



ЗАЩИЩЕННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА ЭНЕРГОПОТРЕБЛЕНИЯ

О.М. Петрова

д.т.н., ст.н.с., ведущий специалист, «Compania Dekart» SRL

В данной статье предлагается создание защищенной автоматизированной системы учета и контроля энергопотребления, базирующейся на современных методах и средствах защиты информации. Предлагаемый подход должен стать базой для включения информационной составляющей рынка энергии в электронное государство.

Ключевые слова – цифровая подпись, система учета, энергопотребление.

1. ВВЕДЕНИЕ

Неустойчивость рынка энергоносителей, продолжающееся сокращение не возобновляемых источников энергии, трудности экономики как РМ, так и остальных государств СНГ, заставляют с большим вниманием относиться к проблеме энергосбережения. Одним из базовых шагов по решению данной проблемы является точный учет и контроль потребления энергии. В то же время современный уровень развития информационных технологий (ИТ) позволяет говорить о создании электронного государства (электронного правительства, электронного образования, электронной медицины и т.п.) [11]. Применение достижений ИТ в энергосистемах позволит не только решить часть проблем последних, но и придать компонентам ИТ новый качественный уровень.

2. ПРОБЛЕМЫ СИСТЕМ УЧЕТА ЭНЕРГОПОТРЕБЛЕНИЯ В РЕСПУБЛИКЕ МОЛДОВА

Система учета энергопотребления может использоваться в чисто технических целях для определения узких мест локальных энергосистем, выявления точек максимального потребления энергии и возможности снижения энергозатрат. С другой стороны системы учета могут быть использованы в коммерческих целях при расчетах поставщиков энергии и потребителей. Идеальный вариант – наличие единой системы учета (и управления) энергоресурсов в рамках государства. Данная система смогла бы стать средством контроля в энергосистеме государства на всех этапах производства, транспортировки энергоносителей и энергопотребления, обеспечивая техническими средствами многокомпонентный механизм согласования экономических интересов поставщиков и потребителей энергии. В этом случае единая государственная система учета

энергоресурсов смогла бы стать составной частью проектов «Электронное государство» и «Электронное правительство» [6 – 11].

В настоящее время в Республике Молдова автоматизированные системы учета существуют только в крупных компаниях (в частности, занимающихся либо производством энергии, либо транспортировкой энергоносителей). На уровне бытовых потребителей учет сводится к снятию показаний счетчиков самим потребителем и передаче этих данных поставщику, а также визитам представителей компаний-поставщиков для съема показаний счетчиков с последующим занесением вручную информации в базу данных компьютера. В обоих случаях имеет место человеческий фактор. Кроме того, в уже существующих автоматизированных системах учета слабым местом являются средства передачи информации, что снижает надежность данных систем. Проблемы существуют как непосредственно с каналами связи, так и защитой передаваемой информации от несанкционированного доступа, возможности модификации.

3. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Наиболее надежным, по мнению автора, техническим инструментом, применяемым для защиты информации, в настоящее время является технология РКІ (Public Key Infrastructure). РКІ - система защиты информации на основе открытых ключей, т.е. система цифровой подписи с одновременным шифрованием или без него. Данная технология подразумевает наличие у каждого участника системы пары взаимосвязанных ключей (секретного и открытого), причем открытый ключ сертифицируется (заверяется) центром сертификации открытых ключей. Обмен электронными документами¹ между участниками рынка энергии (организациями-поставщиками, компаниями, занимающимися

¹ Согласно закону РМ «Об электронном документе и цифровой подписи» [1] электронный документ - информация в электронной форме, создаваемая, структурируемая, обрабатываемая, хранимая, передаваемая с помощью компьютера, других электронных устройств или программных и технических средств, подписанная в соответствии с настоящим законом цифровой подписью.

транспортировкой и распределением, и потребителями) должен осуществляться в защищенном режиме, т.е. каждый электронный документ должен быть подписан цифровой подписью ответственного лица. При получении подписанного электронного документа должна происходить проверка цифровой подписи. Во время данной процедуры решаются две задачи. Первая – получатель убеждается в том, что документ подготовлен именно тем лицом (представителем организации), кто его подписал. Вторая задача – получатель документа может убедиться в том, что электронный документ пришел к нему в не модифицированном виде. Согласно закону РМ «Об электронном документе и цифровой подписи» [1] цифровая подпись под электронным документом имеет те же права, что и обычная подпись под документом на бумажном носителе.

4. ПЕРСПЕКТИВЫ СОЗДАНИЯ ГОСУДАРСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В РЕСПУБЛИКЕ МОЛДОВА И ВКЛЮЧЕНИЯ В НЕГО ЭНЕРГЕТИЧЕСКОГО СЕКТОРА

В настоящее время уже начата работа по созданию системы защищенного электронного документооборота (ЭДО) в рамках государства. Технической базой безопасности системы ЭДО является PKI. В рамках проекта будет создано хранилище сертификатов открытых ключей граждан Республики Молдова – Public Key Directory. Предполагается, что любой гражданин будет иметь собственную пару ключей (секретный и открытый) и сертификат открытого ключа. Все выданные центрами сертификации открытых ключей сертификаты помещаются в Public Key Directory и являются общедоступными (по чтению). В случае компрометации секретного ключа (кражи, потери носителя с ключом, порчи ключа, увольнения сотрудника и т.п.) соответствующий сертификат открытого ключа помещается центром сертификации в список отозванных сертификатов. Таким образом, обеспечивается невозможность незаконного использования злоумышленником похищенных ключей для подделки чужой подписи.

Принятие закона о цифровой подписи [1] дает правовую основу для построения иерархии доверительных пространств [4] относительно центров сертификации внутри отдельного государства. При этом вышестоящий центр сертификации сертифицирует ключи нижестоящих центров. На самой вершине данной пирамиды должен стоять национальный центр сертификации государства (можно привести аналогию с банковской системой – центральный банк и остальные банки). Кроме того, существует возможность кросс-сертификации двух одноуровневых центров сертификации. Это позволяет обмениваться подписанными электронными документами не только в границах одного предприятия, отрасли,

государства, но и между различными отраслями и даже различными государствами [4, 5].

В данном случае повышается надежность взаимозачетов и взаиморасчетов между партнерами, между поставщиками услуг и клиентами. Поскольку показатели измерительных приборов в автоматизированных системах передаются по каналам связи в виде пакетов данных, они по определению являются электронными документами. Данные электронные документы подлежат защите, т.к. они служат базой для финансовых расчетов между субъектами рынка энергии. Для создания защищенной автоматизированной системы учета и контроля энергопотребления требуется включение в стандартную схему элементов PKI. При применении технологии PKI в целях защиты информации возникает возможность включения части автоматизированных систем учета энергопотребления (в рамках предприятия, отрасли, бытовых потребителей и государства в целом) в единую систему защищенного ЭДО государства.

5. ПРЕДЛАГАЕМАЯ СТРУКТУРА ЗАЩИЩЕННОЙ СИСТЕМЫ УЧЕТА ЭНЕРГОПОТРЕБЛЕНИЯ

Предлагается следующая схема базового блока системы учета энергии (см. рис. 1).

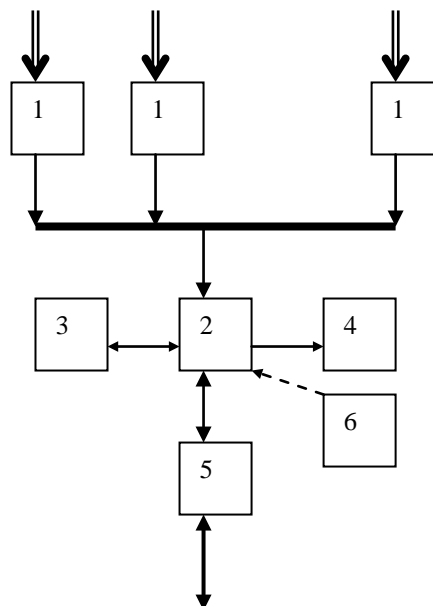


Рис. 1

- 1 – электронный измерительный прибор учета потребления энергии;
- 2 – микрокомпьютер;
- 3 – блок памяти для хранения показаний измерительных приборов в подписанном виде;
- 4 – блок визуализации;
- 5 – блок сопряжения с каналом передачи информации;
- 6 – носитель с секретным ключом лица, ответственного за блок учета, Key Storage Device.

Электронный измерительный прибор 1 соединен с микрокомпьютером 2. Через установленные промежутки времени или по сигналу с пульта управления организации-поставщика (электроэнергии, газа, тепловой энергии) производится съем показаний измерительного прибора, полученные значения выводятся на блок визуализации 4. Одновременно с этим в микрокомпьютере 2 выполняется операция генерации цифровой подписи под пакетом данных с показаниями счетчика и происходит запись подписанных показаний прибора учета в блок памяти 3 (секретный ключ ответственного лица попадает в микрокомпьютер из носителя 6). По окончании операции подписанный электронный документ поступает на блок сопряжения с каналом передачи информации 5. В качестве канала связи могут быть использованы телефонная линия, радио канал, GSM и т.п. В общем случае к микрокомпьютеру могут быть подключены несколько измерительных приборов – электроэнергетики, газа, горячей воды. По каналу связи информация поступает на пульт управления организации-поставщика. Одновременно с этим происходит накопление полученной информации в базах данных для последующего использования при расчетах за потребленную энергию. При такой структуре облегчается взаимосвязь поставщика энергии и потребителя. Возникает возможность передачи каких-либо сообщений поставщика с визуализацией их в блоке 4. В качестве хранилища секретного ключа могут быть использованы smart-карты, Token'ы. Объем памяти данных устройств позволяют хранить там не только секретный ключ, но и информацию, полученную от прибора учета. В этом может возникнуть необходимость при решении спорных вопросов, связанных с поставкой и потреблением энергии.

6. ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАЩИЩЕННОЙ СИСТЕМЫ УЧЕТА ЭНЕРГОПОТРЕБЛЕНИЯ

Предлагаемая схема базового блока системы учета энергии может быть усовершенствована за счет следующих модификаций. Перед передачей данных на пульт управления поставщика энергии вместо одной будут выполняться две операции:

1. показания приборов учета подписываются цифровой подписью лица, ответственного за прибор учета;
2. подписанные данные кодируются с помощью одного кодов, обнаруживающих и исправляющих ошибки (например, БЧХ).

В такой модификации возникает необходимость при передаче данных на значительные расстояния при возможных плохих каналах связи, например от прибора учета, стоящего в удаленном населенном пункте и т.п.

Замена механических приборов учета электронными,

тем более соединенными с микрокомпьютером, дадут возможность реально использовать многотарифную систему учета энергопотребления.

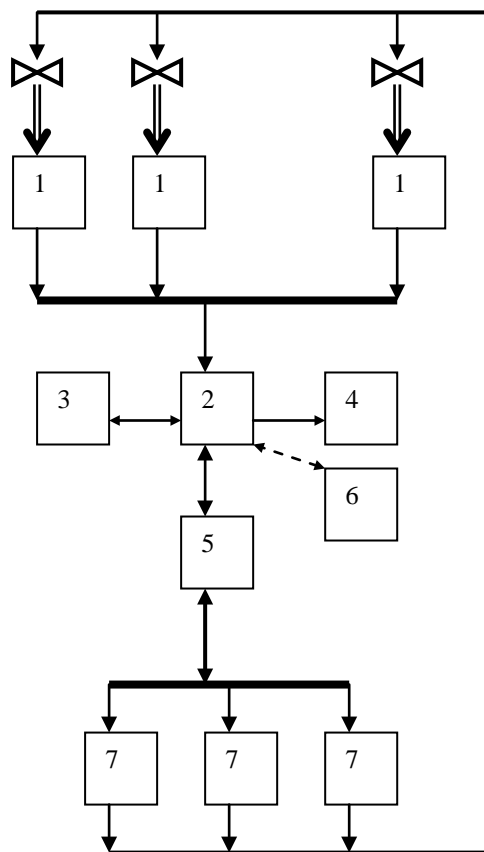


рис. 2

- 1 – электронный измерительный прибор учета потребления энергии;
 2 – микрокомпьютер;
 3 – блок памяти для хранения показаний измерительных приборов;
 4 – блок визуализации;
 5 – блок сопряжения с каналом передачи информации;
 6 – носитель с секретным ключом лица, ответственного за блок учета, Key Storage Device;
 7 – пульт управления организации-поставщика энергии.

Также возникает возможность замены базового блока учета энергопотребления на блок учета и управления энергопотреблением. При возникновении аварийной ситуации, либо при отсутствии платежей за потребленную энергию компания-производитель или компания поставщик по сигналу пульта управления прекращает подачу энергии потребителю.

Кроме того, хранилище секретного ключа (Key Storage Device) может быть использовано для облегчения платежей потребителя за израсходованную энергию. После получения информации с блока учета компания-поставщик выставляет потребителю счет (в электронном виде),

подписанный цифровой подписью ответственного лица финансовой службы компании-поставщика. Счет по каналу связи поступает в микрокомпьютер 2. Потребитель поверяет цифровую подпись под электронным счетом, и, если верификация проходит успешно, записывает счет на Key Storage Device. Поскольку построение электронного государства связано с улучшением оснащения средствами вычислительной техники, связи организаций, учреждений, граждан, то предполагается, что с домашнего компьютера, в отделениях банков, учреждений связи или иных специально созданных мест, любой гражданин сможет произвести оплату по электронному счету, хранящемуся на Key Storage Device.

8. ЗАКЛЮЧЕНИЕ

Внедрение защищенной автоматизированной системы учета и контроля энергии позволит сделать процесс учета более эффективным и прозрачным. Кроме того, данная система смогла бы стать одной из составных частей общегосударственной системы «электронное государство».

ЛИТЕРАТУРА

- [1] Закон Республики Молдова «Об электронном документе и цифровой подписи» (N 264-XV от 15.07.2004)
- [2] Закон Республики Молдова «Об электронной торговле» (N 284-XV от 22 июля 2004 года)
- [3] Закон Республики Молдова «Об информатизации и государственных информационных ресурсах» (N 467-XV от 21.11.2003)
- [4] Куцый А. Инфраструктура современных криптографических систем защиты информации// Acta Academia, Кишинев: Evrica, 1999. С. 135 – 142.
- [5] Черешкин Д. Основные положения по формированию единого информационного пространства стран-участниц СНГ// Acta Academia, Кишинев: Evrica, 1999. С. 312 - 315.

- [6] Дрожжинов В.И. Мониторинг услуг электронного правительства// http://www.processconsulting.ru/project/conclusion/zak_droj.pdf
- [7] United States Department of the Interior Bureau of Land Management. Information Recourses Management Strategic Plan (2002-2005)// <http://www.blm.gov/nhp/efoia/wo/fy02/im2002-180attach2.pdf>
- [8] Implementing the President's Management Agenda for E-Government. E-Government Strategy// http://www.whitehouse.gov/omb/egov/downloads/2003egov_strat.pdf
- [9] E-Gov Related Legislation Overview// http://www.whitehouse.gov/omb/egov/about_leg.htm
- [10] Larsen E., Rainie L. The Rise of the E-Citizen. How People Use Government Agencies' Web Sites// Pew Internet & American Life Project http://www.pewtrusts.com/pdf/vf_pew_internet_e-citizens.pdf
- [11] Постановление Президента РМ "О создании информационного общества в Республике Молдова" N 1743-III от 19.03.2004



О.М. Петрова родилась в 1966 г. Закончила с отличием в 1987 г. Кишиневский политехнический институт (специальность «Автоматика и телемеханика»). В 1991 г. защитила кандидатскую диссертацию по теме «Оптимальное масштабирование в АЦВС». В 1995 г. присвоено звание старшего научного сотрудника. Является автором и соавтором более 40 печатных научных и научно-популярных работ в отечественных и зарубежных изданиях, в том числе монографии. С 1987 по 1998 гг. работала в Академии наук Молдовы. С 1998 – ведущий специалист компании Dekart.