УДК 004.052(045)

Е.А. Зубарева, Г.Л. Рябцев, И.В. Басанцов, С.В. Белов

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА УКРАИНЫ В УСЛОВИЯХ ДИДЖИТАЛИЗАЦИИ ЭКОНОМИКИ

Ключевые слова: диджитализация, цифровая экономика, электронное правительство, информационная безопасность, качество обслуживания, криптографическая защита информации.

Введение

В настоящее время в Украине сложились благоприятные условия для создания экономических и управленческих систем, позволяющих осуществить «цифровой скачок» на новую ступень развития общества, минуя промежуточные стадии. Основы для этого заложены в Концепции развития цифровой экономики и общества Украины на 2018–2020 годы [1]. Надлежащая ее реализация позволит создать электронное правительство (e-Goverment) как базовый элемент системы эффективного и результативного взаимодействия власти, бизнеса и гражданского общества. В документе предусматривается внедрение различных стимулов для развития цифровой экономики. Задача этих стимулов заключается в том, чтобы поощрять бизнес и граждан использовать информационно-коммуникационные технологии (ИКТ), т.е. сделать их доступными. Для предприятий переход к цифровой экономике определяется как Industry 4.0 (Индустрия 4.0) — четвертая индустриальная революция, намечающая векторы развития многих отраслей экономики и особенно финансовых институций. Собственно Концепция и предусматривает появление и развитие в Украине Индустрии 4.0.

Индустрия 4.0 — это следующий этап цифровизации (или диджитализации, от англ. digital) производства и промышленности, на котором ключевую роль играют такие технологии и концепты, как «интернет вещей», «большие данные» (big data), «предиктивная аналитика», облачные вычисления, искусственный интеллект, робототехника, 3D-печать, «дополненная реальность» и т.п.

При этом бизнес сможет успешно развивать элементы Индустрии 4.0, т.е. коммуникации человека с самим собой, собственным телом и разными вещами; машин с машинами (самоорганизация производственных сил, взаимодействие сборочных единиц и средств производства, «интернет вещей»), а также человека с другим человеком (координация мыслительных процессов группы, нейроинтерфейсы, сборка коллективных субъектов). Для граждан «цифровая экономика» будет означать переход на новый уровень цифровых сервисов, возможность получения государственных услуг в электронной форме, что сведет к минимуму коррупци-

онные риски [2] и будет способствовать скорейшей интеграции Украины в единое цифровое пространство ЕС. Первыми шагами в этом направлении стали электронные реестры, быстро развивающиеся сервисы в области открытых данных, доступа к публичной информации, в том числе с использованием персональных устройств.

Реализация поставленных задач требует правового и институционального применения передовых информационных технологий, создания единого информационного пространства и надежной инфраструктуры, безопасного функционирования сервисов доступа, приема и обработки больших массивов информации с достаточной скоростью, максимальной интероперабельности при взаимодействии систем и баз данных по единым стандартам и унифицированным правилам.

За последние десятилетия в рамках реализации ряда проектов наработано значительное количество типовых эффективных решений по указанным направлениям: база стандартизации правил и форматов взаимодействия всех участников, политики доступа, защита персональных данных, применение средств защиты, обеспечение юридической значимости документов и т.п., определенных директивами ЕС.

Все эти вопросы рассматривали S. Northcutt, J. Novak, В.В. Домарев, А.Ю Щеглов, Р.А Калюжный, Б.А. Кормич, А.А. Баранов. Анализ их работ свидетельствует о том, что обеспечение безопасности и надежности функционирования информационно-телекоммуникационной инфраструктуры, как неотъемлемой составляющей системы электронного правительства, актуально и имеет важное научно-практическое значение.

1. Постановка проблемы

Основой системы электронного правительства Украины должна стать Единая информационно-коммуникационная платформа (ЕИКП) [3–6], внедрение которой направлено на предоставление качественных административных услуг в электронном виде в режиме «единого окна» при обеспечении надежной защиты информации.

Следует отметить, что ЕИКП — это информационно-коммуникационная система автоматизированного информационного взаимодействия органов государственной власти, бизнеса и граждан, поэтому должна проектироваться как многофункциональная сервис-ориентированная, распределенная и адаптивная система обработки информации.

На сегодняшний день системы документооборота в большинстве случаев являются локальными комплексами, обеспечивающими деятельность отдельных государственных и коммерческих структур, но они неспособны взаимодействовать друг с другом для обеспечения необходимого качества предоставляемых сервисов. Вопросами внедрения унифицированного электронного документооборота и организации защиты информации в информационных системах в государстве сегодня занимаются Министерство юстиции, Госспецсвязи, Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации (НКРСИ), а для банковской системы — Национальный банк. Но в связи с отсутствием единого координирующего органа, а также четко определенных полномочий и ответственности на данном этапе не решены многие проблемные вопросы:

— отсутствие необходимого уровня стандартизации в сфере ИКТ в соответствии с международными и европейскими стандартами;

— несовместимость внедренных автоматизированных информационных систем государственных органов из-за 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 разными государственными службами, недостаточная полнота и достоверность хранимой информации;

— отсутствие единых правил, регламентов обмена информацией и форматов данных в информационных системах органов власти с использованием электронной подписи (ЭП), определенной законом, а также альтернативных средств подтверждения подлинности;

— недостаточное количество сервисов предоставления широкого спектра услуг в электронном виде органами власти и местного самоуправления гражданам и бизнесу в режиме «единого окна».

Развитие сервисов и инфраструктуры электронного правительства включает в себя несколько этапов, характерных для любого государства, переходящего на обмен данными и предоставление информационных услуг в электронном виде.

1. Определение перечня приоритетных услуг, разработка пилотных проектов для их реализации и подготовка к внедрению. Формирование единой информационно-телекоммуникационной инфраструктуры электронных услуг, определение единых схем идентификации, применение электронных подписей и определение необходимого уровня доверия (высокий, средний, низкий) к услугам и применяемым схемам идентификации.

2. Оптимизация порядка предоставления административных услуг, внедрение приоритетных услуг в промышленную эксплуатацию, широкое привлечение физических и юридических лиц к использованию электронных услуг.

3. Предоставление электронных услуг во всех сферах общественной жизни, интегрированных электронных услуг, а также внедрение трансграничных электронных услуг.

В настоящее время практически завершен первый этап, начато выполнение второго, а также проектируется ряд пилотных проектов для третьего этапа.

Использование ИКТ при предоставлении административных услуг обеспечивает ряд преимуществ, таких как улучшение качества обслуживания при низкой задержке предоставления услуг в круглосуточном режиме, снижение эксплуатационных затрат, повышение производительности работы и т.п. С другой стороны, применение ИКТ связано с необходимостью решить вопросы с безопасностью, такие как обеспечение конфиденциальности личной информации (персональных данных), высокий уровень доверия к защите этой информации, а также к самим системам и поддержание правового статуса информации.

Модель информационной безопасности ЕИКП предусматривает, что информация с ограниченным доступом, которая обрабатывается платформой, должна сохранять конфиденциальность, целостность и доступность. Это обеспечивается путем применения Комплексной системы защиты информации (КСЗИ), которая предназначена для защиты от несанкционированного доступа (НСД), реализации заданных политик безопасности информации и применения организационно-правовых, инженерно-технических мероприятий и использования аппаратных, программно-аппаратных и программных средств защиты информации [7].

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

Успешное внедрение электронного правительства в Украине является, безусловно, очень важной задачей. Поэтому все вышеупомянутые аспекты сви-

детельствуют о необходимости создания развитой информационно-телекоммуникационной инфраструктуры, а также актуальности изучения вопросов, связанных с разработкой технических средств и организационных методов ее безопасного функционирования.

Цель проведения исследований — разработка решения, позволяющего повысить безопасность функционирования информационно-телекоммуникационной инфраструктуры системы е-правительства для поддержания требуемого уровня качества обслуживания (QoS, Quality of Service) пользователей, а также интероперабельность для схем идентификации и обработки электронных документов в бизнес-приложениях.

Для достижения поставленной цели необходимо решить такие задачи:

— определить ключевые понятия качества обслуживания (сервисов) для безопасного функционирования системы;

— сформулировать требования безопасности для необходимого качества обслуживания (сервисов);

— разработать техническое решение для повышения безопасности функционирования телекоммуникационной инфраструктуры системы электронного правительства.

2. Ключевые понятия качества обслуживания (сервисов) для безопасного функционирования системы

Информационно-телекоммуникационная инфраструктура должна обеспечивать широкополосный доступ к информационным сервисам и возможность одновременного подключения большого количества пользователей. Для этого используют оптоволоконные линии (в качестве базовой магистральной сети) и беспроводную широкополосную связь (для обеспечения доступа к сервисам ЕИКП).

Следует отметить, что развитие компьютерных сетей, а особенно их беспроводных сегментов, требует постоянного совершенствования методов передачи и приема данных, прежде всего, на физическом уровне. Одной из главных проблем беспроводного соединения является невозможность физического ограничения информационного канала и обеспечения его защиты от шумов и помех [8], поскольку это открытая информационная среда распространения сигналов. Поэтому для беспроводных сеансов связи необходимы более надежные и безопасные (по сравнению с кабельными технологиями) соединения.

Анализ условий функционирования подобных систем позволяет сделать вывод о том, что довольно важными являются вопросы проектирования и разработки приемопередающих устройств и различных средств криптографической защиты, от работы которых зависит результирующее надежное функционирование компьютерной сети. Наиболее актуальными в процессе обеспечения соответствующего уровня качества обслуживания являются задачи повышения надежности и безопасности функционирования беспроводных систем.

С точки зрения поддержания безопасного функционирования информационно-телекоммуникационной инфраструктуры, качество обслуживания будем характеризовать

— целостностью (integrity), т.е. соответствием передаваемой, хранимой или отображаемой информации ее внутренней логике, структуре и явно заданным правилам;

— доступностью (availability), т.е. таким состоянием информации, при котором субъекты, имеющие права доступа к ней, могут беспрепятственно ее реализовать;

— безопасностью (security), т.е. состоянием информации, при котором предотвращены несанкционированный доступ к ней, ее искажение, изменение или уничтожение.

Главной задачей является обеспечение комплексной защиты: конфиденциальности (шифрование) контента, защиты линий связи (ЛС), авторизации и аутентификации пользователей и устройств, участвующих в передаче информации [9], и учета специфики обработки мультимедийного трафика (аудио, видео, данных) [10].

Для обеспечения требуемого качества обслуживания целесообразно увеличивать пропускную способность сети за счет аппаратных возможностей и уменьшать нагрузку на нее, организуя очереди и назначая приоритеты трафика (в зависимости от настройки узла связи, приложения, генерирующего трафик) [11]. При этом используют технические средства и организационные меры, способные обеспечить надежную и безопасную работу не только на современном этапе, но и по мере развития таких элементов Индустрии 4.0, как электронная демократия; электронная идентификация; блокчейн; диалоговые системы; цифровые технологические платформы; безналичные расчеты.

Все эти направления требуют достаточного уровня защиты данных в централизованных и распределенных информационно-телекоммуникационных системах (ИТС) с обязательной унификацией требований к самим данным, безопасным средствам доступа, а также использования криптографических сервисов и средств для надежной работы систем.

В настоящей статье рассмотрены возможности программно-аппаратных решений, обеспечивающих указанные свойства.

Согласно исследованиям компании Gartner, в 2017 году выделено десять технологических трендов [12].

1. Искусственный интеллект и глубинное машинное обучение — «умные» устройства на основе интеллектуальных моделей и глубинных нейронных сетей (ГНС).

2. Интеллектуальные приложения — сервисы реального времени на основе виртуальных помощников.

3. «Умные вещи» — промышленные и бытовые устройства на основе «интернета вещей».

4. Виртуальная (VR) и дополненная (AR) реальность — объединение виртуальных и реальных объектов на основе 3D-технологий.

5. Цифровые «двойники» — цифровые динамические модели физических объектов с использованием сенсорных датчиков для имитационного моделирования.

6. Блокчейн и цепочки блоков — распределенные цепочки данных и криптовалюта.

7. Диалоговые системы — динамические сервисы на основе сетей между людьми, процессами, услугами и вещами.

8. Механика приложений и сервисов — синхронизация устройств и технологий по принципу «умного дома».

9. Цифровые технологические платформы — новые платформы, сочетающие информационные системы, опыт работы с клиентами, аналитику и прогнозирование, интернет вещей и деловые экосистемы.

10. Адаптивная архитектура безопасности — многоуровневая система информационной безопасности реального времени, в том числе на основе блокчейн-технологии.

С учетом перечисленного выше предлагаемое авторами в данной статье устройство позволит повысить уровень безопасности реализации технических решений практически по всем указанным трендам.

Анализ особенностей реализации технологий в указанных областях, а также рисков их использования не является предметом исследования данной статьи.

3. Требования безопасности для необходимого качества сервисов

Информационные технологии (в том числе с использованием беспроводных сегментов сетей) приобретают все большее значение. Поэтому вопрос надежного безопасного функционирования является очень актуальным. Слабозащищенные беспроводные каналы открывают практически неограниченный доступ к ресурсам сети любым злоумышленникам, что представляет большую опасность для граждан, бизнеса и государства и, как следствие, вызывает опасение относительно целостности и надежности хранения информации (особенно персональной) и недоверие к предоставляемым сервисам. Обеспечение сетевой безопасности, что является определяющим элементом планирования и использования корпоративной сети (особенно с беспроводными сегментами), включает

— схемы идентификации и работу с различными типами носителей ключей;

— использование различных криптографических алгоритмов и протоколов;

— интеграцию криптографических средств в современные устройства и их использование в различных сервисах.

В связи с развитием технологий в настоящее время существуют различные подходы и направления реализации: блокчейн; веб-сервисы с доступом с различных персональных устройств и защитой транзакций и электронных документов; идентификатор объекта (OID, Object identifier) для построения структурированного эффективного управления ИТС; интероперабельность в функционировании сервисов, систем идентификации; криптографические алгоритмы и протоколы и др.

Техническое направление обеспечения безопасности включает следующее [13]:

— определение мер безопасности и контроля технического обслуживания механизмов обеспечения безопасности и средств защиты;

— реализацию разрешительной системы допуска персонала к выполнению работ, документам и информации;

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

— учет информационных ресурсов, регистрация действий пользователей и персонала, контроль над несанкционированным доступом, действиями пользователей, персонала и сторонних лиц;

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

— применение криптографической защиты информации (КЗИ) для защиты данных;

— надежное хранение и оборот носителей информации, ключей (ключевой документации);

— резервирование технических средств, баз данных и носителей информации;

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

— систематическое обновление технических и программных средств защиты от НСД, программ-вирусов и программных закладок.

Если взять за основу изложенное выше, необходимое качество обслуживания способно гарантировать соблюдение следующих требований [14]:

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

— стойкость криптографической системы (выбор оптимального алгоритма);

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

— случайность генерации ключей и вектора инициализации.

Следует также учесть, что система электронного правительства неизбежно объединит программно-аппаратные комплексы и средства разных производителей. Поэтому дополнительным требованием к системе безопасности является интеграция и унификация применяемых технических решений, совместимость используемых криптографических средств и обеспечение непрерывности защиты.

4. Средства для повышения безопасности функционирования телекоммуникационной инфраструктуры

В рамках е-правительства для повышения качества обслуживания (сервисов) при одновременном ужесточении требований безопасности функционирования его телекоммуникационной инфраструктуры необходимы программные и программно-аппаратные компоненты информационных систем, унифицированные для различных технологий (сервисов) и обеспечивающие интероперабельность. Для Украины, где используют преимущественно зарубежные программные и аппаратные решения, не менее важна их надлежащая адаптация к национальным требованиям. Это касается программных и программно-аппаратных компонентов информационных систем как государственного управления, так и различных видов бизнеса, в первую очередь, связанных с финансами [9].

Для применения криптографических средств в различных сервисах и информационно-телекоммуникационных архитектурах требуются технические решения, обеспечивающие выполнение основных принципов цифровизации, сформулированных в Концепции развития цифровой экономики Украины на 2018–2020 гг. [1], таких как интеграция в европейские и глобальные системы и инфраструктуры для эффективного использования информационно-коммуникационных и цифровых технологий (принцип 5), обеспечение высокого уровня стандартизации сервисов, поддерживающих безопасность технических решений (принцип 6), повышение уровня доверия и безопасности (принцип 7). Другими словами, технические решения в области безопасности и использования криптографии должны быть унифицированы для их эффективного применения в различных технологиях, сервисах и программно-аппаратных решениях и обеспечивать интероперабельность.

Чтобы обеспечить безопасность функционирования сети и размещенных на ее базе сервисов, необходимо реализовать функцию управления защитой информации, позволяющую поддерживать средства обработки информации и компьютерные сети в безопасном работоспособном состоянии, обеспечивая требуемое качество обслуживания. Для решения этой задачи разработано устройство [15], суть которого заключается в возможности применения любых криптографических алгоритмов на базе математических примитивов или математики конечных полей (Finite Field Arithmetic) [16], реализованных производителем в конкретном устройстве и предназначенных для использования других криптографических алгоритмов без внесения изменений в программное обеспечение производителя. Тип и разрядность процессора не играют существенной роли, важен лишь перечень заложенных в устройство математических примитивов, на базе которых и могут быть реализованы криптографические алгоритмы.

Предложенное устройство может использоваться для выполнения криптографических алгоритмов в дополнение к встроенным производителем на стадии производства, для реализации различных криптографических функций: цифровой подписи, аутентификации, хеш-функций, генерации ключей, шифрования и т.п. Это осуществляется путем непосредственного прямого взаимодействия между модулем внутренних программных приложений (internal application) для реализации новых криптографических алгоритмов и блоком математических примитивов, расположенных в существующем модуле криптографических меха-

низмов (например, арифметико-логическом устройстве (ALU, Arithmetic and logic unit)). Для этого в устройство добавлен модуль интерфейса взаимодействия с блоком математических примитивов. Этот модуль встраивается в устройство КЗИ, например смарт-карту, производителем на стадии производства или с помощью специализированного инструментария производителя уже на стадии инициализации. Также он может добавляться в устройство КЗИ (например, HSM, Host security module) разработчиком на базе интерфейса прикладного программирования (API, Application programming interfaces) производителя.

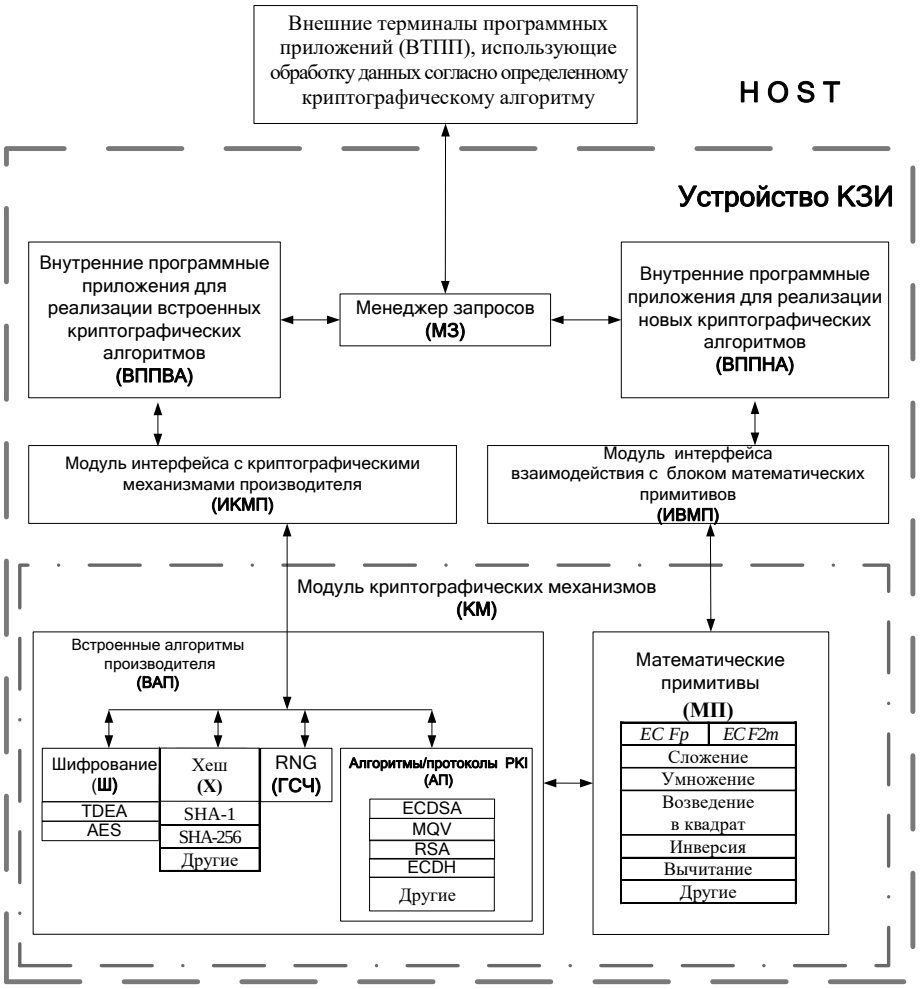
Следует отметить, что в разработанном устройстве, кроме встроенных криптографических алгоритмов, можно выбрать новый алгоритм и передать данные на выполнение операций с криптографическими примитивами в блок математических примитивов, который позволяет применять устройство КЗИ для реализации новых криптографических алгоритмов. Модуль интерфейса взаимодействия с блоком математических примитивов реализуется на базе набора средств для разработки программного обеспечения (SDK, Software development kit) или API производителя. При этом разрядность и тип процессора устройства КЗИ неважны.

Устройство содержит модуль внутренних программных приложений для реализации встроенных криптографических алгоритмов (ВППВА), менеджер запросов (МЗ), модуль внутренних программных приложений для реализации новых криптографических алгоритмов (ВППНА), модуль интерфейса с криптографическими механизмами производителя (ИКМП), модуль интерфейса взаимодействия с блоком математических примитивов (ИВМП), модуль криптографических механизмов (КМ), который обычно реализуется в составе блока встроенных алгоритмов производителя (ВАП), блока шифрования (Ш), блока хеш-функций (Х), блока генератора случайных чисел (ГСЧ) RNG (Random number generator), блока алгоритмов/протоколов (АП) инфраструктуры открытых ключей (PKI, Public key infrastructure) и блока математических примитивов (МП).

Состав модуля криптографических механизмов (КМ) может варьироваться в зависимости от функционала устройства КЗИ, заложенного непосредственно производителем в конкретное устройство для реализации определенных криптографических алгоритмов. Распределение на блоки является логическим, но может быть и физическим (например, разные процессоры, сопроцессоры и т.п.).

На рисунке приведена структурная блок-схема устройства КЗИ для реализации криптографических алгоритмов с использованием математических примитивов.

Принцип работы устройства следующий. Блок внешних терминалов программных приложений, осуществляющий обработку данных по определенному криптографическому алгоритму (ВТПП), передает запрос на обработку данных в устройстве КЗИ менеджеру запросов (МЗ), который распознает запрос на операцию с данными по определенному криптографическому алгоритму и посылает команду на выполнение встроенного алгоритма в модуль ВППВА или нового алгоритма — в модуль ВППНА. При необходимости выполнения операций со встроенными алгоритмами модуль ВППВА взаимодействует с модулем КМ с помощью модуля ИКМП. Модуль КМ содержит блок встроенных алгоритмов производителя ВАП с соответствующими блоками криптографических функций и протоколов: шифрование, хеш-функций, ГСЧ и алгоритмов/протоколов PKI. Выполнение встроенного алгоритма обработки данных блоками криптографических функций осуществляется с помощью блока МП. В случае запроса от блока ВТПП на выполнение нового криптографического алгоритма модуль ВППНА, который содержит реализацию этого нового алгоритма, непосредственно взаимодействует с блоком МП с помощью модуля ИВМП. После криптографических операций с использованием модуля ИКМП или ИВМП результат выполнения операции возвращается в блок ВТПП.



Указанная архитектура технического решения позволяет унифицировать применение различных криптографических алгоритмов как для программных систем/сервисов в операционных системах разных производителей (включая средства безопасности в персональных компьютерах или смартфонах), так и для специализированных аппаратных решений. Такие решения применяются в ИТС электронного правительства, а также финансовых организаций и предназначены для хранения массивов ключей, автоматизированной обработки информации, содержащей подписи данных либо документов, созданных на разных международных или национальных алгоритмах, например RSA, ECDSA, AES, ДСТУ 4145, ГОСТ 34.10, ГОСТ 28147 и др. Такое устройство также позволяет работать с разными алгоритмами шифрования: либо встроенными «по умолчанию», либо предназначенными для реализации локальных национальных политик защиты конфиденциальности/секретности информации при обмене данными.

Предложенное устройство может использоваться как криптографический хост в локальных системах электронного документооборота, обработки финансовых транзакций, а также в корпоративных и глобальных системах, например в системе взаимодействия государственных информационных ресурсов «Трембита».

Необходимо отметить, что такая архитектура позволяет относительно просто подключать новые алгоритмы, расширяя функциональность аппаратных устройств и технических решений для взаимодействия с сервисами разных стран, например криптографическими решениями стран, использующих собственные стандарты криптографической обработки для сервисов государственных услуг, защиты персональных или иных чувствительных данных. При этом данное устройство одновременно с программным средством в виде криптографического сервис-провайдера по предложенному способу применения криптографических алгоритмов в средствах защиты информации [6] обеспечивает значительно более высокий уровень эффективности, интероперабельности и безопасности для информационных систем в целом (по сравнению с большинством действующих систем) за счет интеграции обработки информации и прозрачного взаимодействия разных криптографических сред в одном программно-аппаратном средстве, без построения отдельных комплексов обработки для использования разных криптографических алгоритмов обработки информации.

Предлагаемое устройство успешно реализовано для операционных сред Windows (на ПК) [6], а также на современной модели HSM SafeNet типа Luna и ряде чиповых карт и токенов.

Заключение

1. Система электронного правительства является базовым элементом эффективного и результативного взаимодействия власти, бизнеса и гражданского общества. Однако его создание в Украине обуславливает необходимость существенного повышения качества обслуживания (сервисов) при соблюдении требований безопасности функционирования телекоммуникационной инфраструктуры.

2. Ключевыми понятиями качества обслуживания (сервисов) с точки зрения безопасного функционирования информационно-телекоммуникационной инфраструктуры, в том числе электронного правительства, являются целостность, доступность, безопасность и конфиденциальность информации. При этом используемые для обслуживания средства должны обеспечивать надежную и безопасную работу не только на современном этапе, но и по мере развития Индустрии 4.0.

3. Для обеспечения требуемого качества обслуживания следует гарантировать физическую защищенность, стойкость криптографической системы, достаточную мощность двусторонней аутентификации, случайность генерации ключей и вектора инициализации. При этом должны применяться надежные и, по возможности, универсальные программные и аппаратные средства, позволяющие успешно реализовать функцию управления защитой информации.

4. Безопасность функционирования информационно-телекоммуникационной инфраструктуры для поддержания требуемого уровня качества обслуживания пользователей, а также интероперабельность для схем идентификации и обработки электронных документов в бизнес-приложениях можно повысить, используя разработанное техническое решение. Его высокие эксплуатационные характеристики обеспечены благодаря интегрированной обработке информации и прозрачному взаимодействию разных криптографических сред в одном программно-аппаратном средстве.

5. Разработка успешно реализована как самостоятельное средство криптографической защиты и может быть использована как составная часть систем защищенного электронного документооборота с использованием смарт-карт, криптотокенов, криптокарт SIM и других модулей безопасности, обеспечивающих универсальность и интероперабельность при взаимодействии разнородных информационно-телекоммуникационных систем.

О.О. Зубарева, Г.Л. Рябцев, І.В. Басанцов, С.В. Бєлов

ПІДВИЩЕННЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУ УКРАЇНИ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ ЕКОНОМІКИ

Створення системи електронного уряду України обумовлює необхідність істотного підвищення якості обслуговування (сервісів) з одночасним дотриманням вимог безпеки функціонування телекомунікаційної інфраструктури. Дотепер, на думку авторів статті, не вирішено в повному обсязі питання забезпечення конфіденційності персональних даних, захисту інформації, довіри до неї і самих систем, а також підтримки правового статусу інформації. Особливо важливими вбачаються проектування і впровадження засобів та методів захисту інформації, які забезпечують ефективну й прозору взаємодію різних систем. Із метою розробки рішення, яке дозволяє підвищити безпеку інформаційно-телекомунікаційної інфраструктури електронного уряду та забезпечити необхідний рівень якості, визначено ключові поняття якості обслуговування (сервісів) — цілісність, доступність, безпека й конфіденційність інформації. Автори підкреслюють, що засоби, які використовуватимуться, повинні забезпечити надійну та безпечну роботу не тільки на етапі формування електронного уряду, але й з подальшим розвитком Індустрії 4.0. Сформульовано вимоги безпеки для забезпечення необхідної якості обслуговування. Для цього необхідно гарантувати фізичну захищеність, стійкість криптографічної системи, достатню потужність двосторонньої автентифікації, випадковість генерації ключів та вектора ініціалізації. Розроблено технічне рішення, яке підвищує безпеку функціонування телекомунікаційної інфраструктури. Його високі експлуатаційні характеристики забезпечено завдяки інтегрованій обробці інформації та прозорій взаємодії різних криптографічних середовищ в одному програмно-апаратному засобі. Розробка успішно реалізована як самостійний засіб криптографічного захисту і може бути використана як складова частина у системі електронного уряду України.

Ключові слова: діджиталізація, цифрова економіка, електронний уряд, інформаційна безпека, якість обслуговування, криптографічний захист інформації.

E.A. Zubareva, G.L. Riabtsev, I.V. Basantsov, S.V. Byelov

INCREASING SAFETY FUNCTIONING OF E-GOVERNMENT OF UKRAINE DURING DIGITALIZATION OF ECONOMY

The creation of Ukrainian e-government system necessitates a substantial improvement in the quality of services while observing the safety requirements of the telecommunications infrastructure. Until now, according to the article authors, the ensuring questions of personal data confidentiality, protecting information, ensuring confidence to it and the systems themselves, as well as maintaining the legal status of information, have not been fully resolved. Of particular importance are the design and implementation of information protection tools and methods that ensure the effective and transparent interaction of various systems. In order to develop a solution to improve the security of information and telecommunications infrastructure of e-government system and ensure the required level of quality, the authors determined key concepts the quality of service. They are integrity, availability, security and confidentiality of information. The authors emphasize that the tools used should ensure safe and secure operation not only at the stage of e-government formation, but also as Industry 4.0 develops. Security requirements are formulated to provide the required quality of service. For this purpose it is necessary to guarantee physical security, strength of cryptographic system, sufficient power of two-way authentication, randomness of key generation and initialization vector. The authors have developed a technical solution that increases the safety of the telecommunications infrastructure. Its high operational characteristics are provided thanks to the integrated information processing and transparent interaction of different cryptographic environments in one

hardware and software tool. The development is successfully implemented as an independent means of cryptographic protection and can be used as an integral part of the e-government system of Ukraine.

Keywords: digitalization, digital economy, electronic government (e-government), information security, quality of service, cryptography protection of the information

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. http://zakon.rada.gov.ua/laws/show/67-2018-р
2. Басанцов І.В. Корупція в Україні: сучасні реалії та ефективні засоби протидії: монографія. Суми : СумДУ, 2016. 113 с.
3. Про організацію робіт щодо створення Єдиної інформаційно-комунікаційної платформи органів державної влади: Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 04 жовтня 2012 р. № 501. http://www.krz.gov.ua/uk/activities_nkrzi/ruling2012/1349437554/
4. Про схвалення Концепції Єдиної інформаційно-комунікаційної платформи: Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 24 січня 2013 р. № 34. http://www.nkrz.gov.ua/uk/activities_nkrzi/ruling2013/1359114941/
5. Про схвалення Концепції розвитку системи електронних послуг в Україні: Розпорядження Кабінету Міністрів України від 16 листопада 2016 р. № 918-р. https://www.kmu.gov.ua/ua/npas/249570503
6. Зубарева Е.А., Белов С.В. Система электронного правительства Украины и способ повышения безопасности ее функционирования. *Кибернетика и системный анализ*. 2015. **51**, № 3. С. 178–187. DOI 10/1007/s10559-015-9739-4
7. 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.
8. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. М. : Вильямс, 2003. 1104 с.
9. Зубарева О.О. Методи та засоби забезпечення завадостійкості і безпеки функціонування мереж технології WiMAX : дис. … канд. техн. наук: 05.13.05. К. : Нац. авіац. ун-т, 2013. 173 с.
10. 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. **2(24)**. С. 114–122.
11. Анкудинов Г.И., Стрижаченко А.И. Сети ЭВМ и телекоммуникации. Архитектура и протоколы. СПб : СЗТУ, 2001. 92 с.
12. Top 10 Strategic Technology Trends for 2017. *Gartner*. 14.10.2016. ID: G00317560
13. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения: ГОСТ Р 53110-2008. Введ. 2009-10-01. М. : Ростехрегулирование, 2009. 22 с.
14. Берлин А.Н. Цифровые сотовые системы связи. М. : Эко-Трендз, 2007. 296 с.
15. Патент на корисну модель 67369 Україна, МПК(2006.01) H04L 9/14. Пристрій криптографічного захисту інформації для реалізації криптографічних алгоритмів з використанням математичних примітивів. Заявники та патентовласники С.В. Мартиненко, С.В. Бєлов, О.О. Зубарева та ін. № u201115298; заявл. 23.12.2011; опубл. 10.02.2012, Бюл. № 3.
16. Воройский Ф.С. Информатика. Энциклопедический словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. М. : ФИЗМАТЛИТ, 2006. 768 с.

Получено 17.04.2019