ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

**Информационная технология.
Требования к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы**

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр развития и внедрения компьютерных и информационных технологий «UZINFOCOM» (ГУП Центр «UZINFOCOM»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи и информатизации № 7

3 УТВЕРЖДЕН постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 03.01.2013 № 05-422

4 ВВЕДЕН ВПЕРВЫЕ

5 В настоящем государственном стандарте реализованы нормы Закона Республики Узбекистан «Об информатизации»

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт»

Исключительное право официального опубликования настоящего государственного стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Содержание

1 Область применения..... 1
2 Нормативные ссылки..... 1
3 Термины, определения и сокращения..... 3
4 Общие требования к информационным системам в рамках Национальной информационной системы..... 5
5 Требования к организации интеграции информационных систем..... 6
6 Требования к аппаратному комплексу интегрируемых информационных систем..... 9
7 Требования к межсетевому взаимодействию между информационными системами..... 10
8 Требования к программному обеспечению интегрируемых информационных систем..... 10
9 Требования к обеспечению информационной безопасности при интеграции информационных систем..... 12
Библиография..... 14

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Ахборот технологияси
Миллий ахборот тизимини шакллантириш доирасида давлат органлари томонидан фойдаланиладиган ахборот тизимлари интегрциясига ва ўзаро фаолиятига кўйиладиган талаблар

Информационная технология
Требования к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы

Information technology
Requirements to integration and interaction
of the government organizations information systems,
implemented in formation of the National information system

Дата введения с 01.01.2013 г
до 01.01.2018 г

1 Область применения

Настоящий стандарт устанавливает организационные и технические требования, включающие требования к сетевому подключению, программной части и информационной безопасности интегрируемых информационных систем государственных органов в рамках формирования Национальной информационной системы (далее - НИС).

Требования государственного стандарта обязательны для соблюдения государственными органами, выполняющими интеграцию собственных информационных систем, а также создающих новые информационные системы в рамках формирования НИС.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 12.2.003-91 Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности

ГОСТ 12.2.007.0-75 Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности

O'ZSTANDART AGENTLIGI
3259 son bilan
«03» 01 2013 yilda
Davlat ro'yxatiga olindi

ГОСТ 12.2.061-81 Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности к рабочим местам

ГОСТ 34.321-96 Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными

O‘z DSt 1047:2003 Информационные технологии. Термины и определения

O‘z DSt 1092:2009 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

O‘z DSt 1105:2009 Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных

O‘z DSt 1106:2009 Информационная технология. Криптографическая защита информации. Функция хэширования

O‘z DSt 1109:2006 Информационная технология. Криптографическая защита информации. Термины и определения

O‘z DSt 1135:2007 Информационная технология. Требования к базам данных и обмену информацией между органами государственного управления и государственной власти на местах

O‘z DSt 1204:2009 Информационная технология. Криптографическая защита информации. Требования безопасности к криптографическим модулям

O‘z DSt ISO/IEC 2382-8:2007 Информационные технологии. Информационная безопасность. Термины и определения

O‘z DSt ISO/IEC 13335-1:2009 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. Часть 1. Концепции и модели управления безопасностью информационно-коммуникационных технологий

O‘z DSt ISO/IEC 15408-1:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

O‘z DSt ISO/IEC 15408-2:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

O‘z DSt ISO/IEC 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

O‘z DSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности системы управления информационной безопасностью. Требования

O‘z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

O‘ZBEKISTON RESPUBLIKASI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Примечание – При пользовании настоящим стандартом необходимо проверить действие ссылочных стандартов по указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по O‘z DSt 1047, O‘z DSt 1109, O‘z DSt ISO/IEC 2382-8, а также следующие термины с соответствующими определениями:

3.1.1 **веб-сервис**: Регламентированный вид обслуживания, предоставляемый через Национальную информационную систему потребителю электронного сервиса.

3.1.2 **информационное взаимодействие**: Обмен между участниками электронного документооборота документами заданного вида и по сценариям взаимодействия.

3.1.3 **информационная система**: Организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией.

Примечание – Под «информационной системой» также понимают организационно упорядоченную совокупность средств, реализующих определенные технологические действия посредством информационных процессов, предназначенных для решения конкретных функциональных задач.

3.1.4 **Национальная информационная система**: Совокупность систем, включающая информационные системы государственных органов, отраслевые и территориальные информационные системы, а также информационные системы юридических и физических лиц.

3.1.5 **обеспечение информационной безопасности**: Система мер правового организационно-технического и организационно - экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

3.1.6 **электронное сообщение**: Электронное сообщение Национальной информационной системы определенного формата и структуры, с помощью которого организуется функционирование Национальной информационной системы.

3.1.7 **SOAP**: Простой протокол доступа к объектам (вплоть до спецификации 1.2) для обмена структурированными сообщениями в распределённой вычислительной среде.

3.1.8 **UDDI**: Универсальный метод описания, обнаружения и интеграции веб-сервисов.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

3.1.9 **WSDL**: Язык описания веб-служб, основанный на стандарте XML языка, который определяет способ доступа к веб-службам.

3.1.10 **XML:** Расширяемый язык разметки данных, ориентированный, в частности, на обмен информации между независимыми участниками.

3.1.11 **XML-документ**: Текстовый документ, составленный в полном соответствии со стандартом XML, состоящий из пролога, одного корневого элемента XML, комментариев, декларации типов данных и сервиса.

3.2 В настоящем стандарте применены следующие сокращения:

БД	База данных	
НИС	Национальная информационная система	
ЭЦП	электронно-цифровая подпись	
DNS	domain name system	система поддержки пространства имен
HTTP	hypertext transfer protocol	протокол передачи гипертекста
IPsec	IP security	набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу
RFC	request for comments	комментарии инженерной группы проектировщиков информационно-телекоммуникационной сети Интернет
SOAP	simple object access protocol	простой протокол доступа к объекту
SOAP MTOM	SOAP message transmission optimization mechanism	оптимизированный механизм передачи бинарных данных в структурированных сообщениях
SSL	secure socket layer	протокол защищенных соединений
TLS	transport layer security	безопасность транспортного уровня
UDDI	universal description, discovery and integration	универсальный метод описания, обнаружения и интеграции веб-сервисов
VPN	virtual private network	виртуальная частная сеть
W3C	world wide web consortium	консорциум всемирной паутины
WSDL	web services description language	язык описания веб-служб
XML	extensible markup lan-	расширяемый язык разметки

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

	guage	
XSLT	XSL transformation	правила форматирования и преобразования данных
XSD	XML schema definition	язык описания схем данных
XSL	extensible stylesheet language	расширяемый язык описания таблиц стилей

4 Общие требования к информационным системам в рамках Национальной информационной системы

4.1 В НИС входят информационные системы государственных органов, отраслевые и территориальные информационные системы, а также информационные системы юридических и физических лиц.

4.2 НИС создается с учетом совместимости входящих в ее состав информационных систем с международными информационными системами.

Информационная система – это система, которая организует процессы сбора, хранения и обработки информации о проблемной области. Она может быть размещена на одной или нескольких компьютерных системах. Если информационная система размещена на нескольких компьютерных системах, то она будет рассматриваться как распределенная информационная система.

Данные поступают в информационную систему и исключаются из нее, и эти взаимодействия могут осуществляться или людьми, или процессами.

Управление данными в этом стандарте будет касаться организации и управления постоянными данными. Постоянные данные - это данные, которые хранятся в информационной системе в течение определенного периода времени. Система, которая выполняет функцию организации и управления постоянными данными, называется системой управления данными.

[ГОСТ 34.321, 4.1].

4.3 Информационная система государственных органов может включать:

- транзакционные и учетные подсистемы, обеспечивающие поддержку выполнения государственными органами своих основных задач и функций;
- подсистемы межведомственного информационного взаимодействия между информационными системами, входящими в НИС;
- подсистемы управления ресурсами, обеспечивающими поддержку деловых процессов и административных регламентов в деятельности государственных органов;

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

- информационно-аналитические подсистемы, обеспечивающие сбор, обработку, хранение и анализ данных о результатах выполнения государственными органами своих основных задач и функций;

- подсистемы электронного документооборота;

- подсистемы управления электронными архивами документов;

- подсистемы управления эксплуатацией (включая системы управления инфраструктурными компонентами);

- подсистемы взаимодействия с физическими и юридическими лицами, обеспечивающими предоставление государственными органами через Интернет или другие каналы связи справочной информации и услуг, включая порталы и центры телефонного обслуживания;

- подсистемы обеспечения информационной безопасности;

- офисные подсистемы, используемые сотрудниками государственных органов в своей повседневной деятельности для подготовки документов и обмена информацией.

5 Требования к организации интеграции и взаимодействия информационных систем

5.1 Общие положения

5.1.1 Для организации интеграции и взаимодействия информационных систем необходимо создание инфраструктуры взаимодействия.

5.1.2 Инфраструктура взаимодействия представляет собой единый комплекс информационно-технологических и телекоммуникационных элементов, интегрирующий информационные системы и информационные ресурсы заинтересованных сторон.

5.1.3 Инфраструктура взаимодействия создается для обеспечения:

a) приема обращений, запросов и иных документов заявителей, представляемых для получения государственных услуг, и передачи их в отраслевые и территориальные информационные системы, а также информационные системы юридических и физических лиц;

b) предоставления заявителям сведений, связанных с предоставлением государственных услуг, и результатов предоставления таких услуг;

c) мониторинга процесса взаимодействия информационных систем, входящих в НИС;

d) безопасности взаимодействия информационных систем, входящих в НИС;

e) иных целей организации взаимодействия информационных систем, входящих в НИС.

5.1.4 Каждый элемент инфраструктуры взаимодействия информационных систем, входящих в НИС, должен создаваться и эксплуатироваться с соблюдением следующих требований:

a) обеспечение отсутствия сбоев в функционировании остальных элементов инфраструктуры взаимодействия;

O‘zDSt AGENTLIGI
STANDARTLASHTIRISH VA
MAZGRATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

b) обеспечение бесперебойного взаимодействия элементов инфраструктуры взаимодействия информационных систем, входящих в НИС;

c) обеспечение сохранения функциональных возможностей в полном или уменьшенном объеме при сбоях в работе (отказоустойчивость) и возможности увеличения производительности пропорционально добавленным ресурсам (масштабируемость);

d) иные требования к элементам инфраструктуры взаимодействия, определяемые отдельными нормативно-правовыми актами Республики Узбекистан.

5.1.5 С помощью инфраструктуры взаимодействия обеспечивается:

a) совместимость технологий, используемых в информационных системах, входящих в НИС;

b) оптимизация взаимодействия органов и организаций при предоставлении государственных услуг;

c) эффективность и прозрачность деятельности органов и организаций при предоставлении государственных услуг;

d) минимизация издержек (в том числе финансовых и временных) заявителей при получении государственных услуг;

e) однократный ввод и многократное использование информации в процессе оказания государственных услуг, в том числе за счёт создания единых справочных реестров и применения государственных классификаторов.

5.1.6 К инфраструктуре взаимодействия предъявляются следующие требования:

a) модульное построение с применением единых требований к техническим и программным средствам элементов инфраструктуры взаимодействия, в том числе унифицированных программно-технических средств, стандартизованных интерфейсов для взаимодействия, стандартизованных протоколов обмена данными, единых требований к электронным документам и электронным сообщениям;

b) непрерывный режим функционирования инфраструктуры взаимодействия;

c) обеспечение взаимодействия информационных систем, входящих в НИС;

d) обеспечение однозначной идентификации органов и организаций, заявителей и объема их прав при осуществлении взаимодействия;

e) обеспечение гарантии целостности, подлинности, актуальности и безопасности информации, обмен которой осуществляется при взаимодействии.

5.1.7 Информационные системы должны удовлетворят требованиям наличия и доступности документации, описывающей схемы реализации межсистемного взаимодействия с разрабатываемой информационной системой, способы и форматы обмена данными с данной системой, входные и выходные формы. Требования к межведомственной системе электронного документооборота приведены в O‘z T 45-169 [1].

O ‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

5.1.8 Создание и эксплуатация информационных систем органов и организаций осуществляются исходя из необходимости обеспечения их совместимости с инфраструктурой взаимодействия.

5.1.9 Доступ должностных лиц органов и организаций к информационным ресурсам информационных систем, входящих в НИС, и элементам инфраструктуры взаимодействия, а также доступ заявителей к информационным ресурсам информационных систем органов и организаций и элементам инфраструктуры взаимодействия предоставляется при условии прохождения идентификации, аутентификации и авторизации.

5.2 Порядок организации интеграции и взаимодействия

5.2.1 При взаимодействии информационных систем, входящих в НИС, должна осуществляться идентификация и аутентификация информационных систем по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов или с использованием криптографических методов.

5.2.2 Программными средствами веб-сервиса должны протоколироваться факты приема и отправки каждого информационного сообщения в рамках системы взаимодействия с указанием уникального в рамках веб-сервиса идентификатора сообщения, направления (вида) сообщения (прием или отправка), даты, времени, адресата и контрольной суммы сообщения.

5.2.3 Основу согласованного ведения информационных ресурсов, обеспечивающую их совместимость и взаимодействие, составляют общесистемные информационно-лингвистические средства.

5.2.4 Общесистемные информационно-лингвистические средства – это совокупность языковых средств, обеспечивающих:

a) однозначную идентификацию объектов и субъектов реального мира, информация о которых хранится в информационной системе региона;

b) однозначную интерпретацию данных в процессе функционирования и взаимодействия баз данных и информационных систем;

c) единообразное описание данных;

d) классификацию информации.

В состав общесистемных информационно-лингвистических средств входят:

a) базовый перечень информационных объектов;

b) унифицированные идентификаторы информационных объектов;

c) унифицированные параметры территориальной привязки информационных объектов;

d) стандартные форматы описания данных;

e) справочники баз данных, кадастров, реестров и регистров;

f) классификаторы;

g) словари.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

6 Требования к аппаратному комплексу интегрируемых информационных систем

6.1 Требования к конструкции

Конструкция технических средств информационных систем должна обеспечивать защиту обслуживающего персонала от поражения электрическим током по ГОСТ 12.2.003 и ГОСТ 12.2.007.0. В технических средствах должна быть предусмотрена возможность подключения защитного заземления в соответствии с ГОСТ 12.2.007.0. Конструкция технических средств должна обеспечивать свободный доступ к отдельным узлам и элементам для их технического обслуживания и ремонта, удобное подключение силовых кабелей в соответствии с требованиями ГОСТ 12.2.061.

6.2 Основные требования к серверным помещениям

- Серверная комната должна удовлетворять следующие требования:
- в комнате требуется наличие не менее одной двойной электрической розетки с заземлением на каждые 3 погонных метра любой стены, либо 2 планки розеток, подключенных на различные фидеры для каждой коммутационной стойки;
- комнату следует располагать в стороне от источников электромагнитного излучения, в местах, где возможно впоследствии расширение пространства и есть возможность размещения крупногабаритной аппаратуры;
- максимально допустимая нагрузка на пол должна составлять: распределенная нагрузка - 12 кРа; сосредоточенная нагрузка - 4,4 кН;
- рекомендуется использовать для освещения серверной комнаты лампы накаливания или галогенные лампы, для снижения количества электромагнитных помех;
- рекомендуется иметь подъемный (настланный) пол или систему кабельнесущих лотков;
- система кондиционирования должна обеспечивать поддержку температуры в диапазоне от 18 до 24 0С. Относительная влажность должна поддерживаться в диапазоне от 30 до 50 %;
- размеры серверного помещения должны отвечать требованиям к располагаемому в нем оборудованию или, при отсутствии данных, составлять 0,07 m2 на каждые 10 m2 площади обслуживаемых рабочих мест;
- минимальный допустимый размер серверной комнаты - 12 m2;
- серверная комната должна быть соединена с главным электродом системы заземления здания кондуитом размером 1,5;
- требуемая минимальная высота потолка серверной комнаты должна составлять 2,44 m.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

7 Требования к межсетевому взаимодействию между информационными системами

7.1 Межсетевые соединения информационных систем осуществляются для обмена информацией между различными информационными системами.

7.2 Для осуществления взаимодействия с использованием сетевых протоколов передачи данных необходимо придерживаться протоколов следующих спецификаций:

- протокол передачи гипертекста HTTP версии 1.1/ (RFC 2616) [2];
- расширенный протокол передачи гипертекста версии 1.1 с обеспечением безопасности транспортного уровня TLS;
- протокол защищенных соединений SSL версии 3 – (RFC 5246) [3];
- набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IPsec, - (RFC 4301 [4], RFC 4302 [5], RFC 4835 [6], RFC 2403 [7], RFC 2404 [8], RFC 2405 [9], RFC 4303 [10], RFC 5996 [11], RFC 2410 [12], RFC 2411 [13], RFC 2412 [14]);

Примечание – Допускается применение других видов протокола VPN.

- протоколы использования системы поддержки пространства имен DNS - (RFC 1035 [15]).

7.2 Основные требования к управлению данными при обмене информацией между информационными системами приведены в O‘z DSt 1135.

8 Требования к программному обеспечению интегрируемых информационных систем

8.1 Технологическое обеспечение информационного взаимодействия органов и организаций с применением системы взаимодействия должно достигаться путем использования сервис-ориентированной архитектуры, представляющей собой совокупность веб-сервисов, построенных по общепринятым стандартам, а также путем использования единых технологических решений и стандартов, единых классификаторов и описаний структур данных.

8.2 Программными средствами веб-сервиса должны протоколироваться факты приема и отправки каждого информационного сообщения в рамках системы взаимодействия с указанием уникального в рамках электронного сервиса идентификатора сообщения, направления (вида) сообщения (прием или отправка), даты, времени, адресата и контрольной суммы сообщения.

8.3 При разработке веб-сервиса необходимо придерживаться следующих спецификаций:

- UDDI - версии 2.0 (носит обязательный характер);
- SOAP – (носит обязательный характер);

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH SOHASIDA
NAZORATNI MUVOFIQLASHTIRISH VA
MUROSOLOT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

- WS-I Basic Profile 1.1 - базовый профиль интероперабельности версии 1.1 (носит обязательный характер);

- Web Services Policy 1.2 - политика использования электронных сервисов версии 1.2 (носит рекомендательный характер);

- WS-I Attachments Profile 1.0 - профиль интероперабельности по передаче бинарных данных (носит рекомендательный характер);

- SOAP MTOM (носит рекомендательный характер);

- WS-I Simple SOAP Binding Profile 1.0 - профиль сопоставления данных версии 1.0 (носит рекомендательный характер);

- UDDI 3.0 - версии 3.0 (носит рекомендательный характер).

8.4 При описании данных, а также информации о данных, их составе и структуре, содержании, формате представления, методах доступа и требуемых для этого полномочиях пользователей, о месте хранения, источнике, владельце и используемых наборах символов, применяемых в процессе информационного обмена указанный в 8.3, необходимо придерживаться следующих спецификаций:

- расширяемый язык разметки - набор стандартов XML W3C;

- расширяемый язык описания схем данных версии не ниже 1.0 - стандарт XML W3C;

- расширяемый язык описания таблиц стилей версии 1.1 Extensible Stylesheet Language, XSL v 1.1 - стандарт W3C, включающий правила форматирования и преобразования данных XSLT.

8.5 При разработке веб-сервиса должны быть соблюдены следующие особые условия и ограничения:

- согласно базовому профилю интероперабельности версии 1.1 все описания электронных сервисов и описания схем данных XSD должны создаваться в кодировке UTF-8 или UTF-16 (с указанием этой кодировки в заголовке соответствующего описания);

- в описаниях веб-сервиса запрещены циклические ссылки между описаниями двух и более сервисов (несмотря на то, что язык описания веб-сервиса версии 1.1 это допускает). Однонаправленные ссылки между описаниями веб-сервиса и описаниями схем данных допустимы в любом количестве и сочетании;

- все описания электронных сервисов должны содержать развёрнутую структуру входящих и выходящих параметров. Недопустима передача параметров в виде массивов данных в исходном коде;

- веб-сервис считается доступным только при одновременной доступности и точки доступа электронного сервиса[1)], и описания электронного сервиса. Доступность электронного сервиса обеспечивает оператор информационной системы, в рамках которой функционирует веб-сервис.

[1)] Точку доступа электронного сервиса принято обозначать endpoint.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH XIZMATLARI

9 Требования к обеспечению информационной безопасности при интеграции информационных систем

9.1 Меры по защите информации должны обеспечивать достижение трех основных свойств информации:

– целостности - информация должна быть достоверной и точной, а также защищена от возможных непреднамеренных и злоумышленных искажений;

– доступности - информация и соответствующие автоматизированные службы должны быть доступны, готовы к обслуживанию всегда, когда в них возникает необходимость у имеющего право доступа персонала;

– конфиденциальности - конфиденциальная информация должна быть доступна только тому, кому она предназначена.

9.2 При интеграции к НИС информационная система должна обеспечивать соблюдение следующих общих требований:

– обеспечивать разграничение прав доступа пользователей к данным на базе групп, ролей, а также функций НИС;

– обеспечивать безопасность на уровне операционной системы. Для этого на серверах информационной системы должна быть соответствующим образом настроена политика безопасности и установлены все исправления и обновления.

9.3 В целях реализации информационной безопасности должны быть использованы следующие механизмы безопасности:

– аутентификация;

– межсетевое экранирование;

– средства предотвращения вторжения,

– антивирусные средства.

9.4 Сохранность информации должна быть обеспечена в случае наступления следующих событий:

– импульсные помехи, сбой и потеря электропитания серверов, на которых установлена информационная система;

– сбой общего или специального программного обеспечения (отдельной подсистемы или единичного сервера);

– нарушение работоспособности технических средств, образующих канал связи между серверами, на которых установлен комплекс программ;

– отказ следующих компонентов серверов: процессор, оперативная память, сетевая плата.

9.5 Информационная безопасность каждой информационной системы, подключаемой к НИС, должна соответствовать требованиям, установленным в стандартах: O‘z DSt ISO/IEC 13335-1, O‘z DSt ISO/IEC 15408-1, O‘z DSt ISO/IEC 15408-2, O‘z DSt ISO/IEC15408-3, O‘z DSt ISO/IEC 27001, O‘z DSt ISO/IEC 27002.

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

9.6 Криптографическая защита информации должна удовлетворять требованиям, установленным в стандартах: O‘z DSt 1092, O‘z DSt 1105, O‘z DSt 1106, O‘z DSt 1204.

9.7 Каналы телекоммуникаций системы взаимодействия, выходящие за пределы контролируемых зон участников взаимодействия, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, удовлетворяющих установленным требованиям и находящихся в пределах контролируемых зон участников взаимодействия.

9.8 В целях обеспечения защиты информации, содержащейся в информационных системах, подключенных к НИС, участники информационного взаимодействия:

– обеспечивают при обслуживании информационных систем, подключенных к НИС, исполнение установленных требований по информационной, производственной, технологической и противопожарной безопасности;

– осуществляют контроль доступа посторонних лиц к техническим средствам и каналам связи в контролируемой зоне участника взаимодействия, включая время проведения ремонтных работ и уборки помещений;

– обеспечивают обслуживание информационных систем, подключенных к НИС, только лицами, имеющими право доступа к информации, содержащейся в указанных информационных системах;

– принимают необходимые и достаточные меры, исключающие доступ посторонних лиц к защищаемой (в т.ч. парольной и ключевой) информации, хранящейся на используемых и отчуждаемых носителях информации;

– осуществляют учет лиц, имеющих доступ к конечному оборудованию, обеспечивающему криптографическую защиту каналов связи системы взаимодействия, расположенному в контролируемой зоне участника взаимодействия, а также лиц, имеющих возможность изменения конфигурации информационных систем данного участника взаимодействия, подключенных к системе взаимодействия.

9.9 В целях обеспечения полноценного функционирования инфраструктуры взаимодействия и подключенных к ней информационных систем должна быть обеспечена возможность:

- оперативного переключения на резервный канал с сохранением функций обеспечения безопасности информации для всех каналов связи, выход из строя которых может существенно повлиять на доступность информационных систем, подключенных к системе взаимодействия;

- оперативной замены оборудования, обеспечивающего криптографическую защиту каналов связи, используемых участником взаимодействия для осуществления информационного обмена в рамках системы взаимодействия, в случае выхода такого оборудования из строя.

O ‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH DAVLAT
NAZORATINI KUCHLASHTIRISH
AXBOROT TEXNOLOGIYALARI
JORIY ETISH BOSHQARMASI

Библиография

[1]	O‘z T 45-169:2009	Требования к межведомственной системе электронного документооборота Республики Узбекистан
[2]	IETF RFC 2616 (1999)	Протокол передачи гипертекста HTTP/1.1 (Hypertext transfer protocol - HTTP/1.1)
[3]	IETF RFC 5246 (2008)	Протокол безопасности на транспортном уровне (The transport layer security (TLS) protocol version 1.2)
[4]	IETF RFC 4301 (2005)	Архитектура безопасности Интернет протокола (Security architecture for the internet protocol)
[5]	IETF RFC 4302 (2005)	Заголовок подлинности IP (IP authentication header)
[6]	IETF RFC 4835 (2007)	Применение криптографического алгоритма для вставки безопасности (ESP) в заголовок (AH) (Cryptographic algorithm implementation Req. for encapsulating security payload (ESP) and auth. header (AH))
[7]	IETF RFC 2403 (1998)	Использование HMAC-MD5-96 в пределах ESP и AH (The use of HMAC-MD5-96 within ESP and AH)
[8]	IETF RFC 2405 (1998)	Гипералгоритм ESP DES-CBC для явного IV (The ESP DES-CBC cipher algorithm with explicit IV)
[9]	IETF RFC 2404 (1998)	Использование HMAC-SHA-1-96 в пределах ESP и AH (The use of HMAC-SHA-1-96 within ESP and AH)
[10]	IETF RFC 4303 (2005)	Инкапсуляция безопасности в IP- заголовок (ESP) (IP encapsulating security payload (ESP))
[11]	IETF RFC 5996 (2010)	Протокол обмена Интернет ключами версии 2 (Internet key exchange protocol version 2 (IKEv2)
[12]	IETF RFC 2410 (1998)	Алгоритм NULL и использование IP безопасности The NULL encryption algorithm and its use with IPsec
[13]	IETF RFC 2411 (1998)	Карта документов IP безопасности IP security document roadmap
[14]	IETF RFC 2412 (1998)	Протокол OAKLEY (The OAKLEY key determination protocol)
[15]	IETF RFC 1035 (1987)	Система доменных имен – применение и спецификации (Domain names - implementation and specification)

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

УДК 004.031.42 ОКС 35.020 П 85

Ключевые слова: информационные системы, государственные органы, Национальная информационная система, информационная безопасность, интеграция

O‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

Первый заместитель директора Центра UZINFOCOM — И.Джураев

Заместитель директора – начальник Службы UZ-CERT — Э.Ишимбаев

Начальник группы совершенствования нормативной базы — Д.Акрамова

Главный специалист группы мониторинга ИКТ департамента НИС — Ш.Абдувохидова

Главный специалист группы проектирования и внедрения департамента НИС — Т.Базикалов

Нормоконтроль — Л.Шаймарданова
10.12.2012

СОГЛАСОВАНО

Начальник обеспечения информационной безопасности Узбекского агентства связи и информатизации

У. Мирхамидов
письмо от 08.10.2012
№ 14-8/3514

СОГЛАСОВАНО

Заместитель директора ГУП Центр научно-технических и маркетинговых исследований «UNICON.UZ»

Х.Хасанов
письмо от 03.10.2012
№ 31-05.9/1647

O'ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI

СОГЛАСОВАНО

Начальник отдела информационных ресурсов и информационных систем Узбекского агентства связи и информатизации

О. Умаров
письмо от 24.10.2012
№ 18-8/3728

Начальник развития производства и рынка программных продуктов Узбекского агентства связи и информатизации

З.Рахматуллаев
письмо от 10.10.2012
№ 17-8/3541

O ‘ZSTANDART AGENTLIGI
STANDARTLASHTIRISH, DAVLAT
NAZORATINI MUVOFIQLASHTIRISH VA
AXBOROT TEXNOLOGIYALARINI
JORIY ETISH BOSHQARMASI