1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. —
4. Институт компьютерных наук и технологий
5. **Кафедра «Информационная безопасность компьютерных систем»**

**ОТЧЕТ**

**по лабораторной работе № 14**

По дисциплине «Основы информационной безопасности»

1. Выполнили
2. Студент гр. 13508/13 А.Э.Палёный

\_\_\_\_\_\_\_\_\_\_

1. Проверил
2. Преподаватель

\_\_\_\_\_\_\_\_\_\_ М.О.Калинин

1. Санкт-Петербург
2. 2016
3. Цель

Приобретение навыков безопасности работы в сети Интернет, создания безопасной конфигурации web-браузеров, анализа и контроля механизма cookies.

1. Решаемые задачи
2. 1) Определить месторасположение файлов cookie
3. 2) Определить содержимое файлов cookie
4. 3) Разобраться с настройками Internet Explorer для обеспечения безопасности
5. 4) Проанализировать файлы cookie с сайтов, добавленных в «Ограниченные узлы»
6. Содержание:
7. Ход работы (4-11)
8. Ответы на контрольные вопросы(11-18)
9. Вывод (18)

Ход работы

1. 1) Посещённые сайты
2. [www.google.com](http://www.google.com)
3. [www.4pda.ru](http://www.4pda.ru)
4. [www.habrahabr.ru](http://www.habrahabr.ru)
5. [www.vk.com](http://www.vk.com)
6. [www.wikipedia.org](http://www.wikipedia.org)
7. [www.yandex.ru](http://www.yandex.ru)
8. 2) Авторизация на сайтах

a) www.yandex.ru

b) [www.4pda.ru](http://www.4pda.ru)

c) www.wikipedia.org

Листинг cookies

1. yandexuid

1221198311460403703

yandex.ru/

1024

3833050496

31246424

897507680

30512170

\*

yp

1462995703.ygu.1#1775764605.udn.cDphbGV4eDM4NA%3D%3D

yandex.ru/

1024

3567643008

32111902

1367253088

30512172

\*

yandex\_gid

2

yandex.ru/

1024

622376320

30518205

900157680

30512170

\*

\_ym\_uid

1460404482614343502

yandex.ru/

1088

1181887744

30657011

4245350384

30512171

\*

\_ym\_isad

2

yandex.ru/

1088

2690534656

30512339

4246130384

30512171

\*

Session\_id

3:1460404605.5.0.1460404605000:d7-GHw:cd.0|120047050.0.2.0:3|144091.98606.zHATK8VLuckLM2jH4QSXP\_FSmQE

yandex.ru/

9216

3567643008

32111902

1367253088

30512172

\*

sessionid2

3:1460404605.5.0.1460404605000:d7-GHw:cd.1|120047050.0.2.0:3|144091.215494.yz7j2G1FoM\_g2CW4mlyfM2MYThY

yandex.ru/

9217

3567643008

32111902

1367253088

30512172

\*

L

aHpmZWNZVVJjc2oBcXNoV2IOUwRfY29dODwUNDZLdVg=.1460404605.12339.38005.95eae46001a4e4a691919923fedcfa65

yandex.ru/

1024

3567643008

32111902

1367413088

30512172

\*

yandex\_login

alexx384

yandex.ru/

1024

3567643008

32111902

1367413088

30512172

\*

b) \_\_cfduid

d329c4f6bff6b7ae96dc37e1ef7507b901460404194

4pda.ru/

9728

3391331584

30585596

1545190384

30512171

\*

OAID

0575333f3ef1c3d1d49426884ae8026a

4pda.ru/

1024

4286429696

30585599

2498098496

30512174

\*

\_ym\_uid

1460404214665967484

4pda.ru/

1600

2786855040

30657010

1563940384

30512171

\*

\_ym\_isad

2

4pda.ru/

1600

10534656

30512339

1565820384

30512171

\*

\_ga

GA1.2.227449515.1460404214

4pda.ru/

1600

1602655488

30659022

1851290384

30512171

\*

member\_id

3436056

4pda.ru/

9728

4276429696

30585599

2492008496

30512174

\*

pass\_hash

7249cc667356dafb86e0dd35e05c08ec

4pda.ru/

9728

4276429696

30585599

2492008496

30512174

\*

3) WMF-Last-Access

11-Apr-2016

commons.wikimedia.org/

9216

4188397568

30518542

1365696608

30512177

\*

commonswikiUserID

2817290

commons.wikimedia.org/

9217

1267605248

30518212

1722736608

30512177

\*

commonswikiUserName

Alexx384

commons.wikimedia.org/

9217

1267605248

30518212

1722736608

30512177

\*

centralauth\_User

Alexx384

commons.wikimedia.org/

9217

1267605248

30518212

1722736608

30512177

\*

В файлах cookie, оставленными сайтами [www.yandex.ru](http://www.yandex.ru) и [www.wikipedia.org](http://www.wikipedia.org) хранится техническая информация, но сайт Wikipedia.org дополнительно сохраняет и другие данные пользователя, такие как местоположение и время входа.

Сайт 4pda.ru хранит только техническую информацию о пользователе в зашифрованном виде.

Рассмотрим теперь сайты, добавленные в ограниченные узлы.   
После захода на все сайты из ограниченных узлов, только google.ru оставил свои cookie, но там хранится лишь незначительная техническая информация. Листинг cookie  
NID

78=CjxYxmrazFMJLgJm9AXeb5rMIy15xy2xBfJ1vUaL0n0fSFSNf-Ne3Ncq8IHZXFf0gvYe5ekXVOVYUI1lWvmGaOfisD7BneYSN\_2CIFUZbOYrChdSec1XFV4XMDHyebJY

google.ru/

9216

1484496000

30549000

444933648

30512187

\*

Ответы на контрольные вопросы

1. Cookie — это небольшие текстовые файлы, в которые браузер записывает данные с посещенных вами сайтов. Файлы cookie позволяют сайтам «запоминать» своих посетителей, например, чтобы каждый раз не переспрашивать их логин и пароль. Но они также могут нарушать права пользователя, записывая информацию о пользователе, предварительно его не оповестив об этом.
2. По умолчанию зона «Ограниченные узлы» не содержит названия сайтов

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры | Значение по умолчанию | Рекомендуемое значение | Функциональный смысл и причина выбора. |
| XAML-приложения веб-обозревателя | Включить | Включить | Некоторые веб приложения могут не работать, если функция отключена |
| XPS-документы | Включить | Включить | Если функция отключена, то невозможна работа с XPS документами |
| Свободный XAML | Включить | Отключить | Может быть создан недоброжелателями, что сильно повлияет на безопасность |
| Автоматические запросы на загрузку файлов | Отключить | Отключить | вместо окна с подтверждением на загрузку будет сообщение на панели, информирующее о блокировании загрузки файла. Отключить, так как незаметно можно загрузить файлы-угрозы |
| Загрузка файлов | Разрешить | Разрешить | Если функция включена, то пользователь может выбирать, загружать файл или нет. |
| Загрузка шрифтов | Разрешить | Разрешить | Функция загружает шрифты из интернета. Разрешить, так как она не несёт опасности и делает сайт красивее. |
| Вход | Автоматический вход в сеть только в зоне интрасети | Запрос имени пользователя и пароля | Дополнительная проверка пользователя. Разрешить, так как поможет обеспечить получше безопасность. |
| Блокировать всплывающие окна | Разрешить | Разрешить | Позволяет блокировать рекламные всплывающие окна. Рекомендуется разрешить, так как поможет защитить от рекламы |
| Веб-узлы из зон Интернета с наименьшими правами могут открываться из этой зоны | Разрешить | Разрешить | Рекомендуемое значение разрешить, так как оно предоставляет доступ к сайту. |
| Доступ к источникам данных за пределами домена | Отключить | Отключить | Доступ к источникам данных за пределами домена позволяет веб-странице получать доступ к информации другого сайта. Другой сайт может содержать вредоносное ПО. |
| Запуск программ и файлов в окне IFRAME | Предлагать | Запретить | Если эта функция будет отключена, то пользователи не смогут запускать приложения и загружать файлы в IFRAME. Это защитит компьютер от необдуманных действий пользователя |
| Не запрашивать сертификат клиента, когда он отсутствует или имеется только один | Отключить | Отключить | Сайты без сертификатов являются опасными и могут содержать вредоносное ПО. |
| Запускать файлы на основе содержимого, а не расширения имени файла | Разрешить | Запретить | При проверке файла там может оказаться вирус, который внедриться в эту проверку. Это небезопасно. |
| Отображение разнородного содержания | Предлагать | Предлагать | Если выбрать «Предлагать», то пользователю будет сообщено о том, что на данной странице содержатся небезопасные элементы |
| Передача незашифрованных данных форм | Предлагать | Запретить | При отправке незашифрованных данных злоумышленник может их перехватить и в дальнейшем воспользоваться ими. |
| Перетаскивание или копирование и вставка файлов | Разрешить | Разрешить | Эта настройка позволят выбирать, сможете ли вы перетаскивать или копировать и вставлять файлы из источника в пределах зоны. |
| Переход между кадрами в разные домены | Запрос | Запретить | Позволяет управлять открытием вложенных кадров и доступом к приложениям разных доменов. Если этот параметр политики отключен, пользователи не могут открывать окна и фреймы для доступа к приложениям из других доменов, что обеспечит дополнительную безопасность |
| Разрешить страницам использовать ограниченные протоколы для активного содержимого | Запрос | Запрашивать | Позволит пользователю узнать использует ли страница ограниченные протоколы. Если да то он может поинтересоваться и тем самым защитить себя. |
| Запрещать запущенные сценарием окна без ограничения на размеры и положение | Отключить | Разрешить | Нежелательная реклама не сможет блокировать всю страницу |
| Разрешение канала программного обеспечения | Средний уровень безопасности | Высокий уровень безопасности | При выборе высокого уровня безопасности пользователи не получают уведомлений об обновлениях программного обеспечения по электронной почте, пакеты программного обеспечения автоматически не загружаются и не устанавливаются на пользовательские компьютеры. При среднем обновления не будут автоматически загружаться. |
| Разрешить метаобновление | Разрешить | Отключить | Если этот параметр политики включен, браузер пользователя, загружающий веб-страницу с активным тегом метаобновления, может быть перенаправлен на другую веб-страницу, что небезопасно. |
| Разрешить сценарии для элемента управления обозревателем IE | Отключить | Отключить | Если параметр включён, то страница может через скрипт управлять браузером, что небезопасно. |
| Установка элементов рабочего стола | Предлагать | Запретить | Для то чтобы вредоносное ПО не попало на рабочий стол, нужно запретить этот параметр. |
| Устойчивость данных пользователя | Разрешить | Разрешить | Данные пользователя сохраняются в надёжно XML хранилище на жёстком диске. |
| Активные сценарии | Разрешить | Отключить | Активные сценарии могут нанести вред компьютеру, поэтому рекомендуется их отключить. |
| Выполнять сценарии приложений Java | Разрешить | Предлагать | Предлагать, так как могут нанести вред компьютеру, но если пользователь им доверяет, то может ему помочь. |
| Разрешить операции вставки из сценария | Разрешить | Предлагать | Работа с буфером обмена. Может привести к переполнению буфера или потере данных. |
| Автоматические запросы элементов управления ActiveX | Отключить | Отключить | Не позволяет элементам ActiveX запускать сценарии на выполнение, так как они могут быть небезопасными. |
| Выполнять сценарии элементов ActiveX, помеченных как безопасные | Разрешить | Разрешить | Их безопасность была подтверждена уже ранее, так что они безопасны. |
| Загрузка неподписанных элементов ActiveX | Отключить | Отключить | Неподписанные элементы могут нанести вред компьютеру и не гарантируют безопасности |
| Загрузка подписанных элементов ActiveX | Предлагать | Разрешить | Этот параметр является безопасным, так как цифровая подпись уже предполагает надёжность |
| Запуск элементов ActiveX и модулей подключения | Разрешить | Допущенных администратором | Запуск таких элементов может нанести вред. Так что следует использовать только те, что допущены администратором |
| Использование элементов ActiveX, не помеченных как безопасные | Отключить | Отключить | Такие элементы небезопасны. Этот параметр стоит отключить |
| Поведение двоичного кодов и сценариев | Разрешить | Запретить | При отключении этого парметра небезопасные двоичные коды и сценарии не будут использоваться.  Только приложения с внедрённым диспетчером безопасности будут запускаться. |

1. JavaScript – язык программирования, позволяющий изменить цвет фона страницы или интегрированную в документ картинку, открыть новое окно или выдать предупреждение. Т.е. сделать сайт более наполненным и более коасивым.
2. Потому, что написанная на нём вредоносная программа будет запускаться в браузере, у которого в данный момент будут все права пользователя. Получив эти права, программа может делать с компьютером что угодно. А это может привести к потере данных пользователя.
3. При переходе на не доверенный сайт, мы можем кликнуть на эту страницу. Сработает JavaScript и нас перенаправит на рекламный или вредоносный сайт, что будет являться угрозой компьютеру. Чтобы от этого защитится надо переходить на сайты имеющие несколько сертификатов безопасности.
4. С помощью системы P3P можно настроить, какую информация будет хранить файл cookie. Эта система обеспечивает конфиденциальность при интернет-сёрфинге, так как мы можем запретить использование cookie и сайты и сервера не будут знать о нас много информации.

Вывод:  
Использование технологии cookies значительно упрощает нам жизнь. Так как при заходе на другие сайты мы уже будем авторизированны.  
Но также cookies могут хранить о нас слишком много информации, что не позволит нам оставаться конфиденциальными. Поэтому для уменьшения негативного воздействия cookie нужно заходить на сайты, использующие технологию P3P. Она обеспечит нам конфиденциальность. Но также для конфиденциального сёрфинга по глобальной сети пользователя должен самостоятельно настроить параметры своего.