АНАЛИЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ БЕЗОПАСНОСТИ В КРУПНОМАСШТАБНЫХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ С КЛИЕНТАМИ НА ОСНОВЕ WEB-БРАУЗЕРОВ И СЕРВИС-БРАУЗЕРОВ

Курако Е.А., Орлов В.Л.

Институт проблем управления им. В.А. Трапезникова,
Россия, г. Москва, ул. Профсоюзная, д.65
ovl@ipu.ru, кеа@ipu.ru

Аннотация: Проводится сравнительный анализ применения средств обеспечения безопасности в крупномасштабных системах двух типов: с клиентами на основе web-браузеров и с клиентами на основе сервис-браузеров. Оцениваются методы борьбы с атаками для браузеров двух типов, указываются достоинства и недостатки.

Ключевые слова: средства безопасности, web-браузер, сервис-браузер, угрозы, сложные сети.

Введение

В последнее время крупномасштабные системы со сложной сетевой структурой (сложные сети) часто используют в качестве клиентов web-браузеры. Это дает определенные преимущества, так как не требует инсталляции клиентов (иногда разного типа) на рабочих местах пользователей. Для функционирования достаточно, чтобы на рабочем месте была установлена операционная система с типовым браузером, обеспечивающим доступ к Интернету или выделенной сети. В ряде случаев используются также дополнительные расширения браузеров, реализующие специальные функции, например, функции шифрования и электронной подписи. Нужно иметь ввиду, что в этом случае для разных браузеров используются различные виды расширений. Но возникающая проблема обычно разрешается ограничением числа используемых типов браузеров в рамках проектируемой системы. Каждый web-браузер работает по протоколу HTTP, отправляя HTTP – запросы на web-сервер [1] и получая от него HTTP-ответы (рис.1).

Рис. 7. Схема информационной системы с клиентами на основе web-браузеров

Web-сервер обычно взаимодействует с сервером приложений, который связывается с базой данных, хранящей информацию. Отметим, что взаимодействие web-сервера с сервером приложений на уровне, следующим за HTTP, может вестись по самым разным протоколам.

Другая технология подразумевает использование сервис-браузера [2,3] в качестве клиента (рис.2).

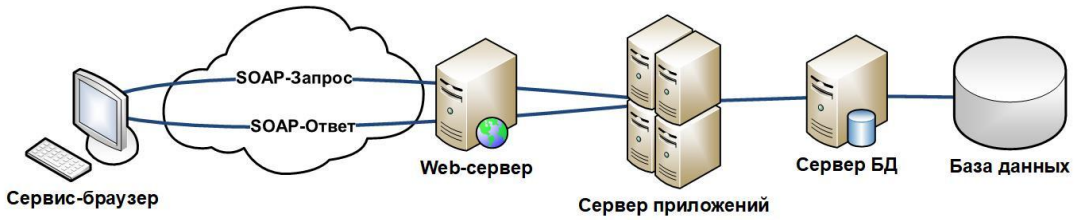

Рис. 8. Схема системы с клиентами на основе сервис-браузеров

Основное отличие web-браузера и сервис-браузера состоит в том, что web-браузер оперирует с HTML-страницами или по крайней мере с операциями для их модификации. Заметим, что современный подход подразумевает не просто передачу и отображение страниц, но и их коррекцию. При этом для обновления страницы в web-браузере достаточно передать информацию на сервер

приложений и получить данные для изменения части страницы. Реально коррекция же в web-браузере происходит с использованием языка JavaScript.

Здесь важна одна тенденция: по мере развития web-программирования существенная часть клиентских программ начинает выполняться непосредственно в web-браузерах, то есть на компьютерах клиента. И это понятно. Зачем (как это предполагалось в классическом варианте) передавать команды на сервер приложений, там изменять HTML-страницу и возвращать ее назад. Достаточно возвратить данные из сервера приложений и с помощью JavaScript обновить страницу на месте.

Но тут возникают несколько проблем. Во-первых, web-браузер весьма сложная программа. И хотя обработка HTML, JavaScript и таблиц стилей CSS проводится по одинаковым правилам, но существуют различные толкования, особенности развития, в результате чего разные web-браузеры могут по-разному отображать содержимое. Поэтому реально ориентация при разработке систем идет на весьма ограниченный набор браузеров, которые широко известны. Но с точки зрения безопасности использование ограниченного набора программ, использующих одинаковые протоколы, ослабляет защитные свойства системы. Во-вторых, вся обработка информации на клиенте идет в режиме интерпретации скриптов, что конечно же дает замедление работы.

Эти недостатки для информационных систем призван устранить сервис-браузер [2,3]. Основное отличие сервис-браузера от web-браузера заключается в следующем:

1) у сервис-браузера в качестве программ, которые пересылаются клиенту по мере их изменения и работают с его стороны, используются не интерпретируемые скрипты, а выполняемые программы, которые в основном разрабатываются на языках программирования с механизмом трансляции;
2) сервис-браузер не получает готовые HTML-страницы, а взаимодействует с сервером приложений исключительно за счет вызовов web-сервисов с использованием web-сервера, как промежуточного звена, и получении в ответах данных для обработки;
3) сервис-браузер является компактной программой, так как в его задачу не входит обработка всего того, чем нагружены обычные браузеры, то есть обработкой HTML, JavaScript, CSS, а он занят только вызовом программных модулей, полученных ранее клиентом и взаимодействием с web-сервисами на сервере приложений.

1 Основные угрозы для web-браузеров

Угрозы для web-браузеров можно разделить на две категории:

- общесистемные;
- определяемые спецификой работы браузера.

Общесистемные не относятся собственно к web-браузеру и HTML-страницам. Более того они могут и не иметь отношения к информационным системам, с которыми работает в настоящее время браузер. Но web-браузер выполняется в среде, созданной операционной системой и взаимодействует с другими компьютерами сложной сети. Более того, в операционной системе запускаются и другие сетевые программы, например, электронная почта, программа сетевой печати, которые по другим протоколам обеспечивают взаимодействие в сложной сети. Более того, в общем случае web-браузер может обеспечивать взаимодействие с другими сайтами сети, не имеющими отношения к информационной системе, которую он обслуживает.

В результате можно утверждать, что при использовании web-браузера в качестве клиента есть вероятность подвергнуться угрозам, характерным для других программ, работающими под управлением операционной системы, имеющий выход в сеть.

Выделим наиболее известные общесистемные угрозы [4], характерные как для частных, так и для общих сетей:

- угроза появления программ «троянов»;
- угроза проникновения на компьютер программ «руткитов»;
- угроза распространения программ «червей»;
- вирусная угроза;
- угроза отказа в обслуживании.

Все эти угрозы в основном отличаются тем, что они распространяются и начинают функционировать вне зависимости от конкретных прикладных программ, работающих на компьютере. Можно не включать в этот список общесистемные комплексы общего назначения, распространяющие произвольную информацию по сети, такие как электронная почта.

Трояны и руткиты появляются в системе как «нужные» программы, причем руткиты часто маскируются под системные программы, черви распространяются самостоятельно, используя, в частности электронную почту. Вирусная угроза может использовать механизмы распространения приведенных выше угроз, но чаще всего распространяются через файловую систему, например, используя флеш-носители.

Угроза отказа в обслуживании, исходящая из одного сетевого компьютера (DoS) или многих компьютеров (DDoS), в этой классификации также отнесена к общесистемным, так как большинство атак этого вида не привязано к конкретным прикладным программам, а активно загружает сетевые каналы, дисковую и оперативную память и прочие ресурсы. В то же время это не означает, что исключаются атаки такого типа на прикладные ресурсы. Например, можно размножать запросы к определенной информационной системе.

Следующий вид – это угрозы, определяемые спецификой работы web-браузера и используемых им протоколов. Что важно, web-браузер в нашем случае взаимодействует с web-приложениями и базами данных. Поэтому мы должны рассматривать угрозы не только непосредственно компьютеру с web-браузером, но всей системе, использующий этот тип браузера в качестве клиента.

Выделим основные виды угроз данного типа:

- фишинг (Phishing) - разновидность угрозы, которая предназначена для получения идентификационных данных (например, пары логин-пароль);
- спуфинг (Spoofing) может использоваться как развитие фишинга для организации перехода на сайт подмены, где пользователь может ввести свои идентификационные данные, передав их таким образом злоумышленнику;
- межсайтовый скриптинг XSS (*Cross-Site Scripting*) это угроза, связанная с возможным получением от сервера скрипта, измененного еще в процессе подготовки или передачи. Вредоносный скрипт выполняется на компьютере клиента и может обратиться к сайту злоумышленника для передачи информации. Межсайтовый скриптинг XSS по существу представляет угрозу введения сценариев в текст HTML-страницы, то есть инъекции фрагментов сценариев;
- межсайтовая подделка запроса CSRF (cross-site request forgery) представляет собой угрозу выполнения операций на других сайтах от имени действующего пользователя, используя его учётные данные и не ставя его (пользователя) в известность. Эта угроза также основывается на инъекции фрагментов сценариев, как и в XSS, но кроме того, осуществляется использование дополнительной подтверждающей информации (чаще всего cookies) в рамках принятых процедур обмена с обслуживающим сервером (например, сервером банка);
- угроза SQL-инъекций основана на том, что хранение данных в серверной группе осуществляется обычно на серверах базы данных. На этих серверах используется распространенный язык SQL, фрагменты которого достаточно легко локализовать, если они находятся в тексте HTML-страницы, изменить и передать на выполнение серверу баз данных. При этом ущерб может быть значительным;
- угроза доступа к данным о паролях требует обеспечения надежного хранения паролей, обычно зашифрованных с использованием однонаправленного шифрования [5];
- угроза выхода в Интернет по решению оператора.

2 Механизмы работы сервис-браузера

2.1 Особенности работы сервис-браузера

Сервис-браузер взаимодействует с сервером приложений без использования HTML-страниц, а передача информации обеспечивается путем вызова сервисов, расположенных на серверах приложений. В то же время следует помнить, что сервис-браузер является браузером, а значит он не должен включать в свой состав конкретные прикладные программы и формы отображения. Это обеспечивается следующим образом. Прикладные программы в общем случае пишутся на одном из языков программирования, имеющим дополнительные средства для вызова web-сервисов. Это может быть C#, Java, Python и другие. Все эти программы в дальнейшем изложении называются «модули». Модули размещаются в хранилище на сервере приложений, но предназначены для выполнения на клиенте (рис.3). Сервис-браузер может по команде оператора вызывать тот или иной модуль с сервера и оставлять у себя на клиенте в кэше для дальнейшего выполнения. То есть вместо HTML-страниц с оформлением средствами CSS и программами JavaScript, выполняющимися на традиционном web-браузере, в сервис-браузер передаются модули, написанные на одном из языков программирования, по существу выполняющие схожие функции.

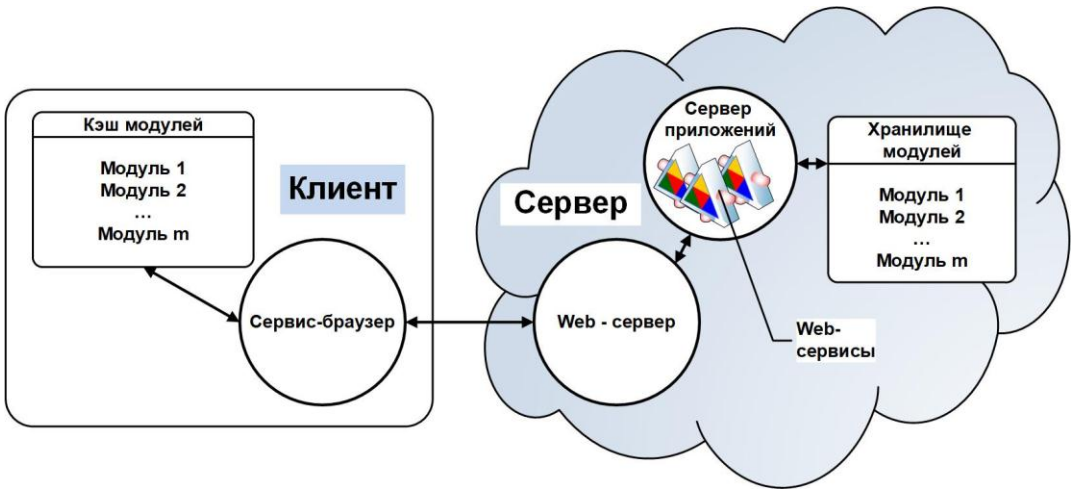

Рис. 9. Загрузка модулей в кэш

Следует отметить две особенности модулей:

1) клиенты, работающие с одной системой, могут использовать различные наборы модулей, входящие в общий набор системы, а значит у каждого клиента может быть свой кэш;

2) при использовании в информационных системах виды оформления и алгоритмы в отличие от данных меняются достаточно редко. Следовательно, процесс передачи модулей из хранилища в кэш осуществляется не часто. В основном это действие происходит при обновлении содержимого хранилища, но в этом случае передача в кэш происходит при очередном обращении к модулю, который обновился. Отметим, что вполне можно представить себе систему, где такое обновление происходит раз в год. Таким образом, обмен модулями практически не нагружает систему в целом.

В то же время, если мы подключаем к системе нового клиента, то на подключаемый компьютер устанавливается только сервис-браузер, который представляет собой весьма компактную программу. Но кэш модулей при его запуске заполняется автоматически из серверного хранилища модулей.

То есть на первой стадии работы клиента подготавливаются все программы и шаблоны оформления. Дальше идет только обмен данными (рис.4). Сервис-браузер предоставляет оператору список доступных ему модулей.

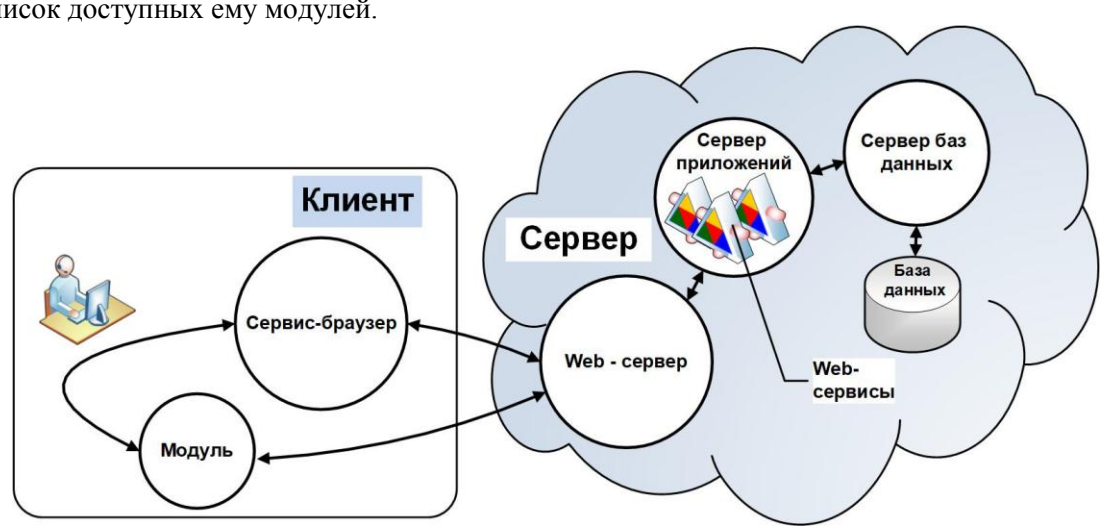

Рис. 10. Работа модулей с данными

Оператор активизирует нужный ему модуль, вводит информацию и запрос из модуля поступает сервисам сервера приложений, а затем на сервер баз данных и собственно в базу данных. Ответ идет тем же путем в обратном направлении.

Нужно отметить, что клиент может работать с несколькими информационными системами. В таком случае появляются несколько кэшей для модулей и несколько изолированных друг от друга баз данных [6].

2.2 Средства защиты информации в сервис-браузерах

Мы видим, что разные клиенты используют разные наборы модулей. Из этого следует, что при использовании технологии сервис-браузера необходимо уже на ранней стадии включение общего

механизма авторизации. То есть каждому пользователю должны быть доступны свои ресурсы. Подключение авторизации уже на первом этапе разработки любой системы дает определенные преимущества для общего проектирования.

Но наряду с механизмом авторизации также на ранней стадии должен быть подключен еще один механизм - механизм аутентификации. Ведь для авторизации пар пользователь-модуль нужно установить возможности того или иного пользователя, а значит перед этим необходимо идентифицировать пользователя – то есть провести аутентификацию. Аутентификация в свою очередь подразумевает подключение средств защиты информации.

Все эти возможности реализуются в сервис-браузере и в сервере приложений. Причем возможен вариант реализации, когда выделяется отдельный сервер приложений для организации защиты информации.

3 Сравнение угроз для web-браузеров и сервис-браузеров

Рассмотрим действие угроз для систем, использующих web-браузеры и сервис-браузеры.

3.1 Сравнение общесистемных угроз для различных браузеров

Рассмотрим основные общесистемные угрозы (Таблица 1).

Таблица 2.Сравнение основных общесистемных угроз для web-браузеров и сервис-браузеров

№	Название	Web-браузеры	Сервис-браузеры
1	Трояны	да	да
2	Руткиты	да	да
3	Черви	да	да
4	Вирусы	да	да
5	Отказ в обслуживании	да	да

Как мы видим из таблицы 1, списки общесистемных угроз для web-браузеров и сервис-браузеров практически не отличаются. Вместе с тем нужно иметь ввиду, что черви чаще всего распространяются по электронной почте, трояны приходят в основном через web-браузеры, руткиты поступают через web-браузеры и файловую систему, вирусы используют все перечисленные пути, а общесистемный отказ в обслуживании инициируется через сетевые механизмы.

Так как при использовании сервис-браузеров, как основы информационных систем, таких программ, как web-браузеры в системе нет принципиально. Следовательно, распространение троянов в сети затруднено, а перемещение руткитов и вирусов ограничено по той же причине, то можно считать, что системы с сервис-браузерами здесь имеют преимущество. Вместе с тем это преимущество может нивелироваться, если допускается применение на компьютерах web-браузеров для других целей, а также, если в операционной среде широко используется электронная почта.

Опасность общесистемного отказа в обслуживании для систем как одного, так и другого типа приблизительно одинакова, так как это связано с компьютерными атаками на уровне сетевых протоколов.

В целом можно сказать, что для комплексов с сервис-браузерами количество атак можно сократить, запретив использование web-браузеров на компьютерах информационной системы. В то же время можно свести их к минимуму для браузеров обоих типов, если вместо электронной почты использовать защищенный мессенджер. Также общий эффект дает использование межсетевых экранов - файрволов, протокола TLS и создание подсетей по типу VPN.

3.2 Сравнение специфических угроз для различных браузеров

Перечень основных угроз, характерные для браузеров рассматриваемых типов представлен в таблице 2.

Рассмотрим основное отличие web-браузеров и сервис-браузеров на уровне начальной аутентификации. Напомним, что механизм аутентификации у web-браузеров не присутствует как встроенный механизм. Такой механизм может быть добавлен с использованием плагинов, которые представляют собой расширение браузера. Вместе с тем возможно и использование JavaScript и соответствующих библиотек для него или реализация аутентификации разработчиками каждого прикладного web-приложения.

Таблица 3.Сравнение специфических угроз для web-браузеров и сервис-браузеров

№	Название	Web-браузеры	Сервис-браузеры
1	Фишинг	Конструирование поддельных сайтов для получения идентификационных данных	Не предоставляют визуальную информацию для конструирования поддельных сайтов
2	Спуфинг		
3	Межсайтинговый скриптинг	Возможное вредоносное изменение скриптов	Передача скриптов отсутствует
4	Межсайтинговая подделка запроса	Подделка запроса с использованием данных аутентификации другого сайта (например, cookies)	Cookies не используются
5	SQL-инъекции	Внедрение вредоносных SQL-выражений	Внедрение вредоносных SQL-выражений
6	Доступ к паролям	Хранение паролей в web-браузере допускается без надлежащей защиты. Возможен запрет	Пароли не хранятся в сервис-браузере
7	Несанкционированный выход в Интернет	Выход возможен. Требуется запрет	Выход в Интернет не предусмотрен

При начальной аутентификации на уровне web-браузера и сервера, как отмечалось выше, в качестве угрозы часто выступает механизм фишинга и спуфинга, который представляет собой конструирование поддельных сайтов со страничками ввода логина-пароля, внешне не отличающихся от настоящих. Эта пара, которая поступает от браузера к серверу (даже зашифрованная), может быть сохранена псевдо-сайтом и впоследствии использована злоумышленником.

Преимущество сервис-браузера здесь заключается в том, что первые процедуры начальной аутентификации производятся на клиенте. Здесь пользователю предоставляется форма ввода, при необходимости проводятся соответствующие операции, например, хеширование и осуществляется обмен с сервером приложений путем вызова web-сервисов. То есть, сервер в этом случае не является стороной, предоставляющей визуальную информацию, в связи с чем возможность его подделки существенно усложняется.

Межсайтинговый скриптинг связан с возможным изменением скриптов. Так как при использовании сервис-браузера скрипты принципиально не передаются, то эта угроза практически уходит. Есть вариант изменения модулей непосредственно в хранилище, но при тщательном проектировании и подписании электронной подписью помещаемых в хранилище моделей с последующей проверкой на стороне клиента надежность работы повышается.

Рассмотрим межсайтинговую подделку запроса. Прежде всего, обычно подделка базируется на коррекции скриптов в HTML-страницах и использовании cookies, которые своим присутствием подтверждают легитимность запроса. Так как сервис-браузер не применяет html-страницы и cookies, то эти угрозы здесь не актуальны. Но при использовании сервис- браузера отдаленный аналог можно найти в попытках вызова из своей системы модулей, принадлежащих другой системе. Но тут работают другие механизмы. Например,

- для доступа к модулю злоумышленник должен иметь меняющийся идентификатор сеанса атакуемой системы;
- ему должен быть известен набор закрытой серверной информации для получения пароля базы данных в конкретной системе.

Здесь важно то, что встроенный в сервис-браузер механизм защиты информации не позволяет делать элементарных ошибок, которые были бы возможны при его отсутствии.

Важен и вопрос SQL-инъекций. Как в системах с web-браузером, так и в системах с сервис-браузером многое зависит от правил формирования SQL-запросов. И там и там не рекомендуется размещать запросы на html-страницах и непосредственно в модулях. Такое размещение приводит к тому, что произвольное изменение SQL-запроса может привести к необратимым изменениям в базе данных. Чтобы этого не случилось, рекомендуется на уровне клиента осуществлять только ввод информации и указания, касающиеся этого ввода. Сами SQL-запросы размещаются либо непосредственно в базе данных в форме хранимых процедур, либо, в крайнем случае, в теле сервисов, при обязательной проверке входных данных.

Угроза доступа к данным о паролях как правило предоставляется web-браузерами, которые хранят пароли для доступа к различным приложениям. Однако практически эти процедуры хранения

рассчитаны на то, что доступ к компьютеру, на котором установлен web-браузер – ограничен. Если это правило не соблюдается, то пароли становятся легкой добычей злоумышленника. Поэтому при использовании в информационных системах хранение паролей средствами браузера не применяется. Что же касается сервис-браузера, то в рамках этой технологии вообще не предусматривается хранение паролей пользователей на стороне клиента. Все пароли хранятся только на сервере, причем они закрываются с использованием однонаправленного шифрования.

Что же касается угрозы выхода в Интернет по решению оператора, то такая возможность принципиально существует для систем, использующих web-браузеры. Естественно, при этом возникают проблемы получения через сеть различных вредоносных программ, поэтому в случае использования web-браузеров для информационных систем выход в Интернет ограничивают.

В системах с сервис-браузерами обратная ситуация. По умолчанию выход в Интернет закрыт и угроза получения по этому каналу программ, подготовленных злоумышленниками, практически исключается.

Заключение

При построении крупномасштабных информационных систем со сложной сетевой структурой в качестве клиентов в настоящее время широко используются web-браузеры, которые базируются на HTML-технологиях и исключают необходимость инсталляции прикладного программного обеспечения на компьютер каждого пользователя.

Наряду с web-браузерами также получили распространение сервис-браузеры, отличающиеся компактностью, встроенной защитой информации и использованием web-сервисов для обмена информацией.

Для оценки целесообразности применения тех или иных технологий проведен сравнительный анализ возможных угроз при использовании как web-браузеров, так и сервис-браузеров. Анализ показал, что в плане защиты от общесистемных угроз оба типа браузеров приблизительно равноценны. В случае возникновения специфических для браузеров угроз сервис-браузер имеет некоторое преимущество ввиду того, что многие компьютерные атаки используют уязвимости, основанные на технологиях использования HTML страниц и скриптов, размещаемых на этих страницах. Кроме того, встроенный в сервис-браузер механизм защиты информации позволяет, как правило, обойтись без сторонних средств для обеспечения безопасности.

Литература

1. *Klaus-Dieter Schewe, Bernhard Thalheim* Design and Development of Web Information Systems. – Berlin, Heidelberg: Springer, 2019. – P. 599.
2. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. М., 2017. Т. 8, № 9. С. 413-421.
3. *Kurako E.A. Orlov V.L.* Service-browser Architecture and Large-scale Information Systems // Proceedings of the 11th International Conference "Management of Large-Scale System Development" (MLSD). Moscow: IEEE, 2018. С. https://ieeexplore.ieee.org/document/8551831.
4. *Ido Dubrawsky* Eleventh Hour Security+. – Syngress, 2009. – P. 232
5. *Козлов А.Д., Орлов В.Л.* Методы и средства обеспечения информационной безопасности распределенных корпоративных систем. – М. ИПУ РАН,2018. -155с.
6. *Orlov V.L. Kurako E.A.* Organization and Management of a Multiple Functional Structure for Large-Scale Informational Processing Systems // Proceedings of the 13th International Conference "Management of Large-Scale System Development" (MLSD). Moscow: IEEE, 2020. С. https://ieeexplore.ieee.org/document/9247755/