ВВЕДЕНИЕ

Учебно-методическое пособие разработано для студентов, проходящих обучение по программам подготовки бакалавров по направлениям «Менеджмент» (38.03.02) и «Бизнес-информатика» (38.03.05) в соответствии с учебной программой по курсу «Методы обеспечения непрерывности бизнеса». Учебный материал предназначен для развития навыков использования эффективных технологий в решении задач создания, управления и модернизации систем безопасности на современных предприятиях. Пособие содержит методические указания по выполнению десяти лабораторных работ в компьютерных классах и полностью учитывает особенности учебно-лабораторной и программно-аппаратной базы факультета цифровой экономики, управления и бизнес-информатики СПбГУТ.

По результатам выполнения приведённых в пособии заданий каждый студент составляет индивидуальный отчёт в формате MS Office, содержащий:

- Титульный лист с указанием названия работы, номера группы, фамилии, имени и отчества автора.
- Результаты в виде таблиц, расчётов, скриншотов или приложений.
- Выводы
- Список использованной литературы

1. СТАНДАРТЫ СИСТЕМ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА

Цель работы.

Целью работы является знакомство с основными стандартами в области систем обеспечения непрерывности бизнеса.

Общие сведения

К наиболее значимым стандартам в области систем обеспечения непрерывности бизнеса можно отнести следующие действующие ГОСТы:

1. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования.
2. ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство.
3. ГОСТ Р 53647.2-2009 Менеджмент непрерывности бизнеса. Часть 2. Требования.
4. ГОСТ Р 53647.4-2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности.
5. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
6. ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.

Все стандарты касаются предпринимаемых в организациях мер для защиты от инцидентов, снижения вероятности их реализации, подготовки ответных действий и восстановления после инцидентов при их возникновении. Общая модель функционирования направленных на это систем базируется на принципе «Планирование - Выполнение - Проверка – Действие».

Требования стандартов должны быть интегрированы в систему менеджмента непрерывности бизнеса организации и применяться наряду с нормативными правовыми актами Российской Федерации и обязательными процедурами в области обеспечения безопасности.

Задание

Используя ГОСТ Р ИСО 22301-2014 «Системы менеджмента непрерывности бизнеса. Общие требования», найти и занести в таблицу 1 определения указанных терминов.

Таблица 1. Термины и определения ГОСТ Р ИСО 22301-2014

№	Термин	Статья ГОСТа	Определение
1	непрерывность бизнеса		
2	менеджмент непрерывности бизнеса		
3	программа менеджмента непрерывности бизнеса		
4	жизненный цикл менеджмента непрерывности бизнеса		
5	система менеджмента непрерывности бизнеса		
6	план обеспечения непрерывности бизнеса		
7	инцидент		
8	план управления инцидентом		
9	критические виды деятельности		
10	устойчивость		
11	риск		
12	менеджмент риска		

Рекомендации

Полный текст ГОСТа можно найти в сети Интернет, набрав в поисковой строке браузера его имя

2. ИНТЕРНЕТ-СЕРВИСЫ ПРОВЕРКИ ЗАЩИЩЁННОСТИ ПОРТОВ ТЕРМИНАЛЬНЫХ УСТРОЙСТВ

Цель работы.

Целью работы является изучение возможностей публичных Интернет-сервисов проверки защищённости терминальных устройств.

Общие сведения

Большинство угроз для подключённых к компьютерной сети терминальных устройств связано с несанкционированным взаимодействием через открытые порты. Термин «открытый порт» означает, что после получения пакета с запросом на соединение по этому порту устройство отвечает пакетом подтверждения связи и может начаться сеанс обмена информацией для работы приложения или какой-либо из служб операционной системы.

Весь пул из 65 536 (2^{16}) номеров портов условно разделён на три части – системные порты, зарегистрированные и динамические.

Системные порты с номерами от 0 до 1023 (2^{10}-1) используются системными процессами для предоставления различных сетевых услуг. Например, 80 порт для протокола HTTP, 23 – для Telnet и т.д. Это позволяет в адресе ресурса не указывать номер порта по умолчанию.

Зарегистрированные порты с номерами от 1024 (2^{10}) до 49151 ($2^{14} + 2^{15} - 1$) по запросам организаций назначаются IANA (Internet Assigned Numbers Authority) для конкретных сетевых сервисов. Например, порт 1512 зарезервирован за службой WINS (Microsoft Windows Internet Name Service), порт 3689 – для протокола DAAP (Digital Audio Access Protocol), используемого в сервисах iTunes и AirPlay компании Apple, и т.д.

Динамические порты с номерами от 49152 до 65535 ($2^{16} - 1$) не регистрируются в IANA и могут по необходимости автоматически назначаться на время сеанса после установления соединения.

Для устранения потенциального несанкционированного воздействия на терминальное оборудование необходимо оставлять открытыми только порты, которые используются известными владельцу терминала и установленными им приложениями и службами операционной системы. Закрытие или открытие портов осуществляется настройкой межсетевого экрана (Firewall).

Существует большое количество как коммерческих, так и общедоступных программ для сканирования и анализа портов. В задании предполагается рассмотреть только публичные Интернет-сервисы.

Задание

1. Осуществить проверку безопасности компьютера (ноутбука, планшета, смартфона) с помощью сервиса «Безопасность вашего компьютера» на портале https://2ip.ru/. Результаты проверки зафиксировать скриншотом.
2. В сети Интернет найти ещё два аналогичных публичных сервиса. Зафиксировать результаты производимой ими проверки портов.

3. Сравнить результаты работы сервисов и сделать выводы.

Рекомендации

1. Сервис размещён по адресу https://2ip.ru/port-scaner/
2. Для поиска сервисов можно использовать запрос в браузере «сканировать порты онлайн».
3. Сравнение результатов работы сервисов произвести с помощью таблицы.

Таблица. Результаты сканирования портов.

Сервис	Количество сканированных портов	Время сканирования	Найденные угрозы
https://2ip.ru/port-scaner/			

3. ИНТЕРНЕТ-СЕРВИСЫ ПРОВЕРКИ АДРЕСОВ ЭЛЕКТРОННОЙ ПОЧТЫ

Цель работы.

Целью работы является проверка адресов электронной почты с помощью публичных Интернет-сервисов.

Общие сведения

Обмен сообщениями по электронной почте является неотъемлемой частью деловой активности любого современного предприятия. В тоже время, вирусные атаки через почтовые отправления стали повседневной действительностью. В сложившихся условиях сервисы проверки почтовых адресов могут оказаться весьма полезными для обеспечения непрерывности любого бизнеса.

Задание

1. Осуществить проверку трёх существующих адресов электронной почты с помощью сервиса «Проверка существования email» на портале https://2ip.ru/. Найти и проверить несуществующий адрес. Результаты проверки зафиксировать скриншотом.
2. В сети Интернет найти ещё два публичных сервиса проверки адреса электронной почты и получить результаты их работы на адресах из предыдущего пункта задания. Зафиксировать полученные сообщения.
3. Сравнить работу сервисов и сделать выводы.

Рекомендации

1. Сервис размещён по адресу https://2ip.ru/mail-checker/. Несуществующий адрес может быть получен из существующего заменой, добавлением или удалением символа(ов).
2. Для поиска сервисов можно использовать запрос в браузере «проверка email».
3. Сравнение результатов работы сервисов произвести с помощью таблицы.

Таблица. Результаты проверки.

Сервис	Проверка существования	Дополнительная информация
https://2ip.ru/mail-checker/		

Кроме самого факта существования адреса электронной почты некоторые сервисы позволяют получить такую дополнительную информацию как наличие и доступность альтернативных почтовых серверов, их приоритет и др.

4. ИНТЕРНЕТ-СЕРВИСЫ ПРОВЕРКИ ДОСТУПНОСТИ САЙТОВ

Цель работы.

Целью работы является проверка доступности сайтов средствами публичных Интернет-сервисов.

Общие сведения

Одним из наиболее популярных видов атак на организацию является ощутимое замедление или полное блокирование доступа к её Интернет-сайту (атака типа «отказ от обслуживания», DoS или DDoS-атака). Кроме действий злоумышленников близкими по результату к этим атакам может оказаться техническое состояние инфраструктуры Интернета на отдельных территориях. Особенно это важно, если на этих территориях находятся действующие или потенциальные клиенты и, следовательно, диагностика доступности сайта организации является неотъемлемой частью мер по обеспечению непрерывности обслуживания существующих и привлечению новых клиентов.

Задание

1. Осуществить проверку доступности сайта СПбГУТ (sut.ru) с помощью сервиса «Доступность сайта» на портале https://2ip.ru/. Результаты проверки зафиксировать скриншотом.
2. С помощью указанного в предыдущем пункте задания сервиса проверить доступность сайта факультета ЦЭУБИ (fem-sut.spb.ru). Зафиксировать результат.
3. Аналогичным образом проверить сайт yandex.ru
4. Сравнить результаты и сделать выводы.

Рекомендации

1-3. Сервис размещён по адресу https://2ip.ru/site-availability/.

4. Сравнение результатов произвести с помощью таблицы.

Таблица. Результаты проверки.

Адрес сайта	Время ответа (мс)				
	Россия	Германия	Нидерланды	Великобритания	США
sut.ru					
fem-sut.spb.ru					
yandex.ru					

5. УТИЛИТЫ ДЛЯ ОПРЕДЕЛЕНИЯ IP АДРЕСОВ

Цель работы.

Целью работы является определение IP адресов ресурсов Интернета по их символьным именам средствами штатных утилит MS Windows.

Общие сведения

Процедура разрешения имён подразумевает определение IP адреса ресурса по его символьному обозначению и наоборот. Специально для решения этой задачи создана сеть серверов DNS (Domain Name System). В операционной системе Windows существует утилита nslookup, представляющая собой клиента службы DNS с полным функционалом. Для решения задачи нахождения только IP адреса по символьному имени можно воспользоваться командами проверки обмена пакетами ping, tracert и pathping. Эти команды работоспособны и для ресурсов с именами на кириллице.

Все перечисленные инструменты встроены в операционные системы MS Windows всех версий и запускаются в DOS-сессии (Командная строка). Запуск командной строки производится инструкцией cmd в окне поиска Wimdows.

Задание

Найти и IP адреса следующих ресурсов:

1. www.rt.ru
2. www.sut.ru
3. www.sut.org
4. www.fem-sut.spb.ru
5. www.yandex.ru
6. www.google.com
7. большой.рф
8. малый.рф

Полученные значения занести в таблицу 1 и сделать выводы.

Рекомендации

Для определения IP адресов необходимо в командной строке набрать используемую команду, пробел и имя ресурса. Команды ping, tracert и pathping выводят искомый адрес в первой строке результатов и прервать дальнейшее выполнение можно одновременным нажатием клавиш Ctrl и C.

Таблица 1. Результаты определения IP адресов.

Имя ресурса	nslookup	ping	tracert	pathping
www.rt.ru				
www.sut.ru				
www.sut.org				
www.fem-sut.spb.ru				
www.yandex.ru				
www.google.com				
большой.рф				
малый.рф				

6. ИНСТРУМЕНТ NSLOOKUP ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ДОМЕНАХ

Цель работы.

Целью работы является получение информации о доменах утилитой nslookup в среде MS Windows.

Общие сведения

При регистрации в системе DNS символьного имени ресурса (домена) записывается много полезной информации. Например, в DNS фиксируется имена почтовых серверов, имена входящих в зону ресурсов и т.д. Эта и другая информация может быть получена с помощью штатной утилиты nslookup.

В настройках DNS имеется возможность закрыть неавторизованный доступ к полной информации о домене, оставляя только то, что необходимо для корректного функционирования ресурса. В частности, для обеспечения требований безопасности блокируется вывод имён ресурсов при неавторизованный запросах.

Задание

С помощью утилиты nslookup для доменов:

1. www.rt.ru
2. www.sut.ru
3. www.sut.org
4. www.fem-sut.spb.ru
5. www.yandex.ru
6. www.google.com

найти имена входящих в зону ресурсов и почтовых серверов.

Полученные значения занести в таблицу 1 и сделать выводы.

Рекомендации

Для вывода имён входящих в зону ресурсов необходимо в командной строке вызвать nslookup без параметров. После запуска утилиты ввести команду ls, пробел и имя домена. Наиболее вероятным результатом будет отказ от передачи зоны домена.

Для получения имён почтовых серверов следует установить тип записи MX (почтовый сервер) путём ввода строки SET TYPE=MX. Задав имя домена, можно получить имя почтового сервера(ов). После завершения исследования выход из nslookup производится командой exit.

Таблица 1. Результаты утилиты nslookup.

Имя домена	Список ресурсов	Почтовые серверы
www.rt.ru		
www.sut.ru		
www.sut.org		
www.fem-sut.spb.ru		
www.yandex.ru		
www.google.com		

7. ИНТЕРНЕТ-СЕРВИСЫ WHOIS

Цель работы.

Целью работы является поиск информации о ресурсах с помощью публичных Интернет-сервисов Whois.

Общие сведения

Регистрация имён ресурсов в сети Интернет производится на коммерческой основе на ограниченное время. В компаниях, осуществляющих эту деятельность, хранится информация, которая может оказаться весьма полезной для анализа рисков взаимодействия с существующими и будущими клиентами или партнёрами.

Доступ к информации регистраторов доменов может быть получен с помощью Интернет-сервисов Whois. Примерами таких сервисов могут служить:

https://www.reg.ru/whois/ ООО «Регистратор доменных имён РЕГ.РУ»

https://www.nic.ru/whois/ АО «Региональный Сетевой Информационный Центр» (RU-CENTER)

https://2ip.ru/whois/ Barzmann Internet Solution GmbH (2ip.ru project)

Помимо текущей информации о ресурсе на некоторых сервисах можно сделать заказ на получение истории имени, списка всех владельцев домена, истории хостинга, реестра имён доменов с одинаковым IP адресом, перечня имён ресурсов в зоне домена и т.д.

Задание

Для доменов sut.ru, fem-sut.spb.ru и google.com с помощью перечисленных выше сервисов получить следующую информацию:

1. имя владельца, организации или администратора домена (Владелец)
2. контактные данные администратора (Контакт)
3. дата регистрации (Дата)
4. дата окончания поддержки (Конец)

Результаты занести в таблицы, сравнить работу сервисов и сделать выводы.

Рекомендации

Результаты работы сервисов занести в Таблицы 1-4.

Таблица 1. Результаты определения Владельца домена.

Домен	Сервис		
	www.reg.ru/whois/	www.nic.ru/whois	2ip.ru/whois
sut.ru			
fem-sut.spb.ru			
google.com			

Таблица 2. Результаты определения Контакта домена.

Домен	Сервис		
	www.reg.ru/whois/	www.nic.ru/whois	2ip.ru/whois
sut.ru			
fem-sut.spb.ru			
google.com			

Таблица 3. Результаты определения Даты регистрации.

Домен	Сервис		
	www.reg.ru/whois/	www.nic.ru/whois	2ip.ru/whois
sut.ru			
fem-sut.spb.ru			
google.com			

Таблица 4. Результаты определения Конца регистрации.

Домен	Сервис		
	www.reg.ru/whois/	www.nic.ru/whois	2ip.ru/whois
sut.ru			
fem-sut.spb.ru			
google.com			

8. АРХИВ САЙТОВ ARCHIVE.ORG

Цель работы.

Целью работы является знакомство с возможностями архива сайтов Archive.org.

Общие сведения

Archive.org – сервис некоммерческой организации Internet Archive, предоставляющей бесплатный открытый доступ к коллекциям оцифрованных материалов, включая веб-сайты, программные приложения, игры, музыку, фильмы, видео, анимацию и книги. В феврале 2021 года архив хранил более 29 миллионов книг и текстов, 8,7 миллиона фильмов, видео и телешоу, 629 000 программ, 16 миллионов аудиофайлов, 3,8 миллиона изображений, 224 000 аудиофайлов и 534 миллиарда веб-сайтов.

Записанные в разное время веб-сайты, доступны по адресу https://web.archive.org/. К сожалению, сайты записываются не полностью и некоторые ссылки на внутреннее содержание могут не работать.

Задание

С помощью сервиса https://web.archive.org/ сравнить вид и определить временной диапазон и количество хранящихся в архиве снимков для следующих сайтов:

1. www.sut.ru
2. www.fem-sut.spb.ru
3. www.google.com

Рекомендации

Временной диапазон и количество снимков в архиве занести в Таблицу 1.

Таблица 1. Параметры архива сайтов.

Сайт	Временной диапазон	Количество снимков
www.sut.ru		
www.fem-sut.spb.ru		
www.google.com		

Размещение требуемой информации на странице сервиса отмечено на рис. 1.

Для сравнения вида сайтов использовать даты, отстоящие примерно на 1 месяц, 1 год и 10 лет от текущего состояния.

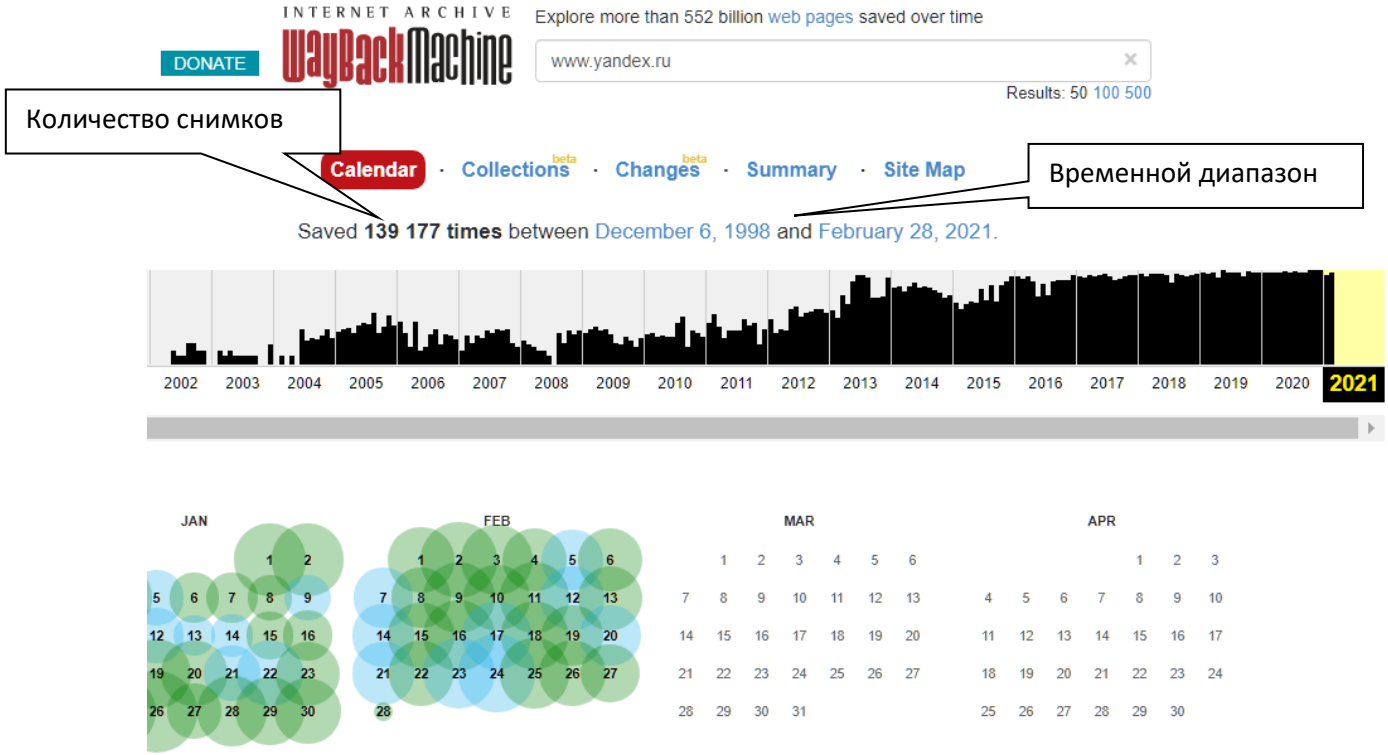

Рис.1. Сайт web.archive.org.

9. ДИРЕКТИВЫ ПОИСКА ROBOTS.TXT

Цель работы.

Целью работы является освоение директив файла robots.txt для поисковых сайтов.

Общие сведения

В работе поисковых сайтов Google, Yandex, Rambler и т.д. используется автоматизированная индексация содержимого Интернет-ресурсов. С помощью файла robots.txt, размещаемого в корневой папке сайта, можно задать параметры работы поисковых роботов, исключить индексацию отдельных разделов, ускорить процедуры и снизить нагрузку на сервер.

Начинается файл robots.txt с директивы User-agent с указанием робота, к которому обращены последующие инструкции. Для обозначения всех роботов используется знак *.

Запрет на индексацию отдельных файлов и папок производится директивой Disallow. Чаще всего Disallow используется для разделов, требующих или авторизованного доступа, или полностью закрытых для внешних пользователей. Необязательная директива Allow формально разрешает индексирование.

Уменьшить трафик при работе роботов можно с помощью директивы Clean param, указав разделы, которые уже загружались и остаются неизменными.

Задание

Рассмотреть директивы в файлах robots.txt следующих сайтов:

1. www.sut.ru
2. www.fem-sut.spb.ru
3. www.google.com

Записать первые 5 строк файлов и проверить возможность доступа к закрытым разделам.

Рекомендации

Для доступа к файлу с директивами в адресном поле браузера следует набрать <Имя сайта>/robots.txt. Первые 5 строк полученного файла, а также результаты проверки неиндексируемых разделов занести в Таблицу 1 по образцу для сайта кодекс.рф.

Таблица 1. Директивы robots.txt.

Сайт	5 строк robots.txt	Комментарий
кодекс.рф	User-agent: * Disallow: /cgi-bin Disallow: /auth/ Disallow: /search/ Disallow: /admin/ …	Директивы для всех роботов Ошибка 404 (не найдено) Ошибка 404 (не найдено) Ошибка 404 (не найдено) Авторизованный доступ
www.sut.ru		
www.fem-sut.spb.ru		
www.google.com		

10. ОПЕРАТОРЫ ОКНА ПОИСКА GOOGLE

Цель работы.

Целью работы является знакомство с некоторыми операторами окна поиска Google.

Общие сведения

Операторы окна поиска Google позволяют существенно уменьшить количество выводимых результатов, сделать их в большей степени соответствующими запросу. В частности, оператор allinurl: позволяет отфильтровать только те ресурсы, в которых содержится заданное слово или слова. Оператор site: для заданного ресурса ограничит вывод только страницами с указанными словами. Оператор filetype: построит список размещённых в Интернете файлов заданного типа, содержащих конкретные слова.

Умелое использование операторов и ошибки реализации мер по обеспечению безопасности могут значительно облегчить получение критической для бизнеса информации.

Задание

1. С помощью оператора allinurl: найти файлы, которые могут содержать пароли пользователей. Проверить наличие данных об аккаунтах в первой из полученных ссылок.
2. С помощью оператора site: найти все страницы ресурсов www.sut.ru и www.fem-sut.spb.ru со словом «пароль». Проверить наличие данных об аккаунтах в первой из полученных ссылок.
3. С помощью оператора filetype: найти файлы Microsoft Excel, содержащие паспортные данные жителей РФ. Выделить две ссылки с правдоподобными данными.

Рекомендации

1. В качестве имён файлов, которые могут содержать пароли пользователей, использовать «пароль.txt» и «password.txt» как показано на рисунке 1.

Рис.1. Команда allinurl.

Результаты занести в таблицу 1.

Таблица 1. Оператор allinurl:.

Запрос	Первая ссылка результата	Комментарий
пароль.txt		
passwords.txt		

2. Использовать команды «site:www.sut.ru пароль» и «site:www.fem-sut.spb.ru пароль»для первого и второго ресурсов соответственно. Результаты занести в таблицу 2.

Таблица 2. Оператор site:.

Ресурс	Первая ссылка результата	Комментарий
www.sut.ru		
www.fem-sut.spb.ru		

3. Использовать команду «filetype:xls Паспорт РФ». Результаты занести в таблицу 3.

Таблица 3. Оператор filetype:.

№ ссылки	Ссылка	Комментарий
1		
2		

СОДЕРЖАНИЕ