят обучение в университете специалисты Российско-сербского гуманитарного центра, Российско-армянского центра гуманитарного реагирования, Международной организации гражданской обороны.

В университете имеются возможности для повышения уровня знания английского языка. Организовано обучение по программе дополнительного профессионального образования «Переводчик в сфере профессиональной коммуникации» студентов, курсантов, адъюнктов и сотрудников.

В университете большое внимание уделяется спорту. Команды, состоящие из преподавателей, курсантов и слушателей – постоянные участники различных спортивных турниров, проводимых как в России, так и за рубежом. Слушатели и курсанты университета являются членами сборных команд МЧС России по различным видам спорта.

Деятельность команды университета по пожарно-спасательному спорту (ПСС) включает в себя участие в чемпионатах России среди ВУЗов (зимний и летний), в зональных соревнованиях и чемпионате России, а также проведение бесед и консультаций, оказание практической помощи юным пожарным, кадетам и спасателям при проведении тренировок по ПСС.

В университете создан спортивный клуб «Невские львы», в состав которого входят команды по 18 видам спорта. В составе сборных команд университета – чемпионы и призёры мировых первенств и международных турниров.

Курсанты и слушатели имеют прекрасные возможности для повышения своего культурного уровня, развития творческих способностей в созданном в университете Институте нравственно-патриотического и эстетического развития. Творческий коллектив университета принимает активное участие в ведомственных, городских и университетских мероприятиях, направленных на эстетическое и патриотическое воспитание молодёжи, а также занимает призовые места в конкурсах, проводимых на уровне университета, города и МЧС России. На каждом курсе организована работа по созданию и развитию творческих объединений по различным направлениям: студия вокала, студия танцев, клуб весёлых и находчивых. Для курсантов и студентов действует студия ораторского искусства, команда технического обеспечения, духовой оркестр. К 75-летию со Дня Победы в Великой Отечественной войне и 30-летию МЧС России на территории учебного заведения был открыт музей истории Санкт-Петербургского университета ГПС МЧС России, в котором обучающиеся, сотрудники, гости университета могут познакомиться со всеми этапами становления учебного заведения – от курсов пожарных техников до высшего учебного заведения.

В федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский университет

Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева» созданы все условия для подготовки высококвалифицированных специалистов МЧС России.

Антошина Татьяна Николаевна, кандидат педагогических наук;
Воронцова Анна Анатольевна, кандидат физико-математических наук;
Кабанов Андрей Александрович кандидат юридических наук, доцент.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Учебное пособие для самостоятельной работы и самоконтроля знаний обучающихся

ISBN 978-5-907724-34-1

Служебное издание
Печатается в авторской редакции
Компьютерная верстка: А.А. Кабанов

Подписано в печать 09.12.2024 Заказ № 78 Формат 60×84 1/16
Печать цифровая Объем 6,25 п.л. Тираж 100 экз.

Отпечатано в Санкт-Петербургском университете ГПС МЧС России
196105, Санкт-Петербург, Московский проспект, д. 149