ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕЖВЕДОМСТВЕННАЯ ИНТЕГРАЦИОННАЯ ПЛАТФОРМА

Общие технические требования

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

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, информатизации и телекоммуникационных технологий № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 03.11.2014 № 05-584

4 ВВЕДЕН ВПЕРВЫЕ

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»

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ИДОРАЛАРАРО ИНТЕГРАЦИЯ ПЛАТФОРМАСИ
Умумий техник талаблар

Информационная технология
МЕЖВЕДОМСТВЕННАЯ ИНТЕГРАЦИОННАЯ ПЛАТФОРМА[1]
Общие технические требования

Information technology.
The interdepartmental integration platform.
General technical requirements

Дата введения 2014-11-03
2023-01-01

1 Область применения

Настоящий стандарт устанавливает общие и технические требования к межведомственной интеграционной платформе, а также требования к сетевому подключению, программной части и информационной безопасности интегрируемых информационных систем и баз данных органов государственного и хозяйственного управления, государственной власти на местах (далее – государственные органы) в рамках интеграции с межведомственной интеграционной платформой.

Требования настоящего стандарта обязательны для соблюдения государственными органами, выполняющими интеграцию собственных информационных систем и баз данных, а также создающих новые информационные системы и базы данных в рамках интеграции с межведомственной интеграционной платформой.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

(Исключен, Изм. № 1)

O‘z DSt ISO 7498-2:2011 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура безопасности

[1] **С изменением № 1, утвержденным постановлением агентства «Узстандарт» от 29.11.2017 № 05-795и**

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 15408-1:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

(Измененная редакция, Изм. № 1)

O‘z DSt ISO/IEC 15408-2:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности

(Измененная редакция, Изм. № 1)

O‘z DSt ISO/IEC 15408-3:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

(Измененная редакция, Изм. № 1)

O‘z DSt ISO/IEC 27001:2016 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

(Измененная редакция, Изм. № 1)

O‘z DSt ISO/IEC 27002:2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

(Измененная редакция, Изм. № 1)

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 1108:2011 Информационная технология. Взаимосвязь открытых систем. Структура сертификата открытого ключа ЭЦП и сертификата атрибута

O‘z DSt 1109:2013 Информационная технология. Криптографическая защита информации. Термины и определения

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

O‘z DSt 2590:2012 Информационная технология. Требования к интеграции и взаимодействию информационных систем государственных орга-

нов, используемых в рамках формирования Национальной информационной системы

O‘z DSt 2814:2014 Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации

O‘z DSt 2815:2014 Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации

O‘z DSt 2816:2014 Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей

O‘z DSt 2817:2014 Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации

O‘z DSt 2927:2015 Информационная технология. Информационная безопасность. Термины и определения

(Введено дополнительно, Изм. № 1)

O‘z DSt ISO/IEC 27033-2:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 2. Руководящие указания по проектированию и внедрению сетевой безопасности

(Введено дополнительно, Изм. № 1)

O‘z DSt ISO/IEC 27033-3:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

(Введено дополнительно, Изм. № 1)

O‘z DSt ISO/IEC 27033-4:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 4. Руководящие указания по проектированию и внедрению сетевой безопасности

(Введено дополнительно, Изм. № 1)

O‘z DSt ISO/IEC 27033-5:2016 Информационная технология. Методы обеспечения безопасности. Сетевая безопасность. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных сетей.

(Введено дополнительно, Изм. № 1)

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 2927, O‘z DSt 1047, O‘z DSt 1109, O‘z DSt 2590, а также следующие термины с соответствующими определениями:

(Измененная редакция, Изм. № 1)

3.1.1 **BPM-модуль**: Специализированное программное обеспечение, позволяющее оптимизировать процессы информационной системы.

Примечание - Эта спецификация строится на базе эталонных реализаций.

3.1.2 **BPEL**: Язык на основе XML для формального описания бизнес-процессов и протоколов их взаимодействия между собой. BPEL расширяет модель взаимодействия веб-служб и включает в эту модель поддержку транзакций.

3.1.3 **адаптер**: Тип программного обеспечения, которое логически располагается между двумя программными компонентами и устраняет различия между ними.

3.1.4 **витрина данных**: Срез хранилища данных, массив тематической, узконаправленной информации, ориентированный на конкретную информационную систему.

3.1.5 **Единый портал интерактивных государственных услуг** (далее - Единый портал): Справочно-информационный портал на Правительственном портале Республики Узбекистан в сети Интернет, обеспечивающий пользователям доступ к сведениям об интерактивных государственных услугах, а также предоставление в электронной форме государственных услуг.

3.1.6 **Единая система идентификации**: Инфраструктурный элемент, обеспечивающий санкционированный доступ заявителей и должностных лиц государственных органов к Единому порталу интерактивных государственных услуг, а также другим информационным системам.

3.1.7 **журналирование**: Процесс записи информации о происходящих с каким-либо объектом (или в рамках какого-либо процесса) событиях в журнал (например, в файл).

3.1.8 **идентификация**: Присвоение субъектам и объектам идентификатора и/или сравнение идентификатора с перечнем присвоенных идентификаторов. Идентификация решает задачу установления личности пользователя.

3.1.9 **ключ, ключевая информация**: Конкретное секретное состояние некоторого набора параметров криптографического алгоритма, обеспечивающее выбор одного преобразования из совокупности возможных для данного алгоритма преобразований.

3.1.10 **конечное оборудование**: Оборудование, расположенное в контролируемой зоне участников взаимодействия, предназначенное для преобразования информации участников взаимодействия в данные для передачи по каналу связи с использованием криптографической защиты и осуществляющее обратное преобразование.

3.1.11 **межведомственная интеграционная платформа**: Совокупность аппаратно-программных средств, предназначенных для интеграции информационных систем электронного правительства в рамках оказания электронных государственных услуг и организации электронного взаимодействия.

(Измененная редакция, Изм. № 1)

3.1.12 **пароль:** Последовательность символов, которая используется как информация аутентификации.

3.1.13 **подсистема журналирования:** Подсистема, осуществляющая ведение процесса журналирования и позволяющая в любой момент времени получить запрашиваемую информацию.

3.1.14 **подсистема передачи данных:** Подсистема, обеспечивающая возможность ввода информации в систему, а также получения необходимой информации из системы.

3.1.15 **поставщик**: Государственный орган, являющийся собственником или владельцем информационной системы.

3.1.16 **пользователь**: Физическое лицо, резидент (нерезидент) Республики Узбекистан, или физическое лицо, выступающее от юридического лица, осуществляющее запрос к информационной системе.

3.1.17 **резидентный режим**: Режим, при котором работа программного обеспечения предполагает самостоятельное выполнение возложенных на неё задач, без участия (или почти без участия) пользователя.

3.1.18 **система безопасности:** Интеграция различных подсистем безопасности с минимальным количеством избыточных элементов, позволяющая создавать единую систему управления, контроля рисков информационной безопасности.

3.1.19 **формально-логическая проверка**: Проверка правильности предоставления значений реквизитов электронного сообщения.

3.1.20 **целевая информационная система**: Информационная система, к которой выполняется запрос на предоставление доступа к информации или услуге.

3.2 В настоящем стандарте применены следующие сокращения:

BPM	Business Process Management – управление бизнес-процессами
BPEL	Business Process Execution Language – язык выполнения бизнес-процессов
IP	Internet Protocol – Интернет протокол
REST	Representational State Transfer – передача состояния прелставления **(Введено дополнительно, Изм. № 1)**
SOAP	Simple Object Access Protocol – простой протокол доступа к объектам
WSDL	Web Services Description Language – язык описания веб-

	сервисов
XML	Extensible Markup Language — расширяемый язык разметки
БД	база данных
ЕСИ	Единая система идентификации
ИГУ	интерактивная государственная услуга
ИР	информационный ресурс
ИС	информационная система
МИП	межведомственная интеграционная платформа
ЭЦП	электронная цифровая подпись

4 Основные положения

4.1 МИП служит для обеспечения взаимодействия и интеграции всех ИС, ИР и БД, а также обеспечивает доступ к центральным БД с целью предоставления государственных услуг в электронном виде и исполнения функций государственных органов в электронной форме.

4.2 МИП представляет собой совокупность информационно-технологических и телекоммуникационных элементов, позволяющих обеспечивать хранение сведений об истории движения в МИП электронных сообщений, а также программных и технических средств, обеспечивающих взаимодействие ИС и БД, используемых при предоставлении в электронной форме государственных услуг и обмене данными между государственными органами в рамках исполнения их функций.

(Новая редакция, Изм. № 1)

4.3 МИП выполняет следующие функции:

- обеспечение взаимодействия между ИС и БД государственных органов;
- предоставление ИС доступа к БД;
- предоставление по необходимости витрин данных;
- ведение списка веб-сервисов и перечня возможных запросов к ним;
- контроль функционирования веб-сервисов;
- проектирование промежуточных веб-сервисов с применением BPM;

(Новая редакция, Изм. № 1)

- маршрутизация сообщений к зарегистрированным веб-сервисам;
- мониторинг процессов взаимодействия, предусмотренных государственными стандартами, соглашениями, заключенными в соответствии с 7.3.44 настоящего стандарта;
- предоставление услуг доверительной третьей стороны и реализация единого пространства доверия;
- уведомление о состоянии отправленных электронных сообщений;

(Новая редакция, Изм. № 1)

- контроль корректности оформления входящих сообщений;
- ведение политики безопасности, применяемой к ЕСИ и зарегистрированным сервисам;
- протоколирование запросов и обращений к зарегистрированным сервисам;
- формирование актуальной статистики использования веб-сервисов;
- идентификация пользователя в системе;
- предоставление соответствующих прав пользователю в зависимости от типа аутентификации и выбираемой услуги.

4.4 МИП обеспечивает:

a) доступ к веб-сервисам ИС и ИР, подключенных к МИП, в том числе центральных БД;

b) получение, обработку и доставку электронных сообщений в рамках информационного взаимодействия государственных органов с обеспечением фиксации времени передачи, целостности и подлинности электронных сообщений, указания их авторства и возможности предоставления сведений, позволяющих проследить историю движения электронных сообщений;

c) защиту передаваемой информации от несанкционированного доступа, ее искажения или блокирования с момента поступления указанной информации в МИП до момента передачи ее в подключенную к МИП ИС;

d) хранение информации, содержащейся в реестре веб-сервисов ИС государственных органов, подключенных к МИП (далее - реестр веб-сервисов), и мониторинг работоспособности веб-сервисов, включенных в данный реестр;

(Новая редакция, Изм. № 1)

4.5 Вся передаваемая информация (данные) между МИП и ИС и БД, а также между элементами МИП должна иметь формат в соответствии со спецификациями, приведенными в O‘z DSt 2590.

5 Архитектура межведомственной интеграционной платформы

5.1 МИП включает в себя:

- базовый аппаратно-программный комплекс;
- основные программные элементы.

5.2 Базовый аппаратно-программный комплекс представляет собой серверную и сетевую инфраструктуру со средой виртуализации, а также базовый набор необходимого программного обеспечения.

5.3 Перечень основных программных элементов включает:

- интеграционную шину;
- хранилище данных;
- витрины данных;

- адресную подсистему;
- подсистему передачи данных;
- журнал;
- средство идентификации;
- реестр прав доступа;
- единое пространство доверия;
- BPM–модуль;
- Портал администратирования;
- система безопасности.

5.4 Архитектура МИП представлена на рисунке 1.

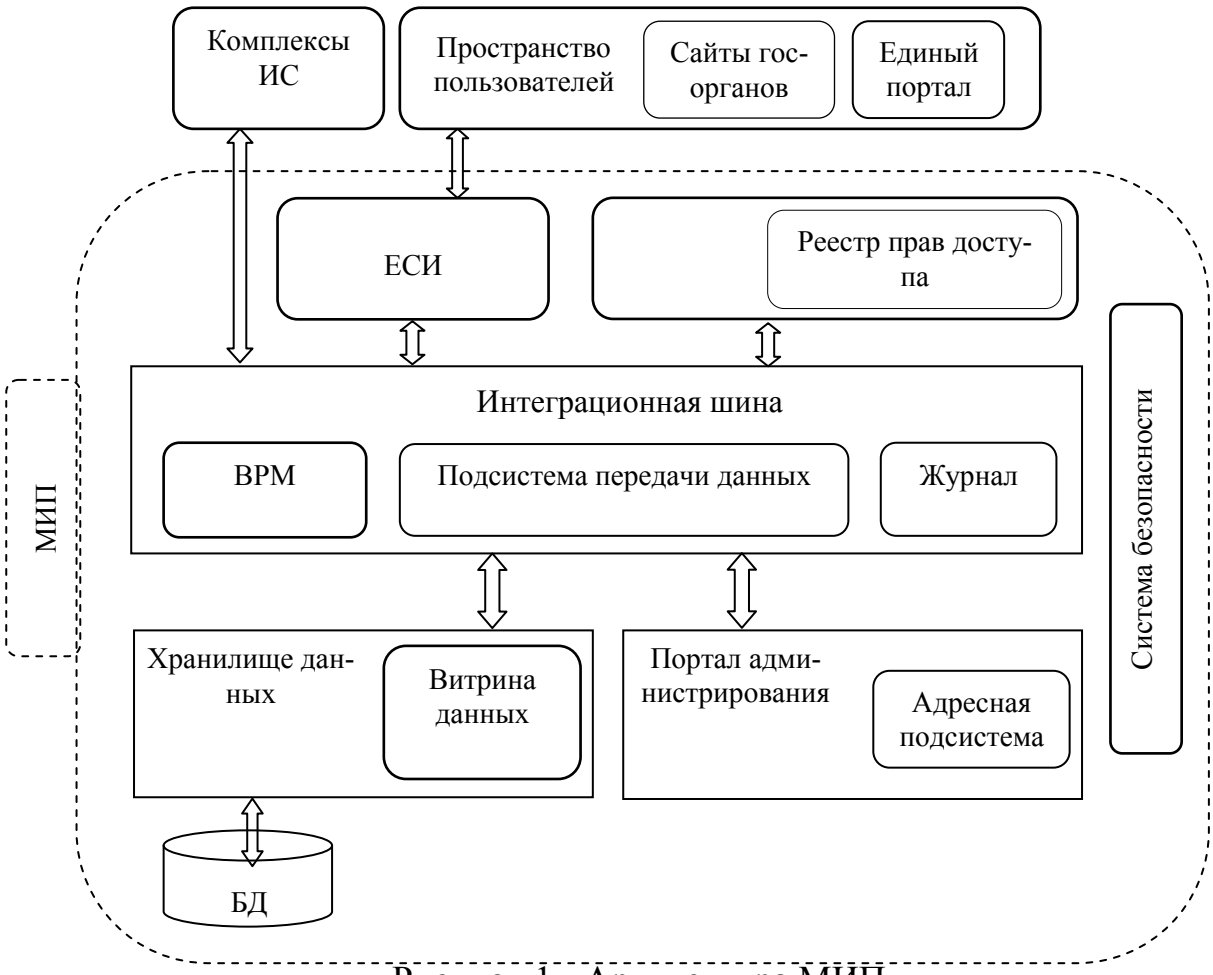

Рисунок 1 - Архитектура МИП

(Новая редакция, Изм. № 1)

6 Элементы межведомственной интеграционной платформы

6.1 Интеграционная шина

6.1.1 Интеграционная шина представляет собой совокупность элементов аппаратного и программного обеспечения.

6.1.2 Основной принцип интеграционной шины - концентрация обмена сообщениями между различными системами через единую точку, в которой, при необходимости, обеспечиваются транзакционный контроль, преобразование данных, сохранность сообщений.

6.1.3 При замене какой-либо ИС, подключённой к МИП, перенастройка остальных ИС не должна осуществляться.

6.2 Хранилище данных

6.2.1 Хранилище данных представляет собой специализированную БД. Хранилище является предметно-ориентированным, оптимизированным для подготовки отчётов и бизнес-анализа.

6.2.2 Входящие данные, поступающие в хранилище, объединяются по категориям и хранятся в соответствии с областями, которые они описывают. Все данные логически объединяются и не подлежат корректировке и удалению.

6.2.3 В результате выделения хранилища данных в отдельную подсистему, появляется возможность анализа различных данных, хранящихся в разных базах. Информация из хранилища передаётся в витрины данных.

6.3 Витрины данных

6.3.1 Технологически, витрины данных представляют собой тематические БД, относящиеся к отдельным аспектам деятельности. Витрины данных позволяют гибко предоставлять доступ к данным, предлагая ИС только необходимую информацию.

6.3.2 МИП должна поддерживать механизм создания витрин данных, сами витрины могут быть предоставлены заинтересованным государственным органам как сервисы.

6.4 Адресная подсистема

6.4.1 Адресная подсистема представляет собой справочник ИС, подключённых к МИП, определяющий их логический или физический адрес, а также перечень разрешённых запросов.

При выполнении запроса сначала происходит обращение к подсистеме передачи данных, после определения местонахождения ИС назначения запроса, запрос перенаправляется к ней. В качестве выводимой информации могут быть адреса не одной, а нескольких целевых ИС.

6.4.2 Основное предназначение адресной подсистемы - определение адреса целевой ИС.

6.4.3 Адресная подсистема выполняет следующие задачи:

- хранение карты ИС;
- хранения перечня запросов к ИС;

- поддержка карты ИС в актуальном состоянии;
- определение отправителя;
- выдача информации об ИС.

6.5 Подсистема передачи данных

6.5.1 Подсистема передачи данных не определяет правомерность доступа к данным, а действует на основании разрешения, полученного от целевой ИС.

6.5.2 Любая информация попадает в МИП и покидает МИП через подсистему передачи данных.

6.5.3 Подсистема передачи данных должна выполнять следующие задачи:

- определение автора сообщения;
- определение получателя сообщения;
- приём вводимых данных;
- передача выводимых данных;
- обеспечение доставки данных.

6.6 Журнал

6.6.1 Журнал предназначен для записи информации о событиях в специально приспособленные для этого БД.

6.6.2 Журналированию подлежат все события, происходящие внутри МИП, в том числе, об истории движения в МИП электронных сообщений при предоставлении ИГУ, исполнении функций государственных органов в электронной форме.

6.6.3 В зависимости от предварительных настроек подсистемы, записи о выполнении операции добавляются в различные журналы.

Уровни журналирования, а также правила ведения записей в различные журналы должны быть гибконастраиваемыми.

6.6.4 Все записи в журнале являются транзакциями. Незавершённая транзакция обозначает, что требуемая операция не была завершена успешно.

6.6.5 Подсистема журналирования получает сообщения от различных элементов МИП с подробным указанием о событии: автор события, целевая ИС, уровень важности события.

6.6.6 От предопределённого набора правил подсистема журналирования определяет журнал или журналы, куда будет добавлена информация о событии.

6.6.7 Подсистема журналирования выполняет следующие задачи:

- создание правил журналирования;
- ведение журналов;
- функция поиска;

- обработка и архивация журналов;
- обработка и ведение статистической информации;
- уведомление о каком-либо событии.

6.6.8 Дополнительной задачей подсистемы журналирования является поддержка журналов в актуальном состоянии, своевременное архивирование неактуальных записей.

6.7 Средство идентификации

6.7.1 Средство идентификации предназначено для точного определения пользователя, который в данный момент взаимодействует с ИС.

6.7.2 Идентификация пользователей производится по средством ЕСИ. Для идентификации пользователя ЕСИ производит аутентификацию одним из доступных способов, каждый из которых предоставляет различный уровень достоверности. Подсистема идентификации получает требуемые данные о юридических и физических лицах из БД юридических и физических лиц соответственно.

(Измененная редакция, Изм. № 1)

6.7.3 Средство идентификации должно иметь модульную структуру для обеспечения совместимости с различными типами аутентификации.

Аутентификация пользователей должна быть произведена с помощью ЕСИ, различными способами: проверка через логин/пароль, проверка через ЭЦП, проверка через биометрические данные потребителя и т.п.

(Измененная редакция, Изм. № 1)

6.7.4 Подсистема идентификации выполняет следующие задачи:

- составление и содержание БД пользователей;
- взаимодействие с внешними системами идентификации;
- определение пользователей;
- журналирование.

6.7.5 Идентификация должна быть представлена в виде взаимодействия ЕСИ и реестра прав доступа.

6.7.6 ЕСИ должна самостоятельно определять и передавать в МИП идентификатор и текущую роль пользователя.

6.7.7 Передаваемые данные шифруются и подписываются ЭЦП ЕСИ.

6.7.8 ЕСИ хранит БД пользователей, проверяет валидность введенных учетных данных пользователя и при необходимости приводит их в неактивное состояние.

(Новая редакция, Изм. № 1)

6.7.9 Полученные данные от ЕСИ сравниваются с данными в БД пользователей и пользователю присваивается единый идентификатор, независимо от способа входа в ИС.

(Новая редакция, Изм. № 1)

6.7.10 БД пользователей представляет собой перечень единых идентификаторов и сопоставленных им учётных данных (логин пользователя, открытый ключ ЭЦП).

6.7.11 Способы аутентификации пользователей могут быть различны и существенно различаться по уровню безопасности.

В зависимости от способа аутентификации один и тот же пользователь получает различные роли.

В зависимости от роли пользователю может быть предоставлен доступ к информации или услугам.

6.7.12 Соответствие вида информации и ИГУ к способу аутентификации представлено в таблице 1.

Таблица 1 - Соответствие вида информации и ИГУ к способу аутентификации

Уровень	Вид информации	Вид ИГУ	Способ аутентификации
(Исключен, Изм. № 1)			
2	Личная доступная информация	- ИГУ двустороннего информационного обмена (ИГУ, не требующие предоставления конфиденциальной информации)	Минимальная аутентификация, на основании логина-пароля или персональных идентификаторов
3	Персональная информация	- ИГУ двустороннего информационного обмена; -транзакционные ИГУ (ИГУ, требующие подписи)	ЭЦП и логин-пароль **(Введено дополнительно, Изм. № 1)**
4	Конфиденциальная информация		Двухфакторная аутентификация

6.8 Реестр прав доступа

6.8.1 Реестр прав доступа предназначен для сопоставления полномочий пользователя и предоставления целевой ИС данных о текущей роли пользователя.

6.8.2 Реестр прав доступа получает необходимые данные об успешно идентифицировавшемся пользователе и передаёт информацию о текущей роли пользователя в подсистему передачи данных и целевую ИС.

6.8.3 На основании получаемых данных целевая ИС разрешает или запрещает предоставление информации или услуги. В каждый момент времени пользователь выступает с правами только одной роли.

6.8.4 Реестр прав доступа предназначен для выполнения следующих задач:

- создание, редактирование и удаление правил доступа;
- создание, редактирование и удаление ролей доступа;
- определение текущей роли пользователя;
- определение всех возможных ролей пользователя.

6.8.5 Роль пользователя может быть одной из следующих:

- физическое лицо (резидент и не резидент Республики Узбекистан);
- представитель иного физического лица;
- представитель юридического лица или субъекта предпринимательства;
- представитель государственного органа.

6.8.6 Роли пользователя должны определяться автоматически в соответствии с совокупностью факторов (способ аутентификации, время входа в ИС, IP-адрес, с которого вошёл пользователь).

6.9 Единое пространство доверия

6.9.1 Единое пространство доверия предназначено для проверки сертификатов ключей ЭЦП, сформированных различными удостоверяющими центрами, ИС государственных органов.

6.9.2 Единое пространство доверия взаимодействует с доверительной третьей стороной при помощи специализированного программного обеспечения, предоставляемого доверительной третьей стороной. На основании данных, полученных от доверительной третьей стороны, происходит присвоение единого идентификатора пользователя, авторизованного при помощи ЭЦП.

6.9.3 БД единого пространства доверия должна обеспечивать хранение информации обо всех пользователях ЭЦП.

6.10 BPM-модуль

6.10.1 BPM-модуль должен выполнять следующие функции:

- моделировать, анализировать и имитировать процессы в МИП и вне ее;
- формировать перечни различных показателей;
- документировать результаты выполнения процессов;
- строить прогнозы по различным показателям процессов.

6.10.2 Функции BPM-модуля состоят в предоставлении внешним информационным системам интуитивно понятного конструктора процессов как сервиса. На основании BPM-модуля ИС смогут выстраивать соб-

ственные цепочки типовых процессов и осуществлять контроль за их выполнением.

6.10.3 BPM-модуль должен иметь следующие возможности:

- импорт файла с процессами, описанными при помощи языка BPEL;
- визуальный конструктор и редактор процессов;
- редактор процессов при помощи языка BPEL.

6.11 Система безопасности

6.11.1 Система безопасности предназначена обеспечивать информационную безопасность МИП.

6.11.2 Система безопасности функционирует в резидентном режиме, постоянно находясь в оперативной памяти и реагируя только на угрозы безопасности, пресекая их.

6.11.3 Система безопасности обеспечивает:

- физическую и логическую целостность серверного и виртуального оборудования, на котором работают сервисы МИП;
- безопасность сетевого соединения;
- безопасность операционной системы за счет специализированного программного обеспечения;
- безопасность программной части элементов МИП;
- целостность, доступность и конфиденциальность БД, содержащихся внутри МИП;
- контроль и управление сессиями, поведением пользователей, правилами входа в ИС.

6.12 Портал администрирования веб сервисов

6.12.1 Портал администрирования веб сервисов (WebService Administration Portal) – это связующее звено, необходимое для осуществления обмена информацией между системами баз данных, информационными системами и другими компонентами систем государственных органов.

6.12.2 Назначением Портала администрирования веб сервисов является обеспечение информационного взаимодействия между государственными органами. Для достижения поставленной цели каждая организация, которая предоставляет данные, должна разработать и внедрить необходимый веб сервис. Таким образом, другие организации смогут воспользоваться предоставляемыми данными посредством вызова веб сервиса через Портал администрирования.

(Дополнен разделом, Изм. № 1)

7 Требования к интеграции информационных систем и баз данных с межведомственной интеграционной платформой

7.1 Подключение информационных систем к межведомственной интеграционной платформе

7.1.1 Для осуществления функционирования МИП назначается уполномоченный орган (далее - оператор МИП).

7.1.2 Оператор МИП осуществляет:

– обеспечение функционирования МИП в соответствии с законодательством Республики Узбекистан в области информации, информационных технологий и защиты информации;

– подключение ИС и БД к МИП;

– формирование и ведение реестра веб-сервисов.

7.1.3 Технологическое обеспечение информационного взаимодействия государственных органов с применением МИП достигается 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.

7.1.4 Подключение ИС к МИП осуществляется в следующих режимах:

– поставщик сведений разрабатывает и предоставляет МИП свой веб-сервис, который предназначен для обработки запросов и выдачи сведений;

– потребитель сведений разрабатывает и подключает к МИП свой адаптер, который запрашивает сведения и получает ответ от МИП.

7.1.5 Для подключения ИС и БД к МИП владелец ИС или БД (далее - оператор ИС):

– обеспечивает защищенный канал связи между своей ИС или БД и МИП;

– разрабатывает адаптеры взаимодействия с МИП в соответствии с настоящим стандартом;

– разрабатывает и регистрирует веб-сервис ИС в реестре веб-сервисов.

7.1.6 Подключению к МИП подлежат ИС и БД государственных органов, межведомственные ИС, используемые при предоставлении ИГУ и исполнении государственных функций.

7.1.7 Для осуществления взаимодействия МИП и ИС и БД необходимо придерживаться спецификаций сетевых протоколов передачи данных, приведенных в O‘z DSt 2590.

7.2 Адаптеры подключения к межведомственной интеграционной платформе

7.2.1 Адаптеры ИС предназначены для подключения ИС к МИП в целях использования веб-сервисов, доступных в реестре веб-сервисов.

7.2.2 Взаимодействие адаптера ИС с МИП осуществляется по протоколам SOAP и REST в асинхронном режиме. При этом протокол REST используется только при отправлении сообщений с ИС в МИП.

(Новая редакция, Изм. № 1)

7.2.3 Процесс взаимодействия адаптера ИС с МИП осуществляется последовательно согласно следующим этапам:

a) адаптер ИС направляет в МИП SOAP-сообщение с указанием названия веб-сервиса и процедуры веб-сервиса для выполнения, а также входящие данные, необходимые для выполнения процедуры;

b) при получении сообщения МИП осуществляет проверку наличия достаточных прав доступа ИС, предусмотренных соглашением согласно 7.3.44, для выполнения запрошенной процедуры веб-сервиса;

c) в случае успешной проверки МИП добавляет запрос в очередь на обработку и возвращает ответ обратившейся ИС с указанием идентификатора запроса и метки времени, после чего обратившейся ИС необходимо отправить запрос на проверку результата;

d) полученные данные адаптер ИС сохраняет в журнале и в указанное время отправляет повторный запрос на получение результата;

e) в случае, если запрос выполнен, МИП возвращает результат об успешном выполнении, либо ошибку с указанием причины отказа. Этапы c) и d) повторяются до тех пор, пока МИП не вернет результат запроса.

7.2.4 Принимаемые сообщения проверяются на валидность, согласно O‘z DSt 1108, с дополнительной проверкой соответствия ИС с зарегистрированным IP-адресом, а также проверкой на наличие вредоносного кода.

(Измененная редакция, Изм. № 1)

7.3 Требования к веб-сервисам, зарегистрированных в реестре веб-сервисов

7.3.1 Документированный способ доступа к ИС, подключаемой к МИП, должен быть реализован в виде веб-сервиса, описание и доступ к которому должен быть описан в виде WSDL-документа.

7.3.2 При разработке веб-сервисов необходимо придерживаться спецификаций, установленных стандартом O‘z DSt 2590.

7.3.3 В МИП подлежат регистрации веб-сервисы, обеспечивающие:

a) взаимодействие ИС, подключенных к МИП;

b) предоставление ИГУ с использованием Единого портала.

7.3.4 Веб-сервисы, обеспечивающие предоставление ИГУ с использованием Единого портала и официальных веб-сайтов государственных органов, должны реализовывать следующие функции:

– направление сведений из заполненных форм заявлений и иных документов на Едином портале в ИС государственных органов;

– обновление на Едином портале информации о ходе предоставления ИГУ поставщиком;

– передачу из ИС государственного органа на Единый портал результата оказания государственной услуги и/или ее отдельных административных процедур (действий).

7.3.5 Регистрацию в реестре веб-сервисов разработанного веб-сервиса осуществляет оператор МИП после предоставления оператором ИС адреса разработанного веб-сервиса, его названия, документированного списка процедур, контрольного примера и другой необходимой информации.

7.3.6 Электронные сообщения, содержащие информацию, отнесенную к государственным секретам Республики Узбекистан, не подлежат обработке в МИП.

Передача конфиденциальной информации осуществляется в соответствии с законодательством Республики Узбекистан.

7.3.7 При описании данных, а также информации о данных, их составе и структуре, содержании, формате представления, методах доступа и требуемых для этого полномочиях (правах) пользователей, о месте хранения, источнике, владельце и др., а также используемых наборов символов, применяемых в процессе информационного обмена, необходимо придерживаться спецификаций, установленных стандартом O‘z DSt 2590.

7.3.8 Входящие электронные сообщения, полученные по каналам связи МИП, проходят контроль в следующем порядке:

– проверка ЭЦП электронного сообщения;

– формально-логическая проверка электронного сообщения;

– в случае наличия прикрепленных к сообщению файлов - их проверка на наличие вредоносного кода.

7.3.9 Проверка ЭЦП электронного сообщения осуществляется операторами ИС, подключенных к МИП, и оператором МИП (далее - участники взаимодействия).

Проверка ЭЦП в электронных сообщениях производится на предмет корректности значений ЭЦП и на предмет действительности соответствующих сертификатов ключей ЭЦП на момент подписания сообщения посредством доверительной третьей стороны.

Проверка подлинности ЭЦП осуществляется в соответствии со стандартом O‘z DSt 1108.

7.3.10 В случае, если проверка корректности одного из значений ЭЦП или проверка действительности одного из сертификатов ключей ЭЦП дала отрицательный результат, отправителю электронного сообщения

направляется уведомление с текстом «Не удалось подтвердить подлинность ЭЦП» или «ЭЦП недействительна.

(Новая редакция, Изм. № 1)

7.3.11 Электронные сообщения, проверка ЭЦП которых дала положительный результат, подвергаются формально-логической проверке значений реквизитов электронного сообщения.

7.3.12 В случае не прохождения формально-логической проверки, электронное сообщение исключается из дальнейшей обработки, данный факт фиксируется и по каналам связи МИП отправителю направляется служебное электронное сообщение, извещающее об отказе в приеме электронного сообщения.

7.3.13 В случае прохождения формально-логической проверки электронного сообщения по каналам связи МИП, отправителю направляется служебное электронное сообщение, извещающее об успешном приеме электронного сообщения ИС, подключенной к МИП.

7.3.14 Если принятое и успешно прошедшее процедуры контроля электронное сообщение является сообщением запроса на предоставление электронной услуги, то ИС поставщика разрешает использование данного веб-сервиса.

7.3.15 Если принятое и успешно прошедшее процедуры контроля электронное сообщение является извещением о готовности данных, то ИС оператора, имеющего право использования веб-сервиса в соответствии с настоящим стандартом, при необходимости, инициирует сервис запроса этих данных.

7.3.16 Общая структура электронного сообщения включает в себя:

- заголовок электронного сообщения МИП (soap:header);
- тело электронного сообщения МИП (soap:body);
- сообщение об ошибке (soap:Fault).

7.3.17 Заголовок электронного сообщения МИП включает:

- передачу сведений об аутентификации и авторизации (WS-security);
- передачу параметров при асинхронном взаимодействии (WS-Addressing).

7.3.18 Тело электронного сообщения МИП в общем случае состоит из следующих элементов:

- блок данных;
- блок присоединенных документов;
- блок ЭЦП.

7.3.19 Блок данных электронного сообщения должен содержать дату и время отправки электронного сообщения в МИП.

7.3.20 Блок присоединенных документов может содержать информацию (текстовую, графическую и др.), прилагаемую к электронному сообщению МИП.

7.3.21 Блок ЭЦП должен содержать одну или несколько ЭЦП, фиксирующих целостность и авторство каждого из блоков данных и каждого из блоков присоединенных документов.

7.3.22 Сообщение об ошибке содержит текстовое описание возникшей ошибки и ее код в рамках ИС, в которой она возникла.

7.3.23 Ответственным за содержание реквизитов электронного сообщения является участник взаимодействия, отправивший данное электронное сообщение, если иное не предусмотрено настоящим стандартом и нормативно-правовыми актами Республики Узбекистан.

7.3.24 Документирование элементов метаданных должно быть выполнено с использованием конструкции:

<xsd:annotation>

<xsd:documentation>Текст описания</xsd:documentation>

</xsd:annotation>

Синтаксическую конструкцию <!-- текст комментария --> рекомендуется применять только в качестве вспомогательных комментариев к описаниям данных, если это необходимо, и не использовать для документирования элементов метаданных.

7.3.25 При формировании наименования элементов метаданных необходимо осуществлять подбор слова или словосочетания из английского языка, соответствующего тому или иному используемому понятию.

7.3.26 Наименования, обозначающие общепринятые аббревиатуры, подлежат транслитерации на латиницу.

7.3.27 Если в английском языке отсутствует слово или словосочетание, достаточно однозначно определяющее описываемое понятие или допускающее большое количество вариантов обратного перевода, допустимо использовать транслитерацию на латиницу.

7.3.28 Все слова в наименовании элемента метаданных необходимо использовать полностью, без сокращений.

7.3.29 Порядок записи слов, в наименовании которых используется два или более слова, должен соответствовать правилам английского языка. Слова должны записываться подряд, без пробела и других знаков между ними.

7.3.30 Наименования метаданных должны записываться строчными буквами, кроме аббревиатур, записываемых полностью прописными (заглавными) буквами. Если используется два или более слова, то каждое последующее слово, кроме первого, должно начинаться с прописной (заглавной) буквы.

7.3.31 По согласованию с оператором МИП допускается использование в качестве первого (а также единственного) слова с прописной (заглавной) буквы.

7.3.32 В наименованиях простых и составных типов (simpleType, complexType) для обозначения их отличия от элементов (element), необходимо добавлять суффикс «Type».

7.3.33 По согласованию с оператором МИП при наименовании элементов метаданных допускается использование кириллицы.

7.3.34 Под контрольным примером обращения к электронному сервису понимается пример обращения к электронному сервису и ответа электронного сервиса на указанное обращение. Контрольный пример обращения и ответа должен быть предоставлен поставщиком в формате протокола обмена структурированными сообщениями.

7.3.35 Назначением контрольного примера является подтверждение работоспособности веб-сервиса при проведении процедуры регистрации, в рамках которой осуществляется отправка веб-сервису запроса, приведенного в контрольном примере, и сравнение полученного ответа веб-сервиса с ответом, приведенным в контрольном примере.

7.3.36 Контрольный пример не должен вызывать выполнение каких-либо операций в ИС поставщика, которые могут привести к возникновению событий, позволяющих ИС участника взаимодействия интерпретировать полученные при выполнении контрольного примера данные как реальные, а не тестовые.

7.3.37 Регистрация веб-сервиса ИС поставщика может считаться завершенной только при условии успешного выполнения контрольного примера, которое предполагает совпадение ответа веб-сервиса с ответом, приведенным в контрольном примере, либо при объективной невозможности возврата веб-сервисом повторяемых данных - его соответствие описанию логики формирования ответа, которое в подобных случаях должно сопровождать предоставляемый контрольный пример.

7.3.38 Контрольный пример может быть использован для настройки модуля МИП, обеспечивающего проверку доступности и работоспособности веб-сервиса, а также для отладки программного кода разработчиками потребителя веб-сервиса.

7.3.39 ИС участников взаимодействия должны обеспечивать гарантированную доставку неискаженных сообщений в рамках информационного обмена между ИС данного участника взаимодействия и МИП в установленные (регламентированные) сроки.

7.3.40 МИП обеспечивает гарантированную доставку неискаженных сообщений с определенным интервалом времени ожидания ответа на запрос, путем определенного количества повторных вызовов веб-сервисов ИС участников взаимодействия за заданный интервал времени.

7.3.41 МИП обеспечивает фиксацию факта доставки неискаженного сообщения, либо факта ошибки при передаче сообщения в рамках информационного обмена между ИС участников взаимодействия и МИП.

7.3.42 Веб-сервисы ИС участников взаимодействия могут разделяться по режиму работы в части обработки сообщений на синхронные и асинхронные веб-сервисы.

7.3.43 В случае времени ответа (получения результата) ИС на входящие электронные сообщения свыше 3 секунд рекомендуется использовать асинхронный режим работы веб-сервиса.

7.3.44 Особенности использования МИП и подключения к ней ИС государственных органов, а также определение прав доступа к процедурам веб-сервисов других ИС, определяются в рамках соглашений между оператором МИП и государственными органами, являющимися владельцами ИС, подключаемых в МИП.

8 Криптографическая защита и обеспечение информационной безопасности

8.1 Криптографическая защита и информационная безопасность МИП обеспечивается путем выполнения требований нормативно-правовых актов и государственных стандартов Республики Узбекистан по информационной безопасности.

8.2 Надежность защиты информации при её хранении и передачи в ИС должна быть обеспечена за счет применения средств криптографической защиты. Применяемые средства криптографической защиты должны обеспечивать устойчивость к взломам и многоуровневую защиту от компрометации ключевой информации.

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

8.3 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.

8.4 При интеграции к МИП ИС должна обеспечивать соблюдение следующих общих требований:

- обеспечивать разграничение прав доступа пользователей к ИС, ИР и БД на базе групп, ролей, а также функций МИП;
- обеспечивать безопасность на уровне приложений. Для этого на серверах ИС должна быть соответствующим образом настроена политика безопасности и установлены все исправления и обновления;
- следует отслеживать действия ИС и регистрировать инциденты информационной безопасности. Для обеспечения идентификации проблем ИС следует вести журналы регистрации сбоев и операций;
- для обеспечения безопасности в сервисах и приложениях, используемых в ИС, необходимо осуществлять проверку входных данных, такими способами как проверка границ или ограничение полей ввода определенными диапазонами входных данных;

- данные, выводимые из приложений, необходимо проверять на корректность для обеспечения уверенности в том, что обработка информации выполнена правильно.

8.5 В целях обеспечения информационной безопасности должны быть использованы следующие механизмы безопасности:

- управление доступом;
- управление передачей данных и операционными процедурами;
- управление активами;
- управление безопасностью сети;
- защита от вредоносного программного обеспечения.

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

- импульсные помехи, сбой и потеря электропитания серверного оборудования, на которых установлена ИС;
- 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 элементов оборудования, которые обеспечивают функционирования ИС;
- взлом ИС или ее составляющих;
- получение несанкционированного доступа к информации;
- внедрение вредоносного кода;
- удаление, порча либо модификация информации;
- недоступность информации;
- чрезвычайные ситуации.

8.7 Информационная безопасность каждой ИС, подключаемой к МИП, должна соответствовать требованиям, установленным в стандартах: O‘z DSt 2814, O‘z DSt 2815, O‘z DSt 2816, O‘z DSt 2817, O‘z DSt ISO 7498-2, 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/IEC 15408-3, O‘z DSt ISO/IEC 27001, O‘z DSt ISO/IEC 27002.

Управление безопасностью сети должно соответствовать требованиям, установленным в стандартах: O‘z DSt ISO/IEC 27033-2, O‘z DSt ISO/IEC 27033-3, O‘z DSt ISO/IEC 27033-4, O‘z DSt ISO/IEC 27033-5.

(Дополнен абзацем, Изм. № 1)

8.8 В целях обеспечения защиты информации, содержащейся в ИС, подключенных к МИП, участники взаимодействия:

- обеспечивают при обслуживании ИС, подключенных к МИП, 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 ИС, подключенных к МИП, только лицами, имеющими право доступа к информации, содержащейся в указанных ИС;

- принимают необходимые и достаточные меры, исключающие доступ посторонних лиц к защищаемой (в т.ч. парольной и ключевой) информации, хранящейся на используемых и внешних 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 ИС данного участника взаимодействия, подключенных к системе взаимодействия.

8.9 Для обеспечения полноценного функционирования инфраструктуры взаимодействия и подключенных к ней ИС, ИР и БД должны быть выполнены следующие мероприятия:

- оборудование должно быть расположено и защищено таким образом, чтобы уменьшить риски от воздействий окружающей среды и возможности несанкционированного доступа;

- силовые кабели и кабели телекоммуникаций, по которым передаются данные или осуществляются другие информационные услуги, необходимо защищать от повреждения или перехвата информации;

- должна осуществляться защита от электромагнитного, акустического и других видов излучения, рациональное размещение излучающих и облучающих объектов, исключающее или ослабляющее воздействие излучения на персонал, ограничение места и времени нахождения работающих в электромагнитном поле, защита расстоянием, т. е. удаление рабочего места от источника электромагнитных излучений, уменьшение мощности источника излучений, использование поглощающих или отражающих экранов; применение средств индивидуальной защиты;

- должен быть обеспечен механизм оперативного переключения в случае необходимости на резервный канал с сохранением функций обеспечения безопасности информации для всех каналов связи, выход из строя которых может существенно повлиять на доступность ИС, подключенных к МИП;

- в обязательном порядке должна проводиться оперативная замена оборудования, обеспечивающего криптографическую защиту каналов связи, используемых участником взаимодействия для осуществления информационного обмена в рамках МИП, в случае выхода его из строя;

- для обеспечения постоянной работоспособности и целостности должно проводиться надлежащее техническое обслуживание оборудования;

- должны быть регламентированы и четко определены процедуры восстановления после возможных сбоев, а также сформированы планы обеспечения непрерывной работы;

- резервное копирование конфиденциальной информации и программного обеспечения должно выполняться на регулярной основе в соответствии с согласованной политикой резервирования;

- должны быть определены соответствующие процедуры защиты документов, носителей информации, данных ввода/вывода и системной документации от повреждения, хищения и несанкционированного доступа.

8.10 ИС государственных органов, интегрируемых с МИП, предназначенные для обработки информации, отнесенной к конфиденциальной информации, подлежат обязательной аттестации в соответствии с требованиями информационной безопасности в установленном законодательством порядке.

УДК 004.031.42 ОКС 35.020 П 85

Ключевые слова: государственные органы, информационные системы, информационная безопасность, интеграция, межведомственная интеграционная платформа

Заместитель директора
Центра UZINFOCOM — Э.Ишимбаев

Начальник отдела
сопровождения и эксплуатации
Департамента по формированию
и развитию НИС — Ш.Абдувохидова

Главный специалист отдела
внедрения и интеграции
Департамента по формированию
и развитию НИС — В.Скобелева

Ведущий специалист отдела
обеспечения информационной
безопасности — О.Каримов

Нормоконтроль
ГУП «UNICON.UZ» — Л.Шаймарданова

СОГЛАСОВАНО

Начальник управления
информационно-коммуникационных
технологий Государственного
комитета связи, информатизации и
телекоммуникационных технологий
Республики Узбекистан

О.Умаров
письмо от 08.08.2014г.
№18-8/4754

СОГЛАСОВАНО

Начальник отдела информационной
безопасности Государственного
комитета связи, информатизации и
телекоммуникационных технологий
Республики Узбекистан

А.Гафуров
письмо от 01.08.2014г.
№14-8/4578

СОГЛАСОВАНО

Вр.и.о. директора
ГУП «UNICON.UZ»

Х.Хасанов
письмо от 29.07.2014г.
№31-04.1/1306

СОГЛАСОВАНО

Генеральный директор
Центра программистов BePro

А.Гафуров
письмо от 01.08.2014г.
№02-01/309

СОГЛАСОВАНО

Заместитель директора
Центра развития системы
«Электронное правительство»

Х.Исаев
письмо от 05.08.2014
№ 04-20/840

СОГЛАСОВАНО

Заместитель директора
Центра обеспечения информационной
безопасности

О.Мирзаев
письмо от 06.08.2014
№ 03-04-01/436

СОГЛАСОВАНО

Заместитель председателя
Службы национальной безопасности
Республики Узбекистан

А.Курбанов
письмо от 02.08.2014
№ 39/2752