СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
SIBERIAN FEDERAL UNIVERSITY

ПРОСПЕКТ СВОБОДНЫЙ- 2017

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ МОЛОДЫХ УЧЕНЫХ

ЭЛЕКТРОННЫЙ СБОРНИК МАТЕРИАЛОВ МЕЖДУНАРОДНОЙ КОНФЕРЕНЦИИ СТУДЕНТОВ, АСПИРАНТОВ И МОЛОДЫХ УЧЕНЫХ “ПРОСПЕКТ СВОБОДНЫЙ 2017” ПОСВЯЩЕННОЙ ГОДУ ЭКОЛОГИИ В РФ

КРАСНОЯРСК, СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
17-21 АПРЕЛЯ 2017 Г.

Министерство образования и науки Российской Федерации
ФГАОУ ВО «Сибирский федеральный университет»

Проспект Свободный - 2017

Материалы научной конференции
посвященной Году экологии в Российской Федерации
17-21 апреля 2017 г.

Электронное издание

Красноярск
СФУ
2017 г.

Прикладная математика, математическое моделирование, информационная безопасность

УДК 004.75

ВЕКТОР АТАКИ ТИПОВОЙ МЕДИЦИНСКОЙ НФОРМАЦИОННОЙСИСТЕМЫ

Хамутников В. А., Давыдов А. Н.

Научный руководитель доцент Демин С. Л.

Сибирский федеральный университет

В современном мире продолжается повсеместная информатизацияразличных сфер жизни общества. Сейчас компьютерные технологии используются в самых важных областях человеческой деятельности, где зачастую обрабатывается информация, представляющая интерес для злоумышленников.Поэтому тема информационной безопасности становится всё актуальней с каждым днём и затрагивает самые разнообразные отрасли, включая государственные информационные ресурсы, и в том числе медицинские информационные системы.

Здравоохранение особенно подвержено кибератакам, ввиду того, что в данной отрасли обрабатывается большой объем персональных данных. Рассматривая статистику кибератак за 2016 год, по данным исследования международной компании Gemalto, занимающейся безопасностью, видно, что самым компрометируемым типом информации оказались персональные данные.На долю хищения персональных данных пришлось 64% всех утечек информации, зафиксированных в первом полугодии 2016 года – или 621 инцидент, в результате которых было украдено более 294 миллионов записей. А наиболее часто атакуемой отраслью оказалось здравоохранение, на которую пришлось 27 % случаев утечки (рисунок 1) [1].

Рис. 1 – Утечка данных по отраслям

На основе вышеизложенного можно заключить, что безопасность информационных ресурсов отрасли здравоохранения, является одной из приоритетных задач государства.А

обеспечение безопасности связано с непрерывным выявлением новых векторов атак и последующим устранением сопутствующих уязвимостей систем.

В рамках данной статьи будет рассмотрен вектор атаки типовой медицинской информационной системы. Медицинская информационная система, далее МИС, представляет собой инструмент управления ресурсами медицинской организации и осуществляет такие функции, как хранение полной информации о пациенте в электронной медицинской карте, фиксация всех действий врачей, а также управление потоком пациентов.

Программное обеспечение МИС функционирует по принципу клиент-сервер. При исследовании безопасности клиент-серверных систем обработки информации, одним из важнейших аспектов является то, каким образом организовано сетевое взаимодействие. База данных МИС располагается в региональных центрах обработки данных, и соединение локальных сетей медицинских учреждений с ними осуществляется посредством шифрованных каналов передачи данных, создаваемых при помощи программно-аппаратных шлюзов безопасности, например, координаторов VipNet.Данные МИС, обрабатываемые в локальной сети до шлюза, передаются открыто, что может быть проверено любым сниффером, например, Wireshark. Данный факт создает пространство для инсайдерских атак, возможности перехвата трафика, а также реализациииатак типа «человек посередине».

Рассматриваемый вектор атаки направлен на использование технологий канального уровня сетевой модели OSI и основывается на несовершенстве сетей Ethernet, коммутации в них, а также незащищенном протоколе ARP. Предлагается рассмотреть две атаки: ARPpoisoning и MACflooding.

Протокол ARP предназначен для преобразования IP-адресов в MAC-адреса. Каждый сетевой хост в процессе взаимодействия с другими хостами сети формирует в кэш-памяти ARP-таблицу, в которой сохраняются IP и MAC адреса известных хостов, с которыми осуществлялся обмен информацией. Впоследствии, извлекая необходимые записи из ARP-кэша, хост может сразу указать в отправляемом фрейме физический адрес получателя, без необходимости опрашивать все хосты в своей подсети. Данный протокол является связующим звеном второго и третьего уровня сетевого взаимодействия OSI. Однако существует проблема, которая заключается в том, что протокол ARP не предусматривает аутентификации, поэтому хост будет всегда доверять данным полученным от другого хоста посредством данного протокола. [2]

Атака ARPpoisoning, или «отравление» ARP-таблицы, основывается на модификацииARP-таблицы жертвы, с целью подмены физического адреса хоста-собеседника, уже знакомого жертве, на физический адрес машины, с которой происходит атака. Подобная модификация осуществляется отправкой с атакующей машины фальшивого

ARP-ответа, в котором указывается обновленный фиктивный MAC-адрес для IP-адреса одного из хостов, с которым машина жертвы обменивается информацией.Согласно механизму работы протокола ARP, машина жертвы примет данный пакет и обновит свою ARP-таблицу. В дальнейшем, отправляя данные на IP-адрес доверенного хоста, эти данные будут приходить на машину атакующего. Во избежание возвращения ARP-таблицы жертвы к исходному виду, необходимо отправлять ARP-ответ не реже, чем каждые 30 секунд. В случае, когда необходимо сохранить коммуникацию жертвы с собеседником, атака ARP poisoning должна также проводиться и в отношении собеседника, а также необходима двухсторонняя пересылка получаемых пакетов, тем самым реализуется классическая атака «человека посередине» (рис. 2).

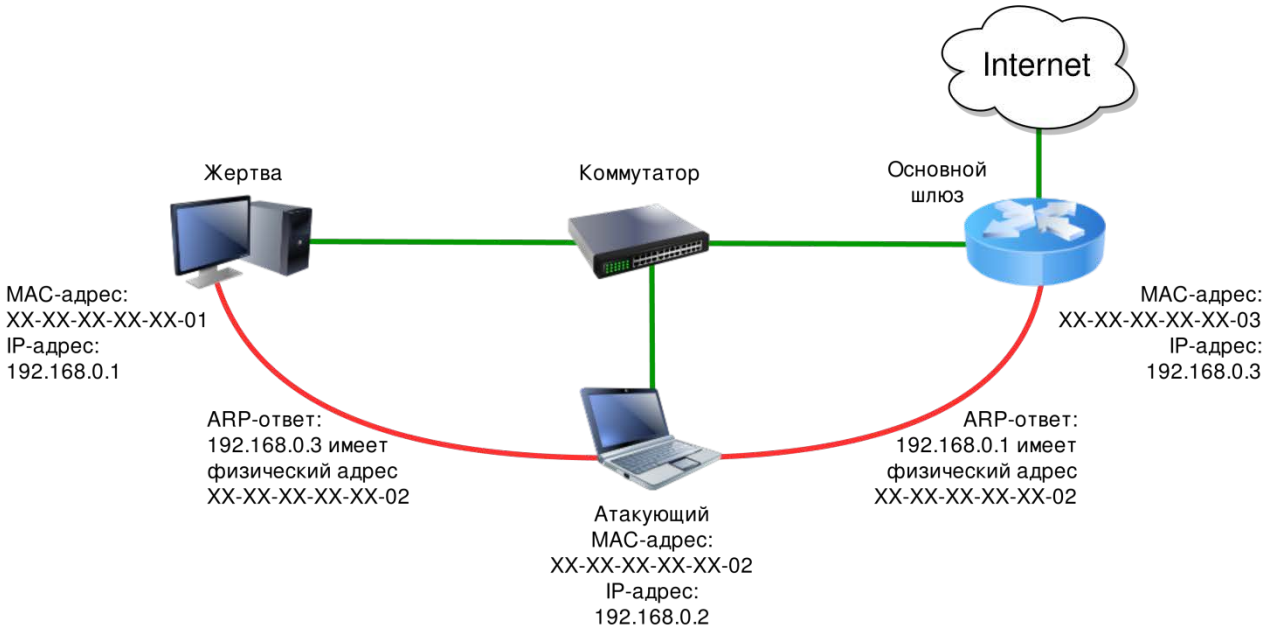

Рис. 2 – Атака ARP poisoning

Таким образом «отравив» ARP-кэш жертвы и хоста, являющего для жертвы основным шлюзом в таблице маршрутизации, становится возможным перехват трафика, передаваемого между клиентом МИС и региональным ЦОД. Перехватив аутентификационные данные оператора МИС, атакующий может авторизоваться в системе и получить доступ к конфиденциальной информации медицинского учреждения. При реализации данной атаки возможно использование готовых инструментов, таких как Ettercap и Cain&Abel.

Еще одной атакой канального уровня является атака MACflooding, или «затопление MAC-адресами», и направлена на коммутационное оборудование. Коммутатор способен хранить в своей памяти ограниченное количество физических адресов, поэтому в случае переполнения таблицы MAC-адресов, коммутатор зачастую переходит в режим концентратора, тем самым осуществляя ретрансляцию принимаемых данных во все свои

порты. Атака MACflooding заключается в интенсивной генерации фреймов с различными физическими адресами и отправке их на коммутатор.

Таким образом, в локальной сети медицинского учреждения,перегрузив коммутатор MAC-адресами, становится возможным перехватывать трафик соседних хостов, подключенных к данному коммутатору. Все дальнейшие действия сводятся к парсингу получаемого трафика, в котором также содержатся аутентификационные данные МИС. При определенном стечении обстоятельств, подобная атака даёт возможность перехватить несколько учетных записей операторов МИС.

Большинство медицинских информационных систем имеют одинаковую архитектуру, а так как большинство локальных вычислительных сетей строится на одинаковых принципах и технологиях, и им свойственны одинаковые уязвимости, рассмотренный в представленной статье вектор атак является актуальным и должен приниматься во внимание администраторами безопасности. В качестве защитных мер от атак канального уровня необходимо корректно настраивать коммутационное оборудование, статически задавать ARP-таблицы, использовать на коммутаторах технологию Port security, а также шифровать трафик при помощи протокола IPSec.

Список использованных источников

1. Утечки данных в 2016 году – предварительные итоги года. Блог компании Gemalto Russia [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/gemaltorussia/blog

2. Олифер В., Олифер Н.Компьютерные сети. Принципы, технологии, протоколы. 4-е изд. — СПб.: Питер, 2010. — 944 е.: ил.

УДК 004.75

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ ЭЛЕКТРОННОГО ПОРТАЛА «ВЕБ-РЕГИСТРАТУРА»

Хамутников В. А., Давыдов А. Н.

Научный руководитель доцент Демин С. Л.

Сибирский федеральный университет

На сегодняшний день в IT индустрии наиболее популярным и перспективным направлением развития являются веб-технологии. Сложно представить современную жизнь людей без информационных веб-сервисов в сети Интернет. Почти каждая коммерческая организация имеет собственное веб-приложение, посредством которого предоставляет информацию для своих клиентов. Помимо этого, данная технология активно поддерживается со стороны государства. Так, например, федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» принуждает все государственные органы и органы местного самоуправления иметь сайт в информационно-телекоммуникационной сети Интернет для предоставления отчетности своей деятельности, и организации здравоохранения не исключение [1].

В прошлом году в Красноярском крае был запущен проект «Веб-регистратура». Данное веб-приложение позволяет записываться на прием к врачу через глобальную сеть Интернет, что существенно разгружает работу медицинских учреждений, а также сохраняет время пациентов. «Веб-регистратура» сразу же завоевала популярность у Интернет-пользователей, и в связи с этим, было принято решение провести исследование защищенности данного портала и осуществить поиск критически важных уязвимостей, описанных в классификаторе угроз международного консорциума по безопасности веб-приложений (WASC TC2) [2].Тестирование на проникновение осуществлялось по методике OWSAP TestingGuide [3]. Таким образом, исследование состояло из двух основных частей: исследование на уязвимости сетевых служб веб-сервера и исследование веб-приложения на осуществление типовых атак.

На начальном этапе веб-сервер был анализирован сетевым сканером Nmap на наличие используемых сетевых служб (рис. 1). В результате проверки были выявлены используемые сетевые службы и их версии, что говорит о наличии недостатка конфигурации веб-сервера (WASC TC: Fingerprinting). Также был произведен анализ скрытого содержимого веб-приложения и его функциональности с помощью инструмента BurpSpider, что позволило выявить средства управления веб-приложением (WASC TC:PredictableResourceLocation).

Также был произведен анализ ручным методом для выявления версий средств администрирования — phpMyAdminверсии 3.3.2 и CMS Wordpress версии 4.7.3. Версии данных средств были указаны на клиентской стороне в мета тегах (WASC TC: InformationLeakage).

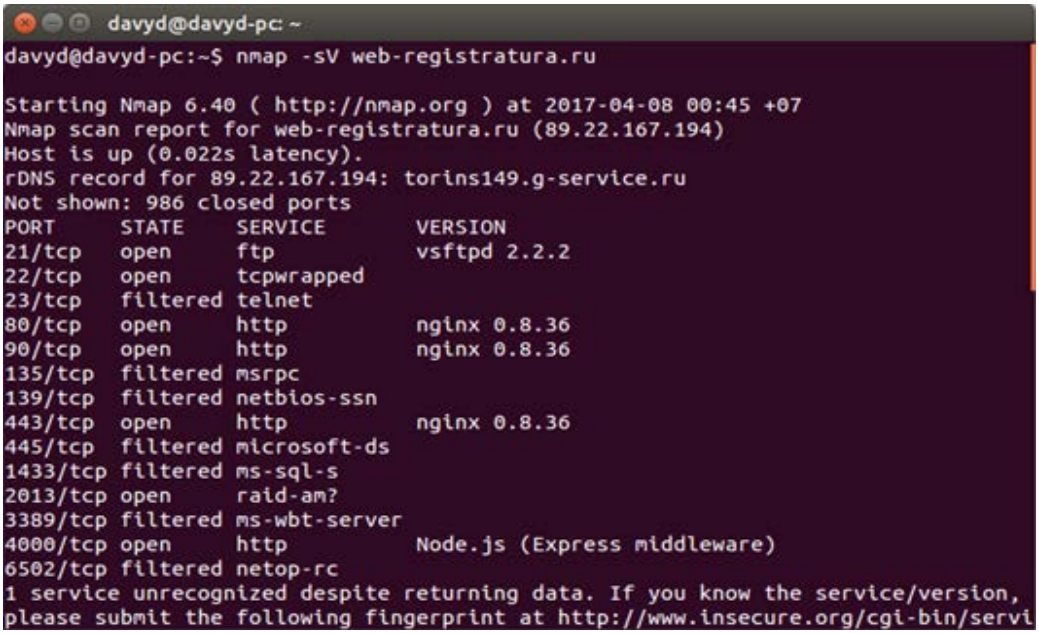

Рис.1 – Результат работы сетевого сканера

На следующем этапе был произведен более детальный анализ используемых сетевых служб на наличие уязвимостей.

FTP сервис версии 2.2.2 обладает весьма серьезной уязвимостью – CVE-2011-0762 [4]. Данная уязвимость позволяет произвести отказ в обслуживании удаленного сервера (WASC TC: DenialofService). Однако для осуществления данной атаки требуется авторизация в сервисе. Логин и пароль отFTP службы можно получить с помощью атаки полного перебора, т.к. на данном сервисе не предусмотрено блокирование доступа из-за большого количества запросов к ресурсу.

На момент написания статьи Wordpress версии 4.7.3 не имел уязвимостей. Однако он также не защищен от атаки полного перебора, т.к. не происходит прекращение доступа к ресурсу из-за большого количества запросов и не имеет системы защиты CAPTCHA. Также форма входа в административную панель Wordpress обладает недостатком, информируя о верном и неверном введённом логине. Впоследствии детального изучения данного сервиса, был выявлен адрес электронной почты одного из администраторов (evgpetrov@torins.ru), что в свою очередь позволило выявить логин администратора – evgpetrov.

В остальных службах и средствах администрирования отсутствуюткритические уязвимости и недочеты конфигурирования.

На втором этапе тестирования «Веб-регистратура» была просканированаинструментом BurpScaner на наличие общеизвестных уязвимостей. В результате исследования было выявлено две критические уязвимости – межсайтовое выполнение сценариев (WASC TC:XSS) и межсайтовая подделка запросов (WASC TC:CSRF).

Межсайтовая подделка запросов позволяет злоумышленнику, злоупотребляя доверием пользователей, отправлять HTTP-запросы к целевому назначению без их ведома. Основной причиной возникновения данной уязвимости является предсказуемое значение URL или форм заполнения на целевом (атакуемом) веб-сайте.С помощью данной уязвимости можно отправлять комментарии на веб-сервис от лица жертвы, либо записываться на прием к врачу, нарушив тем самым работу медицинских организаций, т.к. у врачей не окажется свободного времени для записи на прием.

Межсайтовое выполнение сценариев позволяет атакующему передать веб-серверу исполняемый код, который будет перенаправлен браузеру пользователя. Этот код обычно создается на языках HTML и JavaScript, но могут быть использованы VBScript, ActiveX, Java, Flash или другие поддерживаемые браузером технологии.

Вредоносный код исполняется на стороне пользователя с правами браузера, с помощью которого была загружена инфицированная страница веб-приложения. Таким образом, код получает возможность читать, модифицировать или передавать любые личные данные пользователя, доступные браузеру.

Существует два типа атак, приводящих к межсайтовому выполнению сценариев: постоянные (сохраненные) и непостоянные (отраженные). Основным отличием между ними является то, что в отраженном варианте передача кода серверу и возврат его клиенту осуществляется в рамках одного HTTP-запроса, а в хранимом – в разных. Иначе говоря, при постоянном варианте пользователю не обязательно переходить по вредоносной ссылке, а достаточно посетить уязвимый сайт.

В сервисе «Веб-регистратура» присутствуют оба типа атак, приводящих к межсайтовому выполнению сценариев.Воспользовавшись доверием пользователя можно убедить его записаться на прием к врачу и перенаправить по следующей ссылке:

$$https://web-registratura.ru/index.php?open=system/record\&step=2\&mode=1\&cid=100"\ method=POST\ id='person_data'><\!/form><script\ src="https://testing-suite.000webhostapp.com/1.js"><\!/script><p$$

Пользователю отобразится форма заполнения персональных данных. Таким образом, можно использовать JavaScript-код, который будет передавать post-запрос на веб-сервер злоумышленника с введенными пользователем данными в форму. На рисунке 2 представлены визуальное представление зараженной страницы, а на рисунке 3 – её HTML-код.

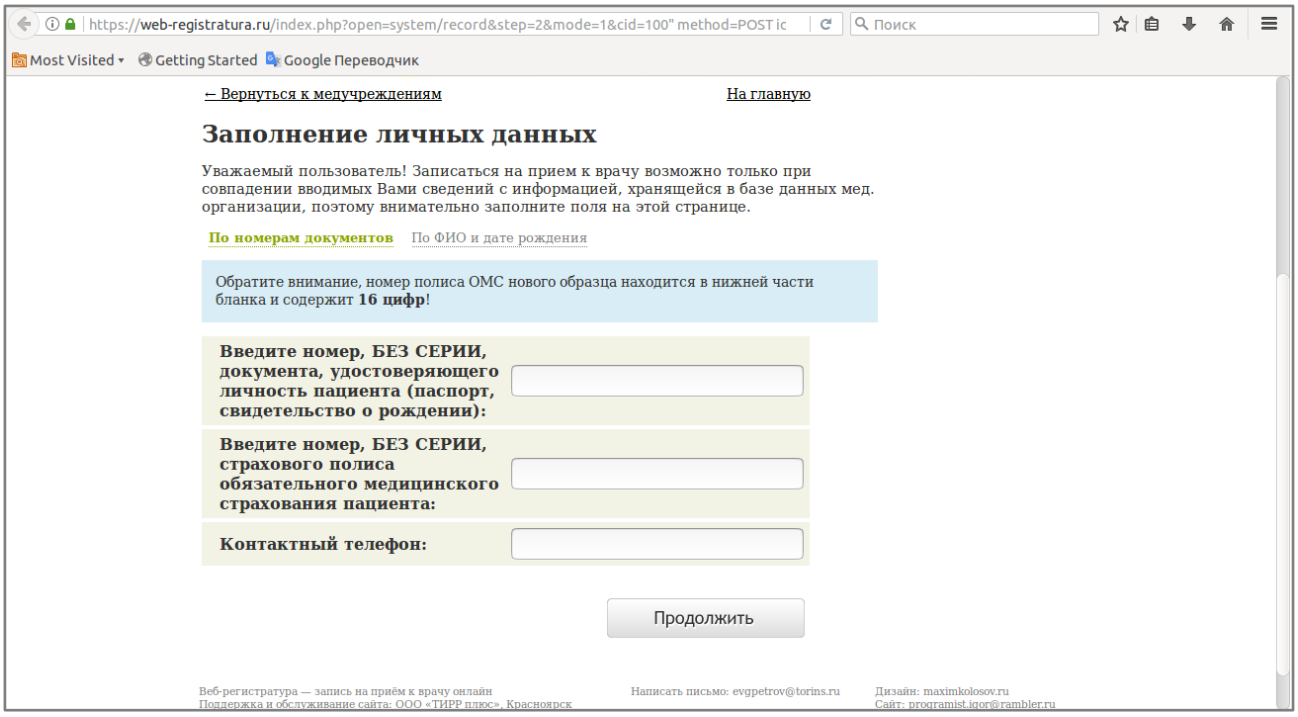

Рис.2 – Визуальное представление веб-страницы с внедренным скриптом

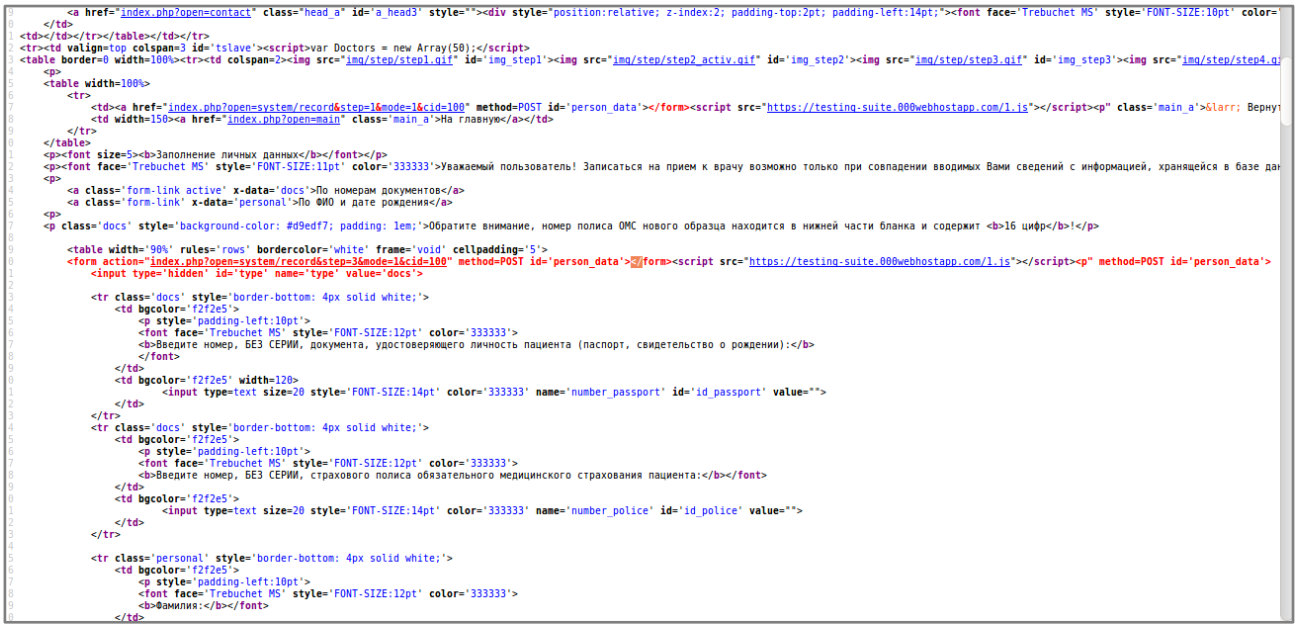

Рис. 3 – Код HTML-страницы с внедренным скриптом злоумышленника

В данном веб-приложении есть раздел отзывов и пожеланий, в котором каждый желающий может оставить свой комментарий. После того, как пользователь оставит комментарий, администратор должен его проверить и утвердить. Утверждение комментария происходит с активной сессией в Wordpress. Через форму комментария можно внедрить на веб-сервер вредоносный скрипт и быть уверенным, что он исполнится на стороне администратора. Таким образом, злоумышленник может похитить сессию администратора,

что позволит ему войти в административную панель Wordpress. На рисунке 4 представлен фрагмент HTML-страницы комментариев с интегрированным зловредным скриптом. Пример вредоносного JavaScript-кода представлен на рисунке 5.

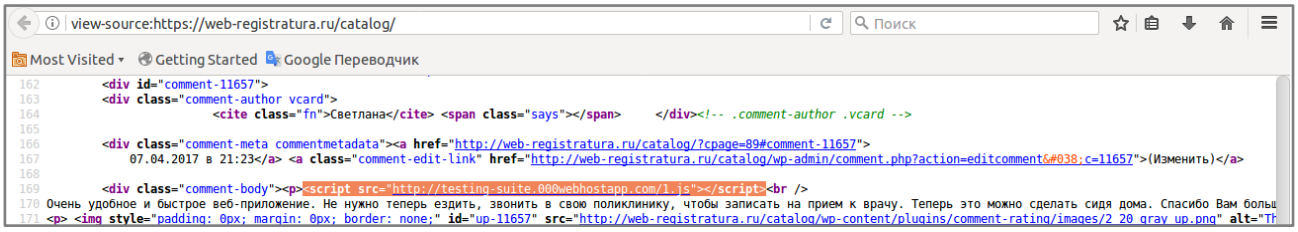

Рис. 4 – Фрагмент кодаHTML-страницы комментариев с внедренным скриптом

```
if (window.XMLHttpRequest) {
    xmlhttp = new XMLHttpRequest();
} else {
    xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
}

xmlhttp.onreadystatechange = function () {
    if (this.readyState == 4 && this.status == 200) {}
};

var body = 'log=' + document.cookie;
xmlhttp.open("POST", 'https://testing-suite.000webhostapp.com/post.php', true)
xmlhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded; charset=utf-8");
xmlhttp.send(body);
```

Рис.5 – Пример кода JavaScript для кражи cookie-файла

На примере электронного портала «Веб-регистратура» были рассмотрены популярные уязвимости, свойственные многим веб-приложениям. А приведенные примеры реализации описанных угроз, являются весомым аргументом в пользу необходимости должного внимания к безопасности веб-ресурсов, даже с учетом того, что данными ресурсами не происходит обработка критически важной информации.

Список использованных источников

1. Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/

2. WASC Threat Classification [Электронныйресурс]. Режим доступа: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

3. OWSAP TestingGuide [Электронный ресурс]. Режим доступа: https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

4. Common Vulnerabilities and Exposures. CVE-2011-0762 [Электронныйресурс]. Режим доступа: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0762

УДК 519.65

УНИВЕРСАЛЬНАЯ ИНТЕРПОЛЯЦИЯ ОРБИТ ГЛОНАСС И GPS ПО ДАННЫМ IGS

Тетерятников А. С.

Научный руководитель д-р физ.-мат. наук Царев С. П.

Сибирский федеральный университет

Эта статья развивает методику линейной интерполяции для орбит спутников ГЛОНАСС и GPS, предложенную в статье [1]. В указанной статье показано, что используя только 6 последовательных позиций спутников, с некоторым установленным интервалом времени, можно найти позицию спутников внутри интервала более точно, чем другими интерполяционными методами.

Определение позиции спутников в любой момент времени является фундаментальной частью в спутниковой навигации. Информация о положении спутников обычно описывается в текстовом виде в формате SP3, который содержит координаты спутников. SP3 файлы берутся из центра IGS (International GNSS Service [2]), где координаты рассчитаны с погрешностью не более 2,5 см и представлены на сайте [3] с интервалом в 15 мин.

Для нахождения координат спутников в любой момент времени используются интерполяционные методы. Наиболее часто применяется на практике интерполяционный полином Лагранжа. В статье [1] указано, что в этом методе среднеквадратическое отклонение невязки составляет 6,5 мм при использовании 10 узловых точек интерполяции, чего хватает для решения многих навигационных проблем.

Методика, предложенная в статье [1], обладает следующими свойствами:

- Нет необходимости выбирать интерполирующую функцию. Здесь функция автоматически адаптируется к любой орбите или временному ряду;

- Как показано в [1], недостаток методики заключается в необходимости предварительного вычисления интерполяционных коэффициентов для каждого интерполяционного шаблона.

В статье [1] показаны результаты расчета для одной целевой точки интерполяционного шаблона. В этой статье приведены результаты расчета для всех точек внутри интерполяционного шаблона с шагом 1 сек.

Методика [1] основывается на известной интерполяционной формуле Лагранжа:

$$L(\hat{t}) = \sum_{i=1}^{n} x(t_i) \cdot a_i(\hat{t}), \qquad (1)$$

где $L(\hat{t})$ - интерполирующая функция для промежуточных моментов времени $\hat{t}$; $x(t_i)$ - позиции спутника в момент времени t_i, i=1.. n; n – количество узлов интерполяции;

$$a_i(\hat{t}) = \prod_{k=1,k\neq i}^{n} \frac{\hat{t} - t_k}{t_i - t_k}.$$

От вида коэффициентов $a_i(\hat{t})$ в формуле (1) зависит, какой способ интерполяции используется (полиномиальная, тригонометрическая или какая-либо другая интерполяция) [4,5,6,7,8].

Как показано в [1], фиксируем n последовательных моментов времени t_i (i=1..n) из SP3 файлов и целевой момент времени $\hat{t} = t_j$ (момент времени в котором будет происходить расчет координаты) в интервале между t_i. Тогда получим фиксированный *интерполяционный шаблон* из n точек t_i и целевой точки t_j. С учетом фиксированного интерполяционного шаблона, для коэффициентов $a_i(\hat{t})$ можно опустить зависимость от $\hat{t}$ и тогда, внеся в (1) $\varepsilon(t_j)$ - величину характеризующую невязку для момента времени t_j, (1) запишем в виде:

$$\underline{x}(t_j) = \sum_{i=1}^{n} a_i \cdot x(t_i) + \varepsilon(t_j), \qquad (2)$$

где a_i неизвестные коэффициенты, $x(t_i)$ – координата спутника из SP3 файла в момент времени t_i; $\underline{x}(t_j)$ - целевая координата (в которой находится спутник в целевой момент времени t_j); $\varepsilon(t_j)$ - неизвестная величина, характеризующая невязку интерполяции для момента времени t_j.

Для нахождения коэффициентов a_i и невязки $\varepsilon(t_j)$ понадобится, как минимум, n+1 уравнение. Как указано в статье [1], сделаем сдвиг во времени для интерполяционного шаблона с шагом 900 секунд. При этом мы считаем, что коэффициенты a_i не изменяются. Совершив m таких сдвигов, получим систему уравнений:

$$\begin{cases} \underline{x}(t_j) = \sum_{i=1}^{n} a_i \cdot x(t_i) + \varepsilon(t_j) \\ \cdots \\ \underline{x}(t_j + 900\mathrm{m}) = \sum_{i=1}^{n} a_{i+m} \cdot x(t_{i+m}) + \varepsilon(t_j + 900m) \end{cases}. \qquad (3)$$

А. С. Пустошилов предоставил программу (на языке программирования Julia [9]), которая считывает координаты из файлов, содержащих координаты спутников, и подготавливает их к последующему решению системы (3) относительно неизвестных a_i методом наименьших квадратов. Расчет производит для узлов интерполяции с шагом 15 мин., а целевая точка отсчитывается с шагом 5 минут от 1 точки интерполяционного шаблона. Программа была переписана так, чтобы она считывала координаты из файлов с шагом 1 сек. Теперь отсчет целевой точки происходит с шагом 1 сек., для шага узлов интерполяции введена переменная и добавлен цикл для перебора целевых точек. Подставив файлы с координатами спутников в программу, программа считывает их, подготавливает данные с координатами к решению системы (3), решает её и создает текстовой файл, содержащий набор коэффициентов, максимум от невязки и среднеквадратическое отклонение невязки (СКО) для каждой целевой точки.

Один из центров IGS (CODE) предоставляет координаты с шагом 1 сек [3]. В программу были подставлены файлы, содержащие координаты для спутников ГЛОНАСС за период 10.03.2017 – 14.03.2017 с шагом 1 сек. Шаг для узлов интерполяции выбран 900 сек. В результате работы программы получен файл, содержащий СКО невязки для каждой целевой точки интерполяционного шаблона. При помощи Julia был построен график зависимости величины СКО невязки от целевой точки (Рисунок 1).

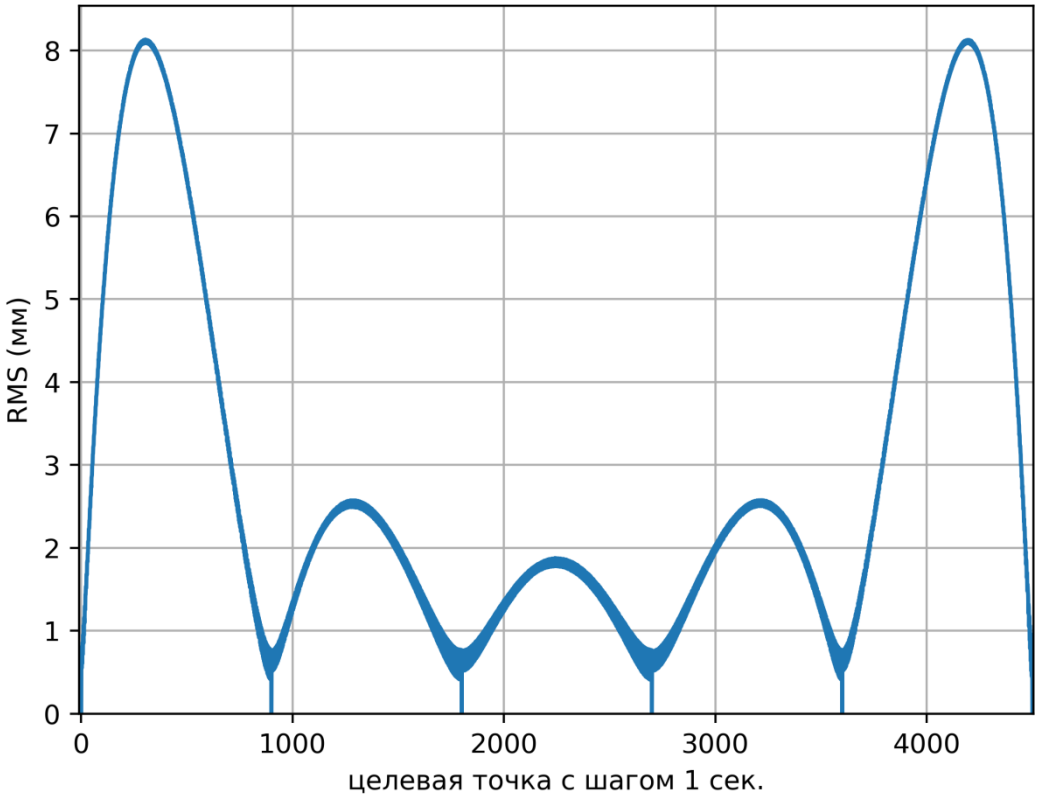

Рис. 1 – СКО(RMS) невязки для спутников ГЛОНАСС по координатам из файлов центра IGS CODE

На рисунке 1 на границах интерполяционного шаблона наблюдается увеличение СКО невязки в 3,1 раза по сравнению с максимумами СКО невязок в середине шаблона. Это явление описывается феноменом Рунге [10]. Наибольшее СКО невязки в середине равно 2,6 мм.

Рисунок 1 подтверждает, что метод, указанный в статье [1], позволяет по 6 точкам находить промежуточные координаты с высокой точностью (в статье [1] СКО невязки в середине шаблона составляет 3.88 мм для спутников ГЛОНАСС).

В программу были подставлены файлы, которые предоставил мне Ю. Ю. Ушаков, рассчитанные по его методике [11] для спутника GPS G01 за 2013 год. Координаты из файлов имеют шаг 1 сек. Шаг для узлов интерполяции был установлен 900 сек. В результате работы программы, получен файл, содержащий СКО невязки для каждой целевой точки. График зависимости величины СКО от целевой точки изображен на рисунке 2.

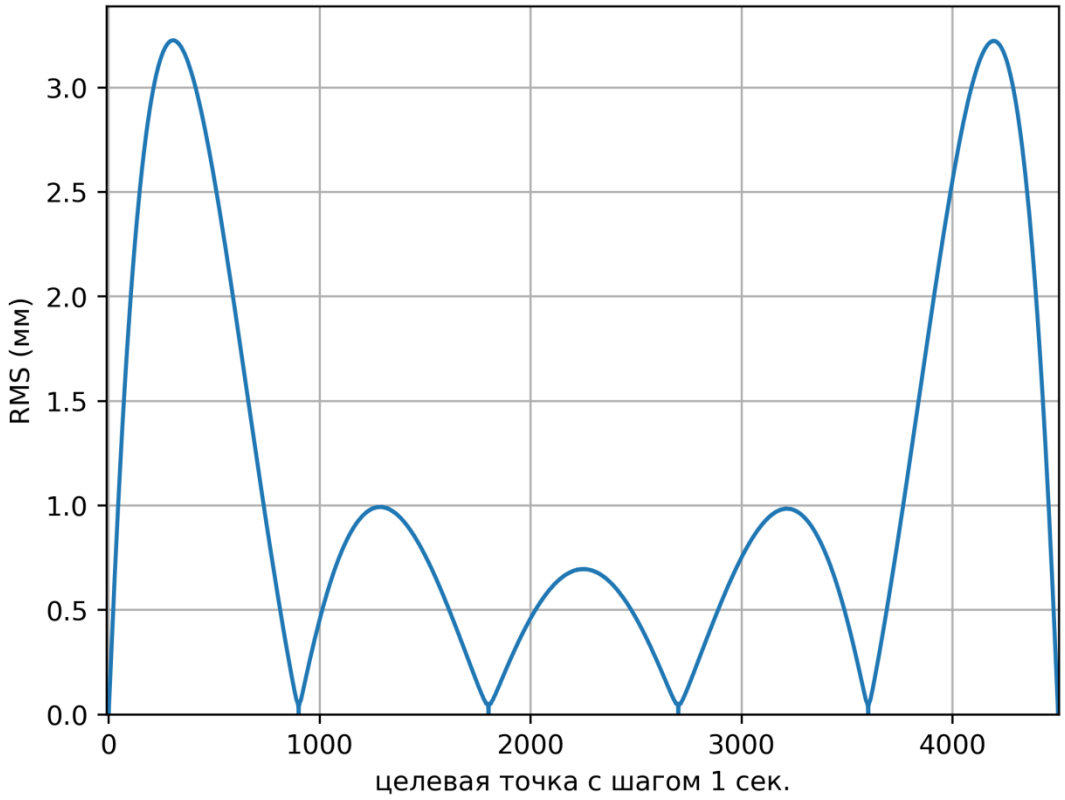

Рис. 2 – СКО(RMS) невязки для спутника GPS G01 по координатам из файлов Ю. Ю. Ушакова

На рисунке 2 на границах интерполяционного шаблона СКО невязки возрастает до 3,4 мм. Это явление описывается феноменом Рунге [10]. Наибольшее значение СКО невязки в середине шаблона равно 1 мм.

В статье [1] расчет производится только для одной целевой точки в середине интерполяционного шаблона. А в этой статье целевая точка перебирается с шагом 1 сек. по

всему интерполяционному шаблону. Таким образом, по рисункам 1 и 2 можно определить СКО невязки для каждой точки интерполяционного шаблона, а не только для середины.

Список использованных источников

1. S. P. Tsarev, A. S. Pustoshilov. Universal Coefficients for Precise Interpolation of GNSS Orbits from Final IGS SP3 Data. 2017 International Siberian Conference on Control and Communications, *SIBCON 2017 - Proceedings 2017*

2. http://www.igs.org/products

3. ftp://cddis.gsfc.nasa.gov или ftp://ftp.igs.org/pub/product/

4. M. Schenewerk. A brief review of basic GPS orbit interpolation strategies. *GPS Solutions*, 2003, vol. 6, 265-267

5. M. Horemuz and J. V. Andersson. Polynomial interpolation of GPS satellite coordinates. *GPS Solutions*, 2006, vol. 10, 67-72

6. Y. Feng and Y. Zheng. Efficient interpolations to GPS orbits for precise wide area applications. *GPS Solutions,* 2005, vol. 9, 67-72

7. H. Yousif and A. El-Rabbany. Assessment of Several Interpolation Methods for Precise GPS Orbit. *The journal of navigation*, 2007, vol. 60, 443–455

8. S. Xue and Y. Yang. Recursive algorithm for fast GNSS orbit fitting. *GPS solutions,* 2016, vol. 20, 151-157

9. http://julialang.org/

10. https://ru.wikipedia.org/wiki/Феномен_Рунге

11. Yu. Ushakov. Evaluation of acceleration and motion model parameters of a space vehicle from IGS final orbits. 2013 International Siberian Conference on Control and Communications, *SIBCON 2013 - Proceedings 2013*, Article number 6693594