2 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 638.235.231

ІНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ (PKI): СОВРЕМЕННЫЕ ТЕНДЕНЦИИ

Вячеслав Татьянин
ООО «АВТОР»

Анотація: **Аналізуються тенденції в побудові PKI-інфраструктур українськими компаніями, проведено порівняльний аналіз українських продуктів та розглянуто питання вибору типу носіїв ключової інформації.**
Summary: **The given material is devoted to the analysis of tendencies in construction of PKI-infrastructures by the Ukrainian companies, the comparative analysis of the Ukrainian products was carried out and the question of a choice of the type of carriers of the key information was considered.**
Ключові слова: **Інформація, інформаційна безпека, PKI, носії ключової інформації**.

Процесс построения глобального информационного общества, объединяющего различные страны и континенты, является одним из самых актуальных процессов сегодняшнего дня. Естественно, что наряду с положительными аспектами развития такого общества, существуют и негативные аспекты. К сожалению, количество таких негативных аспектов с каждым днем увеличивается.

В первую очередь это связано с развитием глобальной сети Internet, которая сейчас является неотъемлемым условием функционирования каждой компании, и позволяет реализовать широчайшие возможности по сбору, обработке и передаче огромной массы информации. Например, по данным прессы, в 2004 году к сети Internet было подключено более 200 млн. ЭВМ в почти 250 странах мира на всех континентах. На начало 2006 года эта цифра естественно увеличилась. И, конечно, с ростом глобальной информационной сети растет и количество специалистов, обладающих достаточными знаниями для совершения «компьютерных преступлений».

Поэтому и рост интереса к информационной безопасности, в частности, к криптографии, стал закономерным явлением.

Сейчас во всем информационном сообществе существенно изменился интерес к криптографии и прикладным решениям на ее основе. Резко расширилась сфера применения криптографических методов для защиты информационных ресурсов, постоянно растет спрос на подобные продукты, расширяются исследования по криптографии.

В связи с этим предложение устройств и решений по криптографической защите информации (КЗИ) существенно увеличилось и потребитель не всегда может определиться, на чем остановить свой выбор.

В данном материале мы попытаемся дать сжатую характеристику тенденций в построении PKI-инфраструктур украинскими компаниями, провести сравнительный анализ украинских продуктов и затронем вопрос выбора типа носителей ключевой информации.

(PKI) – это одно из самых ярких достижений в информационной безопасности. При грамотном построении PKI позволяет предупредить большинство информационных атак на корпоративное информационное пространство. В данном материале мы попытаемся дать сжатую характеристику тенденций в построении PKI-инфраструктур украинскими компаниями и провести сравнительный анализ украинских продуктов. Также затронем вопрос выбора типа носителей ключевой информации, так как они являются одним из главных элементов любой системы защиты.

В настоящее время интеграция PKI в различные системы занимает существенный сегмент мирового рынка информационной безопасности. В последние годы украинские потребители также «доросли» до того уровня, когда необходимость защиты корпоративной информационной среды стала объективной реальностью.

Сейчас в Украине, как количество поставщиков данного продукта, так и его потребителей весьма ограничено. В полном объеме функционирует меньше десятка подобных структур, в основном, в крупнейших украинских банках (напомним, что PKI лежит в основании систем защищенного документооборота в крупных распределенных системах). Также PKI начинает внедряться в госструктурах.

Подобное опережение коммерческих структур по сравнению с государственными объясняется тем, что согласно законодательству Украины государственное учреждение может работать только с аккредитованными центрами сертификации ключей. В Украине первый сертификат об аккредитации ЦСК был получен только в январе нынешнего года (17 января 2006 года первый сертификат об аккредитации ЦСК получило предприятие «Украинские национальные информационные системы», г. Днепропетровск; второй – 10. 03. 2006 г. ГП "Украинские специальные системы", ЦСК "Центр аутентификации Национальной системы конфиденциальной связи"; третий – 31.03.2006г. ЗАО "ИВК", ЦСК), поэтому официальная возможность использовать PKI в государственных структурах появилась совсем недавно.

Вопрос о том, станет ли практика выдачи сертификатов об аккредитации ЦСК отечественным компаниям постоянной, пока остается открытым.

Скорее всего, здесь могут сыграть роль такие факторы.

- Финансовые. Для подачи заявки на аккредитацию продукта необходимо провести комплекс предварительных работ, суммарная стоимость которых довольно высока. К сожалению, пока среди украинских производителей это могут позволить себе единицы.
- Нормативные. Как говорилось ранее, сейчас законодательством Украины постановлено, что работать только с аккредитованными ЦСК обязаны лишь государственные учреждения. Коммерческие и банковские структуры в этом не ограничены. Но отметим тот факт, что нормативная база регулирования банковской деятельности в Украине сейчас развивается и усовершенствуется, поэтому в ближайшее время можно ожидать существенных изменений и в этих вопросах.

Теперь перейдем от организационных и законодательных моментов к практике выбора продукта.

Рассмотрим более детально, что же такое PKI.

Инфраструктура открытых ключей, PKI – это комплексная подсистема, реализующая в рамках информационной системы организации функционирование набора служб безопасности по поддержке гарантированных процедур конфиденциальности и строгой аутентичности доступа. Это осуществляется за счет регламентации управления открытыми ключами пользователей, использования средств шифрования (аппаратных и программных) и механизма электронной цифровой подписи.

Таким образом, поддерживая PKI, организация налаживает в корпоративной системе доверительную среду, гарантирующую авторство, подлинность и целостность электронной информации, циркулирующей в системе, а также обеспечивает действие фактора "неотказуемости от авторства" или "неотрекаемости" при осуществлении бизнес-процессов с использованием технологий электронного документооборота и коммуникаций.

Стратегия создания подсистемы управления электронными сертификатами в автоматизированной информационной системе предприятия предполагает использование PKI, в частности, для следующих целей:

- обеспечение достоверности, безопасности и целостности транзакций, электронных документов и/или почтовых сообщений. Контроль над данными операциями (происхождение, достоверное время создания, прочее);
- обеспечение механизма строгой аутентификации пользователей, аппаратных и программных компонент системы;
- организация виртуальных частных сетей (VPN);
- организация защищенных порталов (доступ через Web);
- закрытие речевых стационарных и мобильных каналов связи;
- организация системы разграничения доступа к сайтам, порталам и приложениям.

Но, даже не смотря на то, что PKI для Украины относительно новый продукт, выбор все же есть. Основное, чего не хватает, – достаточных знаний и достоверной информации для принятия решения о выборе конкретного продукта из существующего предложения. С целью решения данного вопроса нами был проведен сравнительный анализ продуктов, предлагаемых сейчас на украинском рынке информационной безопасности. Для структуризации результаты проделанного анализа представлены в табличной форме.

Таблица 1 – Сравнительный анализ PKI-решений

Программный продукт	**RSA Keon, Certification Authority 6.5**	**ЗАО Сайфер, «Шифр-PKI»**	**ООО НОКК, «Вега»**	**ЗАО «Институт Информационных технологий», ЦСК**	**ООО «АВТОР», CryptoKDC 2.0**

Поддержка сертификатов					
Формат сертификатов	X.509v3	данные отсутствуют	данные отсутствуют	X.509v3	X.509v3
Дополнения сертификатов	да	данные отсутствуют	данные отсутствуют	Да	да, в том числе пользовательские
Методы отзыва/аннулирования сертификатов					
COC (список отозванных/аннулированных сертификатов)	да	свой формат	свой формат	RFC 3280 v2.0	RFC 3280 v2.0
Протокол OCSP (протокол получения статуса сертификата в реальном времени)	да	нет	нет	да	да, возможность установки на отдельный сервер
Точки распространения COC	нет	да	да	да	да
Топология PKI					
Способы сертификации	сетевая и иерархическая	только иерархическая	только иерархическая	только иерархическая	сетевая и иерархическая
Глубина иерархии	любая	до 4-х уровней	любая	любая	любая
Множественные ЦСК/ЦР	да, без ограничений	один ЦСК, множественные ЦР	Множественные ЦР	да, без ограничений	да, без ограничений
Безопасность					
Коммуникация с клиентом	SSL	свой протокол	свой протокол;	PKIX #7/10;	PKIX CMP; PKIX #7/10
Коммуникация между ЦСК/ЦР или аналогичными модулями	PKIX CMP	свой протокол	свой протокол	свой протокол	PKIX CMP; свой протокол
Защита ЦСК/ЦР	смарт-карты; аппаратные ключи	пароль; программный модуль с контролем доступа	пароль; программный модуль с контролем доступа	аппаратные модули безопасности	смарт-карты; аппаратные ключи; аппаратные модули безопасности
Аппаратная защита корневых ключей ЦСК/ЦР	нет	нет	нет	да	да
Поддержка криптографических стандартов	RSA, DSA, ECDSA, MD-2/4/5, SHA-160/224/256/384/512, ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-	ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-95	ГОСТ 28147-89, ГОСТ 34.310-95, ГОСТ 34.311-95	ДСТУ 4145-2002, ГОСТ 28147-89, ГОСТ 34.311-95	ДСТУ 4145-2002, ГОСТ 28147-89, ГОСТ 34.311-95,

	95				
Поддержка каталога (LDAP)					
Собственный каталог или каталог третей стороны	свой каталог и каталог третьей стороны	нет	нет	каталог третьей стороны	свой каталог и каталог третьей стороны
Механизмы регистрации					
Личное присутствие	да	да	да	да	да, не обязательно при передаче стартового сертификата
Web	да	нет	нет	да	да
Электронная почта	да	да	да	да	да
VPN	да	нет	нет	нет	да
Поддержка смарт-карт					
Устройства/ Стандарты	смарт-карты/аппаратные ключи: RSA crypto card, RSA SecureID Стандарты: PC/SC, PKCS#11	смарт-карты/ аппаратные ключи третьих производителей	смарт-карты/ аппаратные ключи третьих производителей	аппаратные ключи третьих производителей	смарт-карты/аппаратный ключи: UKRCOS 1.0, UKRCOS 2.0 Стандарты: ISO 7816-1/2/3, PC/SC, PKCS#11
Защита клиентского ПО	смарт-карты; аппаратные ключи	съемные диски; смарт-карты/ аппаратные ключи третьих производителей	съемные диски; смарт-карты/ аппаратные ключи третьих производителей	съемные диски; аппаратные ключи третьих производителей	смарт-карты; аппаратные ключи; съемные диски
Защита администратора ЦСК	смарт-карты; аппаратные ключи	съемные диски; смарт-карты/ аппаратные ключи третьих производителей	съемные диски; смарт-карты/ аппаратные ключи третьих производителей	съемные диски; аппаратные ключи третьих производителей	смарт-карты; аппаратные ключи
Защита администратора ЦР	смарт-карты; аппаратные ключи	съемные диски; смарт-карты/ аппаратные ключи третьих производителей	съемные диски; смарт-карты/ аппаратные ключи третьих производителей	съемные диски; аппаратные ключи третьих производителей	смарт-карты; аппаратные ключи; съемные диски
Управление ключами					
Автоматическое обновление ключей	нет	нет	данные отсутствуют	нет	да
Автоматическое управление историями ключем	нет	нет	данные отсутствуют	нет	да

Функциональная совместимость					
ЦСК (поддерживаемые стандарты)	X.509v3, PKIX, PKIX CMP, PKCS#11, CRL v2.0	нет	данные отсутствуют	X.509v3, PKCS #7, #8, #10, CRL v2.0, OCSP, RFC 3161 (ISO/IEC 18014)	X.509v3, PKIX, PKIX CMP, PKCS #8, #7, #10, #11, #12, CRL v2.0, OCSP, RFC 3161 (ISO/IEC 18014)
ЦР (поддерживаемые стандарты)	X.509v3, PKIX, PKIX CMP, PKCS#11, CRL v2.0	нет	данные отсутствуют	X.509v3, PKCS #7, #8, #10, CRL v2.0, OCSP, RFC 3161 (ISO/IEC 18014)	X.509v3, PKIX, PKIX CMP, PKCS #8, #7, #10, #11, #12, CRL v2.0, OCSP, RFC 3161 (ISO/IEC 18014)
Криптографическое аппаратное обеспечение	PKCS#11	свой API	свой API	свой API	ISO 7816-1/2/3, , PKCS#11, свой API

Сбор информации осуществлялся из следующих открытых источников:

1. http://www.keon.ru/index2.php?page=29&nav=resh
2. http://www.rsasecurity.com/rsalabs/node.asp?id=2124
3. http://www.x509.ru/
4. http://www.author.kiev.ua/
5. http://www.cipher.kiev.ua/
6. http://www.nokk.kiev.ua/
7. http://www.ivk.org.ua/
8. Печатные и электронные рекламные материалы компаний-разработчиков.

Для наглядности, результаты по некоторым вышеизложенным критериям и 3-м дополнительным приведем в виде диаграммы 1. Оценка будет производиться по привычной пятибалльной системе, где оценке

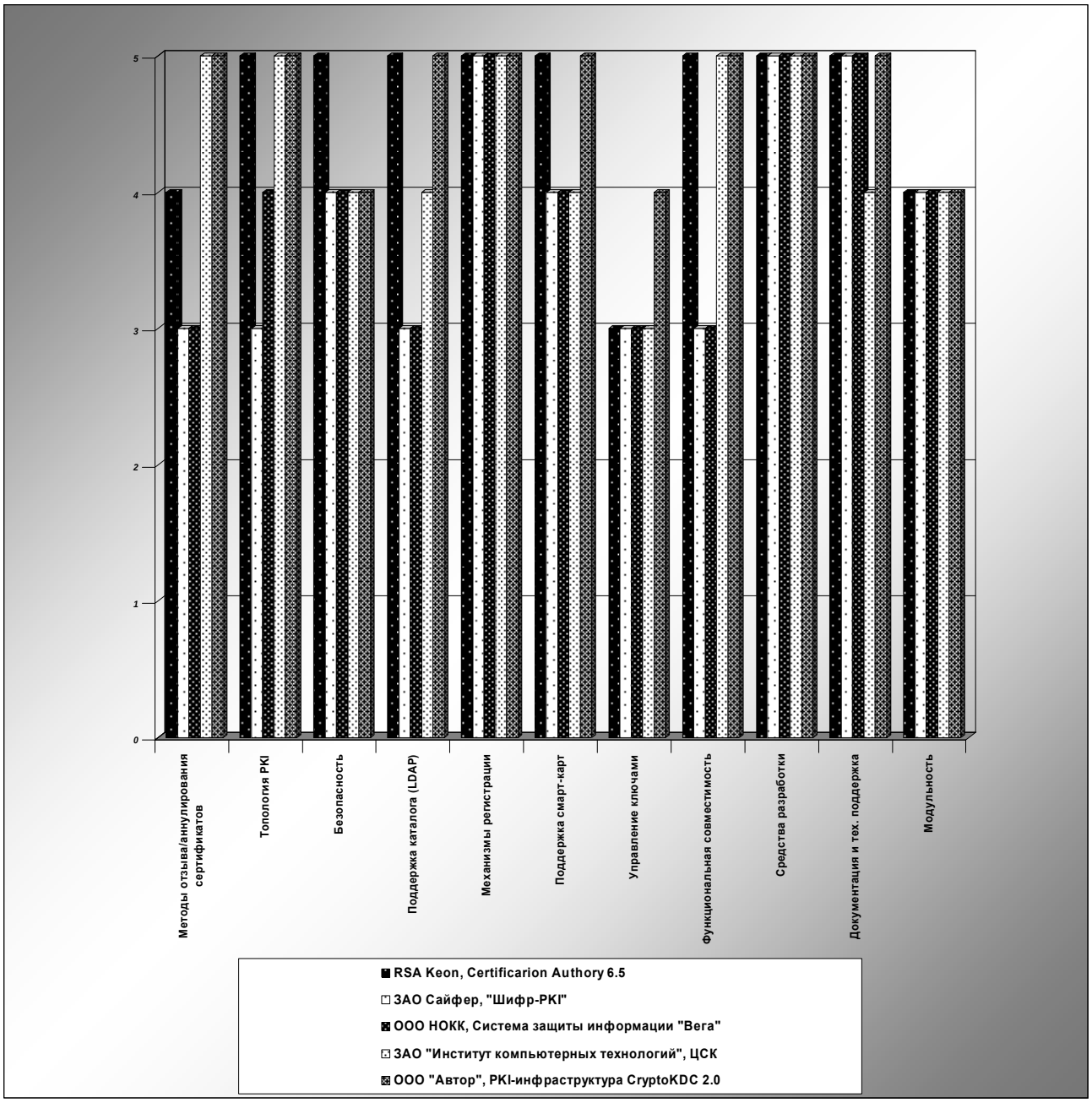
- Отлично – соответствуют 5 делений оценочной диаграммы;
- Хорошо – 4;
- Удовлетворительно – 3.

Из вышеперечисленных компонентов системы хотелось бы более подробно остановиться на носителях ключевой информации.

Ключевая информация является секретной и самой важной составляющей системы защиты. Большинство известных атак по вскрытию и преодолению систем защиты направлены на получение секретной информации: ключей электронной цифровой подписи, ключей шифрования, ПИНов-доступа, паролей, идентификаторов, которые хранятся на носителях ключевой информации (НКИ).

Известные способы хранения ключей с использованием перфокарт, дискет, магнитных карт, электронных карт памяти (Memory card), Touch-memory имеют главный недостаток - хранимая в них информация может быть прочитана с помощью специальных, относительно недорогих средств и в относительно небольшие сроки. Эти носители ключей легко могут быть скопированы, подделаны и эмулированы.

Из того следует вывод, что неправильно выбранный тип носителя может катастрофически повлиять на безопасность всей системы (внедрение которой на предприятии стоит не мало).



Носители ключевой информации
Диаграмма 1 – Результат сравнения PKI-решений

Специалисты в сфере информационной защиты утверждают – **единственно надежным способом защитить секретную информацию, находящуюся на внешнем носителе, является использование криптографических алгоритмов, которые выполняются микроконтроллером, встроенным в защищаемую память. Данный тип носителей относится к классу микропроцессорных карт (Smart card).**

Смарт-карта

Кристалл для смарт-карты (рис. 1) в базовой конфигурации состоит из центрального процессора (CPU),

однократно программируемой памяти (ROM), оперативной памяти (RAM), энергонезависимой электрически перепрограммированной памяти (EEPROM), секретной логики (Security Logic), интерфейса ввода/вывода информации (I/O).

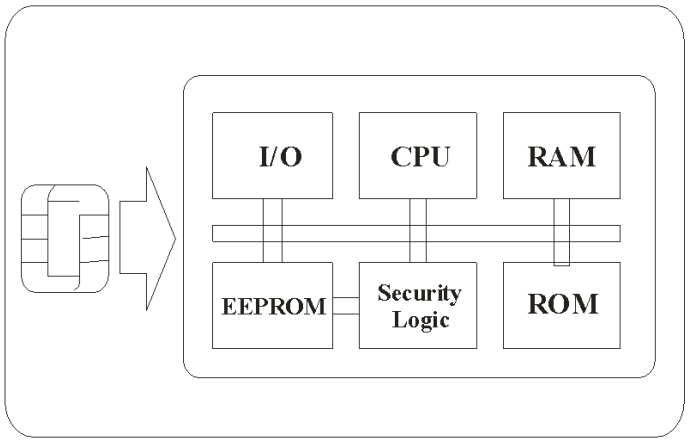


Рисунок 1 – Кристалл смарт-карты

Микропроцессор является сердцем кристалла. Он обеспечивает управление всеми элементами периферии, выполняет вычислительные операции и криптографические преобразования. Мозг карточки - память программы, которая определяет интеллект карточки и заставляет процессор функционировать по заданным правилам. Память программы находится в области ROM и программируется на заводе изготовителе кристаллов, а данный процесс называется маскированием кристалла. Он связан с технологическими операциями по изготовлению кремниевых пластин, поэтому стоит очень дорого. Маскирование экономически целесообразно выполнять при заказах нескольких сотен тысяч кристаллов.

Программа смарт-карты создается в форме операционной системы. Это обеспечивает гибкость в применении, позволяет создавать универсальные средства для многих приложений и гарантирует пользователям независимость от разработчиков операционных систем при создании собственных приложений. Карточная операционная система функционально похожа на операционную систему компьютера: имеет файловую организацию данных, защищает их от несанкционированного доступа, разграничивая права пользователей, управляет интерфейсами обмена и собственной периферией (EEPROM, таймер, генератор шума, криптографический сопроцессор, датчики и прочее), позволяет запускать приложения пользователя, выполняет команды операционной системы и сервисные функции. Основные требования к операционной системе изложены в международном стандарте ISO 7816.

Последние достижения в технологии производства кристаллов позволяют в чипе прежних размеров дополнительно размещать криптопроцессоры Triple DES, RSA на эллиптических кривых (ECC), таймер, порт UART, модуль подсчета CRC, генераторы случайных чисел, дополнительную оперативную память, одновременно два интерфейса ввода/вывода – контактный и бесконтактный. Для примера приведем характеристики смарт-чипов SLE66CLxxxP компании Infineon:

- EEPROM – от 4 кбайт до 64 кбайт
- CPU – 8 бит, 8/16 бит, 16 бит
- Интерфейсы – ISO 7816, ISO 14443, USB
- RAM – от 2 кбайт до 8 кбайт
- ROM – от 7 кбайт до 196 кбайт
- Со-процессоры: ECC, DES, RSA
- Соответствие критерию *CC EAL4+* (*"Common Criteria Evaluation Assurance"*)

В Евросоюзе действует нормативный документ CWA 14169 (Рабочее соглашение Еврокомитета по стандартизации (CEN/ISSS) о защищенных устройствах формирования электронной подписи *EAL4+*), регламентирующий применение средств электронной цифровой подписи с использованием усиленных сертификатов. Сейчас в Украине присутствует ***только одно решение***, ***позволяющее обслуживать усиленные сертификаты в соответствии с европейскими нормами и Украинскими стандартами.*** Это носители ключевой информации ООО «Автор», особенностью которых является их реализация на смарт-

картах с собственной операционной системой «УкрКОС» («УкрКОС» – единственная в мире ОС, одновременно соответствующая и международным, и Украинским стандартам). Все криптографические преобразования, включая генерацию ключевой информации, формирование и проверку электронной цифровой подписи, осуществляются внутри самого носителя.

Ключ безопасности USB

Альтернативой использования смарт-карт являются секретные ключи USB.

В настоящее время на рынке представлено большое количество ключей USB, но к сожалению, большинство из них строятся на обычных отдельных элементах микроэлектронной промышленности: микроконтроллер общего применения с внутренней или внешней памятью, что не обеспечивает гарантированный уровень безопасности хранимой в нем информации. USB-ключ считается надежным только в том случае, если он построен на смарт-чипе, что позволяет в полной мере использовать механизмы защиты смарт-карт технологии.

Рекомендации по выбору типа НКИ

При принятии решении о типе используемого НКИ надо учитывать тот фактор, что НКИ находится в постоянном обращении и использовании, поэтому может быть утерян, испорчен или сломан. С этой точки зрения экономически выгоднее разделение дорогостоящих электронных ключей на дешевые смарт-карты и стационарные устройства карт-ридеры. Также, например, бесконтактная смарт-карта очень удобна при одновременном ее использовании в системах контроля доступа. Однако при мобильном применении НКИ, например, использование NoteBook в командировках или при on-line операциях не со своего стационарного компьютера, более удобным в эксплуатации является ключ безопасности.

Заключение

В заключении хочется еще раз отметить, что качество, надежность и безопасность информационного обмена – это те критерии, которые должны лежать в основе всех информационно-телекоммуникационных систем. Поэтому при создании на предприятии комплексных систем информационной безопасности необходимо отталкиваться именно от этих принципов.

Обращаем Ваше внимание, что данная работа не ставит перед собой цель однозначно характеризовать надежность каждого продукта. В зависимости от требований к уровням безопасности информационной среды Вашей организации каждое решение может проявить как свои преимущества, так и недостатки, и порой поможет избежать лишних затрат при построении PKI.

Искренне надеемся, что проведенная нами работа позволит Вам максимально учесть все нюансы при построении PKI-инфраструктуры и выбрать тот продукт, который обеспечит Вам твердую почву под ногами в зыбком море информации.

УДК 681.3

НЕСИМЕТРИЧНЕ КОДУВАННЯ З ВИКОРИСТАННЯМ ЛИШКОВИХ КЛАСІВ

Вячеслав Василенко
Національний авіаційний університет

Анотація: **Пропонується використання несиметричного блокового криптографічного перетворення для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем з використанням системи числення в лишкових класах.**
Summary: **The use of asymmetrical sectional cryptographic transformation for the tasks of providing of confidentiality of information's holding object of the automated systems with the use of scale of notation in remaining classes is offered.**
Ключові слова: Криптографічні перетворення, лишкові класи, несиметричні ключі, системи числення.

І Вступ

Відомо, що сенсом криптографічних перетворень є така зміна початкового повідомлення (тесту,