УДК 681.322

М.Ф.БОНДАРЕНКО., д-р техн. наук, И.Д. ГОРБЕНКО, д-р техн. наук, С.П. ЧЕРНЫХ, А.В. ПОТИЙ, канд. техн. наук

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ КАК ОСНОВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАЦИОНАЛЬНЫХ, ВЕДОМСТВЕННЫХ И КОММЕРЧЕСКИХ СИСТЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Введение.

В настоящее время на международном уровне создана нормативная база и сформировались устойчивые взгляды на решения проблем обеспечения информационной безопаности различных систем информационных технологий (ИТ-систем). ИТ-система представляет собой организационно-техническую систему, которая включает в себя:

– совокупность технических средств передачи и обработки информации (ИТ-продуктов), объединенных в функционально полный комплекс;

– совокупность методов и алгоритмов обработки информации в виде соответствующего программного и математического обеспечения;

– информационные и иные ресурсы;

– персонал и пользователей, объединенных по организационно-структурному, тематическому, технологическому, функциональному и другим принципам для осуществления автоматизированной обработки информации.

Подробно взгляды на обеспечение инофрмационной безопасности в национальных системах нами рассмотрены в работах [8-10]. Общим выводом является то, что безопасность систем информационных технологий (ИТ-систем) достигается путем решения взаимосвязанной совокупности задач защиты. Основными задачами защиты является обеспечение конфиденциальности, доступности, целостности и наблюдаемости. Для решения этих задач в рамках ИТ-системы создается комплексная система обеспечения безопасности, которая объединяет административные, технические и криптографические средства защиты (аппаратные, программные, программно-аппаратные), алгоритмическое, математическое, программное, информационное и иное обеспечение и персонал, отвечающий за реализацию в ИТ-системе политики безопасности. В современных ИТ-системой основой решения перечисленных выше задач являются методы криптографии.

В данной статье авторы рассматривают возможность создания в Украине полноценной инфраструктуры открытых ключей, целью наиболее полного удовлетворения потребностей собственников ИТ-систем в обеспечении информационной безопасности и предоставления полного спектра услуг безопасности.

1. Инфраструктура безопасности

В функциональном плане задачи защиты решаются путем реализации функций (услуг) безопасности. На рисунке 1 представлена модель обеспечения безопасности информационных технологий, которая рекомендована Национальным институтом стандартизации и технологий США (NIST) в качестве базовой технической модели [7,9].

Данная модель существенно расширяет существующие модели безопасности и соответсвует концепции обеспечения безопасности ИТ-систем, заложенной в таких документах как ISO/IEC 15408 «Общие критерии оценки ИТ-безопасности», ISO/IEC 17779 «Управление безопасностью», CEM 97/017 и CEM99/045 «Методология оценки ИТ-безопасности».

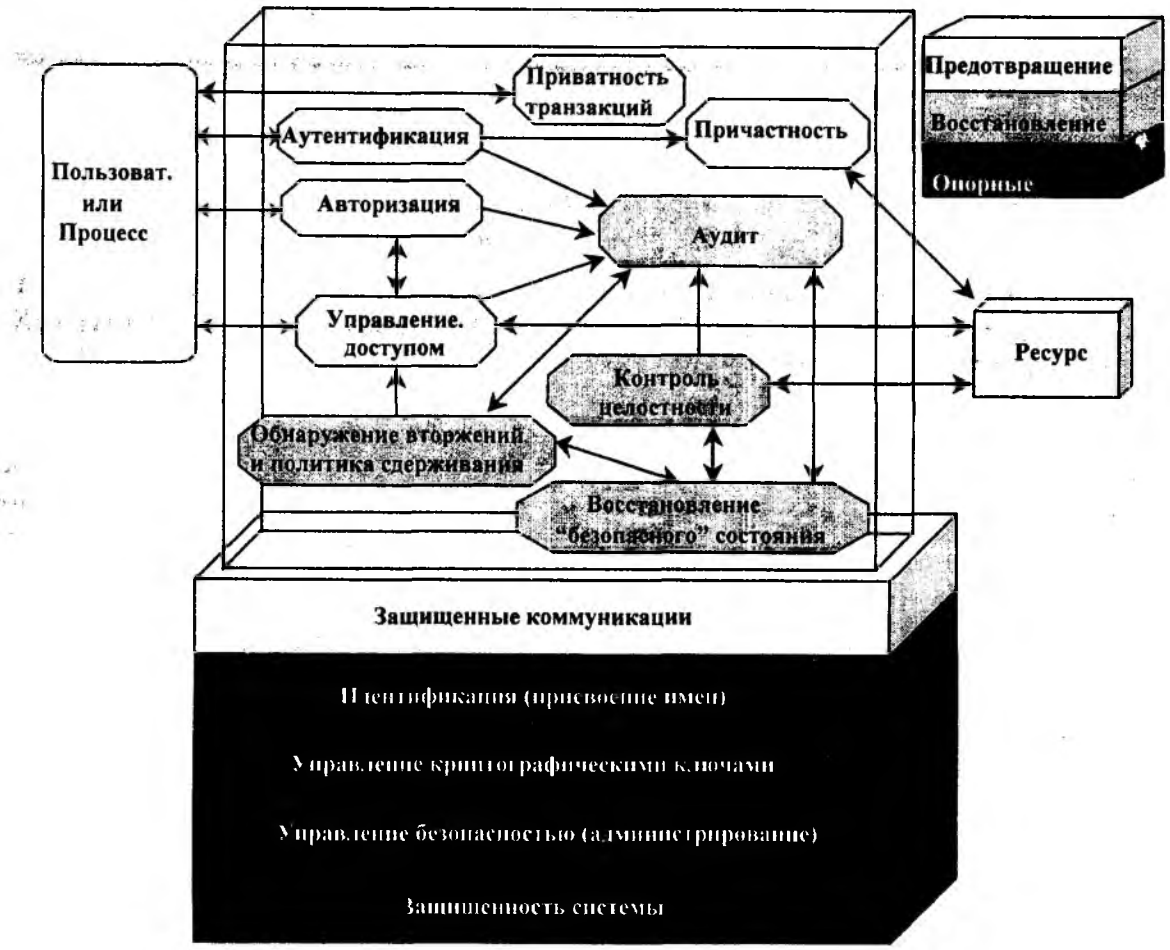

Рис.1

Базовая модель определяет три класса услуг безопасности:

- услуги предотвращения нарушений безопасности;
- услуги обнаружения и восстановления безопасности;
- опорные услуги безопасности.

Рассматриваемые услуги безопасности позволяют решить широкий спектр различных задач обеспечения безопасности, которые присутствуют в любой ИТ-системе. К таким задачам относятся идентификация пользователей, обеспечения конфиденциальности сообщений, управление доступом к различным документам, соблюдение конфиденциальности личной информации (приватности), обеспечение причастности и многие другие. Взаимодействующие объекты и субъекты при установке контакта, при обмене сообщениями (как в on-line, так и в off-line режимах) должны быть твердо «уверены» в личности абонента или подлинности ресурса.

Сейчас можно с уверенность сказать, что основным технологическим инструментом решения этих и других задач в ИТ-системах являются криптографические технологии и особенно методы открытой криптографии. Задачи обеспечения целостности, конфиденциальности, аутентификации, доступности, причастности решаются путем реализации механизмов шифрования, генерации кодов аутентификации сообщений, цифровой подписи, хеширования в основании которых лежит использование одного или нескольких криптографических примитивов [8]. Для решения задач защиты пользователи должны использовать несколько классов криптографических механизмов безопасности. Корпоративные сети отличаются распределенностью (как временной, так и пространственной) информационных и иных ресурсов.

Поэтому одной из важных задач является распределение криптографических ключей и иной служебной информации, необходимой для эффективного управления безопасностью. Основой надежной и эффективной работы криптографических механизмов является управление ключами, которое является опорной услугой безопасности. В международной и национальной практике стандартизации модели, технологии и методы управления ключами рассматриваются в отдельных нормативных документах, что только подчеркивает базисную роль управления ключами.

Согласно международному стандарту ISO/IEC 11770 под *управлением ключами* понимают совокупность методов и процедур, используемых для установления и управления ключевыми взаимоотношениями между авторизованными объектами.

Стандарт определяет одиннадцать функций управления ключами: генерация, регистрация, сертификация, распределение, инсталляция, хранение, формирование производной или разворачивание, архивирование, отмена (аннулирование), дерегистрация и уничтожение ключа. Жизненный цикл управления ключами в общем виде представлен на рис.2. [11]

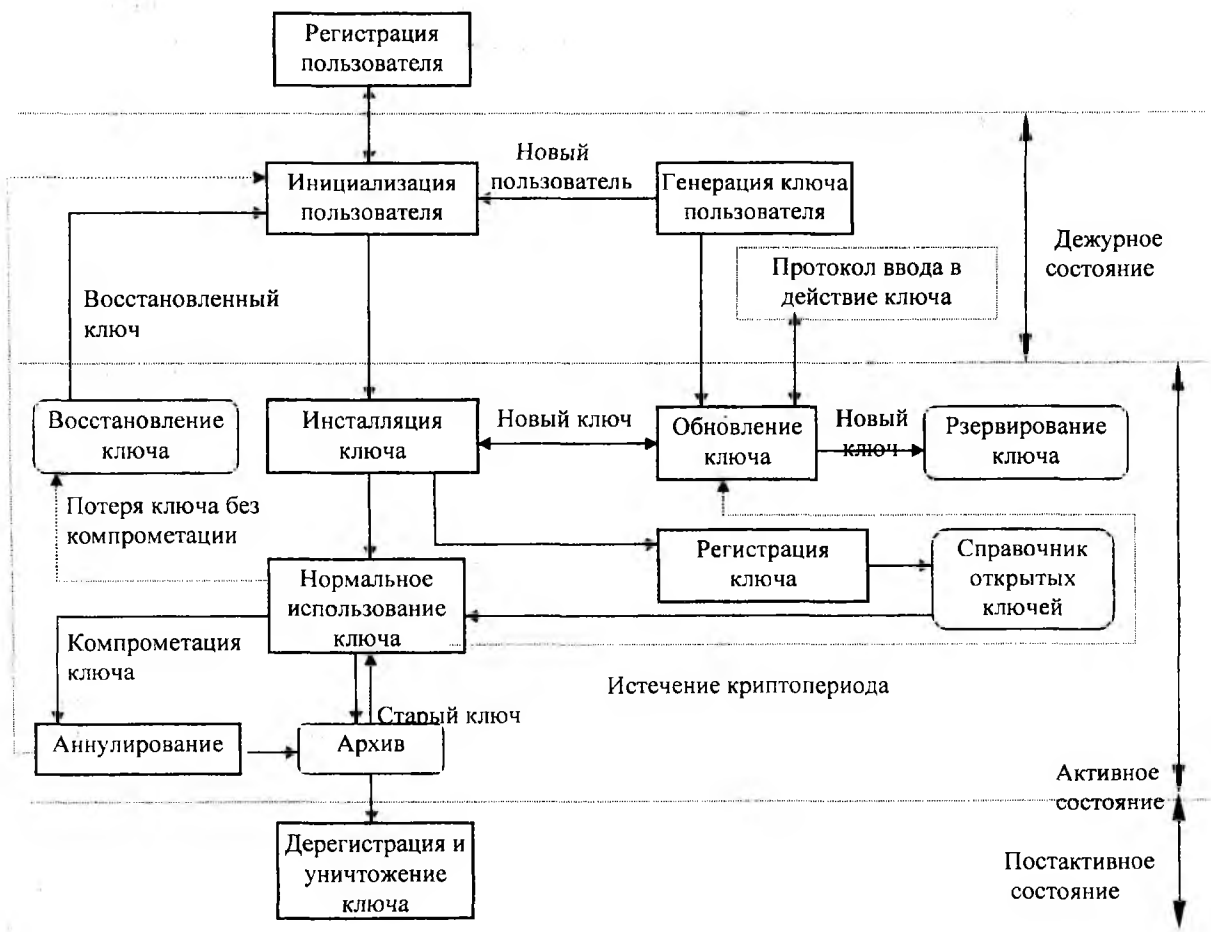

Рис. 2

Для достижения необходимого уровня конфиденциальности, нужно распределить между абонентами симметричные ключи шифрования. Данная задача может быть решена тремя способами:

1) непосредственный обмен ключами между сторонами с использованием механизмов симметричного шифрования;
2) обмен ключами с использование механизмов симметричного шифрования и привлечением доверительной третьей стороны (например, центр распределения ключей или центр передачи ключей);

3) обмен ключами с использование методов несимметричной криптографии с привлечением доверительной третьей стороны (ДТС).

Первый способ эффективен только в малых закрытых системах.

Второй способ может быть распространен и на большие системы. Однако использование механизмов симметричной криптографии не позволяет реализовать услугу причастности при ключевых взаимоотношениях. В связи с этим данный метод нашел широкое распространение лишь в военных системах, и неприемлем в ИТ-системах, которые принадлежат другим ведомствам (здравоохранение, почта, связь, банковская система и т.п.).

Наиболее приемлемым на сегодня способом распределения ключей в ИТ-системах различной принадлежности (государственные и коммерческие) является третий способ, основа которого есть создание доверительной третьей стороной цифрового сертификата открытого ключа. Если ДТС свяжет открытый ключ с пользователем или системой, то есть проверит подлинность стороны владеющей личным ключом, то можно осуществить полный спектр услуг безопасности. Пользователи получают в своё распоряжение услуги целостности, аутентификации и причастности через реализацию механизмов цифровой подписи. Симметричные ключи могут быть распределены путем использования либо транспортных протоколов (протоколов передачи ключей), либо протоколов согласования или установления ключей. А это, в свою очередь, позволит обеспечить необходимый уровень конфиденциальности.

Сертификат ключа – это цифровой документ, подписанный органом или администратором сертификации (Certificate Authority, AC) и подтверждающий однозначное соответствие между открытым ключом и идентификационной информацией пользователя-владельца ключа.

Однако одного сертификата недостаточно для решения всех задач защиты. Для обеспечения безопасного взаимодействия ИТ-систем, принадлежащих различным ведомствам, организациям и предприятиям необходимо создать сеть взаимодействующих администраторов сертификации. Такая сеть реально взаимодействующих АС формирует инфраструктуру безопасности ведомственного, регионального и, наконец, национального масштаба, в рамках которой пользователи могут получить качественные услуги безопасности. Инфраструктура безопасности, которая обеспечивает распределение сертификатов открытых ключей, поддерживает защищенный обмен сообщениями, надежную идентификацию и аутентификацию, электронную коммерцию получила название **инфраструктуры открытых ключей (Public Key Infrastructure, PKI).**

2. Инфраструктура открытых ключей

В настоящее время в отечественной практике нет какого-либо законодательно или нормативно закрепленного определения понятия инфраструктуры открытых ключей. Нами предлагается определение, которое является синтезированным из ряда документов Национального института стандартизации и технологий США (NIST) [3-6].

Инфраструктура открытых ключей представляет собой комплексную организационно-техническую систему, которая обеспечивает необходимые услуги для использования криптографических технологий с открытыми ключами. Основная цель PKI – обеспечение, путем применения цифровых сертификатов, надежной связи (ассоциирования) открытых ключей с объектами, что позволяет другим объектам проверить эту связь и получить необходимые услуги для осуществления управления ключами в распределенных системах. PKI интегрирует цифровые сертификаты, криптографию с открытыми ключами и органы сертификации в единую архитектуру безопасности корпоративной сети. Обычно инфраструктура открытых ключей создается с целью решения следующих задач:

- осуществление выпуска в обращение сертификатов для отдельных пользователей;
- регистрации программного обеспечения оконечных пользователей;
- объединения сертификатов в специальные справочники сертификатов и обеспечение их обслуживания;

– реализации механизмов управления, обновления, восстановления и аннулирования сертификатов;
– предоставления дополнительных услуг поддержки управления сертификатами.

Международный стандарт ISO/IEC 11770 определяет основные компоненты PKI. На рисунке 3 представлена модель организации сертификации, которая закреплена в стандарте. Данная модель сертификации характеризует взаимосвязь между основными логическими объектами, которые принимают участие в формировании и управлении сертификатами.

Рис.3

Орган сертификации или *администратор сертификации* (АС) это доверенный объект, который несет ответственность за организацию и осуществление процесса сертификации открытых ключей пользователей, а также ручается за подлинность открытых ключей. Это включает выполнение таких действий как назначение открытым ключам уникальных имен посредством подписанных сертификатов, управление назначением порядковых номеров сертификатам, аннулирование сертификатов и других действий. Орган сертификации является основным компонентом PKI. Он включает в себя аппаратное и программное обеспечение, иное оборудование, персонал и как минимум обладает двумя атрибутами: собственным именем и собственной ключевой парой. АС выполняет четыре основные функции PKI [3]:

– выпуск сертификатов (т.е. создает и подписывает их);
– поддержку информации о статусе сертификатов (информация состояния сертификатов) и ведет список аннулированных сертификатов (CRL);
– публикацию текущих (имеющие силу) сертификатов и последней версии CRL, для того, чтобы пользователи могли получить самую свежую информацию о состоянии сертификатов и возможности использования услуг безопасности;
– поддержку архивов информации состояния сертификатов, у которых истек срок действия.

Орган сертификации выпускает для каждого объекта *цифровой сертификат* или *сертификат открытого ключа* (public key certificate). Это список данных связанных с конкретным пользователем, включающий открытый ключ (или ключи) этого пользователя подписанный органом сертификации. Таким образом, сертификат состоит из двух полей – поля данных и поля подписи. Поле данных содержит, как минимум, открытый ключ пользователя и иден-

тификационную информацию пользователя (например, идентификатор пользователя). Поле подписи содержит подпись органа сертификации, которая является поручительством за аутентичность открытого ключа пользователя. Сертификат также может содержать и другую дополнительную информацию, например, указатели, каким образом может быть использован тот или иной ключ. В настоящее время формат сертификата определяется стандартом ITU-T X.509. Каждый пользователь должен быть приписан к конкретному органу сертификации, и обладать доверенной копией ключа проверки подписи этого органа. Орган сертификации может выпускать сертификаты как для отдельных пользователей, так и для других органов сертификации. АС вставляет свое имя в каждый сертификат (и CRL), которые он формирует, и подписывает их на своем личном ключе. Таким образом, обеспечивается доверие пользователей к АС (непосредственно, либо через сертификационный путь). Для обеспечения надежной работы АС должен использовать сертифицированные криптографические модули.

Сервер имен (name server) несет ответственность за управление пространством имен пользователей, с целью обеспечения каждого пользователя уникальным неповторяющимся именем.

Справочник сертификатов или *депозитарий* (certificate directory or repository) это база активных цифровых сертификатов (т.е. действующих), которая обеспечивает поддержку сертификатов в on-line режиме, т.е. в состоянии полной готовности к использованию их пользователями. Обычно депозитарием является база данных или сервер, доступные для пользователей в режиме только для чтения. Пополнение и поддержку справочника осуществляет орган сертификации. Пользователи также могут иметь свои справочники сертификатов. В этом случае за их поддержку отвечает сам пользователь. Все приложения PKI достаточно сильно зависят от эффективности реализации услуги справочника сертификатов, поскольку именно через депозитарий осуществляется распределение всей информации о состоянии сертификатов и собственно самих сертификатов. Услуга справочника реализуется в соответствии с требованиями стандарта ITU-T X.500.

Центр генерации ключей осуществляет генерацию пар открытый/закрытый ключ, а также генерацию симметричных ключей и паролей. Центр генерации ключей может быть частью оборудования пользователя, если пользователь самостоятельно генерируют себе ключи, либо частью органа сертификации, либо вообще может являться отдельной доверительной системой

Орган регистрации или *администратор регистрации* (registration authority) несет ответственность за авторизацию объектов, отличающихся уникальными именами, в качестве члена домена безопасности или доверительного домена. Основная задача органа регистрации – проверка содержания информации в сертификате. Сертификат может содержать информацию предоставленную объектами, регистрирующих сертификаты, например номер лицензий или сведения о последнем платеже. Сертификат может содержать информацию третьей доверительной стороны и другую информацию. Чаще всего орган регистрации представляет собой сервер с соответствующим программным обеспечением, который управляется одним администратором. Орган сертификации может взаимодействовать с несколькими аккредитованными органами сертификации.

Орган сертификации создает и поддерживает *список аннулированных сертификатов* (Certificate Revocation List (CRL)). CRL является списком порядковых номеров или других идентификаторов сертификатов, которые были аннулированы определенным органом сертификации и служит для оповещения в on-line режиме об аннулировании сертификатов. На сегодняшний день CRL является самым распространенным способом оповещения пользователей об аннулировании сертификатов

Архив представляет собой базу данных, содержащую информацию о сертификатах, у которых истек срок действия. Архив используется для долговременного хранения информации состояния сертификатов. Используя архив, можно убедиться, что конкретные выведенные из действия сертификаты, действительно были выпущены данным органом сертификации. При

возникновении споров относительно старых документов, которые были подписаны на выведенных из действия ключах, также будет полезна архивная информации, предоставленная органом сертификации.

Пользователями PKI могут быть как организации, так и отдельные пользователи (физические лица). Эта категория не имеет права выпуска сертификатов. Они доверят другим компонентам PKI. На основе этого доверия они получают и осуществляют проверку сертификатов других пользователей. Различают две категории пользователей PKI. К первой категории относятся *пользователи сертификата* (пользователи, доверяющие сертификату) – это пользователи, которые используют сертификат, с целью определения принадлежности открытого ключа другому объекту. Другой категорией являются *держатели сертификатов* – пользователи, которые могут подписывать документы и совершать иные действия с помощью сертификатов.

В зависимости от масштабов организации, степени зависимости функционирования организации от информационных технологий, основных функций организации состав компонентов PKI и их функции могут варьироваться. Совсем не обязательно, что в конкретной реализации эти объекты будут раздельными. В отдельных случаях некоторые из них вообще могут не существовать.

3. Услуги PKI

Основными услугами PKI, являются услуги управления сертификатами. Услуги управления сертификатами – это услуги, образующие ядро инфраструктуры с открытыми ключами. К основним услугам относятся следующие услуги [1]:

- **выпуск сертификата** для пользователей и администраторов сертификации;
- **аннулирование сертификата** в случае компрометации секретных ключей пользователя или в других ситуация, определенных в политике сертификации;
- **приостановление действия сертификата** с последующим автоматическим восстановлением или аннулированием сертификата;
- **публикация сертификатов** через каталог сертификатов (в соответствии с требованиями X.500 или иных нормативных документов и стандартов), с целью обеспечения доступа к спискам действующих сертификатов заинтересованных лиц;
- **хранение сертификата** с возможностью восстановления сертификата;
- **архивирование сертификатов вышедших из употребления** с целью обеспечения возможности проверки электронных документов, сделок и других операций, выполненных с использованием данных сертификатов.

Кроме основных услуг, в PKI могут поддерживаться и дополнительные услуги:

- **регистрация.** Услуги регистрации обеспечивают регистрацию и контроль индивидуальной информации объектов процессов сертификации;
- **хранение информации в архиве.** И Услуга предназначена для долговременного хранения и управления цифровыми документами и другой информации;
- **нотариальная сертификация,** которая включает аутентификацию отправителя, подтверждения целостности и юридической силы цифровых документов;
- **создание резервных копий и восстановление ключей;**
- **поддержка каталога.** Данная услуга обеспечивает всесторонне управление и обеспечение информацией относительно пользователей или атрибутивной информацией;
- **поддержка услуг причастности;**
- **услуги корректировки и управления историей ключей.**

Реализация всех услуг и взаимодействие объектов процесса сертификации осуществляется в рамках единой политики сертификации. Под **политикой сертификации** понимают совокупность правил, отражающих и регулирующих порядок применения сертификатов в конкретной совокупности приложений с общими требованиями по обеспечения информационной безопасности. Политика сертификации является составной частью политики безопас-

ности и применяется пользователями сертификата с целью принятия решения о достаточной степени доверия к сертификату для его применения [2, 12].

4. Архитектура PKI

Держатели сертификатов, в зависимости от принадлежности к организации или сообществу, могут получать сертификаты от различных органов (администраторов) сертификации. Поэтому PKI обычно является совокупностью нескольких администраторов сертификации, связанных доверенными путями.

В организации (например, в банке) разворачивается своя PKI. В настоящее время выделяется два основных типа архитектуры PKI – **иерархическая** и **сетевая.** С целью обеспечения возможности взаимодействия пользователей, которые принадлежат различным ведомствам, ведомственные PKI объединяются через **узловые органы сертификации.**

Остановимся на данных типах архитектур более подробно.

В PKI, построенной на принципах иерархии все администраторы объединяются по принципу иерархического соподчинения (рис. 4). Корневой (центральный, главный) АС выпускает сертификаты для подчиненных АС, а те в свою очередь для АС следующего уровня иерархии или своим пользователям. В иерархических PKI любые связывающиеся стороны знают открытый ключ главного администратора. Любой сертификат может быть верифицирован через проверку сертификационного пути от главного АС. Обычно такая инфраструктура строится в ведомственных корпоративных системах, в которых существует необходимость и возможность полностью контролировать размер и конфигурацию сети.

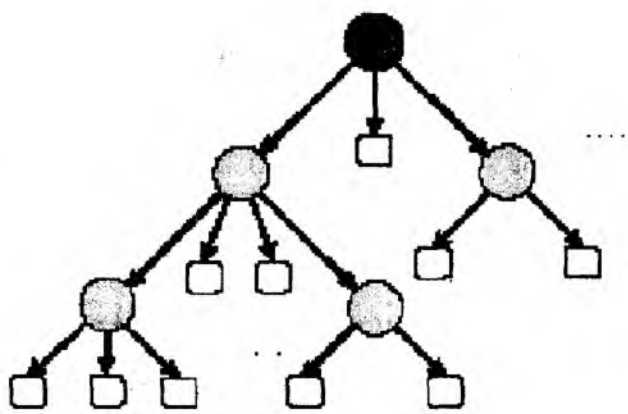

Рис. 4

В сетевой архитектуре PKI (рис.5) все администраторы являются равными или одноранговыми, т.е. не размещаются на различных уровнях иерархии. В сети доверенные отношения между равными АС поддерживаются независимой взаимной кросс-сертификацией администраторов.

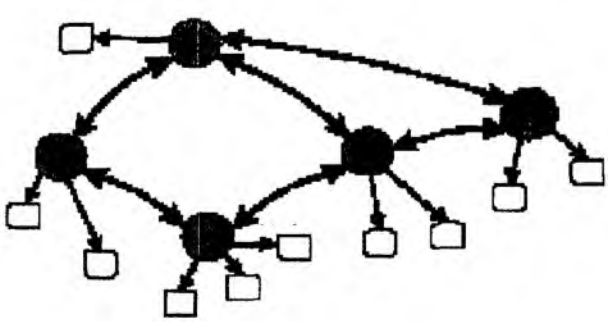

Рис. 5

Связывающиеся стороны знают открытый ключ «ближайшего» администратора, который и выпускает для них сертификаты. Верификация сертификатов происходит путем верификации сертификационного пути сертификатов, который проходит от данного доверенного администратора. Под *сертификационным* путем понимают упорядоченную последовательность сертификатов, которые вместе с открытым ключом исходного объекта в пути, могут быть обработаны для получения оконечным объектом пути [12]. Администраторы сертификации выпускают кросс-сертификаты, т.е. выпускают сертификаты друг для друга, а затем объединяют их в *пару кросс-сертификатов*. Данная архитектра применяется в открытых сетях, с неконтролируемым подсоединением (удалением) абонентов. Особое распространение она получила в системах электронной коммерции через Internet.

Архитектура узловых администраторов была разработана для объединения ведомственных PKI. Архитектуры объединяются путем введения нового администратора, который называется узловым. Узловой АС не выпускает сертификаты для пользователей PKI. Все пользователи, независимо от архитектуры PKI, рассматривют узловой АС промежуточным узлом. Узловой АС обеспечивает равноправные отношения между ведомственными PKI. При соединении иерархических архитектур, узловой АС обеспечивает взаимодействие главных АС, при соединении сетевых – с одним из АС каждой сети. При соединении различных архитектур узловой АС устанавливает отношение главного АС иерархической PKI с одним из АС сетевой PKI.

5. Архитектура Национальной PKI

В настоящее время можно говорить о реальной интеграции ведомственных, коммерческих и общенациональных информационных сетей. Пользователи имеют потребности в использовании ресурсов сетей различной принадлежности для решений своих задач. Требуемый уровень безопасности взаимодействия сетей при сохранении требуемого уровня доступности ресурсов сегодня может быть достигнут путем построения Национальной архитектуры PKI. Но для этого в рамках государства необходимо на законодательном уровне установить правовые взаимоотношения между государственными и коммерческими органами сертификации. Данная проблема усложняется еще и тем, что в Украине на данные момент получили лишь PKI, принадлежащие кредитно-финансовым учреждениям (банковские платежные системы) и системам электронной коммерции. В других государственных учреждениях данные технологии пока еще к сожалению не нашли широкого применения.

Основной проблемой Национальной PKI является создание сертификационных путей между различными ведомствами и организациями, которые будут обеспечивать высокий уровень доверительности. Национальная PKI должна объединять государственный и негосударственный сектора инфораструктуры. Одним из путей решения этой проблемы применение администраторами сертификации проверенных механизмов, специфицированных в стандартах и удовлетворение требования, предъявляемых к кросс-сертификатам.

На рисунке 6 представлена Национальная архитектура PKI, рекомендуемая NIST [3,6].

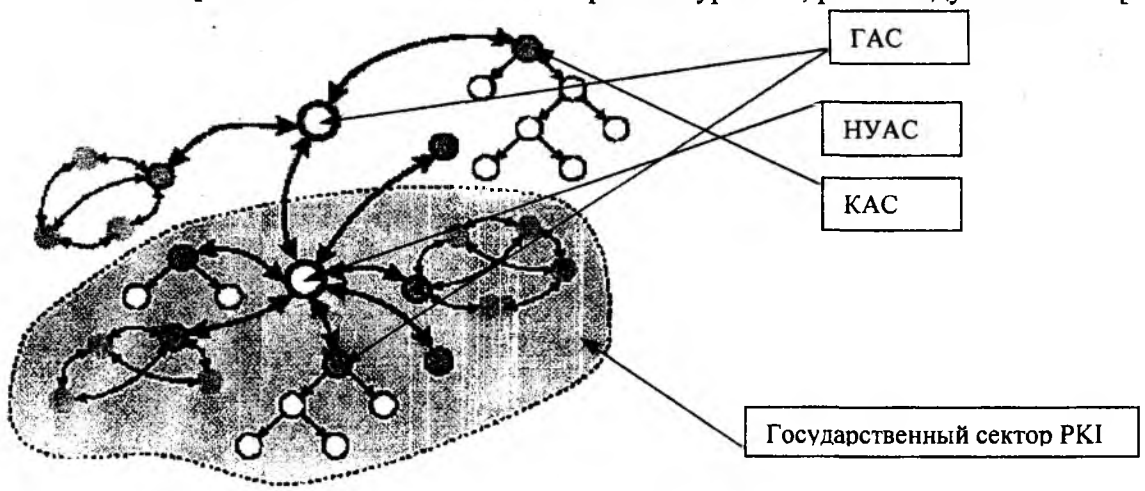

Рис. 6

Основными архитектурными компонентами данной архитектуры являются:

1. **Орган управления Национальной политикой сертификации**. Данный орган устанавливает общую политику в Национальной PKI, и утверждает правила и процедуры доверительных доменов в Национальной PKI. Данный орган осуществляет оправление Национальным узловым органом сертификации и Национальным депозитарием.
2. **Доверительные домены.** В национальном масштабе, доверительный домен являются частью Национальной PKI, который функционирует под управление единой органа управления политики сертификации. В домене может существовать один или более администраторов сертификации. Каждый доверительный домен имеет одного главного администратора сертификации (principal CA) и доменный депозитарий.
3. **Орган управления политикой сертификации домена** утверждает практические действия администраторов сертификации домена и осуществляет наблюдение (отслеживает) эти действия. Орган организует работу или осуществляет надзор за депозитарием домена.
4. **Администраторы сертификации:**
   - Узловой администратор сертификации. Это Национальный узловой администратор сертификации (НУАС), функционирующий под управленеим органа управления Национальной политики сертификации. Цель НУАС – обеспечить узел доверия, посредством которого будут построены доверительные пути между различными доверительными доменами Национальной PKI, а также между ведомственными (государственными) и коммерческими PKI. Орган управления Национальной политикой сертификации утверждает главных администраторов доверительных доменов, которые имеют право выпускать кросс-сертификаты с Национальным узловым АС. Отметим, что НУАС не является корневым АС, поскольку он не является началом сертификационных путей.
   - Главный АС (ГАС) это АС, который внутри доверительного домена отвечает за выпуск кросс-сертификатов с НУАС. Любой доверительный домен может иметь одного ГАСа. В домене с иерархической архитектурой ГАСом является корневой АС. В домене сетевой архитектуры – любой из АС, обычно назначаемый НУАСом.
   - Одноранговый АС (ОАС) – администратор в доверительном домене сетевой архитектуры. ОАС обладает собственным сертификатом, который распределяется среди держателей сертификатов и используется ими для инициализации сертификаци-

онных путей. ОАС также выпускает кросс-сертификаты с другими ОАС своего доверительного домена.

➢ Корневой (центральный) АС (КАС) – администратор, который в доверительном домене иерархической архитектуры является началом всех сертификационных путей. Держатели сертификатов и связывающиеся стороны получают сертификат КАС каким-либо надежным способом (например, при личной встрече уполномоченных лиц) и все доверительные пути начинаются с этой точки. Для иерархических архитектур КАС одновременно является и ГАСом данного домена.

➢ Подчиненные АС (ПАС) – администраторы в домене иерархической архитектуры, не являющиеся начальными точками доверительных путей. ПАС получают сертификаты от своих АС, находящихся на высшем уровне иерархии, и в свою очередь выпускают сертификаты для своих подчиненных АС.

5. **Депозитарии** являются on-line средствами, которые поддерживают в актуальном состоянии базу сертификатов и информацию о статусе сертификатов. Депозитарии в Национальной PKI предоставляют информацию посредством протокола LDAP (Lightweight Directory Access Protocol), а также другими средствами. За поддержку депозитария и CRL сертификатов АС отвечает Орган управления Национальной политики сертификации.

6. **Депозитарий НУАС.** Общепринятым решением является открытый доступ к депозитарию НУАС через Internet. Депозитарий содержит следующую информацию:

- все сертификаты, выпущенные НУАСом;
- все сертификаты, удерживаемые НУАСом;
- все пары кросс-сертификатов, содержащие удерживаемый и выпущенные НАУСом сертификаты;
- текущую версию CRL для всех сертификатов, выпущенных НУАСом;
- большинство или все сертификаты, выпущенные администраторами Национальной PKI, с целью поддержки в поиске сертификационных путей;
- большинства или все пары кросс-сертификатов между администраторами сертификации Национальной PKI;
- другие сертификаты и CRL, определенные органом управления Национальной политикой сертификации.

Национальный узловой администратор сертификации является объединяющим элементом для объединения на общих методологических принципах ведомственный администраторов сертификации в единую Национальную PKI. НУАС, как уже отмечалось выше, не является корневым АС, однако он играет важную ***системную*** роль. Он соединяет доверительные домены посредством пар кросс-сертификатов уполномоченных главных администраторов сертификации и является *узлом доверия.* Необходимо отметить, что в теории распределения ключей *модель доверия* и *доказательство доверия*, являются весьма важными и принципиальными вопросами. В Украине в настоящее время теоретические вопросы моделирования доверия и доверительных отношений в гетерогенных сетях пока изучены недостаточно. Орган управления Национальной политики сертификации осуществляет надзор за деятельностью НАУС и определяет требования для осуществления процессов кросс-сертификации с НАУСом. Доверительные домены, осуществляющие кросс-сертификацию с НАУСом могут находится как в государственной, так и в коммерческой области.

Государственные и негосударственные АС, функционирующие в доверительных доменах, обязаны удовлетворять требованиям, определенным Органом управления Национальной политики сертификации. С целью определения возможности осуществления деятельности субъектов хозяйственной деятельности в области распределения сертификатами, необходимо разработать и законодательно закрепить лицензионные осуществления соответствующей деятельности и процедуры аттестации и аккредитации органов сертификации. К процессам кросс-сертификации могут быть допущены только аккредитованные АС. Для таких админи-

страторов НУАС обеспечит надежное соединение с общей доверенной сетью Национальной PKI.

Однако для обеспечения реально гибкости в ведомственных взаимоотношениях, необходимо избегать монополии НУАС в определении политики сертификации. Для это НАУС должен быть ограничен относительно вмешательства в деятельность ведомственных АС, а именно:

- ведомства не могут быть ограничены условиями полной адаптации к политике сертификации НАУС. Более, того необходимо создать такие условия на рынке данных услуг, при которых ведомства могут использовать другие правила сертификации, определенные либо их собственными органами управления политикой сертификации, либо коммерческими провайдерами услуг сертификации;
- ведомства не могут быть ограничены в праве взаимодействия с другими ведомственными и коммерческими организациями исключительно через НАУС. Как альтернатива, необходимо предоставить возможность непосредственного взаимодействия организация на договорных основах.

Эти и другие вопросы, которые несомненной появятся при более детальном изучении проблем построения Национально PKI, должный учитываться при разработке соответствующих нормативно-правовых документов всех уровней государственного управления.

Заключение

Для всесторонней проработки вопросов построения Национальной PKI, видится целесообразным создать под эгидой Департамента специальных телекоммуникационных систем и защиты информации, Госстандарта Украины, Министерства образования и науки рабочий комитет, который возглавит разработку и создание Национально PKI. В частности рабочие группы комитета могут решать следующие задачи:

- обеспечение руководства и оказание методической, теоретической поддержки в разработке PKI, которая опирается на использование коммерческих продуктов, удовлетворяющих требованиям национальных и международных стандартов;
- определение и нормативно закрепление требования ведомственным PKI;
- выработка рекомендаций по определению политики, процедур и выбору стандартов, которые направлены на поддержку PKI;
- осуществление надзора за деятельностью объектов PKI, в пилотных проектах по реализации Национальной PKI;
- осуществление руководства и надзора за технологиями управления ключами;
- определение технологии, необходимые для эффективной реализации Национальной PKI;
- поддержка связи с заинтересованными государственными, промышленными, научными и общественными организациями;
- разработка требования по взаимодействию, совместимости и безопасности продуктов и протоколв, связанных с реализацитей Национальной PKI;
- выработка рекомендация относительно создания, демонстрации и функционирования Национальной PKI и др.

На наш взгляд проведение работ по созданию Национально PKI в Украине являются крайне актуальными и весьма своевременными, особенной учитывая тот факт, что в Верховной раде уже лежит проект Закона о цифровой подписи. Его реальная работа может быть построена только при условии создания в Украине Национальной инфраструктуры открытых ключей.

Список литературы: 1. *В. Горбатов, О. Полянская.* Доверенные центры как звено обеспечения безопасности корпоративных ресурсов. // JetInfo №11 (78). – 1999. – С. 13-20. 2. *ISO/IEC 9549-8:1993| ITU-T Recommendation X.509.* Information Technology – OSI – The Directory: Authentication Framework. 3. *D.R. Kuhn, V.C. Hu, W.T. Polk, S.J. Chang.* Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST SP 800-32. – 2000. 4. *ISO/IEC 11770:1996.* Information Technology – Security techniques – Key management. 5. *G. Stoneburner.* Underlying Technical Models for Information Technology Security. NIST SP 800-44 – 2001. 6. *Anabelle Lee.* Guideline for Implementing Cryptography in the Federal Government. NIST SP 800-21 – 1999. 7. *ISO 7498-2:1989* – Open System Interconnection Reference Model – Security Architecture. 8. *Потий А.В.* Криптография в защите информации. // Служба безопасности. - №4-5. – 2001. – С.7-9. 9. *Горбенко И.Д., Бондаренко М.Ф., Скрипник Л.В., Потий А.В.* Перспективы применения международного стандарта ISO/IEC 15408 в Украине. В сб. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – №3. – 2001. 10. *Бондаренко М.Ф., Черных С.П., Горбенко И.Д., Замула А.А., Ткач А.А.* Методологические основы концепции и политики безопасности информационных технологий. // Радиотехника: Всеукр. Межвед. Научн.-техн. сб. 2001. Вып.19. – С.5-16. 11. *A. Menezes, P. van Oorschot, S. Vanstone.* Handbook of Applied Cryptography. – CRC Prerss, Inc. – 1997. 12. *S.Chokhani, W. Ford.* Internet X.509 Public Key Infrastructure Certificate Policy and Certifications Framework. – RFC 2527, 1999.

Харьковский национальный университет радиоэлектроники. Служба безопасности Украины.

Поступила в редколлегию 09.04.2002.