НОВЫЕ СРЕДСТВА КИБЕРНЕТИКИ, ИНФОРМАТИКИ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СИСТЕМНОГО АНАЛИЗА

Е.А. ЗУБАРЕВА, С.В. БЕЛОВ

УДК 004.052(045)

СИСТЕМА ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА УКРАИНЫ И СПОСОБ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ЕЕ ФУНКЦИОНИРОВАНИЯ

Аннотация. Исследованы ключевые понятия качества обслуживания, влияющие на безопасное функционирование системы электронного правительства. Проанализированы параметры и требования безопасности для обеспечения надежной работы системы. Предложен способ повышения безопасности функционирования телекоммуникационной инфраструктуры.

Ключевые слова: электронное правительство, телекоммуникационная инфраструктура, информационная безопасность, качество обслуживания, криптографическая защита информации.

ВВЕДЕНИЕ

Современный этап развития научно-технического прогресса характеризуется интенсивной разработкой и внедрением новых информационно-коммуникационных технологий (ИКТ) при переходе от «индустриального общества» к «обществу информационному». Уровень развития информационного пространства и общества значительно влияет на экономику, обороноспособность и политику государств.

Информационное общество базируется на глобальном информационном пространстве и включает разнообразные информационные ресурсы, эффективно взаимодействующие посредством общедоступных сетей для удовлетворения потребностей пользователей в информационных продуктах и услугах в различных сферах: технологической, социальной, экономической, культурной и политической. В настоящее время в Украине сложились благоприятные условия для качественных изменений в области создания систем электронного управления и формирования информационного общества.

Одним из важнейших этапов становления информационного общества является разработка и внедрение системы электронного правительства (*e*-Goverment, *e*-правительства) как системы эффективного взаимодействия органов государственного управления, граждан и бизнеса с помощью услуг, предоставляемых на базе ИКТ. Основой *e*-правительства должна стать единая инфраструктура межведомственного информационного взаимодействия органов государственной власти (ОГВ) и органов местного самоуправления.

Отметим, что в настоящее время еще не создана необходимая единая инфраструктура межведомственного информационного взаимодействия для решения важнейших задач и, как следствие, нет единого национального информационного пространства предоставления населению административных услуг в электронном виде. Не решены вопросы стандартизации функционирования ИКТ, законодательного и нормативного обеспечения применения передовых ин-

формационных технологий, соответствующих лучшим мировым практикам, а также обязательного соблюдения требований международных стандартов по информационной безопасности с учетом национальных особенностей.

За последние десятилетия в рамках реализации ряда проектов разработано большое количество типовых эффективных решений по следующим направлениям, определенным директивами ЕС: база стандартизации правил и форматов взаимодействия всех участников, политики доступа, применение средств защиты, обеспечение юридической значимости документов и т.п.

Вопросы информационной безопасности рассмотрены в научных работах многих видных отечественных и зарубежных ученых: S. Northcutt, J. Novak, В.В. Домарева, А.Ю. Щеглова и др. Мировой опыт реализации проектов *е*-правительства показывает, что решение задач по обеспечению безопасности и надежности функционирования информационно-телекоммуникационной инфраструктуры как неотъемлемой составляющей системы электронного правительства чрезвычайно актуально и имеет важное научно-практическое значение.

АНАЛИЗ ПРОБЛЕМЫ

По решению Национальной комиссии, осуществляющей государственное регулирование в сфере связи и информатизации (НКРСИ) [1], разработана единая информационно-коммуникационная платформа (ЕИКП), которая является составляющей *е*-правительства, а также определены основные концептуальные положения ее создания [2].

Отметим, что ЕИКП — это информационно-коммуникационная система автоматизированного информационного взаимодействия ОГВ, бизнеса и граждан, поэтому должна проектироваться как многофункциональная сервис-ориентированная, распределенная и адаптивная система обработки информации.

Концептуальные решения ЕИКП направлены на объединение в единую систему информационных систем (ИС) ОГВ и органов местного самоуправления; предоставление административных услуг в режиме «единого окна»; развитие и повышение качества предоставления услуг в электронном виде населению и бизнесу, а также обеспечение надежной защиты информации.

Анализ состояния информационных ресурсов Украины позволяет сделать вывод о том, что ИС органов власти и местного самоуправления создавались для решения локальных задач без учета необходимости их взаимодействия, что предопределило:

— несовместимость внедренных автоматизированных ИС государственных органов ввиду отсутствия унифицированных требований к созданию таких систем и регламентов обмена информацией;

— отсутствие унифицированной инфраструктуры электронного взаимодействия государственных органов с гражданами и предприятиями;

— многократное дублирование сбора и обработки данных различными государственными службами, недостаточная полнота и достоверность хранимой информации;

— отсутствие единых правил, регламентов обмена информацией и форматов данных в ИС органов власти, использующих электронную цифровую подпись.

В настоящее время большинство систем документооборота являются локальными комплексами, обеспечивающими деятельность определенных государственных и коммерческих структур, но они не способны взаимодействовать. Вопросами внедрения унифицированного электронного документооборота и организации защиты информации в ИС занимаются: Агентство Госинформнауки, Министерство юстиции, Госспецсвязь, НКРСИ, а в банковской системе — Наци-

ональный банк. Но поскольку не существует единого координирующего органа с четко определенными полномочиями и ответственностью, не решены многочисленные проблемные вопросы, а именно:

— не достигнут необходимый уровень стандартизации в сфере ИКТ, соответствующий международным и европейским стандартам;

— не создан действенный механизм координации и регулирования деятельности государственных органов при разработке проектов в области информатизации;

– не отлажена унифицированная и эффективная инфраструктура обмена информацией между ОГВ и не созданы четкие правовые основы обмена информацией;

— не разработана система единых (общегосударственных) справочников и классификаторов, электронных реестров и баз данных;

— не предоставляются качественные услуги в электронном виде органами власти и местного самоуправления гражданам и бизнесу в режиме «единого окна»;

— неэффективно используются бюджетные средства ОГВ на проектирование и создание ИС;

— не устранено несоответствие международным, в частности европейским, стандартам в сфере ИКТ, возникшее в результате самоизоляции Украины от международного и европейского информационного сообщества.

Важнейшим условием эффективного взаимодействия различных ИС является унификация технологических решений и интерфейсов для создания и обработки электронных документов при применении множества слабо интегрированных программно-технических решений. Особое внимание следует уделить разработке и внедрению средств и методов защиты информации, позволяющих «прозрачно» взаимодействовать различным системам для поддержания необходимого уровня защищенности компонентов систем электронного документооборота и массивов документов с разными уровнями доступа к ним.

Использование ИКТ в предоставлении административных услуг обеспечивает такие преимущества, как улучшение качества обслуживания при незначительной задержке предоставления услуг в круглосуточном режиме, снижение эксплуатационных затрат, повышение производительности работы и т.п. Однако применение ИКТ связанно с необходимостью решать следующие вопросы информационной безопасности: обеспечение конфиденциальности личной информации (персональных данных), ее защиты, доверия к ней и непосредственно к системам, а также поддержка правового статуса информации.

Модель информационной безопасности ЕИКП предусматривает соблюдение конфиденциальности, целостности и доступности информации с ограниченным доступом, обрабатываемой в данной платформе. Это обеспечивается комплексной системой защиты информации от несанкционированного доступа для реализации заданных политик безопасности информации, применением организационно-правовых, инженерно-технических мероприятий, а также использованием аппаратных, программно-аппаратных и программных средств защиты информации [3].

Построение ЕИКП на базе международных стандартов электронного правительства, опыта и лучших практик создания аналогичных систем в США, ЕС и Российской Федерации позволит обеспечить быструю интеграцию в международное информационное пространство и эффективное электронное взаимодействие с международным сообществом.

Успешное внедрение системы электронного правительства в Украине является, безусловно, очень важной задачей. Поэтому все описанные аспекты свидетельствуют о необходимости создания единой информационно-телеком-

муникационной инфраструктуры, а также об актуальности изучения вопросов, связанных с разработкой технических средств и организационных методов ее безопасного функционирования.

Цель проведения исследований — обеспечение безопасности функционирования телекоммуникационной инфраструктуры системы *e*-правительства для поддержания соответствующего уровня качества обслуживания пользователей при предоставлении административных услуг в электронном виде.

Для достижения поставленной цели необходимо:

— исследовать ключевые понятия качества обслуживания для поддержания безопасного функционирования системы;

— проанализировать параметры и требования безопасности для обеспечения необходимого качества обслуживания;

— разработать способ повышения эффективности безопасности функционирования телекоммуникационной инфраструктуры.

ИССЛЕДОВАНИЕ КЛЮЧЕВЫХ ПОНЯТИЙ КАЧЕСТВА ОБСЛУЖИВАНИЯ ДЛЯ ПОДДЕРЖАНИЯ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Информационно-телекоммуникационная инфраструктура должна обеспечивать широкополосный доступ к информационным сервисам и возможность одновременного подключения большого количества пользователей. Для этого используются оптоволоконные линии (в качестве базовой магистральной сети), организующие соединение межрегиональных информационно-технологических центров, а также беспроводная широкополосная связь в городах. Сеть беспроводной широкополосной связи должна обеспечить доступ к сервисам ЕИКП для населения, предприятий и организаций.

Отметим, что развитие компьютерных сетей, особенно их беспроводных сегментов, требует постоянного совершенствования методов передачи и приема данных прежде всего на физическом уровне. Одна из главных проблем беспроводного способа соединения состоит в том, что такой информационный канал невозможно физически ограничить и защитить от воздействия шумов и помех [4], поскольку он представляет собой информационную среду с открытым способом распространения сигнала. Поэтому для проведения беспроводных сеансов связи нужны способы соединений более надежные, чем кабельные технологии.

Анализ условий функционирования подобных систем подтверждает важность вопросов проектирования и разработки приемо-передающих устройств и различных средств криптографической защиты информации (КЗИ), от работы которых зависит надежное функционирование компьютерной сети. Наиболее актуальны в процессе обеспечения соответствующего уровня качества обслуживания (Quality of Service, QoS) задачи повышения надежности и безопасности функционирования беспроводных систем.

В плане поддержки безопасного функционирования сети QoS характеризуется тремя основными свойствами: целостность, доступность и безопасность обслуживания. Первое и второе свойство зависят от возникновения помех и ошибок во время передачи информации, поэтому особенно важна поддержка надежности функционирования сети. На третье свойство существенно влияет уровень защиты сети от несанкционированного доступа, умышленных действий хакеров и различных помех. В беспроводных сегментах сети существует только беспроводная среда передачи данных. Поэтому главной задачей является реализация мер по обеспечению комплексной защиты в системе, в том числе: конфиденциальности (шифрования) контента, защиты линий связи (ЛС), надежной авторизации и аутентификации пользователей, а также устройств передачи информации и т.п. [5].

При проектировании современных мультисервисных сетей нужно учитывать условия обеспечения качества их обслуживания. Спецификой данных сетей является необходимость обработки мультимедийного трафика (аудио, видео и другие данные) [6]. Службы реального времени (телефония, трансляция видео и т.п.) предъявляют повышенные требования к транспортной сети, согласно параметрам качества которой часто определяют, существует ли возможность у операторов связи предоставлять услуги служб реального времени. Исследование механизмов поддержки качества обслуживания помогает определить технические средства и организационные меры, позволяющие обеспечивать и поддерживать на надлежащем уровне качество функционирования сети.

Для обеспечения QoS необходимо увеличить пропускную способность сети за счет аппаратных возможностей и применить методы для уменьшения нагрузки на сеть [7]. Для этого используются назначение приоритетов трафика и организация очередей. Назначение приоритетов состоит в делении трафика на классы. Пакеты можно разбить на приоритетные классы в зависимости от настройки узла связи, приложения, генерирующего трафик и т.п. После установки приоритетов однотипные пакеты объединяются в очереди для дальнейшей обработки. Фактически очередь представляет собой некоторый участок памяти маршрутизатора или коммутатора, где для обработки собраны пакеты одного класса.

АНАЛИЗ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ ДЛЯ ОБЕСПЕЧЕНИЯ НЕОБХОДИМОГО КАЧЕСТВА ОБСЛУЖИВАНИЯ

В последнее время интенсивно расширяется применение информационных технологий (в том числе с использованием беспроводных сегментов сетей), поэтому актуально решение вопроса надежного безопасного функционирования. Слабозащищенные или вообще незащищенные беспроводные каналы открывают практически неограниченный доступ к ресурсам сети любым злоумышленникам, что представляет большую опасность для граждан, предприятий и государства в целом и, как следствие, вызывает недоверие к предоставляемым сервисам, качеству информации и надежности хранения данных, включая персональную информацию. Сетевая безопасность стала критичным элементом планирования и использования корпоративной сети, особенно если она имеет беспроводные сегменты. Поэтому возникает необходимость в анализе параметров и требований к безопасности для поддержки соответствующего уровня QoS и гарантии безопасного функционирования компьютерных сетей, особенно для уязвимых беспроводных участков, что важно для дальнейшей разработки программно-аппаратных средств поддержки соответствующего уровня качества обслуживания.

Технические требования обеспечения безопасности состоят в следующем [8] :

— определение функциональных мероприятий безопасности и контроль за техническим обслуживанием механизмов ее обеспечения и средств защиты;

— реализация разрешительной системы допуска обслуживающего персонала к выполнению работ, документам и информации управления средствами связи;

— размежевание доступа обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации в подсистемах различного уровня и назначения;

— учет информационных ресурсов, регистрация и контроль за несанкционированным доступом пользователей, обслуживающего персонала и посторонних лиц;

— предотвращение атак и внедрения программ-вирусов и программных закладок в средства связи и автоматизированные системы;

— применение средств КЗИ для обрабатываемых данных;

— надежное хранение носителей информации, ключей (ключевой документации) и их обращение, которое исключает несанкционированное копирование, подмену и уничтожение;

— резервирование технических средств, баз данных и носителей информации;

— оснащение информационных систем и средств связи устройствами защиты от сбоев электропитания и помех в ЛС;

— постоянное обновление технических и программных средств защиты от несанкционированного доступа к средствам связи, а также современнных антивирусных продуктов.

Выполнение этих требований важно для безопасного надежного функционирования сети и обеспечения доверия ее пользователей.

При выборе архитектуры компьютерной сети и проектировании устройств защиты необходимо учитывать следующие параметры и требования [9]:

— скорость работы в реальном масштабе времени с незначительными задержками сетевых приложений;

— потребляемая мощность;

— легкость интеграции и встраивания;

— гибкость развития и возможности усовершенствования;

— стоимость внедрения;

— общая стоимость владения для пользователя (заказчика);

— операционная зависимость от других внешних компонентов системы;

— физическая защищенность (защита от неумелого использования и выявление вмешательства);

— стойкость криптографической системы (выбор оптимального алгоритма);

— мощность двусторонней аутентификации (с использованием токенов, смарт-карт, криптографических карт и сертификатов);

— случайность генерации ключей и вектора инициализации.

Для обеспечения безопасного функционирования и поддержки соответствующего качества обслуживания имеют важное значение последние четыре требования.

Отметим, что в современных ИКТ используются программно-аппаратные средства различных производителей, в том числе программные комплексы систем электронного документооборота, программно-аппаратные телекоммуникационные средства, протоколы обмена информацией, средства хранения ключевой информации. При этом в системе *е*-правительства нужно обеспечить не только высокие показатели обработки и передачи информации для всех компонентов, но и необходимый уровень защиты, определяемый требованиями национальной безопасности и особенностями национального законодательства в этой области. Для упрощения построения разнообразных систем, значительной экономии при внедрении и адаптации в системах различного назначения, необходимо учитывать требования разграничения уровня доступа, обеспечения непрерывности защиты, совместимости используемых криптографических средств, а также максимальной унификации их применения в выполняемых задачах. Таким образом, актуален вопрос обеспечения полифункциональности применяемых технических решений зарубежных производителей и их интеграции в отечественные комплексы.

РАЗРАБОТКА СПОСОБА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

В настоящее время в Украине и за рубежом значительно расширилась сфера применения криптографических методов и средств защиты информационных ресурсов, постоянно возрастает на них спрос, а также проводятся фундамен-

тальные исследования в области криптографии. В связи с этим актуальны разработка методов повышения безопасности функционирования, создание и применение устройств КЗИ. Поскольку в Украине используются преимущественно зарубежные программные и аппаратные средства, особое значение имеют методы, обеспечивающие их адаптацию к национальным требованиям и универсальность применения в различных технических системах, информационных технологиях и средах. Это касается программных и программно-аппаратных компонентов информационных систем государственного управления и бизнеса, в первую очередь, связанного с финансами.

Для обеспечения безопасности функционирования сети и размещенных на ее базе сервисов необходимо успешно реализовать функцию управления защитой информации, которая позволяет поддерживать средства обработки информации и компьютерные сети в безопасном работоспособном состоянии с соответствующим уровнем качества обслуживания. Для решения этого вопроса в работе [10] предложен способ применения криптографических алгоритмов в средствах защиты информации. Его суть заключается в обеспечении возможности применения дополнительных криптографических алгоритмов (механизмов) на базе математических криптографических операций (криптографических примитивов), реализованных производителем в конкретном программно-аппаратном средстве КЗИ для использования других криптографических алгоритмов без внесения каких-либо изменений в программное обеспечение производителя.

Отметим, что значительное количество существующих технических решений разработано для реализации конкретного набора криптографических алгоритмов, встроенных производителем в средство КЗИ на стадии производства. Большинство таких технических решений (СМАРТ-карты, Host Security Module, HSM) ориентировано на применение конкретных международных криптографических алгоритмов, поэтому их нельзя непосредственно использовать для криптографических преобразований новых (национальных) криптографических алгоритмов. Именно для решения этой задачи и разработан предложенный способ.

На рис. 1 приведена алгоритмическая схема применения способа использования криптографических алгоритмов в средствах защиты информации.

С помощью определенного интерфейса программного обеспечения производителя, который единовременно добавляется в систему внутренних операций (операционную систему) средства КЗИ, реализуются новые криптографические алгоритмы, обеспечивающие универсальность использования средства КЗИ. Применение этого способа для создания нового поколения криптографических средств с расширенной функциональностью позволит без затрат на разработку и создание устройств для каждого нового криптографического алгоритма применять эти средства КЗИ для различных приложений и сервисов.

Предложенный способ позволяет с помощью криптографических примитивов средства КЗИ создавать и загружать в него программную реализацию новых криптографических алгоритмов электронной цифровой подписи, аутентификации, шифрования и т.д., которые отличаются от реализованных в этих средствах производителем на стадии разработки, а также является дополнением к интерфейсам обращения к криптографическим библиотекам работы с математическими преобразованиями на эллиптических кривых, предусмотренным стандартом PKCS #11. Данный способ является связующим программным обеспечением middleware, дополняющим библиотеки разработчика для различных операционных сред.

Применение описанного способа для создания нового поколения криптографических средств с расширенной функциональностью (например, с использованием криптографических примитивов на эллиптических кривых над полем Галуа

EC Fp: простым полем GF(p) или бинарным полем EC GF (2^m)) позволит без затрат на разработку и создание устройств для каждого нового криптографического алгоритма (например, ГОСТ 34.10-2001 или ДСТУ 4145-2002 и т.п.) использовать эти средства КЗИ для различных приложений и сервисов (бизнес-сектор, банковский и государственный секторы) с применением национальных криптографических алгоритмов, а также алгоритмов, разработанных в других странах. Поэтому указанные средства КЗИ с программным обеспечением, реализующим предложенный способ, можно применять не только в государствах, где используются международные криптографические алгоритмы, но и в странах, имеющих национальные криптографические алгоритмы (например, в странах бывшего СССР), как на уровне компьютерных операционных систем, так и для завершенных аппаратных решений средств обеспечения информационной безопасности.

Рис. 1. Алгоритмическая схема применения способа использования различных криптографических алгоритмов в средствах КЗИ

На рис. 2 изображена общая структурная блок-схема реализации способа применения криптографических алгоритмов в средствах КЗИ.

Предложенный способ состоит из следующих этапов:

— записывается специальное программное обеспечение (СПО), в котором реализуется обработка запросов от внутренних программных приложений на выполнение криптографических преобразований в соответствии с алгоритмами, заложенными производителем устройств или созданными по правилам, предусмотренным производителем для иных криптографических алгоритмов;

— в средство КЗИ записывается СПО, которое содержит реализацию нового криптографического алгоритма, отличного от реализованных производителем в средстве КЗИ и взаимодействующего с СПО обработки запросов на выполнение криптографических преобразований от внутренних программных приложений, записанных в средство КЗИ на предыдущем этапе.

Загруженное на втором этапе СПО также взаимодействует с внешними по отношению к средству КЗИ программными приложениями, для которых необхо-

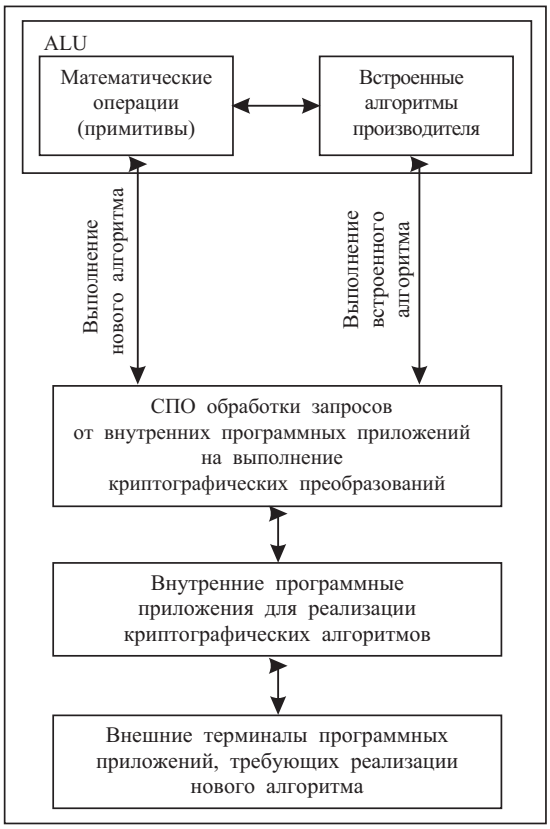

Рис. 2. Структурная блок-схема реализации способа использования криптографических алгоритмов в средствах КЗИ

димо выполнить криптографические преобразования в соответствии с реализованным новым криптографическим алгоритмом. С этой целью и применяются аппаратные модули безопасности HSM. Данное СПО реализуется в виде функционального модуля (Functionality Module, FM), специально предназначенного для подобных HSM-устройств. Это позволяет существенно расширить функциональность уже существующих средств КЗИ для создания нового поколения устройств.

Метод аналогично применяется и для других средств хранения ключевой информации и выполнения криптографических операций.

Разновидностями описанного способа являются следующие операции:

— записывается СПО, взаимодействующее с базовым программным обеспечением производителя (операционной системой устройства, например, СМАРТ-картой или защищенным USB-токеном) и использующее реализованные в постоянной памяти средства КЗИ криптографические примитивы (математические операции), зафиксированные в маске постоянного запоминающего устройства и необходимые для выполнения криптографических преобразований, предусмотренных криптографическим алгоритмом;

— записывается СПО, использующее криптографические примитивы (математические операции), реализованные в специализированном криптографическом процессоре (сопроцессоре);

— записывается СПО, взаимодействующее со средством КЗИ, изготовленным в виде отдельного компьютерного блока – аппаратного модуля безопасности HSM.

Одним из важнейших вопросов при построении сложной системы является ее масштабируемость, т.е. возможность увеличения количества клиентов без потери всех функциональных возможностей данной системы (производительности центральных узлов системы, безопасности и контролируемого увеличения элементов системы с определенным уровнем гарантий).

Внутренние программные приложения, в том числе СПО, можно записать в перепрограммируемое постоянное запоминающее устройство и непосредственно в постоянное запоминающее устройство средства КЗИ. Предложенный способ успешно реализован на современной модели HSM SafeNet типа Luna и ряде чиповых карт и токенов.

ЗАКЛЮЧЕНИЕ

Для обеспечения безотказной работы систем и компонентов *e*-правительства с учетом необходимого уровня качества обслуживания необходимо применять надежные и универсальные программные и аппаратные средства, позволяющие успешно реализовать функцию управления защитой информации. Для этого предложен способ обеспечения безопасной работы программных приложений, компьютерных сервисов и телекоммуникационной инфраструктуры с использованием разнообразных криптографических методов. Он полезен как при проектировании различных информациноных систем ОГВ, так и для дальнейшей реализации конкретных мер по обеспечению надежного помехоустойчивого функционирования существующих компьютерных сетей различного назначения.

СПИСОК ЛИТЕРАТУРЫ

1. Про організацію робіт щодо створення Єдиної інформаційно-комунікаційної платформи органів державної влади [Електронний ресурс]: Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 04 жовтня 2012 р. № 501 / Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації. — http://www.nkrz.gov.ua/uk/activities_nkrzi/ruling2012/1349437554/.
2. Про схвалення Концепції Єдиної інформаційно-комунікаційної платформи [Електронний ресурс]: Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 24 січня 2013 р. № 34 / Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації. — http://www.nkrz.gov.ua/uk/activities_nkrzi/ruling2013/1359114941/.
3. Бєлов С.В., Мартиненко С.В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики // Зб. наук. пр. (ІПМЕ ім. Г.Є. Пухова НАН України. — 2005. — Вип. 28. — С. 68–79.
4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. — М.: Вильямс, 2003. — 1104 с.
5. Зубарева О.О. Методи та засоби забезпечення завадостійкості і безпеки функціонування мереж технології WiMAX: Дис. … канд. техн. наук / НАУ. — Київ, 2013. — 173 с.
6. Зубарева Е.А., Шевцова Е.В. Системный анализ процессов передачи мультимедийного трафика в беспроводных сетях видеоконференцсвязи повышенной помехозащищенности // Електроніка та системи управління: зб. наук. пр. — 2010. — Вип. 2(24). — С. 114–122.
7. Анкудинов Г.И., Стрижаченко А.И. Сети ЭВМ и телекоммуникации. Архитектура и протоколы. — СПб.: СЗТУ, 2001. — 92 с.
8. ГОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения. — Введ. 01.10.2009. — М.: Ростехрегулирования, 2009. — 22 с.
9. Берлин А.Н. Цифровые сотовые системы связи. — М.: Эко-Трендз, 2007. — 296 с.
10. Пат. на корисну модель 66790 Україна, МПК(2006.01) H04L 9/14. Спосіб застосування криптографічних алгоритмів у криптографічних засобах захисту інформації. Заявники та патентовласники С.В. Мартиненко, С.В. Бєлов, О.О. Зубарева та ін. — № u201113881; Заявл. 25.11.2011; Опубл. 10.01.2012, Бюл. № 1. — 6 с.

Поступила 29.04.2014