ОДОБРЕНЫ

на заседании Правительственной комиссии по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности

протокол
от 23 июня 2021 г. № 2

Единые стандарты обмена информацией информационных систем с автоматизированной информационно-управляющей системой единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (АИУС РСЧС)

Москва 2021

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ

АИУС РСЧС – автоматизированная информационно-управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций;

ГО – гражданская оборона;

ГУ НЦУКС – Главное управление «Национальный центр управления в кризисных ситуациях» МЧС России;

МЧС России – Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;

ОИВ – органы исполнительной власти субъектов Российской Федерации;

ОМСУ – органы местного самоуправления;

ОПУ – организации (подразделения), создаваемые ФОИВ, ОИВ, ОМСУ и организациями для обеспечения их деятельности в области защиты населения и территорий от чрезвычайных ситуаций, управления силами и средствами, предназначенными и выделяемыми (привлекаемыми) для предупреждения и ликвидации чрезвычайных ситуаций, осуществления обмена информацией и оповещения населения о чрезвычайных ситуациях;

РСЧС – единая государственная система предупреждения и ликвидации чрезвычайных ситуаций;

СКЗИ – сертифицированные криптографические средства защиты информации;

ФОИВ – федеральные органы исполнительной власти;

ЧС – чрезвычайная ситуация.

1. Нормативно-правовые основы организации информационного взаимодействия в области защиты населения и территорий от ЧС

Настоящие Стандарты обмена информацией разработаны в соответствии с пунктом 3 постановления Правительства Российской Федерации от 30 ноября 2016 г. № 1272 для организации информационного взаимодействия. Участниками информационного взаимодействия являются органы повседневного управления РСЧС всех уровней.

В соответствии с постановлением Правительства Российской Федерации от 24 марта 1997 г. № 334 «О порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» сбор и обмен информацией осуществляются через ОПУ РСЧС. МЧС России координирует работу по сбору и обмену информацией, осуществляет сбор и обработку информации, представляемой ФОИВ и ОИВ.

В соответствии с пунктом 22 Положения, утвержденного постановлением Правительства Российской Федерации от 30 декабря 2003 г. № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций» информационное обеспечение в РСЧС осуществляется с использованием АИУС РСЧС.

Перечень передаваемой информации определяется двусторонними соглашениями об осуществлении информационного обмена (приложение № 1) и регламентами информационного взаимодействия (приложение № 2), заключаемыми МЧС России и его территориальными органами, ФОИВ, государственными корпорациями и организациями, ОИВ в соответствии с пунктом 9 Положения, утвержденного приказом МЧС России от 26 августа 2009 г. № 496 «Об утверждении Положения о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» (зарегистрировано в Минюсте России 15 октября 2009 г. № 15039).

2. Общие положения

2.1. Взаимодействие АИУС РСЧС с внешними информационными системами

Настоящие Стандарты определяют правила взаимодействия АИУС РСЧС с внешними информационными системами (далее – иные информационные системы).

Под взаимодействием АИУС РСЧС с иными информационными системами понимается совокупность информационных процессов, направленных на получение и использование оператором АИУС РСЧС (ГУ НЦУКС, установлен приказом МЧС России от 01 октября 2019 г. № 549 (с изм. от 23 марта 2020 г. № 199) информации, содержащейся в иных информационных системах, и включение такой информации в автоматизированном режиме в АИУС РСЧС, а также на получение и использование операторами иных информационных систем информации, содержащейся в АИУС РСЧС.

Взаимодействие АИУС РСЧС и иных информационных систем осуществляется:

на основании и в порядке, предусмотренном двусторонними соглашениями об осуществлении информационного обмена и регламентами информационного взаимодействия, заключаемыми оператором АИУС РСЧС и территориальными органами МЧС России с ФОИВ, государственными корпорациями и организациями, ОИВ на федеральном и региональном уровнях соответственно;

с учетом программно-технических средств АИУС РСЧС, используемых оператором АИУС РСЧС в интеграционном сегменте АИУС РСЧС (далее – подсистема информационного взаимодействия АИУС РСЧС).

Организация информационного взаимодействия осуществляется с использованием сертифицированных СКЗИ, а также должны быть выполнены требования нормативных правовых актов Российской Федерации в области защиты информации, не составляющей государственную тайну.

Состав, формат, сроки и способы обмена информацией, включая требования по защите информации, которая должна предоставляться в АИУС РСЧС и в иные

информационные системы, определяется двусторонними соглашениями об осуществлении информационного обмена и регламентами информационного взаимодействия (в т.ч. регламентами, заключенными в территориальных органах МЧС России) и не содержит сведений, составляющих государственную тайну.

Организация взаимодействия АИУС РСЧС и иных информационных систем осуществляется оператором АИУС РСЧС (операторами иных информационных систем):

самостоятельно или с привлечением учреждений (организаций), находящихся в их ведении, или иных учреждений (организаций)[1] в соответствии с законодательством Российской Федерации (с учетом обозначения в двусторонних соглашениях об осуществлении информационного обмена и регламентах информационного взаимодействия);

на принципах соблюдения полноты, достоверности предоставляемой информации (в информационных запросах и информационных сообщениях, установленных сроков ее предоставления), получаемой, обрабатываемой и размещаемой в рамках информационно-технологического взаимодействия, а также конфиденциальности информации, доступ к которой ограничен законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также о коммерческой тайне и иной охраняемой законом тайне.

2.2. Мероприятия, выполняемые оператором АИУС РСЧС

Оператор АИУС РСЧС реализует требования к технологиям информационного взаимодействия в подсистеме информационного взаимодействия АИУС РСЧС, в том числе к форматам представления информации в рамках данного сегмента.

Оператор АИУС РСЧС применяет программно-аппаратные средства, обеспечивающие целостность и достоверность передаваемых данных (сообщений) согласно настоящим Стандартам. Применяемые при разработке и использовании

---

[1] МЧС России обеспечивает полное исключение доступа иных учреждений (организаций), привлекаемых для организации взаимодействия, к сведениям АИУС РСЧС, содержащих персональные данные, владельцами которых являются ФОИВ и ОИВ.

интерфейсов технологии, стандарты и спецификации должны соответствовать нормативно установленным и общепринятым стандартами требованиям в области информационных технологий и программного обеспечения.

При разработке решений по взаимодействию АИУС РСЧС и иных информационных систем оператор АИУС РСЧС обеспечивает их соответствие требованиям нормативных правовых актов Российской Федерации в области защиты информации, не составляющей государственную тайну, и учитывать решения, заложенные в подсистему информационной безопасности АИУС РСЧС.

Оператор АИУС РСЧС обеспечивает фиксацию и хранение сведений об истории движения в подсистеме информационного взаимодействия АИУС РСЧС электронных сообщений, а также ведение журнала обращений пользователей системы к электронным сервисам подсистемы информационного взаимодействия АИУС РСЧС и электронным сервисам поставщиков (иных информационных систем).

В подсистеме информационного взаимодействия АИУС РСЧС оператором обеспечивается ведение реестров информационных запросов и информационных сообщений, наполнение хранилища данных АИУС РСЧС. Интерфейс администрирования подсистемы информационного взаимодействия предназначен для управления процессами информационного взаимодействия (запросов данных от иных информационных систем). Подсистема предоставляет возможность разграничения прав доступа пользователей к информации АИУС РСЧС, а также осуществляет настройку импорта данных в определенные поля различных типов объектов.

Доступ к подсистеме информационного взаимодействия предоставляется оператором АИУС РСЧС администратору АИУС РСЧС территориального органа или учреждения МЧС России (региональный уровень администратора) после выполнения требований по информационной безопасности (достигается путем обращения к оператору АИУС РСЧС и согласования с ним выполненного перечня). Порядок работы с подсистемой информационного взаимодействия определяется соответствующими инструкциями, которые разрабатываются оператором АИУС

РСЧС и доводятся до пользователей АИУС РСЧС информационными письмами в установленном порядке (внутренний документооборот организации регулируется локальными актами, распоряжениями, приказами и т.д., с внешними – соглашениями между сторонами).

2.3. Мероприятия, выполняемые в территориальных органах (учреждениях и организациях) МЧС России (региональный уровень)

Взаимодействие АИУС РСЧС и иных информационных систем (на региональном уровне) выполняется в соответствии с двусторонними соглашениями об осуществлении информационного обмена и регламентами информационного взаимодействия (заключенными на региональном уровне) с использованием сертифицированных СКЗИ, а также должны быть выполнены требования нормативных правовых актов Российской Федерации в области защиты информации, не составляющей государственную тайну.

Двусторонние соглашения об осуществлении информационного обмена и регламенты информационного взаимодействия, предусматривающие взаимодействие АИУС РСЧС и иных информационных систем (на региональном уровне), согласовываются с оператором АИУС РСЧС. К реализации взаимодействия АИУС РСЧС и иных информационных систем (на региональном уровне) возможно привлечение сторонних организаций (в соответствии с регламентами информационного взаимодействия, заключенных на региональном уровне).

До реализации взаимодействия АИУС РСЧС и иных информационных систем (на региональном уровне) общедоступная информация, получаемая территориальным органом или учреждением МЧС России в соответствии с двусторонними соглашениями об осуществлении информационного обмена и регламентами информационного взаимодействия регионального уровня, может быть передана оператору АИУС РСЧС (в т.ч. посредством протоколов ftp[2], sftp, ftps) для изучения и анализа структуры данных и последующей интеграции в АИУС РСЧС на федеральном уровне.

---

[2] Справочно: Способ двустороннего обмена данными между компьютерами – протокол File Transfer Protokol

Администратор АИУС РСЧС территориального органа, учреждения или организации МЧС России осуществляют контроль взаимодействия АИУС РСЧС и иных информационных систем (регионального уровня) в подсистеме информационного взаимодействия. Доступ к подсистеме информационного взаимодействия другим пользователям АИУС РСЧС не предоставляется. Администратор АИУС РСЧС (регионального уровня) определяется нормативным документом территориального органа или учреждения МЧС России.

2.4. Мероприятия, выполняемые оператором иной информационной системы

Для подключения иной информационной системы к подсистеме информационного взаимодействия АИУС РСЧС ее оператор (поставщик или потребитель), согласно регламенту информационного взаимодействия, разрабатывает интерфейсы взаимодействия с подсистемой взаимодействия АИУС РСЧС в соответствии с настоящими Стандартами.

Защита информации от несанкционированного доступа в зоне ответственности оператора иной информационной системы обеспечивается в соответствии с руководящими документами в области информационной безопасности в Российской Федерации.

При необходимости, для организации информационного взаимодействия, допускается проводить предварительные мероприятия по планированию совместных решений по защите информации.

Операторы иных информационных систем обеспечивают передачу в зоне своей ответственности информации, предусмотренной для включения в АИУС РСЧС, оператору АИУС РСЧС в соответствии с настоящими Стандартами.

Обязанность оператора иной информационной системы по предоставлению информации для включения в АИУС РСЧС в установленный срок считается выполненной со дня регистрации в реестре информационных сообщений подсистемы информационного взаимодействия АИУС РСЧС соответствующего сообщения,

полученного от оператора иной информационной системы и содержащего необходимую информацию.

В случае непредставления оператором иной информационной системы информации или предоставления информации с нарушением установленного срока оператор такой системы обязан обосновать причины непредставления указанной информации в АИУС РСЧС.

3. Требования к взаимодействию информационных систем с АИУС РСЧС

Взаимодействие иных информационных систем с АИУС РСЧС осуществляется с использованием распределенного программного брокера сообщений (например, Apache Kafka), унифицированных структурированных открытых форматов для передачи данных (единых форматов для информационного взаимодействия) на основе расширяемого языка разметки (XML и RDF), типы и описание которых размещаются оператором АИУС РСЧС в системе в разделе «Справочная информация» в срок не позднее чем за 14 дней до момента начала использования таких форматов в АИУС РСЧС.

При взаимодействии иных информационных систем с АИУС РСЧС прием и передача информации должны осуществляться с использованием стандартных сетевых протоколов передачи данных, в том числе:

а) протокола передачи гипертекста (HTTP[3]) версии 1.1 или выше;

б) расширенного протокола передачи гипертекста (HTTPS[4]) с обеспечением безопасности транспортного уровня (TLS[5]) версии 1.0 или выше.

При разработке веб-сервисов для взаимодействия иных информационных систем с АИУС РСЧС необходимо придерживаться следующих форматов и протоколов:

---

[3] Справочно: Протокол передачи гипертекста - Hypertext Transfer Protocol (HTTP)
[4] Справочно: Расширение протокола HTTP, поддерживающее шифрование
[5] Справочно: Безопасность транспортного уровня обозначается TLS (Transport Layer Security)

1. Для взаимодействия по XML:

протокол обмена структурированными сообщениями (SOAP[6]) версии 1.1 или выше;

язык описания веб-сервисов и доступа к ним (WSDL[7]) версии 1.1 или выше;

расширяемый язык описания схем данных (XSD[8]) версии 1.0 или выше.

2. Для взаимодействия по RDF:

открытый протокол обмена структурированными сообщениями – стандарт Консорциума Всемирной паутины World Wide Web Consortium (W3C) https://www.w3.org/TR/sparql11-protocol/;

язык описания электронных сервисов – стандарт Консорциума Всемирной паутины World Wide Web Consortium(W3C) https://www.w3.org/TR/2012/REC-owl2-overview-20121211/;

модель представления данных https://www.w3.org/TR/rdf11-mt/.

3. Для взаимодействия по JSON:

Для передачи связанных данных – форматы JSON и JSON-LD, которые являются рекомендацией Консорциума Всемирной паутины World Wide Web Consortium (W3C) https://json-ld.org/.

Для повышения качества и унификации данных, а также расширения возможностей их использования предлагается использование технологий связанных данных (Linked Data) – онтологий для описания предметной области.

Введение общего для всей системы описания предметной области (списки объектов, их свойств, связей, типов данных, правил проверки корректности объектов и т.д.) на базе языка описания онтологий OWL позволит:

стандартизировать структуру объектов и связей при обмене;

---

[6] Справочно: Протокол обмена структурированными сообщениями (Simple Object Access Protocol, SOAP) опубликован по адресу в информационно-телекоммуникационной сети Интернет: http://www.w3.org/TR/soap/

[7] Справочно: Язык описания электронных сервисов версии 1.1 (Web Services Description Language, WSDL 1.1) опубликован по адресам в информационно-телекоммуникационной сети Интернет: http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html, http://www.w3.org/TR/wsdl

[8] Справочно: Язык описания схем данных (XML Schema Definition, XSD) - один из языков описания структуры электронных сообщений

повысить оперативность подключения внешних информационных систем за счет отсутствия необходимости сложной конвертации данных;

повысить унификацию данных и, как следствие, упростить дальнейшую разработку и поддержку системы;

использовать возможности семантического поиска;

использовать единое описание предметной области для хранения связанных данных и реляционных данных.

Для предотвращения снижения качества онтологии (повышения избыточности и семантического дублирования описаний) процесс внесения изменений в онтологию предлагается централизовать – все изменения вносятся единым владельцем онтологии.

При подключении иных информационных систем, содержащих данные, предметная область которых еще не отражена в онтологии, предлагается внедрить этап разработки описания предметной области. Владелец данных осуществляет описание предметной области и интегрируемых данных. При этом разработанное описание согласовывается с владельцем онтологии перед непосредственной разработкой механизма интеграции владельцем данных и проведением испытаний.

Для обеспечения единого доступа, поиска, обмена и предоставления геопространственных данных по HTTP протоколу в виде графического изображения, тайлов, пространственной информации в сети TCP\IP, а также описания условий получения геоданных и описания характеристик сервера по предоставлению этих данных, метаданных, пространственной информации об объектах карты в виде набора атрибутивной, описательной и векторной информации рекомендуется использовать стандарты W3C помимо OGC WMS, OGC WMTS, OGC WFS, OGC WFS-T, OGC WCS, TMS(OSGeo).

4. Перечень используемых нормативных правовых актов Российской Федерации

Федеральный закон Российской Федерации от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон Российской Федерации от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Указ Президента Российской Федерации от 11 июля 2004 г. № 868 «Вопросы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий»;

Указ Президента Российской Федерации от 21 января 2004 г. № 21 (ред. от 05.06.2020) «О структуре федеральных органов исполнительной власти»;

Постановление Правительства Российской Федерации от 24 марта 1997 г. № 334 «О порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

Постановление Правительства Российской Федерации от 30 декабря 2003 г. № 794 «О единой государственной системе предупреждения и ликвидации чрезвычайных ситуаций»;

Постановление Правительства РФ от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия»;

Постановление Правительства Российской Федерации от 30 ноября 2016 г. № 1272 «Об утверждении правил обеспечения на федеральном уровне Национальным центром управления в кризисных ситуациях координации деятельности органов

повседневного управления единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций и органов управления гражданской обороной, организации информационного взаимодействия федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций»;

Основы государственной политики Российской Федерации в области защиты населения и территорий от чрезвычайных ситуаций на период до 2030 года, утвержденные Указом Президента Российской Федерации от 11 января 2018 г. № 12;

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646;

Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении Требований к системам обнаружения вторжений»;

Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении Требований к средствам антивирусной защиты»;

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ Минэкономразвития России от 9 января 2018 г. № 10 «Об утверждении Требований к описанию и отображению в документах территориального планирования объектов федерального значения, объектов регионального значения, объектов местного значения и о признании утратившим силу приказа Минэкономразвития России от 7 декабря 2016 г. № 793»;

Приказ МЧС России от 26 августа 2009 г. № 496 «Об утверждении Положения о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» (зарегистрирован в Министерстве юстиции Российской Федерации 15 октября 2009 г. № 15039);

Приказ МЧС России от 1 октября 2019 г. № 549 (с изменениями от 23 марта 2020 г. № 199) «О вводе в постоянную (промышленную) эксплуатацию

и утверждении Положения о Многоуровневом сегменте АИУС РСЧС-2030 на федеральном, межрегиональном и региональном уровнях»;

Приказ МЧС России от 11 июня 2020 г. № 410 «Об организации информационного обмена между Министерством Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и федеральными органами исполнительной власти, государственными корпорациями и организациями»;

Распоряжение МЧС России от 10 февраля 2020 г. № 89 «Об утверждении Регламента функционирования и эксплуатации автоматизированной информационно-управляющей системы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций».