ISSN 2221-3198

Геология и геофизика юга России

№ 4 / 2017

УДК 550.34:004.4
DOI: 10.23671/VNC.2017.4.9525

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ДОСТУПА К ВЕБ-ИНТЕРФЕЙСУ СИСТЕМЫ ГЕОИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ С ИНФОРМАЦИОННОЙ БАЗОЙ ДАННЫХ О СЕЙСМИЧНОСТИ И СЕЙСМИЧЕСКИХ РИСКАХ

© 2017 А. С. Кануков, к.т. н.

Геофизический институт – филиал ФГБУН ФНЦ «Владикавказский научный центр Российской академии наук», Россия, 362002, РСО-Алания, г. Владикавказ, ул. Маркова, 93а, e-mail: cgi_ras@mail.ru

Статья посвящена вопросу обеспечения безопасного доступа к веб-интерфейсу системы геоинформационного моделирования с информационной базой данных о сейсмичности и сейсмических рисках. С развитием высоких технологий большое распространение получили различные геоинформационные системы, предназначенные для сбора, хранения, анализа и графической визуализации пространственных данных и связанной с ними информации о представленных в ГИС-объектах. В Геофизическом институте создана карта инженерно-геологического районирования территории города Владикавказа, освещающая вопросы геологического строения, гидрогеологических условий, литологии, морфологии, тектоники, распространения различных типов грунтов на рассматриваемой территории. Данная карта интегрирована в геоинформационную систему. При создании подобных систем необходимо учитывать тот факт, что если для геоинформационной системы реализуется возможность доступа с помощью веб-сервиса, то он должен иметь средства для аутентификации пользователей и поддержку базовых алгоритмов шифрования для защиты от несанкционированного использования данной системы. На основе программного обеспечения с открытым исходным кодом выполнена защита канала связи с геоинформационной системой от несанкционированного доступа.

Ключевые слова: базы данных, карты сейсмической опасности, ГИС, геоинформационное моделирование шифрование, протоколы доступа.

С развитием современных технологий всё большее распространение получают различные информационные системы. Особое место в данном ряду принадлежит геоинформационным системам, предназначенным для сбора, хранения, анализа и графической визуализации пространственных данных и любой связанной с ними информации [Географическая…]. Благодаря развитию программ с открытым исходным кодом, создание геоинформационной системы становится всё более простой задачей.

При их создании необходимо учитывать тот факт, что если для геоинформационной системы реализуется возможность доступа с помощью веб-сервиса, то он должен иметь средства для аутентификации пользователей и поддержку базовых алгоритмов шифрования для защиты от несанкционированного использования данной системы.

HTTPS (Hypertext Transfer Protocol Secure) – расширенный протокол HTTP, который поддерживает шифрование. Данные, которые передаются по данному протоколу HTTPS, «внедряются» в криптографические протоколы SSL или TLS, при этом обеспечивается защита этих данных. В отличие от HTTP, для которого используется TCP-порт 80, в HTTPS по умолчанию использует 443-ий TCP-порт.

Протокол HTTPS разработан компанией Netscape Communications Corporation. Он создавался для обеспечения аутентификации пользователя и установлении защищённого соединения. HTTPS широко используется в веб мире для приложений, для которых критично наличие безопасного соединения с пользователем, примером могут служить платежные системы.

HTTPS не выступает в роли отдельного протокола. Это обычный протокол HTTP, который работает через шифрованные транспортные механизмы, такие как SSL и TLS. С его помощью обеспечивается защита от атак, которые основаны на «прослушивании» сетевого соединения – начиная от снифферских атак и заканчивая атаками типа «человек-посередине», при условии использования шифрующих средств и проверенного сертификата сервера, которому доверяют.

Для корректной работы с протоколом HTTPS необходимо произвести подготовку веб-сервера для обработки https-соединений, для этого необходимо получить или сгенерировать и установить в систему сертификат. Сертификат представлен двумя частями (2 ключа) – «общедоступный» и «закрытый». Общедоступная часть сертификата используется для шифрования трафика от пользователя к серверу при защищённом соединении, закрытая часть – для расшифровки полученного от пользователя зашифрованного трафика на сервере. Сертификат, как правило, необходимо подписать у уполномоченной стороны, которая является гарантом для пользователей, что обладатель сертификата является тем, кем он представляется.

На некоторых сайтах используются собственные сгенерированные сертификаты. Существует возможность создать такой сертификат, не обращаясь в компанию-сертификатор. Такие сертификаты создаются для серверов, работающих под управлением Unix, при помощи таких утилит, как ssl-ca от OpenSSL или gensslcert от SuSE. Подписываются такие сертификаты этим же сертификатом и называются самоподписанными (self-signed). Полученные сертификаты являются менее надёжными, чем те сертификаты, которые были подписаны компаниями-сертификаторами. Их использование защитит от пассивного прослушивания, но без проверки данного сертификата другими способами (к примеру, по звонку владельцу и проверке контрольной суммы сертификата) данный метод не может являться достаточно безопасным.

SSL (англ. Secure Sockets Layer – уровень защищённых сокетов) – криптографический протокол, которым обеспечивается установление безопасного соединения между клиентом и сервером. SSL изначально разработан компанией Netscape Communications [Introduction to SSL…]. Впоследствии на основании протокола SSL 3.0 был разработан и принят стандарт RFC, получивший имя TLS.

Данный протокол устанавливает конфиденциальный обмен данными между сервером и клиентом, которые используют TCP/IP, при этом для шифрования используется асимметричный алгоритм с открытым ключом. При данном виде шифровании используются два ключа, причем каждый из них может быть использован для шифрования сообщений. В таком случае, если для шифрования используется один ключ, то для расшифровки, соответственно, необходимо использовать другой ключ. В подобной ситуации можно получать шифрованные сообщения, опубликовав открытый ключ, и скрыв секретный ключ.

SSL представляет из себя канал, имеющий 3 основных свойства:

Аутентификация. Сервер всегда аутентифицируется, в то время как клиент может аутентифицироваться в зависимости от алгоритма.

Целостность. Обмен сообщениями должен включать в себя проверку целостности.

Частность канала. Шифрование используется также после установления соединения для всех отправляемых впоследствии сообщений.

Кроме того SSL обладает следующими свойствами:

Совместимость: Программисты могут создавать различные приложения, которые будут использовать SSL и впоследствии будут иметь возможность успешного обмена криптографическими параметрами, не имея доступа к коду чужих программ.

Расширяемость: SSL стремится обеспечивать рабочие пространства, для которых новые открытые ключи и сложные методы шифрования могут быть интегрированы в случае необходимости.

Относительная эффективность: работа протокола с использованием SSL требует большой скорости обработки от центрального процессора, например в случае работы с открытыми ключами. По данной причине протокол SSL был интегрирован в необязательную сессию схемы кеширования, в целях уменьшения числа соединений, которые необходимо устанавливать с нуля. Кроме того, большое внимание уделяется тому, чтобы уменьшить сетевую активность.

Аутентификация и обмен ключами

SSL поддерживает 3 разных типа аутентификации:

аутентификация обеих сторон (клиент – сервер),

аутентификация сервера с неаутентифицированным клиентом,

полная анонимность.

Каждый раз, когда сервер проходит аутентификацию, канал становится безопасным против попыток перехвата данных между веб-сервером и браузером, но если устанавливается полностью анонимная сессия, то она, по своей сути, уязвима к подобной атаке. Анонимный сервер не сможет аутентифицировать клиента. Если же сервер прошел аутентификацию, то его сообщение сертификации обеспечивает правильную сертификационную цепочку, которая ведет к доверенному центру сертификации. Другими словами, аутентифицированный клиент обязан предоставить серверу допустимый сертификат. Каждая из сторон отвечает за проверку сертификата другой стороны на предмет того, что он еще не истек или не был отменен. Главной целью процесса обмена ключами является создание «секрета» клиента (pre_master_secret), который известен только серверу и клиенту. Секрет в дальнейшем будет использован для создания общего секрета (master_secret). Он необходим для того, чтобы создавать сообщения для проверки сертификатов, ключей шифрования, секретов MAC и сообщения «finished». При отправке верного сообщения «finished», стороны докажут друг другу, что они знают правильный секрет.

Анонимный обмен ключами

В случае необходимости установки полностью анонимной сессии для создания ключей обмена можно использовать алгоритмы RSA или Диффи-Хеллмана. Если используется RSA, то клиент шифрует секрет, используя открытый ключ сервера, не имеющего сертификата. Открытый же ключ клиент получает из сообщения по обмену ключами от сервера. Результат должен быть послан в сообщении по обмену ключами от клиента. Поскольку перехватчик не может знать закрытый ключ сервера, то он будет не в состоянии расшифровать секрет. Если же используется алгоритм Диффи-Хеллмана, то открытые параметры сервера будут содержаться в

сообщениях по обмену ключами от сервера. Перехватчик, у которого нет приватных значений, не сможет найти секрет.

Обмен ключами при использовании RSA и аутентификация

В данном случае аутентификация сервера и обмен ключами могут быть скомбинированы. Открытый ключ может быть включен в сертификат сервера или использован как временный ключ RSA, который отправляется в сообщениях обмена ключами от сервера. В случае использования временного ключа RSA, сервер сможет воспользоваться временным ключом RSA только один раз, для создания сессии. Проверив сертификат сервера, клиент зашифрует секрет открытым ключом сервера. После успешного декодирования секрета будет создано сообщение «finished», что означает, что сервер знает закрытый ключ, который соответствует сертификату сервера.

Если RSA используют для обмена ключами, то для аутентификации клиента будет использовано сообщение по проверке сертификата клиента. Клиент генерирует подпись, вычисленную из master_secret, а также всех полученных ранее сообщений протокола рукопожатия.

Протокол записи (Record Layer)

Протокол записи является уровневым протоколом. Для каждого уровня сообщения включаются следующие поля: длина, описание и проверки. Протокол записи получает сообщения, которые необходимо передать, фрагментирует их в управляемые блоки, шифрует и отправляет результат. Получаемые данные им расшифровываются, проверяются, распаковываются, собираются и доставляются к вышележащим уровням клиента.

Существует четыре протокола записи: протокол рукопожатия, протокол тревоги, протокол изменения шифра, протокол приложения (application data protocol). В случае, когда SSL реализацией получается тип записи, который для неё неизвестен, то данная запись будет проигнорирована. Любой протокол, который создается для использования вместе с SSL, необходимо хорошо продумать, так как будут возникать атаки на него. Необходимо отметить, что из-за типа и ограничения длины записи, протокол не защищается шифрованием. Внимание необходимо уделить минимизации трафика.

Протокол рукопожатия (handshake)

SSL клиент и сервер должны договориться об установке связи с использованием процедуры рукопожатия. В момент рукопожатия клиент и сервер могут договориться о различных параметрах, которые они будут использовать для обеспечения безопасности соединения.

Рассмотренные подходы были использованы в разработанной геоинформационной системе по работе с картами сейсмической опасности территории Республики Северная Осетия-Алания [Заалишвили и др., 2010; Заалишвили и др., 2012; Заалишвили, 2014] с выведенной кадастровой информацией [Радионов, Гончарова, 2010] (рис. 1).

Сейсмологические исследования для различных целей, в т. ч. для задач строительной отрасли, выполняются в нашей стране уже свыше века. Оценка сейсмической опасности обычно сводится к вычислению максимально возможных сейсмических воздействий, которые необходимо учитывать при строительстве в сейсмических районах. Сейсмическая опасность отражается на картах сейсмического районирования той или иной территории. В нашей стране в зависимости от задач и

необходимой детальности картирования сейсмической опасности рассматриваются три уровня сейсмического районирования:

1. общее сейсмическое районирование (ОСР) – для всей территории страны;

2. детальное сейсмическое районирование (ДСР) – для ограниченных площадей и отдельных регионов;

3. сейсмическое микрорайонирование (СМР) – для городов, населенных пунктов и строительных площадок.

В результате целого ряда исследований по оценке сейсмической опасности Геофизическим институтом в 2006-2010 гг. были созданы оригинальные карты детального сейсмического районирования (ДСР) Республики Северная Осетия-Алания [Заалишвили и др., 2008; Заалишвили, Дзеранов, 2010], карты сейсмического микрорайонирования территории (СМР) г. Владикавказа и др. [Заалишвили и др., 2010, 2011а – в; Заалишвили, Рогожин, 2011; Заалишвили, Джгамадзе, 2011, 2012; Zaalishvili et al., 2010; Заалишвили, 2013]. Очевидно, что картографические материалы должны соответствовать мировому уровню, предъявляемому к пространственным данным и, в первую очередь, обладать возможностью непосредственного включения в любые современные информационные системы.

Таким образом, цель нашей работы состояла в разработке веб-интерфейса безопасного доступа к информационной базе данных, включающих информацию о сейсмичности и сейсмических рисках той или иной территории.

Объектом исследования являлись существующие информационные картографические системы и карты сейсмической опасности исследуемой территории.

При попадании на главную страницу разработанной системы необходимо пройти авторизацию для получения доступа к данным. Очевидно, что в геоинформационной системе должны иметься средства для аутентификации пользователей. Базовая авторизация реализована в Geoserver, но уязвима к атакам перехвата авторизационных данных, позволяющих просматривать карты без регистрации на web-сервисе. Выходом из данного положения является использование так называемой https-обвязки, при которой все данные между клиентом и сервером шифруются.

С помощью рассмотренных методов обеспечения безопасности может быть введена поддержка протокола https, даже если исходное программное обеспечение его не поддерживает, что может иметь место в случае уже готовой системы. Для этих целей подходит программа pound, которая, «слушая» определённый порт, работает через него по безопасному протоколу https. Данные, поступающие на этот порт, расшифровываются и перенаправляются на внутренний порт, который «слушает» программа, и в которую мы вводим поддержку протокола https.

Для работы сервиса pound необходимо получить и установить в систему сертификат [Introduction to SSL…]. Сертификат состоит из двух ключей – открытый и закрытый. Открытый ключ используется для шифрования трафика от клиента к серверу в защищённом соединении, закрытый ключ – для расшифровывания полученного от клиента зашифрованного трафика на сервере. После генерации открытого и закрытого ключей на основе открытого ключа формируется запрос на сертификат в Центр сертификации (ЦС), в ответ на который ЦС высылает подписанный сертификат. ЦС при подписывании проверяет клиента, что позволяет ему гарантировать, что держатель сертификата является тем, за кого себя выдаёт. Каждый подписанный сертификат имеет срок действия и за создание/продление подписи обычно взимается плата.

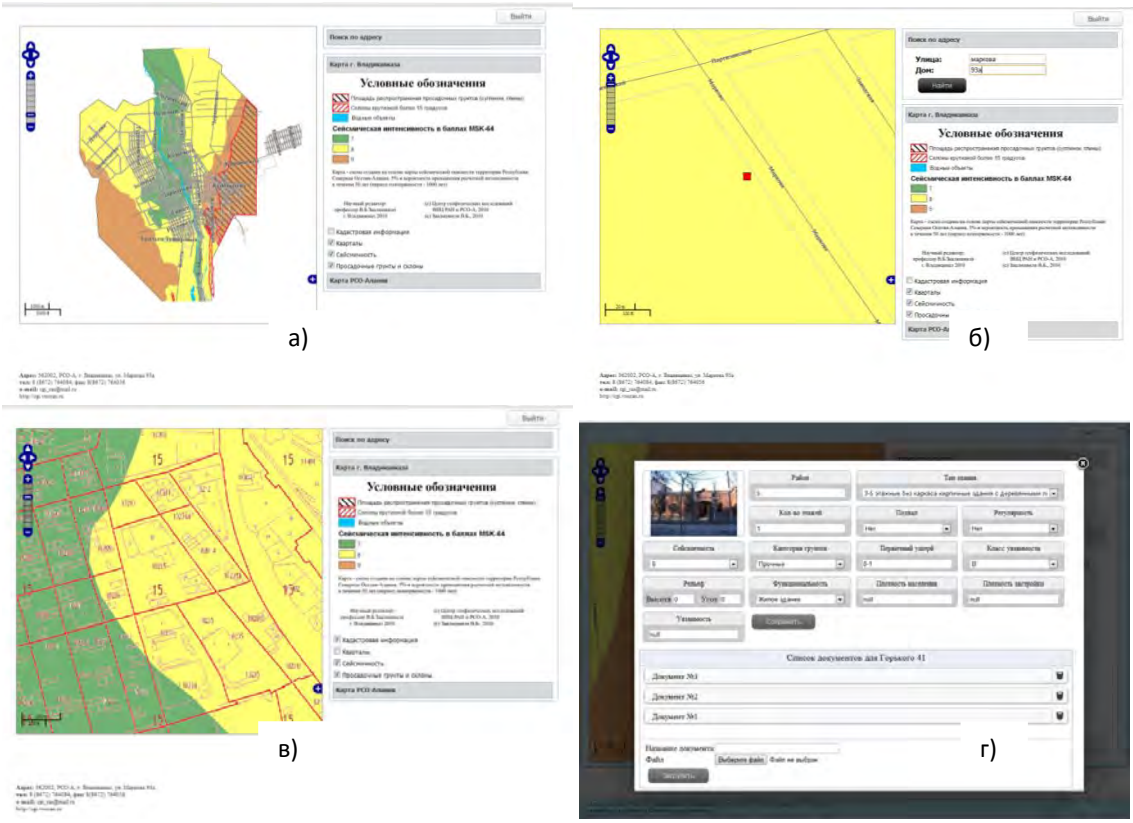

Рис. 1. а) главная страница защищенного веб-сервиса с картой г. Владикавказа; б) реализация функции поиска объекта по адресу; в) вывод кадастровой информации; г) база данных сейсмического риска застройки

Однако существует возможность создать подобный сертификат, не обращаясь в Центр сертификации. Они могут быть созданы для станций, которые работают под Unix/Linux, что также говорит в пользу выбора данной системы. Подписываются такие сертификаты сами собой и потому называются самоподписанными (self-signed). Если не проверить данный сертификат каким-либо другим способом, то использование данного протокола может быть подвергнуто атаке «man-in-the-middle», то есть «человек-в-середине». Суть её в том, что нарушители могут подключаться к каналу, по которому устанавливается защищённое соединение, и перехватывать все запросы, идущие между сервером и клиентом. При этом нарушитель представляется клиенту как сервер, а серверу как клиент. Так как подтвердить тот факт, что сервер является тем, за кого себя выдаёт можно только с помощью сертификата выданного ЦС, подобные атаки легко осуществимы для самоподписанных сертификатов. В то же время, непосредственная передача самоподписанного сертификата по закрытому каналу и установка его в систему как доверительного позволяет избегать подобных атак.

Таким образом, авторизация является двухуровневой, но происходит прозрачно для пользователя. То есть, необходимо ввести только свои логин/пароль, далее система сама проведёт авторизацию не только на веб-сервисе, но и на Geoserver'е, и начнет шифровать весь поток данных. Это позволяет защитить канал связи с геоинформационной системой от несанкционированного доступа.

Выводы

1. Установлено, что не существует абсолютно безопасной системы. Каждая из систем имеет свои слабые места.

2. Использование шифрованного протокола HTTPS позволяет свести к минимуму возможность несанкционированного доступа к данным.

3. Использование ассиметричного алгоритма шифрования RSA с длиной ключа 256 бит делает нецелесообразным метод взлома путём прямого подбора ключа.

4. Использование подписанного сертификата позволяет использовать максимальную степень защищённости канала передачи данных, делая чрезвычайно сложной процедуру взлома.

5. Рассмотренные в статье подходы были использованы в разработанной геоинформационной системе по работе с картами сейсмической опасности территории Республики Северная Осетия-Алания

Литература

1. Географическая информационная система. URL: http://www.gisa.ru/13058.html (Дата обращения 2.02.2017 г.)

2. Заалишвили В.Б., Аракелян А.Р., Макиев В.Д., Мельков Д.А. К вопросу сейсмического районирования территории республики Северная Осетия-Алания // Труды I международной конференции «Опасные природные и техногенные геологические процессы на горных и предгорных территориях Северного Кавказа», Владикавказ, 20-22 сентября 2007. – Владикавказ. – 2008. – С. 263-278.

3. Заалишвили В.Б., Дзеранов Б.В. Оценка сейсмической опасности территории РСО-Алания // Труды научно-практической конференции «Молодые ученые в решении актуальных проблем науки». Владикавказ. – 2010. – С. 342-345.

4. Заалишвили В.Б., Мельков Д.А., Дзеранов Б.В., Кануков А.С. Оценка сейсмической опасности урбанизированной территории на основе современных методов сейсмического микрорайонирования (на примере г. Владикавказа) // Труды международной научно-практической конференции «Молодые ученые в решении актуальных проблем науки». Владикавказ, 22-23 мая 2010 г. – 2010. – С. 348-351.

5. Заалишвили В.Б., Мельков Д.А., Габараев А.Ф., Дзебоев Б.А., Дзеранов Б.В., Кануков А.С., Шепелев В.Д. Использование микросейсм при уточнении карт инженерно-геологического районирования территории, являющихся основой сейсмического микрорайо-нирования // Материалы Всероссийской научно-практической конференции, посвященной 10-летию со дня основания КНИИ РАН «Наука и образование в Чеченской республике: состояние и перспективы развития» 7 апреля 2011 г., КНИИ РАН. – 2011а. – С. 335-342.

6. Заалишвили В.Б., Рогожин Е.А. Оценка сейсмической опасности территории на основе современных методов детального районирования и сейсмического микрорайонирования // Сейсмостойкое строительство. Безопасность сооружений. – М.: ВНИИНТПИ, 2011. – №3. – С. 31-43.

7. Заалишвили В.Б., Джгамадзе А.К. Инженерно-геологическое районирование города Ардон РСО-Алания // Труды IV Кавказской международной школы-семинара молодых ученых «Сейсмическая опасность и управление сейсмическим риском на Кавказе», Владикавказ, 24-26 октября 2011 г. – 2011. – С. 102-106.

8. Заалишвили В.Б., Дзеранов Б.В., Габараев А.Ф. Актуализация карт сейсмической опасности территории Республики Северная Осетия-Алания // Труды

IV Кавказской международной школы-семинара молодых ученых «Сейсмическая опасность и управление сейсмическим риском на Кавказе», Владикавказ, 24-26 октября 2011 г. – 2011б. – С.155-167.

9. Заалишвили В. Б., Дзеранов Б. В., Габараев А. Ф. Оценка сейсмической опасности территории и построение вероятностных карт // Геология и геофизика Юга России. – 2011 в. – С. 48-58.

10. Заалишвили В. Б., Мельков Д. А., Кануков А. С. Информационная система обеспечения градостроительной деятельности на основе информационной базы данных сейсмичности и сейсмического риска // Информатизация и связь. ISSN 2078-8320. – № 5. – 2012. – С. 14-18.

11. Заалишвили В. Б., Джгамадзе А. К. О создании карт инженерно-геологического районирования территорий населённых пунктов Республики Северная Осетия-Алания, как основы сейсмического микрорайонирования // Материалы II Всероссийской научно-технической конференции «Современные проблемы геологии, геофизики и геоэкологии Северного Кавказа», 8-12 ноября 2012 г. – Грозный. – 2012. – С. 442-446.

12. Заалишвили В. Б. К вопросу создания единой карты детального сейсмического районирования // Материалы Международного симпозиума «Устойчивое развитие: Проблемы, Концепции, Модели», посвященного 20-летию КБНЦ РАН, ФГБУН КБНЦ РАН, Том II, 28 июня – 3 июля 2013 г. – 2013. – С. 106-110.

13. Заалишвили В. Б. Некоторые проблемы практической реализации сейсмического микрорайонирования. Факторы, формирующие интенсивность землетрясения // Геология и геофизика Юга России. – 2014. – № 3. – С. 3-39.

14. Радионов Г. П., Гончарова Л. И. Публичная кадастровая карта: успехи и трудности // Вестник Росреестра. – 2010. – № 3. – С. 23-27.

15. Introduction to SSL. URL: https://developer.mozilla.org/en/Introduction_to_SSL (дата обращения: 18.02.17 г.).

16. Zaalishvili V. B., Melkov D. A., Dzeranov B. V. Modern seismic hazard assessment methods (in example territory of Vladikavkaz-city) // Proceedings of 14th European conference of earthquake engineering. 30 August – 03 September, Ohrid, Republic Macedonia, 2010, 8 pp.

DOI: 10.23671/VNC.2017.4.9525

MAINTAINING SAFE ACCESS TO WEB INTERFACE OF GEOINFORMATION MODELING SYSTEM WITH INFORMATION DATABASE OF SEISMICITY AND SEISMIC RISK

© 2017 A. S. Kanukov, Sc. Candidate (Tech.)

Geophysical institute VSC RAS, Russia, 362002, RNO-Alania, Vladikavkaz, Markov Str., 93 a, e-mail: cgi_ras@mail.ru

The article is devoted to maintenance of safe access to the web interface of the geoinformation modeling system with an information database on seismicity and seismic risks. With the development of high technologies, various geoinformation systems were widely used to collect, store, analyze and graphically visualize spatial data and associated information about the objects represented in GIS objects. A map of the geological-engineering zoning of the territory of the Vladikavkazcity, covering geological structure, hydrogeological conditions, lithology, morphology, tectonics, distribution of various types of soils in the territory under consideration, was created in the Geophysical Institute. This map is integrated into the geoinformation system. When creating such systems, it is necessary to take into account the fact that if for a geoinformation system a web service accessis realized, then it must have means for user authentication and support of basic encryption algorithms to protect against unauthorized use of this system. On the basis of open source software, the communication channel with the geoinformation system is protected from unauthorized access.

Keywords: databases, seismic hazard maps, GIS, geoinformation modeling, encryption, access protocols.

Refere.nces

1. Geograficheskaja informacionnaja Sistema [Geographic information system]. URL: http://www.gisa.ru/13058.html (Data obrashhenija 2.02.2017 g.). (in Russian)

2. Zaalishvili V.B., Arakeljan A.R., Makiev V.D., Mel'kov D.A. K voprosu sejsmicheskogo rajonirovanija territorii respubliki Severnaja Osetija-Alanija [On the issue of seismic zoning of the territory of the Republic of North Ossetia-Alania]. Trudy I mezhdunarodnoj konferencii «Opasnye prirodnye i tehnogennye geologicheskie processy na gornyh i predgornyh territorijah Severnogo Kavkaza», Vladikavkaz, 20-22.09.2007. Vladikavkaz, 2008, pp. 263-278. (in Russian)

3. Zaalishvili V.B., Dzeranov B.V. Ocenka sejsmicheskoj opasnosti territorii RSO-Alanija [Seismic hazard assessment of the territory of North Ossetia-Alania]. Trudy nauchno-prakticheskoj konferencii «Molodye uchenye v reshenii aktual'nyh problem nauki». Vladikavkaz, 2010, pp. 342-345. (in Russian)

4. Zaalishvili V.B., Mel'kov D. A., Dzeranov B.V., Kanukov A.S. Ocenka sejsmicheskoj opasnosti urbanizirovannoj territorii na osnove sovremennyh metodov sejsmicheskogo mikrorajonirovanija (na primere g. Vladikavkaza) [Seismic hazard assessment of the urbanized territory on the basis of modern methods of seismic microzonation (on the example of Vladikavkaz)]. Trudy mezhdunarodnoj nauchno-prakticheskoj konferencii «Molodye uchenye v reshenii aktual'nyh problem nauki». Vladikavkaz, 22-23.05.2010, pp. 348-351. (in Russian)

5. Zaalishvili V.B., Mel'kov D. A., Gabaraev A.F., Dzeboev B.A., Dzeranov B.V., Kanukov A.S., Shepelev V.D. Ispol'zovanie mikrosejsm pri utochnenii kart inzhenerno-geologicheskogo rajonirovanija territorii, javljajushhihsja osnovoj sejsmicheskogo mikrorajo-nirovanija [The use of microseisms for the refinement of geological-engineering zoning maps of the territory, which are the basis of seismic microzonation]. Materialy Vserossijskoj nauchno-prakticheskoj konferencii, posvjashhennoj 10-letiju so dnja osnovanija KNII RAN «Nauka i obrazovanie v Chechenskoj respublike: sostojanie i perspektivy razvitija» 7 aprelja 2011 g., KNII RAN, 2011, pp. 335-342. (in Russian)

6. Zaalishvili V.B., Rogozhin E.A. Ocenka sejsmicheskoj opasnosti territorii na osnove sovremennyh metodov detal'nogo rajonirovanija i sejsmicheskogo mikrorajonirovanija [Seismic hazard assessment of the territory on the basis of modern methods of detailed zoning and seismic microzonation]. Sejsmostojkoe stroitel'stvo. Bezopasnost' sooruzhenij. – M.: VNIINTPI, 2011, No.3, pp. 31-43. (in Russian)

7. Zaalishvili V.B., Dzhgamadze A.K. Inzhenerno-geologicheskoe rajonirovanie goroda Ardon RSO-Alanija [Geological-engineering zoning of the Ardon city in North Ossetia-Alania]. Trudy IV Kavkazskoj mezhdunarodnoj shkoly-seminara molodyh uchenyh «Sejsmicheskaja opasnost' i upravlenie sejsmicheskim riskom na Kavkaze», Vladikavkaz, 24-26.10.2011, pp. 102-106. (in Russian)

8. Zaalishvili V.B., Dzeranov B.V., Gabaraev A.F. Aktualizacija kart sejsmicheskoj opasnosti territorii Respubliki Severnaja Osetija-Alanija [Updating seismic hazard maps of the territory of the Republic of North Ossetia-Alania]. Trudy IV Kavkazskoj mezhdunarodnoj shkoly-seminara molodyh uchenyh «Sejsmicheskaja opasnost' i upravlenie sejsmicheskim riskom na Kavkaze», Vladikavkaz, 24-26.10.2011, 2011a, pp.155-167. (in Russian)

9. Zaalishvili V.B., Dzeranov B.V., Gabaraev A.F. Ocenka sejsmicheskoj opasnosti territorii i postroenie verojatnostnyh kart [Seismic hazard assessment of the territory and construction of probability maps]. Geologija i geofizika Juga Rossii, 2011b, pp. 48-58. (in Russian)

10. Zaalishvili V. B., Mel'kov D. A., Kanukov A. S. Informacionnaja sistema obespechenija gradostroitel'noj dejatel'nosti na osnove informacionnoj bazy dannyh sejsmichnosti i sejsmicheskogo riska [Information system for urban development activities based on an information database of seismicity and seismic risk]. Informatizacija i svjaz'. ISSN 2078-8320, No.5, 2012, pp. 14-18. (in Russian)

11. Zaalishvili V. B., Dzhgamadze A. K. O sozdanii kart inzhenerno-geologicheskogo rajonirovanija territorij naseljonnyh punktov Respubliki Severnaja Osetija-Alanija, kak osnovy sejsmicheskogo mikrorajonirovanija [On the construction of geological-engineering zoning maps of the territories of populated areas in the Republic of North Ossetia-Alania as the basis of seismic microzonation]. Materialy II Vserossijskoj nauchno-tehnicheskoj konferencii «Sovremennye problemy geologii, geofiziki i geojekologii Severnogo Kavkaza», 8-12.11.2012, Groznyj, 2012, pp. 442-446. (in Russian)

12. Zaalishvili V. B. K voprosu sozdanija edinoj karty detal'nogo sejsmicheskogo rajonirovanija [On the issue of creating an integrated detailed seismic zoning map]. Materialy Mezhdunarodnogo simpoziuma «Ustojchivoe razvitie: Problemy, Koncepcii, Modeli», posvjashhennogo 20-letiju KBNC RAN, FGBUN KBNC RAN, Vol. II, 28.06-3.07.2013, 2013, pp. 106-110. (in Russian)

13. Zaalishvili V. B. Nekotorye problemy prakticheskoj realizacii sejsmicheskogo mikrorajonirovanija. Faktory, formirujushhie intensivnost' zemletrjasenija [Some problems of practical realization of seismic microzonation. Factors that are forming the intensity of an earthquake]. Geologija i geofizika Juga Rossii, 2014, No.3, pp. 3-39. (in Russian)

14. Radionov G. P., Goncharova L. I. Publichnaja kadastrovaja karta: uspehi i trudnosti [Public cadastral map: successes and difficulties]. Vestnik Rosreestra, 2010, No.3, pp. 23-27. (in Russian)

15. Introduction to SSL. URL: https://developer.mozilla.org/en/Introduction_to_SSL (data obrashhenija: 18.02.17 g.).

16. Zaalishvili V. B., Melkov D. A., Dzeranov B. V. Modern seismic hazard assessment methods (in example territory of Vladikavkaz-city) //Proceedings of 14th European conference of earthquake engineering. 30 August –03 September, Ohrid, republic Macedonia, 2010, 8 pp.