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»**

**Лабораторная работа 14**

1. «Безопасная эксплуатация web-браузеров»
2. по дисциплине «Практикум по информационной безопасности»

Выполнил:

студент гр. 13558/1 Никулкин В. А.

Проверил:

ассистент преподавателя Алексеев. И. В.

1. Санкт-Петербург
2. 2017

**Цель работы**

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

**Ход работы**

Cookies находятся по адресу:

C:\Users\Vadim\AppData\Local\Microsoft\Windows\INetCookies

1. Список посещенных сайтов:
2. google.ru
3. youtube.com
4. ru.wikipedia.org
5. mail.ru
6. vk.com
7. championat.com
8. Сайты, на которых была выполнена авторизация
9. mail.ru
10. Содержание Cookies
11. NID97=W4psBDSszoaBXg28iWdJPAueLPJSKqtbEsf7QuCh4X97lOv5xAMch\_\_B94DR6H8PdP-VQiL55T\_gBLsGLspuCD3hPi0AaPY8YLDeHc-83nDQCrCEv7aIzEDmVzTYyT1Tgoogle.ru/921617312913923061357337295847030576760\*OGPC65517568-1:google.ru/10882447276803058279537792730930576760\*
12. PREFf1=50000000&f5=30youtube.com/1088327003955230723613351366065530576762\*VISITOR\_INFO1\_LIVEfxQXUfeqbVYyoutube.com/9216288936448030625745348928420130576762\*
13. WMF-Last-Access-Global26-Feb-2017wikipedia.org921767525836830583117178291599430576762\*
14. mrcuD9C958B34FB6477CD1A713E647B2mail.ru/1024126553267231311018249122716830576763\*FTID0mail.ru/102465780121634459479256070285130576763\*VID0cOnFd3EnDHY0000060C14nY:::mail.ru/1024114035456030650390271085006030576763\*bR0MEAJCX/QcAalztBljbeENpKjUhhhea4AMAAAhnFz+VAAAAmail.ru/102426878105630650189255214251330576763\*Mpop1488146273:6c5d437307746974190502190805001b0305061d07094b6a515f475a020608081f05007a1656585b445b5e5e5b6e42565d585d0f00135f5950551f4b40:***личные\_данные***:mail.ru/1024214456307230594868254199941730576763\*tobLD1AAAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAgAAAADABQGzgcAmail.ru/1024175166899230612973252949932730576763\*p8VMLAJa3swAAmail.ru/1024227507225630723614253293721130576763\*searchuid8882036241488144017mail.ru/1024130553267231311018253371823830576763\*
15. remixlang0vk.com/1024335115059230650873196036978330576764\*remixlhk1dc4ec754b1d0624fbvk.com/1024216302515230650013196036978330576764\*remixflash24.0.0vk.com/1088183485849630582799196380681330576764\*remixscreen\_depth24vk.com/1088398878105630650189196380681330576764\*remixdt0vk.com/1088398878105630650189196665694330576764\*
16. mobile0championat.com/102468833881632108254381286435530576764\*\_gaGA1.2.1200082901.1488146922championat.com/1088358010496030723615382559307130576764\*\_gat1championat.com/1088123255526430576766382559307130576764\*\_ym\_uid1488146923754421411championat.com/108875933721630721604382856182030576764\*last\_visit1488136122679::1488146922679championat.com/1088243142272030777930382943029730576764\*\_ym\_isad2championat.com/1088226798412830576932382943029730576764\*\_ym\_visorc\_41870499bchampionat.com/108835765337630576769383757185430576764\*mp\_40a18f2536e25f9bd2bf60308b3bdfef\_mixpanel%7B%22distinct\_id%22%3A%20%2215a7c780012779-08a90fa5ce5d44-1e221f51-100200-15a7c780013512%22%2C%22%24initial\_referrer%22%3A%20%22%24direct%22%2C%22%24initial\_referring\_domain%22%3A%20%22%24direct%22%7Dchampionat.com/1088156381376030650190384089206730576764\*mp\_mixpanel\_\_c0championat.com/108824909606430576966384089206730576764\*
17. Анализ структуры и содержания:

Cookie файлы состоят из имен посещенных сайтов, содержат информацию о перемещениях по сайту, позволяют получать сведения о предпочтениях и запросах. При авторизации на сайте, также сохраняются личные данные пользователя. Если злоумышленник сможет получить доступ к cookie файлам, то в его руках могут оказаться личные данные пользователя, с помощью которых может быть проведен взлом с последующей кражей информации.

1. Список сайтов, добавленных в “Ограниченные узлы”:

1 google.ru

1. youtube.com

3. ru.wikipedia.org

1. mail.ru
2. vk.com
3. championat.com
4. При добавлении сайта в “Ограниченные узлы” cookies не были получены.
5. Так как cookies получены не были, то никакая информация не может быть доступна злоумышленнику.
6. Ответы на контрольные вопросы:
7. Cookies используются для: аутентификации пользователя; хранения персональных предпочтений и настроек пользователя; отслеживания состояния сеанса доступа пользователя; ведения статистики о пользователях.
8. Изначально в зоне “Ограниченные узлы” нет сайтов, пользователь по своему усмотрению может помещать туда сайты.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Настройки безопасности | Функциональный  смысл | Значение по  умолчанию | Рекомендованное  значение | Обоснование |
| xaml-приложения веб-обозревателя | XAML-приложения браузера (XBAP) объединяет возможности веб-приложений и многофункциональных клиентских приложений. | включить | отключить | Чтобы злоумышленник не мог получить доступ к информации с помощью xaml-приложения |
| xps-документы | Формат документа, который можно использовать для просмотра, сохранения, подписи и защиты содержимого документа. | включить | отключить | Чтобы злоумышленник не мог получить доступ к информации с помощью xps-документы |
| свободный xaml | Свободные файлы XAML являются XAML-файлами, которые не могут быть идентифицированы с помощью пакета URI. Это означает, что они не являются файлами ресурсов, содержимого или начального узла. | включить | отключить | Чтобы злоумышленник не мог получить доступ к информации с помощью свободных xaml |
| Скачивание файлов | Эта настройка позволяет управлять разрешением загрузки файлов из выбранной вами зоны | включить | отключить | Чтобы пользователь не скачал файл, содержащий вирус |
| Скачивание  шрифта | Текущая настройка позволяет управлять разрешением загрузки HTML-шрифтов с веб-страниц этой зоны. | включить | отключить | Чтобы пользователь не скачал шрифт, содержащий вирус |
| запуск компонентов не снабженных сертификатом Authenticode | Authenticode — технология корпорации Майкрософт, использующая стандартную для отрасли криптографию в целях подписания кода приложения цифровым сертификатом, который удостоверяет подлинность издателя приложения. | включить | отключить | Такая настройка, так как компоненты, не снабженные сертификатом Authenticode  Могут содержать вредоносное ПО |
| Запуск компонентов, снабженных сертификатом Authenticode | Эта настройка позволяет управлять выполнением компонентов .NET Framework из Internet Explorer, подписанных с помощью Authenticode. | включить | отключить | Такая настройка так как, такие компоненты могут быть использованы злоумышленником для получения информации |
| Разрешения для компонентов с манифестами | Манифесты компонентов — это файлы, в которых содержатся списки важных параметров и данных компонентов. | Высокий  уровень  безопасности | отключить | Такая настройка, чтобы злоумышленник не получил сведения о важных параметрах и данных компонентов |
| вход | Этот параметр позволяет управлять настройкой параметров входа | Автоматический вход в сеть только в зоне интрасети | Запрос имени пароля и пользователя | Такая настройка, чтобы только пользователи конкретной сети имели к ней доступ |
| Блокировать всплывающие окна | При помощи текущего параметра можно управлять появлением нежелательных всплывающих окон. | Включить | включить | При помощи текущего параметра можно управлять появлением нежелательных всплывающих окон. |
| Веб-узлы зон Интернета с меньшими правами могут открывать узлы из этой зоны | Этот параметр позволяет управлять переходом в эту зону веб-узлов зон с меньшими правами | включить | отключить | Если данный параметр отключен, потенциально опасные переходы запрещены. |
| Включать путь к локальному каталогу при загрузке файлов на сервер | Текущая настройка определяет, будут ли передаваться сведения о локальном пути при загрузке файла через HTML-форму. | включить | отключить | Если этот параметр не активен, то сведения о пути будут удаляться при загрузке файла через HTML-форму, и злоумышленник не получит доступ к данным |
| Возможность пробной проверки MIME | Эта функция предотвращает изменение типа файла на другой, более опасный. | включить | отключить | Если этот параметр выключен, то процессы Internet Explorer  будут разрешать пробной проверке MIME обработку файла как файла потенциально более опасного типа. |
| Доступ к источника данных за пределами домена | Эта настройка управляет доступом Internet Explorer к данным другой зоны безопасности с помощью парсера MSXML (Microsoft XML) или ADO (ActiveX Data Objects). | отключить | отключить | Такая настройка, чтобы не открывать потенциально опасные файлы |
| Запуск программ и небезопасных файлов | Текущая настройка определяет, отображается ли запрос «Открытый файл - предупреждение системы безопасности» при запуске исполняемых или других небезопасных файлов | предлагать | предлагать | Текущая настройка определяет, отображается ли запрос «Открытый файл - предупреждение системы безопасности» при запуске исполняемых или других небезопасных файлов |
| Запуск программ и файлов в окне IFRAME | Данный параметр системного реестра позволяет управлять данными о том, можно ли запускать приложения и загружать файлы по ссылкам в окнах IFRAME на HTML-страницах в этой зоне. | предлагать | отключить | Данную настройку нужно отключить, чтобы не запускать приложения и не загружать файлы в окнах IFRAME на страницах в этой зоне. |
| Использовать фильтр SmartScreen | Параметр определяет, сканирует ли фильтр фишинга страницы в данной зоне. | включить | включить | Параметр определяет, сканирует ли фильтр фишинга страницы в данной зоне. |
| Не запрашивать сертификат клиента, когда он отсутствует или имеется только один | Следующая настройка позволяет управлять получением пользователями запроса выбора сертификата, если он отсутствует или имеется в единственном числе. | отключить | отключить | Следующая настройка позволяет управлять получением пользователями запроса выбора сертификата, если он отсутствует или имеется в единственном числе. |
| Отображение разнородного содержимого | Данная настройка позволяет вам управлять отображением небезопасных элементов и предупреждениями безопасности об отображении веб-страниц, содержащих как безопасные, так и небезопасные элементы. | предлагать | предлагать | Данная настройка позволяет вам управлять отображением небезопасных элементов и предупреждениями безопасности об отображении веб-страниц, содержащих как безопасные, так и небезопасные элементы. |
| Передача незашифрованных данных форм | Текущая настройка позволяет управлять разрешением передачи данных HTML-форм на веб-страницах этой зоны. | включить | предлагать | Если выбран параметр «Предлагать», вы получите запрос отправки данных HTML-форм на веб-страницах этой зоны и сможете контролировать какие данные, следует отправлять |
| Перетаскивание или копирование и вставка файлов | Эта настройка позволят выбирать, сможете ли вы перетаскивать или копировать и вставлять файлы из источника в пределах зоны. | включить | предлагать | Если выбрана такая настройка, то вам придется самим выбирать, будете ли вы перетаскивать файлы из данной зоны, и тогда будет меньше шансов, что данные будут перехвачены |
| Переход между окнами и фреймами через разные домены | Данный параметр позволяет управлять открытием вложенных кадров и доступом к приложениям разных доменов. | отключить | отключить | Данный параметр позволяет управлять открытием вложенных кадров и доступом к приложениям разных доменов. |
| Разрешать запущенные скриптом окна без ограничений на размеры и положение | Данная настройка позволяет управлять ограничениями запускаемых сценариями всплывающих окон и окон со строками заголовка и состояния. | отключить | отключить | Данная настройка позволяет управлять ограничениями запускаемых сценариями всплывающих окон и окон со строками заголовка и состояния. |
| Разрешить веб-страницам использовать ограниченные протоколы для активного содержимого | Данная настройка позволяет вам определить, можно ли использовать ограниченные протоколы для активного содержимого веб-страниц. | отключить | отключить | Данная настройка позволяет вам определить, можно ли использовать ограниченные протоколы для активного содержимого веб-страниц. |
| Разрешить веб-узлам открывать окна без строки адреса или строки состояния | Текущая настройка определяет, могут ли веб-узлы открывать новые окна Internet Explorer без строки состояния или строки адреса. | включить | отключить | Такая настройка нужна, чтобы пользователь через строки адреса мог следить за открываемыми сайтами |
| Разрешить метаобновление | Эта настройка позволяет выбирать, может ли браузер выполнять редирект на другую веб-страницу, если автор веб-страницы использует тег метаобновления для перенаправления на другую веб-страницу. | включить | отключить | Такая настройка нужна ,чтобы пользователя автоматически не могло перенести на какую-то другую страницу |
| Включить перетаскивание содержимого из разных доменов между окнами | Этот параметр политики позволяет задавать возможность перетаскивания содержимого из одного домена в другой, когда исходный и конечный пункты размещения находятся в одном окне. | отключить | отключить | Такая настройка нужна, чтобы содержимое одного домена не попадало в другое, так как таким образом информация может быть похищена |
| Включить перетаскивание содержимого из разных доменов между окнами | Этот параметр политики позволяет задавать возможность перетаскивания содержимого из одного домена в другой, когда исходный и конечный пункты размещения находятся в разных окнах | отключить | отключить | Такая настройка нужна, чтобы содержимое одного домена не попадало в другое, так как таким образом информация может быть похищена |
| Разрешить скрипты для элемента управления обозревателем Internet Explorer | Этот параметр определяет, может ли страница управлять внедренными элементами управления веб-браузера через скрипт. | отключить | отключить | Такая настройка нужна, чтобы злоумышленник не мог использовать заранее прописанные скрипты |
| Преобразование для просмотра фильтров прежних версий | Этот параметр политики указывает, будет ли Internet Explorer преобразовывать визуальные фильтры прежних версий в данной зоне. | включить | отключить | Такая настройка нужна, чтобы не могло произойти взлома с помощью фильтров предыдущих версий |
| Устойчивость данных пользователя | Данная настройка позволяет управлять сохранением на жестком диске информации в журнале браузера, в папке избранного или в хранилище XML. | включить | отключить | Такая настройка нужна, чтобы пользователь не мог установить элемнты из этой рабочей зоны на рабочий стол, так они могут содержать вредоносное ПО |
| Разрешить установку .NET Framework | Данная настройка представляет установку компонентов среды выполнения WinFX. | включить | отключить | Такая настройка, чтобы не могли установиться нежелательные компоненты |
| Активные скрипты | Этот параметр позволяет управлять разрешением выполнения кодов сценариев на веб-страницах данной зоны. | отключить | отключить | Такая настройка нужна, чтобы злоумышленник не смог воспользоваться заранее прописанными скриптами |
| Включить фильтр XSS | Этот параметр определяет обнаружение и предотвращение работы фильтра запуска скриптов между узлами (XSS) в указанной вами зоне. | включить | включить | При включении этого параметра, фильтр XSS будет включен для всех узлов в этой зоне, и будет предотвращать запуск скриптов |
| Выполнять скрипты приложений Java | Данный параметр позволяет вам управлять разрешениями для приложений Java. | включить | отключить | Такая настройка нужна, чтобы не запускались приложения Java, так как они могут содержать вредоносное ПО |
| Разрешить веб-узлам запрашивать информацию с помощью окон со сценариями | Текущая настройка определяет, отображаются ли диалоговые окна запросов сценариев автоматически. | включить | отключить | Такая настройка нужна, чтобы диалоговые окна отображались только по запросу пользователя |
| Разрешить обновление строки состояния через скрипт | Данный параметр системного реестра позволяет управлять возможностью сценария обновлять строку состояния в пределах зоны. | включить | отключить | Выбор данной настройки нужен для того, чтобы скрипт не мог автоматически обновлять строку состояния |
| Разрешить программный доступ к буферу обмена | Эта настройка позволяет управлять скриптами, выполняющими операции с буфером обмена | предлагать | отключить | Выбор данной настройки нужен для того, чтобы скрипт не мог автоматически выполнять операции с буфером обмена |
| Автоматические запросы элементов управления ActiveX | Данная настройка позволяет определять, можно ли автоматически получать запрос при установке элементов управления ActiveX. | отключить | отключить | Выбор данной настройки нужен для того, чтобы пользователь в любой момент мог запрашивать элементы управления |
| Выполнять скрипты элементов ActiveX, помеченных как безопасные | Текущая настройка позволяет управлять взаимодействием скриптов и элементов управления ActiveX, помеченных как безопасные для выполнения скриптов. | включить | отключить | Выбор данной настройки нужен для того, чтобы пользователь мог вмешиваться в работу скриптов |
| Запуск элементов ActiveX и модулей подключения | Данная настройка позволяет управлять запуском элементов управления ActiveX и подключаемых модулей на страницах указанной зоны | включить | отключить | Выбор данной настройки нужен для того, чтобы пользователь мог сам определять какие элементы управления запускать |
| Включить Фильтрацию ActiveX | Фильтрация ActiveX в Internet Explorer запрещает сайтам устанавливать и использовать приложения, с помощью которых веб-сайты предоставляют контент | включить | включить | Выбор данной настройки нужен для того, чтобы сайты не могли устанавливать на ПК приложения, с помощью которых у них предоставляют контент |
| Поведение двоичного кодов и скриптов | Эта настройка управляет динамическим поведением двоичного кода и скриптов: компонентами, инкапсулирующими специфические возможности элементов HTML, к которым они были присоединены. | включить | отключить | Выбор данной настройки нужен для того, чтобы поведение двоичного кода и скриптов полностью было подчинено пользователю |
| Показывать видео и анимацию на веб-странице, не использующей внешний медиапроигрыватель | Данный параметр позволяет проигрывать видео и анимацию через тег dynsrc/img в указанной зоне. | отключить | отключить | Выбор данной настройки нужен для того, чтобы пользователь не мог просматривать потенциально опасные видео |
| Разрешить использовать ActiveX без запроса только утвержденным доменам | Этот параметр определяет отображение запроса на разрешение элементов управления ActiveX для других веб-сайтов помимо веб-сайта, установившего элементы управления ActiveX. | отключить | включить | При включении этого параметра отобразится запрос, прежде чем будет возможно запустить элементы управления ActiveX с веб-сайтов в этой зоне, и пользователь сам будет контролировать процесс |
| Разрешить запуск элементов управления ActiveX, которые не использовались ранее, без предупреждения | Текущая настройка отвечает за использование на веб-сайтах элементов управления ActiveX, которые ранее использовались только с соответствующими предупреждениями. | включить | отключить | Выбор данной настройки нужен для того, чтобы пользователь сам мог выбирать, какие элементы управления запускать |
| Разрешить сценарии | Эта настройка позволяет управлять выполнением скриптов | отключить | отключить | Выбор данной настройки нужен для того, чтобы пользователь не использовал скрипты, то есть заранее прописанные сценарии. Это нужно, так как скрипты могут использовать злоумышленники |
| Загрузка неподписанных элементов ActiveX | Следующий параметр позволяет управлять разрешением на загрузку неподписанных элементов ActiveX из данной зоны. | отключить | отключить | Выбор данной настройки обоснован тем, что такие элементы потенциально опасны |
| Загрузка подписанных элементов ActiveX | Этот параметр управляет загрузкой пользователями подписанных элементов управления ActiveX с веб-страниц в данной зоне. | предлагать | отключить | Выбор данной настройки обоснован тем, чтобы пользователь сам контролировал, какие файлы скачивает |

1. JavaScript обычно используется как встраиваемый язык для программного доступа к объектам приложений. Наиболее широкое применение находит в браузерах как язык сценариев для придания интерактивности веб-страницам. С помощью Javascript злоумышленник может написать сценарий, который будет нарушать конфиденциальность информации. Примером такой уязвимости является JavaScript Hijacking, позволяющую злоумышленникам получать доступ к конфиденциальной информации, содержащуюся в JS-сообщениях. С помощью такой атаки можно было украсть список контактов в Google Gmail, так как Google хранил список контактов текущего пользователя в незащищенном JS-формате, таким образом злоумышленник мог украсть его.  
   Основной способ защиты от JavaScript Hijacking – предотвращение прямого выполнения JS ответа

Наиболее совершенным способом защиты против JavaScript Hijacking является выбор и той и другой тактики.

1. Платформа для предпочтений конфиденциальности (англ. Platform for Privacy Preferences или **P3P**) — это протокол, позволяющий сайтам информировать браузер о предполагаемом получении личных данных пользователя.

9. Выводы по работе:

Cookies содержат разную информацию, такую как, личные данные пользователя, сайты, которые он посещал, его предпочтения и запросы.

Несмотря на то, что Cookies могут быть полезны, они также несут угрозу конфиденциальности пользователя, так как могут быть украдены злоумышленником и тот сможет получить доступ к личной информации.

Для обеспечения безопасности, необходимо правильно настраивать параметры безопасности браузера.