ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

ҚазҰТЗУ ХАБАРШЫСЫ

ВЕСТНИК КазНИТУ

VESTNIK KazNRTU

№4 (116)

АЛМАТЫ 2016 ИЮЛЬ

Учредитель:

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Регистрация:

Министерство культуры, информации и общественного согласия
Республики Казахстан № 951 – Ж "25" 11. 1999 г.

Основан в августе 1994 г. Выходит 6 раз в год

Адрес редакции:

г. Алматы, ул. Сатпаева, 22,
каб. 904, тел. 292-63-46
n. fedossenko @ ntu. kz

Нами определялась паропроницаемость пленок, полученных из этих систем, и таким путем исследовалась зависимость между паропроницаемостью, с одной стороны, и гидрофильностью пленкообразователя, а также характером его диспергирования – сдругой. Из полученных данных следует, что гидрофильность полимера сильно влияет на паропроницаемость, полученной на его основе пленки.

Ключевые слова: паропроницаемость кожи, водостойкость кожи, гидрофильные полимеры, физико-механические и гигиенические свойства.

I.S. Jiyembetova, A.I. Ibrayeva

Study of factors affecting performance properties obtained hydrophobically leather shoes for army

Summary.Work has been done to identify: 1) the effect of different types of coatings to water vapor permeability of the skin, and 2) the degree of lowering the water vapor permeability of the skin, finished with emulsion coatings. This method involves the evaporation of moisture through the test material at high temperatures and intense humidity on one side of the material and normal humidity - on the other side. For the production of coatings on the skin of the solution of hydrophobic polymers, their aqueous dispersions and solutions entering the hydrophilic polymers. We determined vapor permeability of films obtained from these systems, and thus investigated the relationship between water vapor permeability, on the one hand, and hydrophilic film former, and the nature of its dispersion - on the other. The data obtained indicate that the hydrophilic polymer strongly influences the permeability to water vapor, obtained based on this film.

Keywords:water vapor permeabilityof the skin, waterproof material, hydrophilic groups, physical, mechanical and hygienic properties.

УДК 004.056.5

Р. Г. Бияшев[1], С. Е. Нысанбаева[1], Е. Е. Бегимбаева[2]
([1]Институт информационных и вычислительных технологий КН МОН РК,
[2]Казахский национальный университет им. аль-Фараби,
Казахстан, г. Алматы, enlik_89@mail.ru)

РАЗРАБОТКА МОДЕЛИ ЗАЩИЩЕННОГО ТРАНСГРАНИЧНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

Аннотация. Статья посвящена исследованию предложенной модели обеспечения трансграничного обмена и защиты информации при трансграничном взаимодействии в интегрированной системе. Представлена схема защищенного трансграничного информационного взаимодействия. Трансграничное взаимодействие в интегрированной системе обеспечивается за счет создания и использования интеграционного сегмента и национальных сегментов. Представлена модель схемы взаимодействия сторон в интеграционной системе с использованием интеграционного шлюза.

Ключевые слова: информационное взаимодействие, трансграничный обмен, пространство доверия, информационная безопасность, цифровая подпись.

Обеспечение защищенного трансграничного информационного взаимодействия для каждой независимой страны является важной задачей. Укрепления доверия и безопасности между взаимодействующими странами (сторонами) в информационном обмене выходят на первый план. Принимая во внимание трансграничный характер вопросов обеспечения информационной безопасности электронных документов при трансграничном информационном обмене, требуется дальнейшее совершенствование международного сотрудничества в данной области, соответствующего принципам равноправного международного информационного обмена. Обусловлено это тем, что актуализируется проблема равноправного участия Республики Казахстан в международном информационном обмене и в процессах международного регулирования информационной безопасности.

Электронное взаимодействие, а в особенности трансграничное, электронное взаимодействие, подразумевает совместную работу множества разнородных информационных систем. Механизмы управления правами в каждой из них могут строиться на различных принципах и реализовываться различными способами [1].

Так как трансграничное взаимодействие – это взаимодействие субъектов различных правовых полей, то одной из основных проблем при трансграничном информационном взаимодействии (ТИВ) является нерешенность комплекса организационных, технологических и правовых вопросов обеспечения юридической значимости электронной информации в интегрированной системе. В число основных проблем обеспечения информационного взаимодействия входит разработка эффективного и надежного механизма управления правами субъектов и обеспечения каждой из сторон этого взаимодействия собственной информационной безопасности и защиты своего информационного суверенитета.

Решение задач надежной и эффективной интеграции территориально распределенных государственных информационных ресурсов и информационных систем органов государств-членов, обеспечения взаимодействия органов власти государств-членов в электронном виде, в том числе предоставление возможности обмена электронными документами, имеющими юридическую силу (или взаимно признаваемыми таковыми), является одним из ключевых направлений работ по созданию и внедрению интегрированной информационной системы Евразийского экономического союза (ЕАЭС) [2].

Обмен электронными данными между сторонами информационного обмена в интегрированной системе обеспечивается за счет создания и использования национальных сегментов (далее - сегмент) и интеграционного шлюза (далее - шлюз). Эти сегменты представляют собой совокупность защищенной системы передачи данных, входящих в состав каждого узла взаимодействующих сторон информационного обмена (рис. 2).

Юридическая сила электронного документа при ТИВ в интегрированной системе подтверждается на основе применения службы доверенной третьей стороны (ДТС). Инфраструктура ДТС и удостоверяющего центра (УЦ) размещается в национальных сегментах, и организуются на уровне каждой взаимодействующей стороны. УЦ обеспечивает сертификатами ключей подписи для взаимодействия уполномоченных доверенных третьих сторон национальных сегментов интегрированной системы.

Основными задачами ДТС являются:

- осуществление подтверждения подлинности электронных документов и цифровой подписи (ЦП) субъектов информационного взаимодействия в фиксированный момент времени;
- осуществление гарантий доверия в трансграничном обмене электронными документами;
- обеспечение правомерности применения ЦП в исходящих и входящих электронных документах и сообщениях в соответствии с правилами и требованиями законодательства той взаимодействующей стороны, где находится доверенная третья сторона [3].

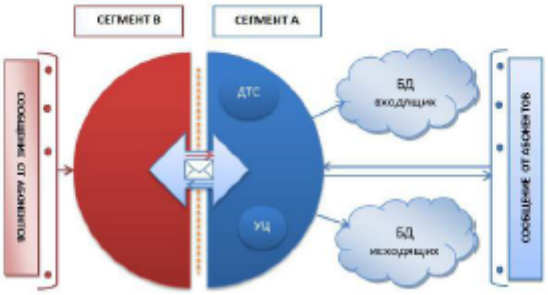

Рис. 2. Схема взаимодействия сегмента в интегрированной системе

При документообороте в трансграничном пространстве доверия могут возникать конфликтные ситуации. Эти ситуации могут быть связаны с формированием, доставкой, получением, подтверждением получения электронного документа, а также с использованием в данных документах

ЦП. Разрешение конфликтных ситуаций должно входить в задачи удостоверяющего центра. Конфликтные ситуации могут возникать в следующих случаях:

- неподтверждение подлинности защищенных электронных документов средствами проверки ЦП получателя;
- оспаривание факта идентификации владельца ЦП, подписавшего электронный документ;
- заявление отправителя или получателя электронного документа об его искажении;
- оспаривание факта отправления и (или) получения защищенного электронного документа;
- оспаривание времени отправления и (или) получения защищенного электронного документа;
- иные случаи возникновения конфликтных ситуаций.

При реализации схемы защищенного ТИВ применяются основные термины и определения модельного закона «О трансграничном информационном обмене электронными документами» [3].

В данной работе предлагается модель схемы взаимодействия двух сторон в интегрированной системе. Рассмотрим моделируемую технологию на примере передачи информации от абонентов стороны «А» абонентам стороны «В».

Информационное взаимодействие между сторонами «А» и «В» при обмене конфиденциальными электронными документами предлагается осуществлять с помощью специальной автоматизированной системы ТИВ – интеграционного шлюза.

Интеграционный шлюз состоит из двух или более автоматизированных рабочих мест в зависимости от числа взаимодействующих сторон. Каждое автоматизированное рабочее место является собственностью одной из взаимодействующих сторон и защищается принятыми в соответствующей стороне средствами защиты. Каждая из взаимодействующих сторон определяет для своего рабочего места криптографические средства, аппаратно-программные средства защиты информации от несанкционированного доступа и другие технические и программные средства.

При передаче информации по защищенному каналу с помощью интеграционного шлюза должно быть обеспечено выполнение требований целостности, доступности, конфиденциальности информации в процессе трансграничной передачи.

С целью разработки методологии создания электронного трансграничного пространства доверия предполагается установить круг понятий, основными из которых являются понятия электронного документа как объекта трансграничного обмена и получателей документов, как субъектов (абоненты) обмена.

В составе национальных сегментов интегрированной системы должны функционировать:

- программно-аппаратный комплекс доверенной третьей стороны (ДТС);
- удостоверяющий центр (УЦ).

На рис. 2 представлена схема взаимодействия сторон «А» и «В» трансграничного информационного обмена. Взаимодействующие стороны имеют разные стандарты криптографической защиты информации. Поэтому обмен информацией между сторонами «А» и «В» передается по защищенному каналу в открытом виде с помощью интеграционного шлюза.

В интеграционный шлюз со стороны «В» пересылается в открытом виде сообщение *M* (объект), которое содержит заголовок. Заголовок сообщения содержит сведения об отправителе, адресате, пути следования, дата, метка времени отправления и получения, метка секретности и др. Резервная копия с заголовками фиксируется и хранится во входящих и соответственно исходящих Базах Данных (БД).

Рассмотрим национальный сегмент стороны «А» и информационный обмен между абонентами стороны «А» (субъект) и сегментом. Полученное в открытом виде сообщение *M* необходимо переслать абоненту стороны А.

Метка секретности в заголовке сообщения предоставляет сведения о конфиденциальности содержания сообщения и позволяет ограничить список получателей, которые могут открыть, переслать, отправить сообщение. Метки секретности для субъектов (степень благонадежности) и объектов (степень конфиденциальности информации) имеют следующие категории:

1. особо важности;
2. совершенно секретно;
3. секретно;
4. конфиденциально;
5. не секретно.

Наличие метки секретности проверяется удостоверяющим центром. При наличии метки секретности сообщение шифруется и подписывается цифровой подписью, иначе сообщение только подписывается ЦП.

Абонент имеет право получать только те документы, уровень секретности которых не превышает его собственный уровень. Если метка секретности абонента не превышает метки секретности сообщения, то ему это зашифрованное сообщение с ЦП не пересылается. А отправителю сообщения посылается информация с причиной отказа, т.е. отправляется «информация об отказе для отправителя». Данные о сообщении отправляются в БД исходящих объектов для разрешения возможных конфликтных ситуаций.

Выполнение правовой функции электронного документа обеспечивается за счет реквизитов документа. Одним из реквизитов электронного документа является цифровая подпись. Такая подпись предназначена для идентификации лица, которым подписан передаваемый электронный документ, а также для установления отсутствия изменений в документе после его подписания.

Выделяется удостоверяющий центр (подразделение или внешняя организация), который с помощью специализированного программного обеспечения генерирует так называемые «сертификаты ключей» для каждого пользователя. Ключ ЦП состоит из закрытого ключа (он доступен только своему владельцу, с его помощью владелец может подписать документ ЭП) и открытого ключа (он доступен всем, с его помощью можно определить, кто и когда подписал электронный документ).

В трансграничном информационном обмене каждая из взаимодействующих сторон разрабатывает свои национальные криптографические средства. Основой для создания в предлагаемой модели криптографических средств являются системы шифрования и формирования цифровой подписи, разработанные с использованием алгебраического подхода на базе непозиционных полиномиальных систем счисления (НПСС) или полиномиальных систем счисления в остаточных классах (полиномиальных СОК) [4]. Криптосистемы, разработанные на базе НПСС, называют нетрадиционными, непозиционными или модулярными.

В предлагаемой модели взаимодействия сторон будет использована система цифровой подписи, разрабатываемая на базе систем ЦП с открытым ключом и НПСС. Применение НПСС позволяет создавать эффективные криптографические системы повышенной надежности, с помощью которых обеспечивается конфиденциальность, аутентификация и целостность хранимой и передаваемой информации [5-7]. При разработке нетрадиционных асимметричных криптографических систем может существенно сократиться длина ключей без потери криптостойкости.

Проводятся работы по созданию модулярной системы ЦП с открытым ключом. При создании этой системы используется модифицированный алгоритм DSA на базе НПСС, который описан в работе [8].

На сегодняшний день нет единой модели технологии трансграничного обмена информации. Разрабатываемая модель технологий защищенного трансграничного информационного обмена будут способствовать созданию национального сегмента и развитию отечественных средств обеспечения информационной безопасности. Результаты этих работ будут применены при реализации структурной схемы трансграничного информационного обмена в Республики Казахстан.

*Исследования проводятся в рамках грантового финансирования Министерства образования и науки Республики Казахстан.

ЛИТЕРАТУРА

[1] Сазонов А.В. Инфраструктура и технология управления правами субъектов в трансграничном пространстве // Общие вопросы безопасности информации и объектов №3, 2012, С.83-87.

[2] Концепция использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов //http://www.tks.ru/news/law/2014/10/08/0006.

[3] Модельный закон «О трансграничном информационном обмене электронными документами» // http://www.pvti.ru/.

[4] Акушский, И.Я., Юдицкий. Д.И. Машинная арифметика в остаточных классах. - М.: Советское радио, 1968. - 439 с.

[5] Bijashev, R.G. and Nyssanbayeva, S.E.: Algorithm for Creation a Digital Signature with Error Detection and Correction //Cybernetics and Systems Analysis. №4, 2012, PP. 489-497.

[6] Р.Г. Бияшев, Разработка и исследование методов сквозного повышения достоверности в системах обмена данными распределенных АСУ: Дис. на соискание уч. степ.докт. тех. наук. - М., 1985. - 328 с.

[7] Biyashev R., Nyssanbayeva S., Begimbayeva Y., Magzom M. Modification of the Cryptographic Algorithms, Developed on the Basis of Nonpositional Polynomial Notations //Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015), Vienna, Austria, 2015, PP.170-176.

[8] Biyashev R., Nyssanbayeva S., Begimbayeva Ye., Magzom M. Building modified modular cryptographic systems // International journal of applied mathematics and informatics, Volume 9, 2015, pp. 103-109.

Р.Г. Бияшев, С.Е. Нысанбаева, Е.Е. Бегимбаева

Қорғалған трансшекаралық ақпараттық алмасу моделін зерттемелеу

Түйіндеме. Мақала ұсынылған біріктірілген жүйеде трансшекаралық алмасудағы ақпаратты қорғау мен трансшекаралық алмасуды қамсыздандыру моделін зерттемелеуге арналған. Қорғалған трансшекаралық ақпараттық алмасу сұлбасы ұсынылған. Біріктірілген жүйедегі трансшекаралық алмасу интеграциялық сегмент пен ұлттық сегментті құру мен қолдану арқылы қамсыздандырылады. Интеграциялық жүйедегі интеграциялық шлюзді қолдану арқылы жақтардың әрекеттесу сұлбасының моделі көрсетілген.

Негізгі сөздер: ақпараттық алмасу, трансшекаралық алмасу, сенім кеңістігі, ақпараттық қауіпсіздік, сандық қолтаңба.

R. G. Biyashev, S. E. Nyssanbayeva, Ye.Y. Begimbayeva

The protected cross-border information exchange models development

Summary. The proposed model of ensure cross-border exchange and information security in the cross-border interaction in the integration system are investigated. A schema of the protected cross-border information exchange is proposed. Cross-border interaction of sides for information exchange in the integrated system is provided by the creation and use of the integration segment and national segments. The model of sides' interaction scheme of the integration system using the integration gateway is presented.

Keywords: information interaction, cross-border exchange, a space of trust, information security, digital signature.

УДК 666.189.3

Б. Е. Жакипбаев, А. А. Абдуллин, А. Ш. Кулмаханова, Е. С. Утеулиев
(Южно-Казахстанский государственный университет им. М.Ауэзова,
Шымкент, Республика Казахстан, *E-mail: Bibol_8484@mail.ru)

СИНТЕЗ АРХИТЕКТУРНО-СТРОИТЕЛЬНОГО ТЕПЛОИЗОЛЯЦИОННО-ДЕКОРАТИВНОГО ЦВЕТНОГО ПЕНОСТЕКЛА (ПЕНОКРЕМНЕЗЕМА) НА ОСНОВЕ МЕСТНЫХ ШИРОКОДОСТУПНЫХ АМОРФНО-КРЕМНЕЗЕМИСТЫХ ОПОК ТУРКЕСТАН-УРАНГАЙСКОГО МЕСТОРОЖДЕНИЯ

Аннотация. Пеностекло известно главным образом в качестве ячеистого теплоизоляционного материала, получаемого путем спекания смеси стекольного порошка и газообразователя с последующим отжигом вспененного материала.

Однако синтез архитектурно-строительного цветного пеностекла (пенокремнезема) является менее известным. Хотя этот материал может быть использован в качестве теплоизоляционно-декоративного покрытия в строительстве, особенно в дизайне внутреннего и внешнего интерьера.

Синтезированные образцы цветного пенокремнезема содержат разную окраску, которые, помимо внешнего эстетического вида одновременно, улучшено влияют на физико-технические характеристики.

В данном исследовании решаются вопросы получения цветного пеностекла (пенокремнезема) теплоизоляционно-декоративного назначения непосредственно из широкодоступных аморфно-кремнеземистых природных опок, исключив из схемы традиционной технологии экономически невыгодный и энергоемкий процесс варки и грануляции специальной многокомпонентной стекломассы.

Ключевые слова: пеностекло, пенокремнезем, теплоизоляционно-декоративное, аморфно-кремнеземистое сырье, опоки, силикато-натриевая смесь, красители.