Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

сигналов для целей защищенного информационного обмена [4]. Среди основных недостатков представленной модели следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами, так же как это требуется для современных систем передачи информации [4].

Одной из особенностей описываемой схемы приемо-передающей части УИКО является возможность использования широкого класса ХС, записанных в перезаписываемые накопители хаотических последовательностей. Данный факт позволяет значительно повысить защищенность радиоканала от комплексных угроз (просмотр, подмена, перехват, радиоэлектронное подавление).

Список литературы

1. Иванюк П.В., Политанский Л.Ф., Политанский Р.Л., Элияшив О.М. Хаотическое маскирование информационных сигналов с использованием генератора на базе системы Лю // Технология и конструирование в электронной аппаратуре. 2012. № 3. С. 11-17.

2. Осипов Д.Л., Жук А.П., Гавришев А.А. Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Патент РФ № 2560824. 2015. Бюл. № 23. 15 с.

3. Жук А.П., Гавришев А.А., Осипов Д.Л. К вопросу о разработке защищенного устройства управления робототехническим комплексом посредством беспроводного канала связи // T-Comm: Телекоммуникации и транспорт. 2016. Т.10. № 12. С. 4-9.

4. Гавришев А.А., Жук А.П. Моделирование устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Прикладная информатика. 2017. Т. 12. № 1(67). С. 68-78.

ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕЛОРУССКОЙ ЭЛЕКТРОННОЙ КАРТЫ

В.В. КОЗЛОВСКИЙ

ООО «Лайт Вел Организейшн»

Мировой опыт свидетельствует о широком использовании различных современных технологий оказания электронных услуг с помощью интегрированных систем на основе внедрения разного рода многофункциональных электронных карточек, включающих несколько приложений: идентификационное (идентификация личности, замена паспорта), электронно-цифровая подпись, платежное (банковская карточка для расчета за товары и услуги или снятия наличных), транспортное (для оплаты проезда), получение льгот и скидок и другие.

В настоящее время в Республике Беларусь отсутствует единая система, которая бы носила ярко выраженный интеграционный характер и обеспечивала бы работу множества разнородных государственных информационных систем с использованием единой электронной карточки. Например, отсутствует единая система идентификации и аутентификации пользователей при взаимодействии с государственными информационными ресурсами, а также не созданы инфраструктуры открытых ключей, функционирующие в рамках Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и обеспечивающие использование сертификатов открытых ключей пользователей.

Разработка основ создания Белорусской интегрированной сервисно-расчетной системы (БИСРС) проводится в соответствии с Указом Президента Республики Беларусь от 08.11.2011 № 515 «О некоторых вопросах развития информационного общества в Рес-

публике Беларусь», постановлением Совета Министров Республики Беларусь от 28 марта 2011 г. № 384 «Об утверждении Национальной программы ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011-2015 годы», а также Планом мер по организации работ, направленных на создание и внедрение Белорусской интегрированной сервисно-расчетной системы, утвержденным заместителем Премьер-министра Республики Беларусь Румасом С.Н. 21 января 2012 г. № 30/225-2230.

БИСРС – интегрированная информационная система, объединяющая разнородные автоматизированные системы посредством использования единого инструмента для получения электронных информационных и платежных услуг на всей территории Республики Беларусь на основе единых правил. В результате внедрения БИСРС должны повыситься прозрачность осуществляемых социальных трансфертов и произойти сокращение расходов на организацию взаимодействия ведомственных и межведомственных систем электронного взаимодействия.

Базовыми компонентами БИСРС являются:

Единая система идентификации физических и юридических лиц (далее – ЕС ИФЮЛ);

Белорусская электронная карточка (далее – БЭК).

Большинство стран реализуют проекты использования различных электронных идентификационных карточек, используемых в отдельных областях взаимодействия государства с гражданами, бизнесом и собственно государственными служащими. Наибольшее распространение получила универсальная карточка, представляющая собой многофункциональную микропроцессорную именную пластиковую карточку с защищенной операционной системой. Данная карточка является материальным носителем персональных данных держателя карточки и поддерживает приложения, связанные с предоставлением и учетом мер социальной поддержки и других информационных сервисов, и услуг. Предполагается, что в Беларуси такой карточкой будет Белорусская электронная карточка (БЭК).

Основные области применения унифицированных платежных карточек:

банковские услуги, взаимодействие граждан с «электронным правительством»;

санкционированный доступ к информационным ресурсам;

налогообложение граждан;

гражданское страхование; использование в системах контроля доступа;

электронная торговля (оплата услуг через Интернет), оплата за товары и услуги в торговых точках, проезда в общественном транспорте, коммунальных платежей и др.

Основными сторонами, заинтересованными в создании БИСРС, являются:

граждане, использующие БЭК для получения услуг;

юридические лица, использующие БЭК для получения услуг;

органы исполнительной власти и другие организации, предоставляющие государственные услуги (ведомства);

субъекты Республики Беларусь;

банки;

поставщики коммерческих сервисов (сервис-провайдеры);

поставщики коммунальных услуг;

объекты торговли и сервиса, реализующие социальные товары/услуги;

операторы сотовой подвижной электросвязи.

Интересы граждан в создании БИСРС.

Заинтересованность граждан в создании БИСРС определяется следующими их потребностями:

сокращение времени получения коммерческих и государственных услуг;

минимизация личных контактов с ведомствами, обеспечивающими предоставление государственных услуг;

повышение доступности коммерческих и государственных услуг;

повышение качества предоставления коммерческих и государственных услуг;

расширение перечня доступных в электронном виде коммерческих, государственных и иных услуг.

Граждане являются основным потребителем услуг БИСРС. Оценка качества услуг со стороны граждан полностью определит коммерческую успешность проекта.

Интересы Правительства в создании БИСРС.

Правительство РБ рассчитывает, что БИСРС станет важной частью общегосударственной системы, обеспечивающей предоставление гражданам государственных услуг в электронной форме, и позволит:

упростить доступ граждан к государственным услугам, сделать их взаимодействие с «государством» простым, быстрым, удобным и выгодным;

обеспечить выполнение органами исполнительной власти требований постановления Совета Министров Республики Беларусь «Об оказании электронных услуг и реализации государственных функций в электронном виде посредством общегосударственной автоматизированной информационной системы» от 09.08.2011 № 1074, связанных с переводом государственных услуг в электронную форму;

повысить управляемость и эффективность деятельности местных органов исполнительной власти, государственных внебюджетных фондов, а также органов местного самоуправления, связанной с предоставлением гражданам государственных услуг;

усилить контроль над деятельностью органов, предоставляющих государственные услуги, со стороны Правительства РБ с целью снижения потерь от нецелевого использования бюджетных средств и ошибок в сфере предоставления государственных услуг;

повысить точность планирования расходных статей бюджетов республиканских и местных органов исполнительной власти, направленных на финансирование деятельности, связанной с предоставлением государственных услуг.

Единая информационная среда государственных органов должна обеспечить эффективную коммуникацию на следующих направлениях:

межведомственное – взаимодействие между государственными органами одного юридического статуса и одного уровня;

межрегиональное – взаимодействие между региональными органами государственной власти;

межуровневое – взаимодействие между центральными и региональными органами власти;

взаимодействие между государством и гражданским обществом.

Взаимосвязь государственных информационных систем и БИСРС

Инфраструктура, создаваемая в рамках проекта БИСРС, выполняет функцию, с одной стороны, по удобной и безопасной доставке услуг различных поставщиков гражданам, а с другой стороны, позволяет гражданину надежно идентифицироваться перед поставщиком услуги и оплатить ее без личной явки.

Таким образом, инфраструктура БИСРС должна взаимодействовать как минимум с:

поставщиками государственных услуг (любого уровня);

поставщиками коммерческих услуг;

поставщиками финансовых услуг (банки);

поставщиками иных услуг.

В качестве поставщика государственных услуг выступают соответствующие органы исполнительной власти, с каждым из которых заключается соглашение об условиях и порядке оказания услуг в электронном виде.

Все государственные услуги планируется предоставлять в рамках общегосударственной автоматизированной информационной системы (ОАИС). ОАИС не является

частью инфраструктуры БИСРС, а является единой точкой подключения инфраструктуры доставки услуг БИСРС и инфраструктуры электронного правительства, реализующей услуги в электронном виде.

Таким образом, для того, чтобы конкретная государственная услуга могла быть доставлена гражданину с использованием БЭК, соответствующий государственных орган или государственная организация должны реализовать электронную услугу посредством ОАИС.

После этого, на основании единого подключения инфраструктуры БИСРС и оператора ОАИС, инфраструктура БИСРС сможет через ОАИС обеспечить идентифицированный запрос гражданина на получение государственной услуги в ОАИС и, при необходимости, подтверждение оплаты.

Интересы органов, предоставляющих государственные услуги, в БИСРС

Реализация проекта создания БИСРС позволит органам, предоставляющим государственные услуги, удовлетворить следующие свои потребности:

обеспечить выполнение требований Постановления Совета Министров Республики Беларусь «Об оказании электронных услуг и реализации государственных функций в электронном виде посредством общегосударственной автоматизированной информационной системы», связанные с переводом государственных услуг в электронную форму;

снизить затраты, связанные с обслуживанием граждан в своих подразделениях при предоставлении государственных услуг, и повысить эффективность процесса предоставления этих услуг;

получить доступ к унифицированной инфраструктуре государственного масштаба, отвечающей требованиям безопасности и юридически полноценно идентифицирующей гражданина при его обращении за услугами.

Соблюдение интересов органов власти, предоставляющих услуги в БИСРС, необходимо для формирования полного спектра услуг, предоставляемых гражданам и юридическим лицам в электронном виде. Игнорирование этих интересов может привести к исключению востребованных услуг из инфраструктуры БИСРС, а, следовательно, ухудшению потребительских свойств смарт-карточек, как продукта.

Интересы банков в БИСРС

Банки с созданием БИСРС рассчитывают:

использовать идентификационное приложение и ЭЦП для расширения дистанционного банковского обслуживания (дистанционное кредитование, привлечение денежных средств во вклады и др.);

повысить эффективность использования банковской инфраструктуры обслуживания клиентов за счет расширения ее функций с целью предоставления гражданам возможности оплачивать государственные и другие услуги;

предоставление дополнительных сервисов, связанных с предоставлением государственных услуг в электронном виде.

Интересы поставщиков коммерческих сервисов в БИСРС

Поставщики коммерческих услуг рассчитывают:

открыть путь своим продуктам и услугам на широкий потребительский рынок;

повысить удобство, безопасность, комплексность своих существующих услуг за счет использования уникальных потребительских свойств инфраструктуры смарт-карточек.

Учет интересов поставщиков коммерческих сервисов позволит сформировать для гражданина широкий спектр услуг, предоставляемых в электронном виде и обеспечить высокую интенсивность использования карточек в различных жизненных ситуациях.

Широта спектра оказываемых услуг, удобство, безопасность и высокая интенсивность использования карточек помогут обеспечить достижение коммерческих целей БИСРС.

Интересы операторов сотовой подвижной электросвязи

Мобильные операторы сотовой подвижной электросвязи в рамках БИСРС обеспечат доступ к государственным услугам с помощью мобильных устройств, имеющих доступ к сети Интернет.

Целесообразность создания БИСРС

Целесообразность внедрения и развития проекта БИСРС обусловлено наличием ряда веских причин.

Во-первых, формирование базовых компонентов БИСРС способствует развитию национальной информационной инфраструктуры Республики Беларусь, что является основополагающим условием для создания рынка информации и «экономики знаний».

Во-вторых, информационно-коммуникационные технологии имеют перспективный резерв для дальнейшей модернизации своей инфраструктуры. Реализация проекта БИСРС позволит упростить функциональное и институциональное совершенствование механизмов государственного управления.

В-третьих, реализация БИСРС приведет к формированию единой транспортной среды, что консолидирует имеющиеся информационные системы государственных органов. На современном этапе большинство информационных сетей государственных органов остаются изолированными, что создает дополнительные проблемы и расходы. Создание единой коммуникационной инфраструктуры позволит внедрить стандарты обмена информацией и унифицированные подходы в политике безопасности информационных ресурсов государственных органов.

В-четвертых, проект БИСРС оптимизирует взаимодействие государства с гражданским обществом и бизнесом. Внедрение информационно-коммуникационных технологий минимизирует непосредственный контакт государственных служащих с гражданами и организациями. Это в свою очередь нивелирует возможность возникновения административного коррупционного поля и противоправных действий с обеих сторон. Вместе с тем, БИСРС стимулирует повышение качества и скорости административных процедур, иными словами усиливает эффективность услуг, предоставляемых государственными органами.

Тем самым, все вышеперечисленное свидетельствует о целесообразности и необходимости активного внедрения информационно-коммуникационных технологий при модернизации системы государственного управления, результатом чего станет формирование нового «электронного» пространства функционирования власти.

Необходимым условием для успешного функционирования БИСРС является массовая автоматизация и создание участниками БИСРС (государственными органами и ведомствами, коммерческими организациями) информационных систем для оказания услуг в электронном виде. В свою очередь, создание массовой электронной идентификационной карточки упростит процессы автоматизации и разработки информационных систем, требующих идентификации пользователей.

Список литературы

1. Указ Президента Республики Беларусь от 08.11.2011 № 515 (ред. от 15.03.2016) «О некоторых вопросах развития информационного общества в Республике Беларусь», Национальный реестр правовых актов Республики Беларусь, 14.11.2011, № 125, 1/13064.

2. Постановление Совета Министров Республики Беларусь от 28.03.2011 № 384 «Об утверждении национальной программы ускоренного развития услуг в сфере информационно-

коммуникационных технологий на 2011 - 2015 годы», Национальный реестр правовых актов Республики Беларусь, 30.03.2011, № 5/33546.

3. Постановление Совета Министров Республики Беларусь от 09.08.2011 № 1074 «Об оказании электронных услуг и реализации государственных функций в электронном виде посредством общегосударственной автоматизированной информационной системы», Национальный реестр правовых актов Республики Беларусь, 11.08.2011, № 5/34288.

О ПОДХОДАХ К ОЦЕНКЕ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ БЛОКЧЕЙН

С.Е. КУЗНЕЦОВ, С.В. МАТВЕЕВ

Пензенский филиал Федерального государственного унитарного предприятия «Научно-технический центр «Атлас»

В настоящее время большое внимание уделяется технологии цепной записи данных и распределенных реестров (блокчейн). Технология цепной записи данных и распределенных реестров, и связанные с ней практические реализации, позиционируются как решения, построенные с использованием криптографии и поэтому безопасные. Исходя из этого, возникает ряд вопросов, связанных с оценкой криптографических качеств технологии блокчейн и оценкой информационной безопасности, используемых в данной сфере решений.

Рассматривая технологию блокчейн, с точки зрения обеспечения безопасности, можно выделить следующие уровни:

пользовательский уровень (или уровень приложений),

уровень сетевого взаимодействия,

уровень консенсуса.

На пользовательском уровне подготавливаются данные для включения в распределенный реестр, формируются запросы на чтение и запись к реестру, организуется взаимодействие между отдельными пользователями, осуществляется управление персональными секретными данными, реализуются меры по обеспечению их безопасности.

Криптографической составляющей процесса взаимодействия пользователя с реестром и другими пользователями являются (от примитивов к протоколам):

функции хеширования, использующиеся в схеме ЭЦП, при формировании адреса пользователей, формировании ключевого дерева, формировании ключа из пароля,

схема ЭЦП, может использоваться для контроля целостности, аутентификации отправителя и получателя,

протоколы обмена данными между пользователем и реестром, и между несколькими пользователями.

Уровень сетевого взаимодействия определяет алгоритмы взаимодействия между узлами сети и распространения сообщений между ними. Изначально на данном уровне не предполагали использование криптографических алгоритмов. Однако тенденция развития технологии распределенных реестров ведет к необходимости использования при межсетевом взаимодействии (peer-to-peer communication) криптографических протоколов, обеспечивающих, как минимум, аутентификацию узлов сети, а желательно, и конфиденциальность передаваемой информации.

Уровень консенсуса определяет способы предоставления данных для хранения в распределенном реестре, алгоритмы верификации данных, их записи, чтения и моди-