**ЛАБОРАТОРНАЯ РАБОТА №7**

«Сравнительный анализ методик проведения аудите информационных технологий и систем обеспечения информационной безопасности. Проверка ссылок»

**Цель работы:** Проведение сравнительного анализа методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ). Проверка на сайте внутренних и внешних ссылок на наличие битых и отсутствующих страницы, наличие страницы 404, ошибка 500.

**Задачи:**

• научиться проверять актуальность ссылки с помощью онлайнсервисов;

• научиться проверять ошибку 500;

• научиться проверять наличие страницы 404.

**Краткие теоретические сведения**

Обязательными элементами любого Web-сайта и Web-приложения являются ссылки. Они помогают пользователям быстро находить необходимую информацию, значительно улучшают пользовательский опыт и являются важной частью функциональности Web-программного обеспечения.

Современные Web-сайты и приложения могут содержать много страниц и тысячи ссылок

Все ссылки должны правильно открываться и вести к требуемым страницам и ресурсам. Поэтому проверка ссылок всегда включается в функциональное тестирование

В рамках функционального тестирования проверяют валидность ссылок, работу сайта с базой данных, формы, которые используются на сайте.

Говоря подробнее про ссылки, проверяют следующее:

• туда ли ведут исходящие ссылки;

• правильно ли работают внутренние ссылки;

• есть ли ссылки, которые ведут на одни и те же страницы;

• проверка ссылок, которые используются для отправления и-мейлов админам сайта;

• выявление страниц, на которые не ведут ссылки;

• определение сломанных ссылок

Проверка всех ссылок на сайте вручную требует много времени и усилий, для этой цели применяют автоматизированное тестирование. Для автоматической проверки ссылок создано много бесплатных и коммерческих инструментов.

Как правило, есть такие ссылки:

• исходящие ссылки; они ведут на определенные внешние ресурсы;

• внутренние ссылки; они ведут на другие страницы этого же сайта;

• навигационные ссылки; они приводят к абзацу или объекту на этой же странице;

• ссылки для отправки электронной почты владельцами сайта, службе поддержки и т.д.

Проверка ссылок осуществляется с помощью специальных сервисов и инструментов.

Инструментарий вебмастера Яндекс и Google:

• http://webmaster.yandex.ru/wmconsole/;

• инструменты для веб-мастеров от Google.

Специализированное программное обеспечение.

Существует целый ряд разного рода программ, проверяющих сайты на битые ссылки: Semonitor, Xenu's Link Sleuth, linkchecker, Shadow Web Analyzer, Link Evaluator.

Интернет-сервисы по проверке битых ссылок проверка осуществляется с сервера сервиса, но придется довольно долго ждать, пока сервис завершит опрос сайта. При этом нельзя разрывать соединение с сервисом, чтобы не потерять результаты.

Примеры Интернет-сервисов: validator.w3.org/checklink, www.graffity.biz/products/link\_checker, Badlinks.ru, Build your Site Map online.

Также необходимо проверить наличие страницы-заглушки при отсутствующих страницах или страниц с не разрешенным доступом. Это называется проверка на «Ошибку 404».

Ошибка 404 или Not Found («не найдено») — стандартный код ответа HTTP о том, что клиент был в состоянии общаться с сервером, но сервер не может найти данные согласно запросу

Ошибку 404 не следует путать с ошибкой «Сервер не найден» или иными ошибками, указывающими на ограничение доступа к серверу

Ошибка 404 означает, что запрашиваемый ресурс может быть доступен в будущем, что, однако не гарантирует наличие прежнего содержания.

В этом случае необходимо приготовить страницу-заглушки с указанием ссылок для возврата.

Кроссбраузерность

Кроссбраузерность – это проверка на правильность (соответствие стандартам) функционирования и отображения Web-приложения в различных браузерах и операционных системах. В наше время стандартизация принимает глобальные масштабы, следовательно, большинство популярных браузеров одинаково обрабатывает код. Но необходимость в тестировании на кроссбраузерность не пропадает, так как много проблем остается не решенными.

Что необходимо проверять при кроссбраузерном тестировании:

• функциональные возможности продукта, реализуемые на стороне клиента;

• правильность отображения элементов графики;

• шрифты и размеры текстовых символов;

• доступность и функциональность разнообразных форм, включая их интерактивность.

На сегодняшний день существует несколько популярных браузеров — FireFox, Opera, Chrome, Netscape, Safari, AOL, Internet Explorer. Некоторые приложения очень зависимы от браузеров. Различные браузеры имеют различные конфигурации и установки, с которыми ваша страница в сети должны быть совместима.

В тестировании нуждаются все основные (среди пользовательской аудитории) браузеры, но особое внимание необходимо уделить IE, если он входит в их число. Именно в нем очень часто возникают проблемы, которые отсутствуют в других браузерах: так, в IE дополнительно рекомендуется обращать особое внимание на масштабируемость, фокус полей и работу JS

Онлайн-сервисы для тестирования:

LoadImpact – сервис нагрузочного тестирования сайтов (за деньги – до 5к одновременных подключений), у которого есть бесплатный тест на 50 одновременных соединений.

BrowserMob – дополнительный, простой, но симпатичный сервис, позволяющий проверить скорость загрузки целевого сайта из 4 разных мест и показывающий много подробных метрик загрузки для каждого из них. Основная задача BrowserMob – автоматическое кроссбраузерное тестирование сайтов.

Alerta – сервис мониторинга аптайм, на сайте которого можно бесплатно проверить доступность (и время ответа) сайта из 11 разных мест. Работает быстро и надежно, никаких капч.

Site24x7 – использует уже 23 географически распределенные точки.

CSE HTML Validator – отличается очень подробными и понятными рекомендациями по исправлению ошибок и потенциальных проблем.

Built with: builtwith.com анализирует заданный сайт и выдает целое досье о нем: веб-сервер, CMS, какая служба статистики используется и так далее.

Microsoft Security Assessment Tool (MSAT) – это средство оценки рисков, предоставляющее информацию о системе безопасности ИТ-инфраструктуры и рекомендации по ее улучшению, основанные на передовом опыте.

Как отмечают разработчики, приложение предназначается для организаций с числом сотрудников менее 1000 человек, чтобы содействовать лучшему пониманию потенциальных проблем в сфере безопасности. В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на вопросы в два этапа.

Первый этап посвящен бизнес-модели компании и призван оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

Вопросы этого этапа разбиты на 6 групп. Первая касается общих сведений о компании – название, число компьютеров, серверов и т.д.

Вторая группа вопросов первого этапа озаглавлена «Безопасность инфраструктуры». Примеры вопросов – «использует ли компания подключение к Интернет», «размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте» и т.д. Остальные группы – «Безопасность приложений», «Безопасность операций», «Безопасность персонала», «Среда».

Надо отметить, что при локализации не все вопросы первого этапа были качественно переведены с английского. Например, вопрос: «Прошла ли ваша организация через «копирование и замена» касающиеся любого основного компонента технологии, за последние 6 месяцев?» Однако во всех случаях можно из контекста понять, о чем идет речь (в приведенном примере вопрос был относительно того, менялись ли используемые технологии обработки информации).

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты. Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

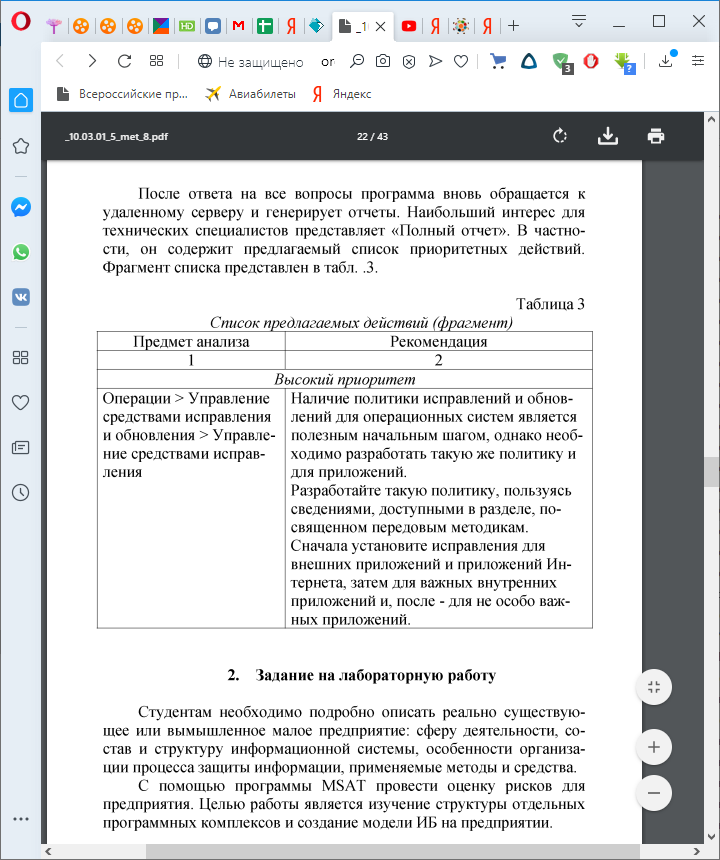
Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса.

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет «Полный отчет». В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в табл. 1.

Таблица 1

Список предлагаемых действий (фрагмент)



**Порядок выполнения работы**

**Задание 1.**

Перед выполнением задания ответьте на вопрос: что такое аудит информационных технологий?

В ходе лабораторной работы, используя ресурсы сети Интернет, необходимо провести сравнительный анализ методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ). Результаты анализа свести в таблицу (табл. 1).

*Таблица 1*

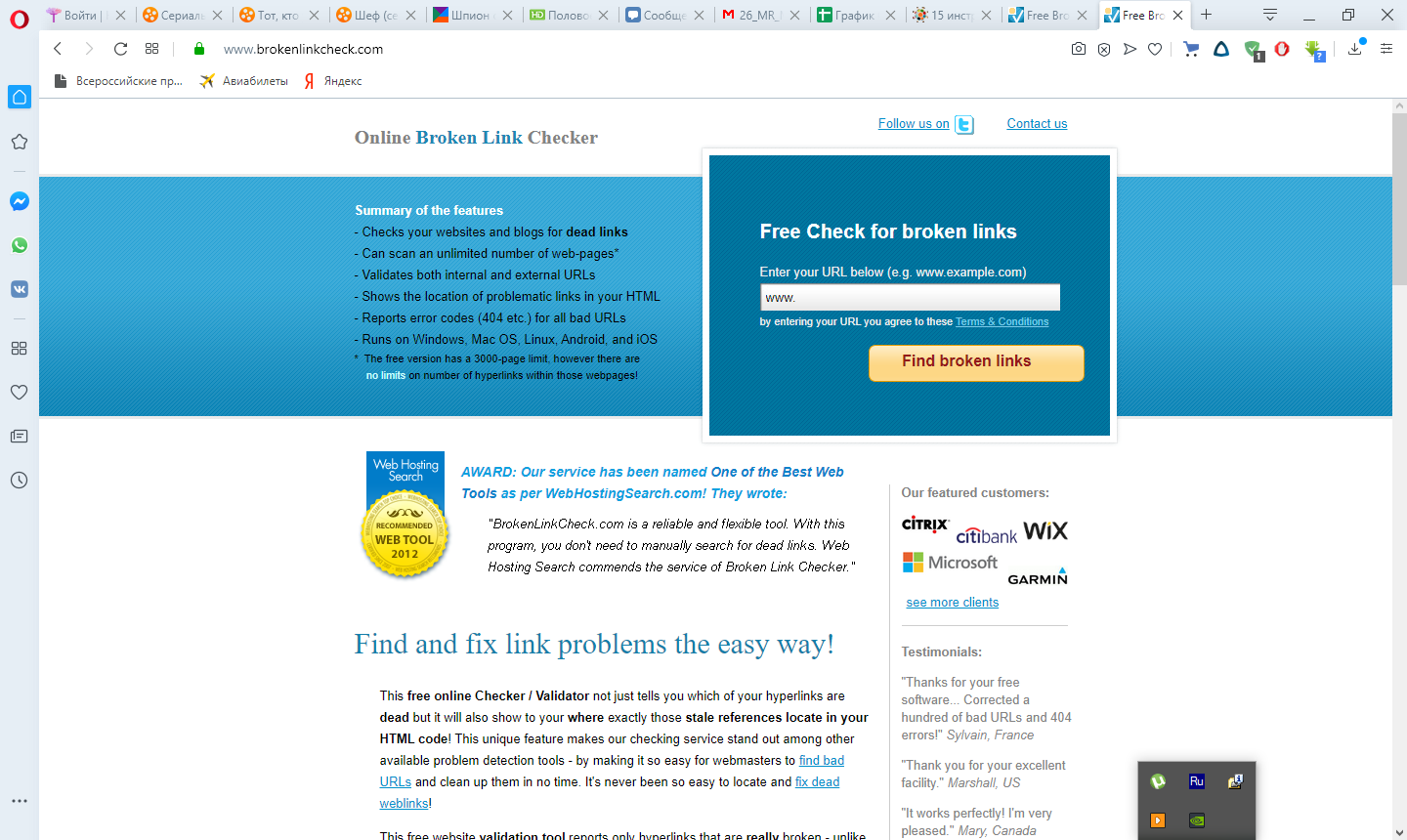
Результаты сравнительного анализа методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №, п/п | Наименование параметра | Активный аудит | Экспертный аудит | Аудит на соответствие  стандартам |
| 1 | Краткое описание |  |  |  |
| 2 | Сфера применения |  |  |  |
| 3 | Применяемости |  |  |  |
| 4 | Достоинства |  |  |  |
| 5 | Недостатки |  |  |  |
| 6 | Описание этапов методики применения на практике |  |  |  |

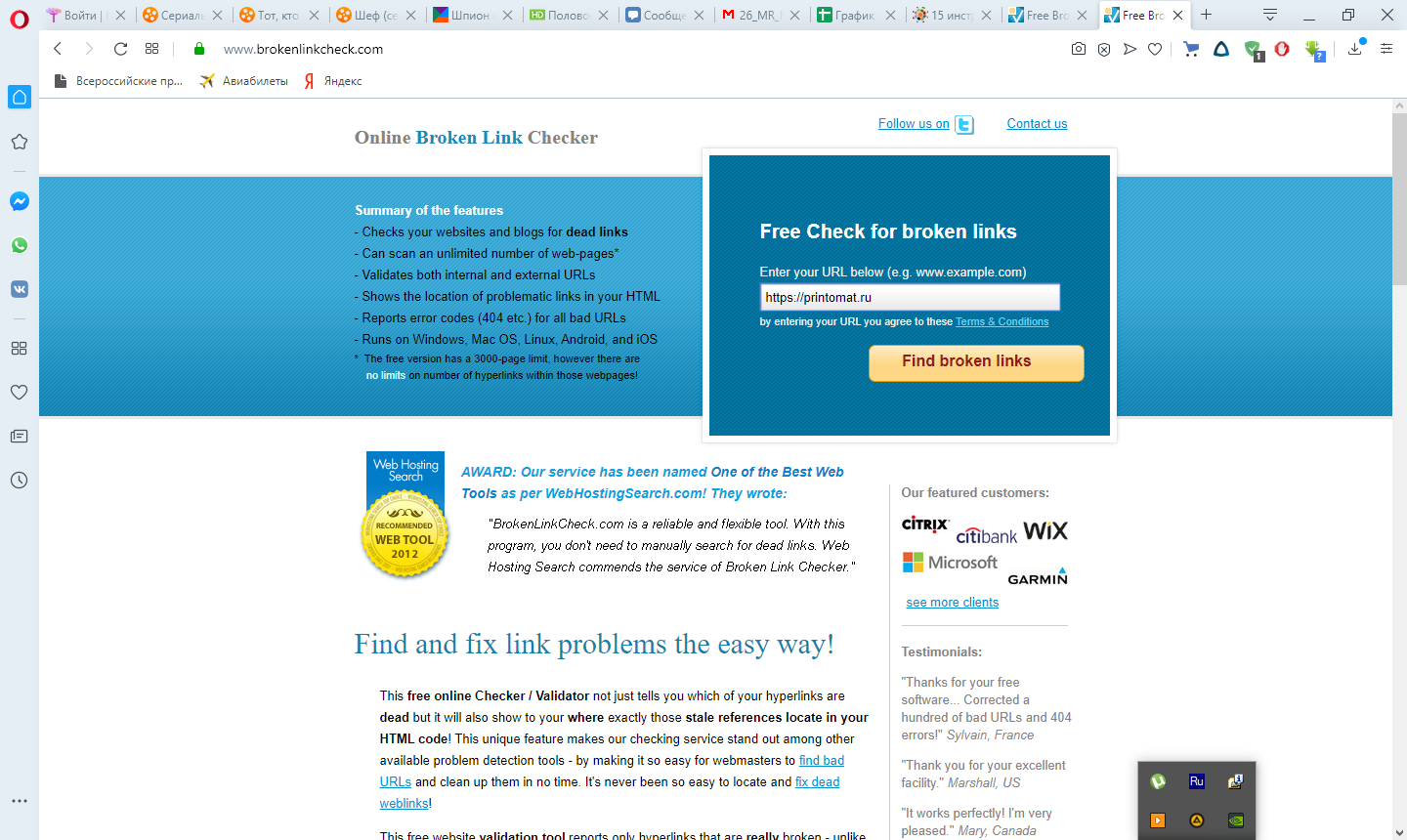
**Задание 2.**

1. Для онлайн проверки сайта на битые ссылки перейдем на сервер

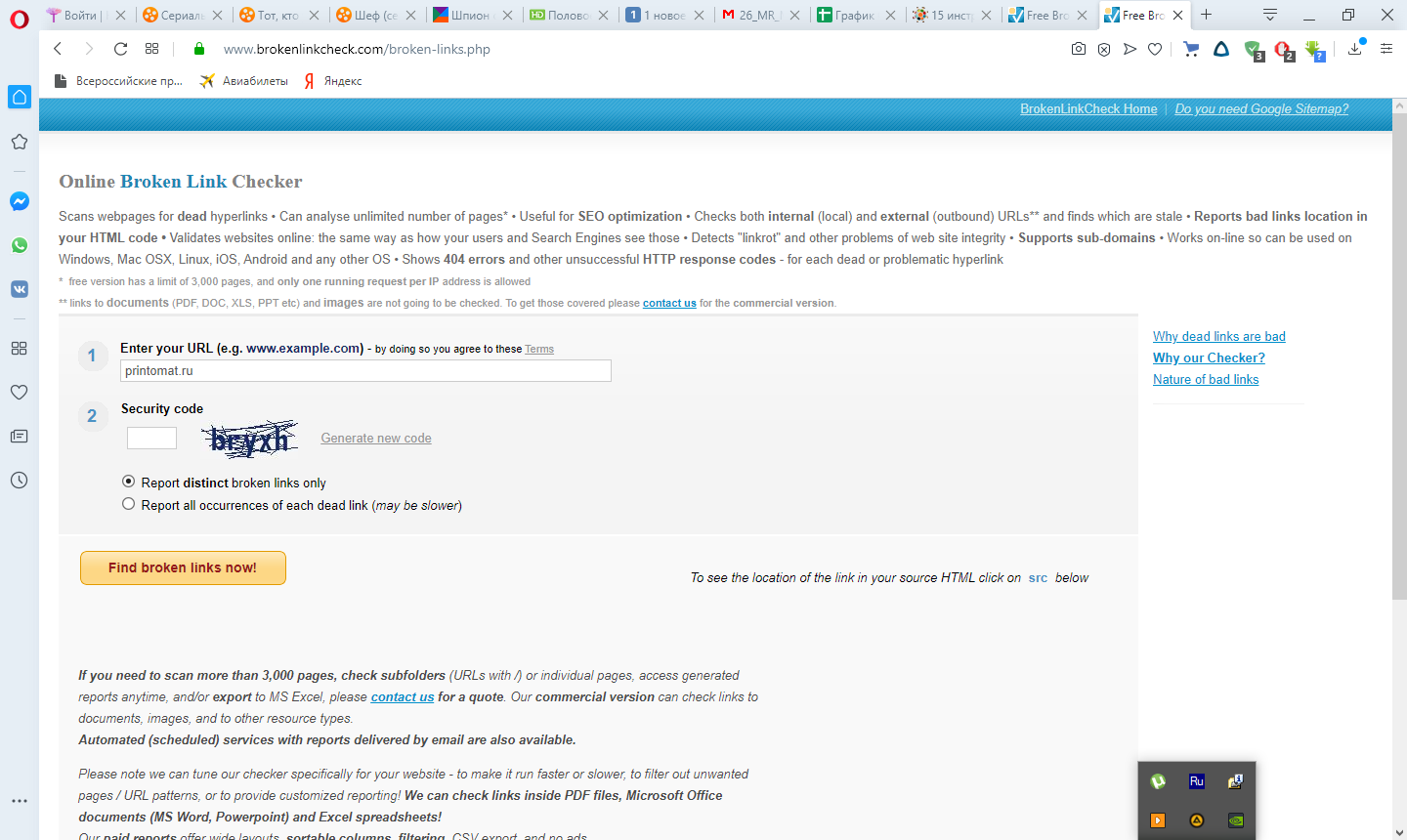
http:\\www.brokenlinkcheck.com



В появившемся окне, под надписью - Enter your URL below (e.g. [www.example.com](http://www.example.com)) – вставьте ссылку для проверки.

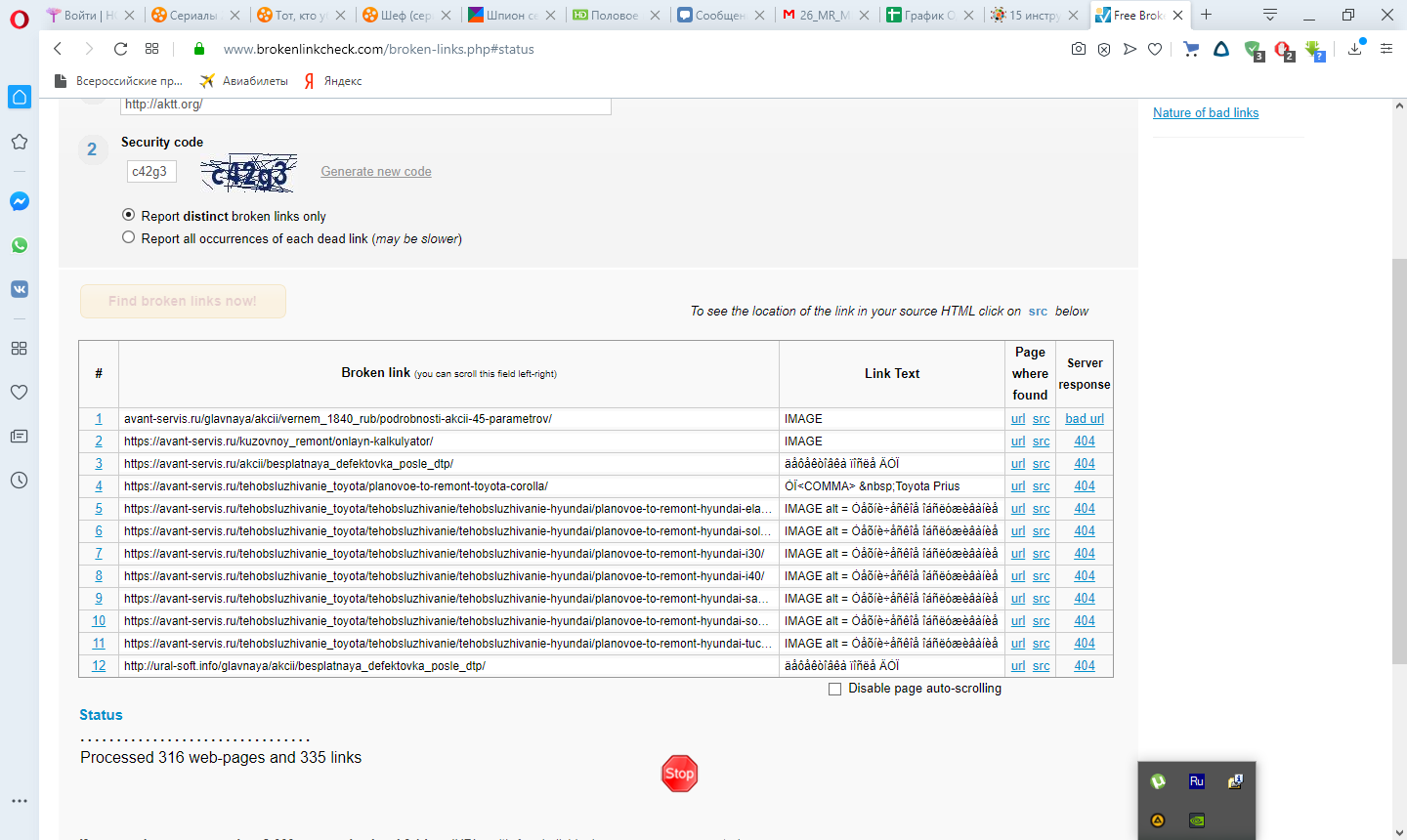


После нажатия на кнопку Find broken links вы перейдете на следующую страницу:



Введите код безопасности с капчи и выберите Report **distinct** broken links only. Затем нажмите на кнопку Find broken links now! И ждите результата поиска.

В процессе поиска у вас будет появляться таблица с нерабочими ссылками:



В отчет вы выписываете найденные битых ссылок, делаете скриншот результата поиска.

В случае, если на сайте была ссылка с ошибкой 500, URL-адрес ошибки копируете и делаете скриншот сайта, перейдя по этому URL-адресу.

То же самое делаете и в случае с ошибкой 404.

*Список сайтов для тестирования:*

<https://printomat.ru>

<https://copy.spb.ru/pechat_i_chtamp/>

<https://armorgames.com>

<https://shikimori.one>

<http://krol96.ru>

<https://chelpipe.ru>

<http://www.zolotoy-venec.ru>

<https://www.ramzavod.ru/metallokonstrukcii>

<https://autouma.ru>

<https://eastinvest.ru>

<https://www.artfacet.ru>

<https://kadikama.ru>

<https://avant-servis.ru>

<https://yummyanime.club>

*Требования к содержанию отчета по заданию 2*

Отчет должен содержать:

1. Количество битых ссылок и скриншот результата.

Количество:

Скриншот:

1. Укажите URL страницы сайта с ошибкой 500 и вставьте скриншот

URL:

1.

2.

3.

Скриншот:

1. Вставьте скриншот страницы сайта с ошибкой 404, укажите название сайта и скриншот страниц.

Скриншот сайта (главная страница):

Страницы «заглушки» (несколько скриншотов страниц, URL-адреса которых помечены ошибкой 404):

**Задание 3.**

Необходимо познакомиться с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью – Microsoft Security Assessment Tool (MSAT). Она бесплатно доступна на сайте Microsoft по ссылке:

<http://www.microsoft.com/ru-ru/download/details.aspx?id=12273>

Необходимо подробно описать реально существующее или вымышленное малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства, кто из сотрудников или подрядчиков имеет доступ к информационной системе предприятия и т.д.

C помощью программы MSAT провести оценку рисков для предприятия.

**Порядок выполнения работы**

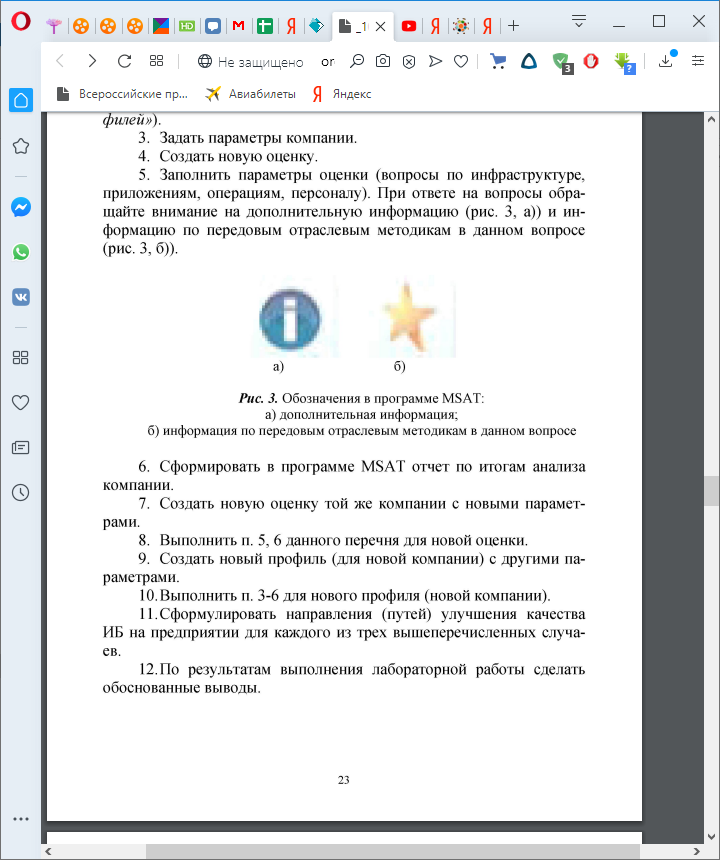
1. Произвести инсталляцию программы (при необходимости).

2. Создать новый профиль (Меню «Файл» -> «Настройка профилей»).

3. Задать параметры компании.

4. Создать новую оценку.

5. Заполнить параметры оценки (вопросы по инфраструктуре, приложениям, операциям, персоналу). При ответе на вопросы обращайте внимание на дополнительную информацию (рис. 3, а)) и информацию по передовым отраслевым методикам в данном вопросе (рис. 3, б))



6. Сформировать в программе MSAT отчет по итогам анализа компании.

7. Сформулировать направления (путей) улучшения качества информационной безопасности на предприятии.

**Требования к содержанию отчета**

Отчет должен содержать:

1. Подробное описание компании/предприятия, которое рассматривается в данной системе (часть данных пойдет в анализ в программе MSAT);

2. Перечисление факторов, которые по мнению разработчиков программы, являются ключевыми в оценке информационной безопасности предприятия (информационная структура предприятия, система защиты и т.д., подробно).

3. Сформированный отчет по итогам анализа исходной компании;

4. Сформулированные направления (путей) улучшения качества ИБ на предприятии.

**Контрольные вопросы**

1. От чего зависит информационная безопасность?
2. Что такое криптографические средства и что к ним относится?
3. Что такое окно опасности?
4. Что такое аудита информационных технологий?
5. Какие методики аудита информационных технологий существуют?
6. Что такое системы обеспечения информационной безопасности?
7. Что такое страницы-«заглушки»?
8. Что такое кроссбраузерность?
9. Что означает ошибка 404?
10. Что означает ошибка 500?