УДК 623.967

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ОБЪЕКТОВ НЕДВИЖИМОСТИ С УДАЛЕННОГО ТЕРМИНАЛА

А. Ю. БАДАЛОВ

ОАО «Научно-исследовательский институт суперЭВМ», г. Москва

e-mail :Badalov@gollard.ru

В статье анализируются задачи передачи защиты информации с удаленного терминала в мультисервисных сетях, используемых в органах государственной регистрации при регистрации объектов недвижимости.

Ключевые слова: мобильные, программно-аппаратные комплексы, инструмент модернизации инфоструктуры государственного регистрационного обслуживания населения, технологический процесс регистрации, система защиты информации в мультисервисной сети, использование указанного метода в банковской сети электронного обслуживания населения.

Введение

Прогресс общества и Государства прямо связан с развитием строительной индустрии, а следовательно и с увеличением объектов Государственной регистрации прав на недвижимость. Разрыв в темпах роста, количества объектов регистрации регионов и развитием, собственно, технологического процесса регистрации приводит к непроизводственным потерям времени населения (образование очередей), обслуживается меньше абонентов, а следовательно казна регионов недополучает финансовое пополнение в виде Госпошлины и налоговых поступлений. В свою очередь, содержание региональных структур службы регистрации, финансируется из регионального бюджета и при депрессивном его наполнении, регион не в состоянии вкладывать денежные средства развитие регистрационной инфраструктуры. Таким образом, положительные, экономические показатели развития регионов, на прямую, зависят от решения задачи своевременного и качественного регистрационного обслуживания населения. Эффективность работы региональных структур управления Федеральной регистрационной службы (УФРС) определяется их способностью удовлетворять потребность населения в услугах по регистрации объектов недвижимости и оценивается отношением обслуженных заявок к общему количеству заявок, поступивших за определенный период.

Если работа региональных структур УФРС не эффективна, например, из-за ограниченной пропускной способности, необходимо привлекать дополнительные инвестиции на их модернизацию. В случае предоставления Государством платных услуг на первое место выдвигается качество и скорость обслуживания населения и, как следствие, рост наполнения региональных бюджетов. Задача оценки эффективности функционирования государственных служб заключается в формализации связей качества обслуживания населения и тарифных ставок Госпошлины за государственную регистрацию и совершение прочих юридически значимых действий в соответствии со ст. 333.33 Налогового кодекса Российской Федерации. Способов решения задачи максимального охвата населения по предоставлению услуг в сфере регистрации и банковского обслуживания можно предложить достаточно много. Вопрос в эффективности предлагаемых решений.

Например, простое увеличение количества региональных отделений регистрационной службы нельзя считать оптимальным методом повышения эффективности обслуживания населения из-за больших капиталовложений и сроков развертывания (консервативности) стационарных регистрационных пунктов. Более дешевым

и гибким способом повышения качества государственного обслуживания населения может стать метод перемещения небольших, мобильных абонентских пунктов (МАП) к потребителям предоставляемых услуг, т.н. «Виртуальный офис» (Рис.1).

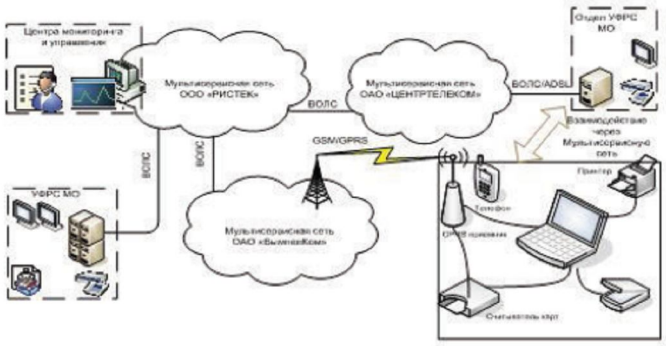

Рис. 1. Функциональная схема интеграции выносного пункта УФРС

При таком подходе, достаточно просто оптимизировать количество мобильных (передвижных) пунктов обслуживания, и следовательно, минимизировать капитальные вложения в модернизацию региональной, регистрационной инфраструктуры посредством поэтапного ввода в эксплуатацию МАП. Современный уровень развития элементной базы и информационных, коммутационных технологий (ИКТ) позволяет создать, как быстро разворачиваемые переносные, так и мобильные (передвижные) абонентские пункты регистрационного и банковского обслуживания населения. На рисунке 2 представлена схема взаимодействия передвижного (выносного) абонентского пункта с региональными банковскими структурами.

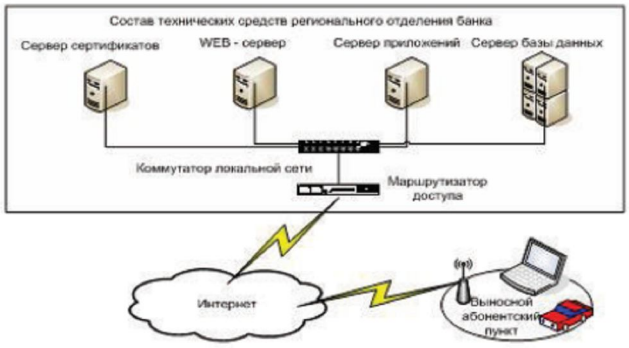

Рис. 2. Схема взаимодействия передвижного (выносного) абонентского пункта с региональными банковскими структурами

Основные принципы построения МАП

1. Безопасность

Основной задачей процедуры регистрации является установление государственных гарантий собственникам недвижимости при обеспечении безусловной конфиденциальности личных данных граждан.

При реализации удаленного обслуживания требуется особая степень защиты. В рамках работы подобной системы должна быть предусмотрена многоуровневая

система безопасности, обеспечивающая заслон от различных угроз. Отдельное внимание уделяется также безопасности работы внутри системы. Таким образом, систему защиты нужно рассматривать как целостный комплексный блок. Если МАП находится в зоне покрытия закрытой мультисервисной сети, с организацией связи по принципу «точка – точка», возможность несанкционированного доступа к передаваемой информации минимальна. Максимальная угроза может исходить при использовании открытых сетей, например Интернет.

Защита от внешних угроз.

Уровень 1 – защита внутренней корпоративной сети отдела УФРС. Чтобы работать с системой, все удаленные операторы должны иметь доступ к веб-серверу банка. Однако обращаться к нему может не только оператор, но и любой другой человек. Поэтому одним из важнейших требований безопасности является выделение так называемой демилитаризованной зоны (DMZ), где и размещаются веб-серверы. Главная особенность этой зоны – максимальная изоляция от корпоративной сети регионального отдела УФРС. Таким образом, серверы отдела становятся относительно недоступными для посторонних, поскольку ни один запрос к системе не попадает в корпоративную сеть напрямую.

В DMZ формируется так называемый выделенный сервер очереди, который только накапливает запросы клиентов, но не передает их в корпоративную сеть банка. Зато размещенный в ней сервер приложений сам периодически обращается к серверу очереди и забирает оттуда только разрешенные системой запросы, руководствуясь при этом правами, установленными для пользователя, от которого эти запросы поступили. Таким образом, вероятность получения несанкционированного доступа к данным, хранящимся в корпоративной сети УФРС, практически равна нулю. Сервер приложений забирает из демилитаризованной зоны только разрешенные запросы.

Уровень 2 – наличие соответствующим образом настроенных, обновляемых и отслеживаемых систем IDS (систем обнаружения и предотвращения атак) на внутреннем и внешнем периметре сети. Позволяет избежать атак на сервера DMZ, а также, в случае взлома сервера в DMZ, минимизировать последствия атаки.

Уровень 3 – защита соединения между Отделом УФРС и удаленным оператором. Вся информация, передаваемая между клиентом и веб-сервером УФРС, шифруется. Для этого могут использоваться различные протоколы шифрования (SSL/TLS (двусторонний SSL), DES(3DES)+RSA и др.) с различными вариантами ключей.

Уровень 4 – безопасный вход в систему. Следует предусмотреть разные способы аутентификации пользователя, в частности:

– по логину и паролю;

– по сертификату электронно-цифровой подписи (ЭЦП);

– по сертификату ЭЦП и паролю.

В данном случае «пароль», которым будет пользоваться клиент, – это не просто набор символов, но еще и инструментарий, позволяющий менять пароли и управлять ими, например, требовать смены пароля через определенные промежутки времени. Совместное использование сертификата и пароля при регистрации в системе гарантирует надежную защиту соединения и однозначную аутентификацию клиентов.

Уровень 5 – Комбинирование промышленных стандартов средств электронно-цифровой подписи и средств криптозащиты информации (СКЗИ) и внутренних разработок по безопасности.

Уровень 6 – Всегда должен высылаться код подтверждения операций. Без ввода данного кода операция не производится.

Защита от внутренних угроз

Все действия удаленных сотрудников и сотрудников регионального отдела тщательно протоколируются системой. Система должна иметь возможность отследить попытку несанкционированного доступа, адреса оборудования и учетные данные, с использованием которых мошенник пробует произвести, какие бы то ни было операции, и по возможности предотвратить проведение этих операций. Для внутренней защиты необходимо четкое разграничение прав доступа и функциональных обя-

занностей сотрудников регионального отдела, обслуживающих систему удаленного обслуживания (по максимуму, для организации сговора необходимо участие всех сотрудников, обслуживающих систему).

2. Ширина полосы пропускания каналов связи

В процессе регистрации предполагается передача большого объема информации, в том числе, картографической в обоих направлениях. По мнению специалистов УФРС по МО, канал связи должен обеспечивать скорость передачи данных не менее 2 Мбит/сек., т.е. канал связи необходимо относить к широкополосным. Существенным ограничением для каналов связи является требование мобильности – возможно, использовать только беспроводные технологии. Необходимую скорость передачи могут обеспечить радиорелейные и спутниковые каналы связи, работающие на несущей частоте более 800 МГц. Однако радиорелейные линии и спутниковые каналы связи предполагают работу со стационарной аппаратурой т.к. требуют точной настройки пространственной ориентации антенны, но в этом случае выносной абонентский пункт теряет мобильность. Каналы передачи данных на основе мобильной связи имеют существенное ограничение по скорости передачи данных – так например мобильные сети, использующие технологию 3G (HSDPA), имеют скорость обратного канала (от терминала в сторону сети) не более 384 Кбит/сек.; мобильные сети, использующие технологию CDMA, – не более 153 Кбит/сек. Наиболее высокие скорости обеспечивают мобильные сети 3,5G (HSUPA) – до 1,9 Мбит/сек., но строительство таких сетей не начато. Требуемую скорость 2 Мбит/сек. обеспечивает технология WiMAX (IEEE 802.1be) – до 5 Мбит/с прямой канал и до 2 Мбит/с обратный канал. В настоящее время, операторами связи активно ведутся работы по развертыванию сетей WiMAX на территории Московской области (Синтерра, Роснет, АртЭКС и д.р.).

Таким образом, оптимально, с нашей точки зрения, связь между региональным отделом УФРС и МАП можно осуществить при использовании технологии WiMAX. В областях, еще не охваченных сетями WiMAX, единственным способом организации широкополосного обмена между оператором МАП и мультисервисной сетью региональных отделов УФРС могут служить локальные сети операторов спутникового Интернета.

3. Электронная цифровая подпись

Согласно процедуре регистрации заявитель должен получить на руки свидетельство, подписанное уполномоченным лицом. В условиях удаленного доступа оператор может обеспечить данное условие только при технической поддержке применения средств электронной цифровой подписи (ЭЦП). В целях создания единого пространства цифровой подписи Постановлением Правительства РФ от 30 июня 2004 года № 319 на Росинформтехнологии возложены функции уполномоченного федерального органа (УФО) исполнительной власти в области ЭЦП [2]. Для реализации функций УФО ФГУП НИИ «Восход» в 2004 году по заданию Росинформтехнологии создал единый государственный электронный реестр (ЕГЭР) сертификатов уполномоченных лиц удостоверяющих центров и сертификатов уполномоченных лиц федеральных органов государственной власти, а также удостоверяющий центр Росинформтехнологии (УЦ). Единый государственный электронный реестр сертификатов ключей подписи уполномоченных лиц обеспечивает:

- возможность доступа пользователей и должностных лиц, в том числе с использованием Internet;
- подтверждение подлинности ЭЦП уполномоченных лиц УЦ в выданных ими сертификатах ключей подписей.

Таким образом, технология мобильных пунктов обслуживания является прекрасной площадкой для «обкатки» технологических решений при создании инфраструктуры единого пространства электронной подписи.

4. Безналичная оплата Госпошлины

В настоящее время, для УФРС платежным документом о внесении Госпошлины за государственную регистрацию являются либо корешок банковского извещения или копия платежного извещения, т.е. бумажный документ. Однако многие банки уже имеют разветвленные сети терминалов безналичной оплаты банковскими кар-

точками («пластиковые деньги»), в том числе как закрытые GPRS сети, так через Интернет. Если УФРС заключит с банком договор об оплате Госпошлины, данной, услуге будет присвоен код оплаты, и достаточно иметь в мобильном комплексе считыватель пластиковых карт и выход в банковскую сеть чтобы осуществлять платеж непосредственно в месте размещения мобильного абонентского пункта.

5. Аппаратная поддержка МАП

Минимальная аппаратная конфигурация МАП:

1. Notebook средней производительности, например Asus Eee 1000, со встроенным GPS;
2. Портативный принтер;
3. Портативный сканер;
4. Спутниковый трансивер с антенной;
5. Радиомодем;
6. Цифровая фотокамера;
7. Считыватель пластиковых карт.
8. Считыватель чипа биопаспортов.

По каждой из позиций выбор достаточно широкий.

Выводы:

- Ежегодный ввод в эксплуатацию одного, двух переносных программно аппаратных комплексов при каждом районном отделе УФРС позволят решить проблему качественного обслуживания населения в сфере Государственной регистрации прав собственности без ущерба для регионального бюджета;
- Развитая инфраструктура мультисервисных, локальных сетей (основа функционирования МАП) позволяет без существенных затрат реализовать принцип «одного окна» при обслуживании населения (оформление прав собственности и оплата услуг осуществляется в одновременно);
- Высокая пропускная способность каналов связи мультисервисных сетей позволяют обеспечить картографическое сопровождение процедуры регистрации объектов недвижимости, что наиболее актуально в удаленной сельской местности.

Заключение:

В материалах статьи доклада представлены материалы по методам материалы защиты информации при использовании мобильных программно-аппаратных комплексов в региональных службах регистрации и банковского обслуживания населения.

Литература

1. В.К. Демин, Н.Н. Тютин, Г.К. Храмешин, С.М. Чудинов «Региональные информационные системы, методы их структурной и функциональной оценки». Белгород, 2008.
2. Смирнова З.В., Светлакова Е.Р. Экономические методы развития факторинга для инновационного развития предприятия, Москва, ГОУ: МАРТИТ, 2009.

ACTUAL OF INTRODUCTION OF MOBILE HARDWARE-SOFTWARE INFORMATION TECHNOLOGIES IN SPHERE OF STATE REGISTRATION SERVICE OF THE POPULATION

A. U. BADALOV

JSC «NII superIBM», Moscow

e-mail :Badalov@gollard.ru

Mobile hardware-software complexes – advanced tool of modernization of a village infrastructure of State registration service of the population. In the report the problems of transfer and protection of the information from the removed terminal in public, multiservice networks are analyzed.

Key words: method of direct search of a condition, computing and multiservice systems, method of structural transformations, method of decomposition of structural transformations with use of mathematical logic, an estimation of reliability computing systems of difficult structure.