дифференциальных и линейных атак. 4-й режим (выработки имитовставки) потенциально уязвим для дифференциального криптоанализа, поскольку использует только 16 циклов шифрования вместо 32. Однако если сообщение с имитовставкой зашифровывается перед передачей, то в этом случае дифференциальная атака на 4-й режим невозможна (поскольку дифференциальный криптоанализ относится к атакам с выбранными открытыми текстами и для его проведения необходимо знание открытых и зашифрованных сообщений). Даже при использовании 4-го режима работы алгоритма шифрования для передачи незашифрованной имитовставки необходимость выбора большого количества открытых текстов и получения соответствующих им зашифрованных делает дифференциальную атаку на этот режим практически неосуществимой в реальных СЗИ. При разработке новых систем для обеспечения имитозащиты можно рекомендовать применение функции хеширования ГОСТ 34.311-95 (с соответствующим добавлением ключевых данных) вместо 4-го режима ГОСТ 28147-89.

При разработке СЗИ следует обеспечивать защиту от атак на реализацию, таких как временная атака, анализ энергопотребления, дифференциальный анализ сбоев, поскольку ни один шифр не может быть защищён от этого вида нападений исключительно математическими методами.

Анализ свойств таблицы подстановок ГОСТ 34.311-95 показал, что в них отсутствуют закладки, делающие шифр уязвимым для известных видов криптоанализа. Более того, проведена оптимизация против дифференциального и линейного криптоанализа. В принципе, существует возможность генерации более стойких таблиц с дополнительными критериями для защиты от дифференциального и линейного криптоанализа, однако и рассмотренная обеспечивает максимальную стойкость трёх режимов ГОСТ 28147-89 и практическую стойкость режима выработки имитовставки. Поэтому можно рекомендовать использование долговременного ключа из ГОСТ 34.311-95 в качестве стандартного для ГОСТ 28147-89 при обеспечении криптографической защиты информации в открытых системах.

Литература: 1. В. И. Долгов, И. В. Лисицкая, Р. В. Олейников, С. А. Головашич, А. С. Коряк. Дополнительные требования к отбору таблиц подстановок для ГОСТ 28147-89. Материалы научно-практической конференции по вопросам криптографической и технической защиты информации. Департамент специальных телекоммуникационных систем и защиты информации Службы Безопасности Украины, Центр Банковских Информационных Технологий. Киев, 2000. 2. B. Schneier. Applied Cryptography. Addison Wesley and Sons, New York, 1996. 3. Р. В. Олейников. Дифференциальный криптоанализ алгоритма шифрования ГОСТ 28147-89. Радиотехника, 119. 2001 г. С. 146-152. 4. K. Kim, S. Lee, S. Park and D. Lee. How to strength DES against two robust attacks. Joint Workshop on Information Security and Cryptology. Inuyata, Japan, January 24-25, 1995. 5. В. И. Долгов, И. В. Лисицкая, С. А. Головашич, Р. В. Олейников. Принципы защиты алгоритма DES от атак дифференциального криптоанализа. Радиотехника, 113. 2000 г. С. 148–157. 6. J. Kelsey, B. Schneier, D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and Triple-DES. Advances in Cryptology – CRYPTO'96, Springer-Verlag, Berlin 1996.

УДК 681.3.06

ПРИНЦИПЫ ПОСТРОЕНИЯ И ИСПОЛЬЗОВАНИЯ МНОГОУРОВНЕВЫХ ЦЕНТРОВ УПРАВЛЕНИЯ И СЕРТИФИКАЦИИ КЛЮЧЕЙ

Иван Горбенко, Александр Волощук*, Елена Качко*, Андрей Свинарев*, Павел Колесников, Татьяна Гриненко

Харьковский национальный университет радиоэлектроники

**АТ "Институт информационных технологий"*

Анотація: **Розглядаються основні положення створення багаторівневого центру сертифікації. Визначаються основні функції центру. Розглядаються проблеми, що з'являються під час розробки багаторівневого центру.**

Summary: **In the proposed report we consider the main statements of multilevel certification center development. Main functions of such centers are: generation, distribution and support of common parameters and keys for whole multilevel network, developing of open key base. It is considered a number of problems, which appears during of key transitions.**

Ключові слова: **Ключі, управління ключами, сертифікація ключів, бази даних ключів, паролів, фіскальний контроль.**

Основные требования по выполнению и функциям

В настоящее время используется три основных модели проектирования и разработки программного обеспечения: водопада, спиральная модель и Microsoft Solutions Frames (MSF- фреймы решений Микрософт). Последняя модель наиболее подходит при разработке систем защиты ввиду следующих достоинств по сравнению с другими моделями.

Модель предусматривает возможность корректировки требований к системе, например, изменение ключевых носителей (дискета, touch-memory, smart card), что не позволяет модель водопада.

Модель четко определяет этап завершения каждой стадии, что не используется в спиральной модели. В системе защиты нельзя хорошо защищать документ, если моделью не предусмотрена стадия завершающего этапа, или не достаточно хорошо будут защищены все ключи, что противоречит концепции системы защиты.

Модель MSF предусматривает выполнение четырех фаз для разработки проекта: анализ, планирование, реализация, стабилизация. Каждая фаза заканчивается вполне конкретным результатом, который четко определен моделью. В ней же определено распределение ролей при выполнении работ. Ниже рассмотрены эти фазы для Центра управления и сертификации ключей.

I Анализ проекта

Опишем основные цели и концепции создания многоуровневого центра сертификации. В комбинационных шифрах с учетом модели взаимного недоверия сложность управления ключами по сравнению с однонаправленным возрастает. Ключи должен генерировать какой-то пользователь (сам себе) личным ключом, не выходящим за пределы пользователя, а открытые ключи назначаются в виде сертификатов пользователям, с которыми связан данный корреспондент. В процессе развязки должна быть обеспечена целостность и аутентичность открытых ключей.

Требуемые показатели конфиденциальности, подлинности, целостности, причастности, а также защищенности от НСД в любой системе защиты обеспечивается только в том случае, если ключи (личные остаются в тайне и недоступны криптоаналитику). При этих условиях для вскрытия системы криптоаналитик должен осуществить "лобовую" атаку на криптосистему (факторизация модуля, решение дискретного логарифма в системах класса Эль-Гамаля и др.). Если личный ключ скомпрометирован, то взлом системы защиты осуществляется мгновенно. Для этого достаточно ввести правильно пароли и ключи. В широком смысле под компрометацией ключей и паролей понимается факт противоправного разглашения ключей и паролей посторонним лицам. В специальном приказе по предприятию определяются лица, которые допущены к работе с ключом. Личный ключ – исключительная собственность пользователя и не может быть передан никому, включая прямых начальников.

Для решения задач генерации, распределения и т. д. ключей создается специальная служба управления ключевыми структурами. Кроме того, в системе должен быть создан центр управления ключами (ЦУК). При этом под управлением ключевыми структурами понимается совокупность процедур, алгоритмов и воздействий (в смысле принятия решений), направленных на генерацию, сертификацию, распределение, передачу, прием, запись, хранение, использование, уничтожение ключевых данных, а также восстановление их в случае компрометации (прямая замена скомпрометированных ключей).

На предприятиях и в организациях, имеющих разветвленную многоуровневую структуру, наиболее остро встает вопрос о распределении ключей и ответственности за их сертификацию по многоуровневому принципу. Цель разработки – создание многоуровневого центра управления ключевыми структурами многоуровневых центров сертификации. Многоуровневый центр должен использоваться в следующих сферах деятельности:

- банковские системы;
- государственные системы;
- предприятия с разветвленной системой партнеров и т. д.

Необходимо организовать защищенный обмен информацией между распределенными территориально клиентами, которые организационно могут быть в подчинении у различных центров управления. Задачи создания многоуровневого центра определены ниже.

- Администрирование пользователей центров текущего и очередного уровней (определение списка рабочих мест для текущего уровня, центров очередного уровня, прав доступа для всех рабочих мест).
- Генерация общесетевых параметров системы и их распространение.
- Генерация ключей сертификации для центра текущего уровня.
- Генерацию ключей арбитра.
- Генерация транспортных ключей для центра очередного уровня или удаленных пользователей.

- Генерация рабочих ключей для пользователей центра текущего уровня.
- Управление базой данных открытых ключей.
- Никакие ключевые данные не должны храниться в открытом виде.
- Задача создания ЦУК связана с обеспечением нормальной работы рабочих мест клиентов системы. На рабочем месте должен выполняться большой спектр клиентского программного обеспечения (платежный документооборот, АРМ клиента банка и другие). Все программное обеспечение должно пользоваться ключами, сгенерированными в сети многоуровневых центров сертификации. Ключи должны храниться в базах данных, формат которых строго стандартизирован и подходит для задач всех пользователей. Таким образом, решено использовать следующие концепции.
- Использовать защищенную базу данных сертификатов.
- База данных должна иметь высокую производительность операций чтения, записи.
- База данных должна хранить сертификаты пользователей в зашифрованном виде.

Опишем концепцию создания многоуровневого центра сертификации. В результате исследования платежных систем УкрСоцБанка определена цель и задачи создания многоуровневого центра. При выполнении этапа анализа разработана концепция системы защиты с многоуровневой архитектурой. Данная концепция учитывает развитие системы защиты и используется для стратегического планирования модулей защиты, которые постоянно охватывают все информационные обмены предприятия (банка).

В концепции в комплексе наиболее важных факторов для данного проекта определены следующие.

- Надежность криптографических алгоритмов; с целью повышения надежности используются ключи максимальной длины для стандартных алгоритмов, общие параметры системы и «открытые ключи» хранятся в защищенном виде, не используются одни и те же ключи для различных алгоритмов.
- Настраиваемость системы; при профилировании системы определяются центры более низких уровней, пользователи, рабочие места с различными правами в использовании криптографических алгоритмов (только цифровая подпись, подпись и шифрование), носители для личных ключей (дискета, touch-memory, smart cart).
- Управление доступом; система не только проверяет наличие личного носителя ключа и знание пароля для этого ключа, но и не «позволяет» выбрать слишком простой пароль, например короче 8 символов или пароли вида «12345678». Личный носитель не должен хранить более одного ключа, определенные части могут храниться на разных ключевых носителях.
- Надежные системы управления ключевыми структурами; ключи хранятся в виде сертификатов, для пересылки ключей используются состоятельные протоколы, ключи пересылаются только в защищенном или подписанном виде.
- Как и для любой системы защиты в данном проекте определяются наряду с техническими и организационные мероприятия, невыполнение которых может свести на нет работу даже самой могучей системы. Так передача личных ключей с паролем, посторонние лица на рабочем месте администратора центра и пользователей могут привести к отрицательным последствиям.
- Использование сертифицированных источников случайных ключей, оперативный контроль ключевых данных.
- Регистрация всех событий в системе, в том числе операций с ключевыми данными, криптографических операций.
- Интеграцию с другими системами; центр должен управлять ключевыми структурами для всех систем организации, в том числе системой электронной почты, файлового обмена, банковских документов, и т. д.

Определены функциональные возможности центра.

- Создание центра очередного уровня.
- Определение рабочих мест и удаленных пользователей центра (РМ и ПЦ).
- Добавление, удаление РМ и ПЦ.
- Генерация общесетевых параметров для всей ключевой системы.
- Генерация ключей сертификации центра.

II Планирование проекта

Этап анализа позволил четко определить цели, задачи, приоритетные направления и функциональные возможности Центра. Рассмотрим фазу планирования, целью которой является разработка плана проекта.

Для составления плана проекта выполним сначала концептуальное, а затем логическое и физическое проектирование.

1. Во время концептуального проектирования определено, что в системе используются следующие криптографические алгоритмы:
   ГОСТ 34.310-95 – цифровая подпись. Длина общесетевого параметра P – 1024 бита, длина Q – 256 бит, длина закрытого ключа X – 256 бит, длина открытого ключа Y – 1024 бит.
   RSA – направленное шифрование. Длина модуля преобразования N и ключей XY – 1024 бит.
   ГОСТ 34.311-95 – хеш-функция. Длина хеш-функции текста – 256 бит.
2. Во время логического проектирования определены базисные классы, наследование, определение составляющих и функций. Для создания многоуровневой структуры использовалась иерархия классов. Для хранения сертификатов разработан модуль программы, реализующий функции работы с базой данных. Для использования стандартов криптографических алгоритмов каждая отдельная реализация была сделана в виде отдельного модуля.
3. Физическое проектирование. Определяются структуры данных, функции и их аргументы. С функциями можно ознакомиться по исходным текстам программы. Интерфейс к функциям одинаковый для всех программных компонентов, работающих внутри системы многоуровневых центров сертификации.

Для реализации защищенной передачи сертификатов по открытым каналам связи разработаны состоятельные протоколы управления ключами. Распространение ключей должно осуществляться посредством использования состоятельных протоколов. Состоятельным называется протокол управления ключами, который обеспечивает их гарантированную конфиденциальность, подлинность, целостность и достоверность на всех этапах жизненного цикла ключа.

Состоятельные протоколы могут быть реализованы с использованием как симметричных, так и несимметричных систем. В каждом протоколе должно применяться несколько уровней ключей. Система должна быть двух- или трех уровневой.

1 уровень. Главные ключи.

2 уровень. Рабочие ключи.

3 уровень. Сеансовые ключи.

1. Ключами сертификации обладают все ЦУК данной модели. Каждый ЦУК имеет свою зону влияния, в которую входят подчиненные ему ЦУК и клиенты, которые обслуживаются данным ЦУК. Ключ сертификации содержит ключ цифровой подписи. Он служит для сертифицирования рабочих ключей клиентов, находящихся в его зоне подчинения. При передаче ключей от одного клиента к другому, если оба клиента находятся в зоне подчинения одного ЦУК, проверяется сертификат открытого ключа первого клиента, выданный их общим ЦУК. Предполагается, что оба клиента доверяют подписи ЦУК, которому они подчинены. На основании проверки сертификата на открытом ключе сертификации центра получатель делает вывод о подлинности ключа отправителя. Открытый ключ сертификации передается всем клиентам, подчиненным данному ЦУК. Смена ключа сертификации проводится ЦУК при следующих условиях:

- при возникновении подозрения о компрометации сертификационного ключа;
- при истечении рекомендуемого срока действия;
- по указанию службы безопасности регионального управления.

После успешного завершения смены ключа сертификации открытая часть ключа отсылается всем клиентам и центрам сертификации, подчиненным данному ЦУК. На практике период плановой смены ключа сертификации выбирается равным 180 дням.

2. Транспортные ключи в многоуровневой модели применяются для передачи рабочих ключей между ЦУК и подчиненными ему клиентами и центрами сертификации. Транспортные ключи содержат ключ подписи и шифрования. Каждый ЦУК генерирует себе пару транспортных ключей: открытую составляющую и закрытую для общения с подчиненными ему отделениями и клиентами. Открытая составляющая передается клиенту. Таким образом возможна передача рабочих ключей на сертификацию от клиента в ЦУК по закрытому каналу. Для возможности направленного шифрования от ЦУК к клиенту создаются транспортные дискеты клиентов, на которые клиенту записываются его секретный транспортный ключ. Открытый транспортный ключ клиента остается в ЦУК. Транспортная дискета клиента передается ему по надежному каналу (например, курьерской почтой).

Аналогично генерируется транспортная дискета для подчиненного ЦУК. Эта дискета генерируется в ЦУК на уровень выше. На нее записывается закрытая часть транспортного ключа ЦУК, открытая часть хранится в центре на уровень выше. Транспортная дискета в подчиненном ЦУК нужна исключительно для приема рабочих ключей от ЦУК верхнего уровня. Срок действия транспортного ключа выбирается равным 180 дням.

Целесообразно совместить функции транспортного ключа подписи и сертификационного ключа для ЦУК. В этом случае при передаче ключей от ЦУК пакет будет подписываться сертификационным ключом центра.

3. Рабочий ключ должен генерироваться корреспондентом по принципу “сам себе” и не выходить из пределов личного владения. Используется для шифрования и подписи сообщений, данных, программ и т. д. В ряде случаев рабочие ключи используются только для шифрования сеансовых ключей. Рабочие ключи генерируются на рабочих местах. Центры сертификации могут создавать рабочие места, ключи для которых генерирует сам центр. Рабочие места могут быть двух типов: рабочее место с правом подписи, рабочее место с правом шифрования и подписи. Личные ключи после генерации записываются на личный съемный носитель пользователя, а открытые ключи сертифицируются и хранятся в базе данных открытых ключей.

Рабочие ключи могут быть сгенерированы на рабочем месте ЦУК, тогда они сразу сертифицируются сертификационным ключом центра, или могут быть созданы клиентом с помощью генератора ключей. Во втором случае открытый рабочий ключ, прежде чем он будет использоваться для передачи информации, должен быть отослан в ЦУК на сертификацию.

4. Сеансовые ключи генерируются на один сеанс обмена сообщениями между отправителем и получателем. Сеансовые ключи требуются в следующих криптографических схемах:

а) в алгоритмах цифровой подписи, таких как ГОСТ 34.310–95, DSS, генерируется случайная составляющая k, которая участвует в формировании цифровой подписи и является личной для стороны, которая ставит цифровую подпись; благодаря числу k каждая новая цифровая подпись отличается от предыдущей.

б) при использовании направленного протокола шифрования, построенного на алгоритмах ГОСТ 28.147 и RSA используется сеансовый ключ шифрования k для ГОСТ 28.147, который генерируется случайно на один сеанс отправки сообщения и хранится в тайне от третей стороны.

5. Выполнен анализ протоколов импортирования, экспортирования ключей и разделения секрета для обеспечения возможности обмена информацией между любыми двумя рабочими местами, находящимися в структуре. Предложена следующая схема распределения открытых ключей, которая заключается в следующем.

После создания главного ЦУК создаются подчиненные ЦУК. Подчинение состоит в том, что для работы каждого следующего центра его ключ сертификации должен быть сертифицирован на уровень выше.

Открытый ключ сертификации ЦУК передается в подчиненные ЦУК на один уровень вниз и на удаленные рабочие места клиента и на один уровень вверх, в главный центр. Таким образом, при обмене открытыми рабочими ключами между рабочими местами подчиненных отделений подпись сертификата может быть проверена открытым ключом сертификации. Открытый ключ сертификации не пересылается в другие ЦУК, но тогда необходимо определить, как гарантировать подлинность рабочего ключа при передаче его в любое отделение в пределах многоуровневой модели.

При передаче открытого ключа удаленному клиенту в сети каждый промежуточный центр сертификации должен проверить подпись подчиненного ему центра. Если подпись верна, то он ставит свою подпись на открытый рабочий ключ и передает его дальше получателю. После доставки ключа получателю сертификат хранится в базе данных получателя с подписью ближайшего центра сертификации.

Выбран протокол передачи сертификатов между центрами и передачи сообщений между рабочими местами. Схема протокола, основанная на алгоритме RSA, приведена на рисунке 1. Схема протокола, основанная на алгоритме Диффи-Хеллмана, приведена на рисунке 2.

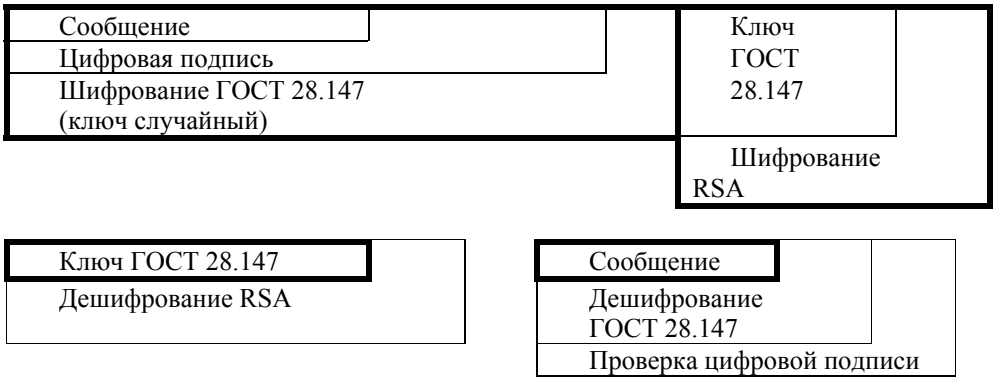

Рисунок 1

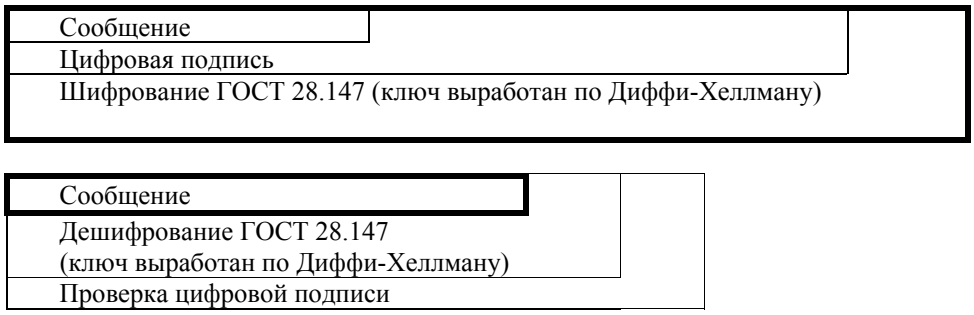

Рисунок 2

К ключам, присылаемым на сертификацию, предъявляются следующие требования.

- Как симметричные, так и несимметричные ключи должны генерироваться с помощью чисто случайных процессов. Для обеспечения надежности применяются комбинированные схемы, в которых используются как случайные, так и псевдослучайные процессы с требуемыми свойствами. Ключи и ключевые параметры должны удовлетворять требованиям: случайности их появления; равновероятности; независимости ключей и символов между собой; неоднородности.
- В качестве конкретных алгоритмов могут использоваться установленные в Украине стандарты симметричных и несимметричных алгоритмов шифрования (ГОСТ 28. 147, DES, RSA).

Требования к ключам различны в зависимости от криптосистемы. Для ГОСТ 28.147-89 необходимо обеспечить генерацию СК длиной 256 бит и ДК (ДК1 – ДК8) 8 строк по 16 столбцов, т. е. 512 бит. В RSA системах ключевые параметры Pj, Qj должны выбираться случайно. Случайно генерируется Ek и проверяется на взаимную простоту с функцией Эйлера (Ek, φ(Nj)) =1, т. е. Ek порождается случайным процессом.

Для генерации ключей создаются специальные комплексы. Задача генерации может возлагаться как на специальный центр, так и непосредственно на пользователя. Для личных целей ключи рекомендуется генерировать лично. Для обеспечения высокого уровня защиты необходимо применять централизованные и децентрализованные принципы генерации ключа, сущность которого заключается в применении многоуровневой ключевой системы.

III Фаза реализации

Программное обеспечение ЦУК включает в себя несколько программных модулей и пакетов, которые предназначены для работы в различных структурных подразделениях многоуровневой иерархической модели центров распространения и сертификации ключей. Программное обеспечение включает в себя следующие пакеты программ. Программное обеспечение ЦУК, которое работает на рабочем месте администратора безопасности в центре распределения ключей. Программное обеспечение генератора ключей, которое работает на стороне клиента и служит для генерации ключей для рабочих мест клиента. Программное обеспечение рабочего места оператора.

Библиотека математических операций многоразрядной точности и реализация стандартов криптографических алгоритмов написаны на языке низкого уровня Assembler. Это обеспечивает высокую производительность работы ядра системы. Реализация функций генерации ключей и общесетевых параметров, а также функции работы с базой данных сертификатов написаны на языке C++. Этот язык программирования выбран потому, что он является системным языком, наиболее удобным для написания профессиональных программных продуктов. Интерфейсная часть написана с использованием среды визуального программирования C++ Builder.

IV Методика настройки и тестирования

Разработана методика настройки и тестирования, которая заключается в следующем.

Необходимо протестировать корректность реализации стандартов криптографических алгоритмов. Для этой цели необходимо воспользоваться сертифицированными средствами тестирования стандартов RSA, ГОСТ 28.147, ГОСТ 34.310-95, ГОСТ 34.311-95. На функциях, реализованных в системе, проверяется выполнение стандартного тестового примера для соответствующего алгоритма. На основании результатов работы тестового примера делается вывод о правильности реализации стандартов. Необходимо тестировать следующие функции:

в RSA – функции генерации модуля преобразования N, функции генерации ключей X и Y, функции прямого и обратного преобразований;

в ГОСТ 28.147 – операции шифрования и дешифрования;

в ГОСТ 34.310-95 – функции генерации общесетевых параметров P, Q, A, функции генерации ключей X и Y, функции наложения и проверки подписи;

в ГОСТ 34.311-95 – функции формирования хеш.

Далее необходимо проверить работу центров сертификации и всей системы в комплексе. Для этого необходимо проверять сначала простейшие функции, выполняемые центром. Сначала нужно установить только центр верхнего уровня и полностью протестировать его работу. Затем наращивают и постепенно усложняют функции, реализуемые центрами сертификации. Далее создается подчиненный центр и тестируется их совместная работа. После дальнейшего создания и тестирования центра третьего уровня можно утверждать о правильности работы системы с неограниченным количеством уровней. Тестируются также удаленные генераторы ключей и их работа совместно с одним из центров. После тестирования работы генератора ключей с одним из центров можно утверждать о правильности работы генератора ключей с любым из центров. Создаются рабочие места в центре и у клиентов, тестируется работа рабочих мест друг с другом. На основании прохождения всех этапов тестирования можно делать вывод о правильности работы системы в целом.

Выводы

Задача создания многоуровневого центра сертификации является актуальной на сегодняшний день, поскольку существуют предприятия и организации с многоуровневой структурой управления. Рассмотрены основные принципы построения многоуровневого центра сертификации. Рассмотрена модель проектирования программного обеспечения Microsoft Solutions Frames, согласно которой была проведена разработка многоуровневого центра управления и сертификации. Описаны цели и задачи создания такого центра, обоснована необходимость его создания. Определены сферы применения центра сертификации. Определены основные функции, которые должен выполнять центр сертификации. На этапе планирования определены стандарты и криптоалгоритмы, которые должны быть использованы в программном обеспечении, обоснованы причины применения именно этих алгоритмов.

Рассмотрена структура ключей в многоуровневом центре сертификации, которая состоит из главных ключей, рабочих ключей, сеансовых ключей. Описано функциональное назначение ключей каждого типа. Рассмотрена работа многоуровнего центра сертификации, построенная на критериях выбора ключевых параметров и оценки качества ключевых данных. Выполнен анализ протоколов импортирования, экспортирования ключей. Приведен состоятельный протокол направленной передачи сертификатов и сообщений по открытому каналу связи.

На этапе реализации и тестирования обоснован выбор программных средств для создания пакета инсталляции системы. Описаны принципы тестирования программного продукта на соответствие его стандартам и корректной его работы.

УДК 681.3

МОДЕЛЮВАННЯ ДОСТУПУ ТА КАНАЛІВ ВИТОКУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Анатолій Антонюк, Віктор Жора*

Інститут програмних систем Національної Академії наук України

**Фізико-технічний інститут НТУУ «КПІ»*

Анотація: **Розглянуто множину можливих доступів до інформації в автоматизованих системах. За допомогою поняття каналів витоку подано формальні визначення загроз інформації.**

Summary: **The report deals with the multitude of possible accesses to information in automated systems. The formal definitions of information threats are proposed using the concept of leakage channels.**

Ключові слова: **Інформація, конфіденційність, цілісність, доступність, спостереженість, захист, доступ, канал витоку, послуга.**