ВЫЯВЛЕННЫЕ ПРОБЛЕМЫ РАЗРАБОТКИ ПРОГРАММ ФОРМИРОВАНИЯ ЕДИНОГО ЦИФРОВОГО ПРОСТРАНСТВА ЕАЭС

[1]Сарьян В.К., [1]Назаренко А.П., [2]Головин С.А.,

[3]Бородин А.С.

[1,2]Федеральное государственное унитарное предприятие Ордена Трудового Красного Знамени научно-исследовательский институт радио (ФГУП НИИР), 105064, Россия, Москва, улица Казакова, 16, e-mail: info@niir.ru

[2]Межотраслевой совет по техническому регулированию и стандартизации в сфере информационных технологий, 22-ой ТК Росстандарта, 119333, г.Москва, ул. Вавилова, д.44, корп. 2

[3]ПАО Ростелеком, ПК «Информационные технологии в интернете вещей» 22-ой ТК Росстандарта, 119333, г. Москва, ул. Вавилова, д.44, корп. 2

В статье описаны проблемы, возникшие в экономиках государств и содружествах (США, АТЭС, ЭС, ЭСКАТО, АСЕАН), приступивших к формированию цифрового пространства (цифровой экономики, информационного общества) раньше, чем ЕАЭС.
Намечены пути решения этих проблем.

Ключевые слова: цифровая экономика, цифровое пространство, информационное общество, ЕАЭС, устойчивое развитие, информационно-управленческая сеть.

PROBLEMS TO BE SOLVED DURING DEVELOPING OF PROGRAMS FOR CREATION OF A SINGLE DIGITAL SPACE WITHIN EAEU

[1]Sarian V.K., [1]Nazarenko A.P., [2]Golovin S.A., [3]Borodin A.S.

[1]Federal State Unitary Enterprise Radio and Research Development Institute (NIIR), 105064, Russia, Moscow, Kazakova street, 16, e-mail: info@niir.ru

[2]Intersectoral Council for Technical Regulation and Standardization in the field of information technologies

[3]OJSC Rostelecom

This paper describes the problems that emerged in economies and the communities, such as the United States, APEC, EC, ESCAP, ASEAN, which start to form digital space (digital economy, information society) before the EAEU. The article describes the causes of these problems and provides possible solutions, which were approved by the International Telecommunication Union, APEC, ESCAP, ASEAN and others. Finally, a proposal on creating a system of administration of a united digital space will be described.

Key words: digital economy, digital space, information society, EAEU, sustainable development, information and control network.

27 октября 2916 года на форуме «Евразийская неделя -2016» состоялась представительная конференция «Цифровая повестка в ЕАЭС», на которой была принята Декларация с таким же названием [1].

Целесообразно в преддверии начала практических работ рассмотреть серьезные проблемы, с которыми столкнулись все страны и содружества, например, такие как США, АТЭС, ЭС, ЭСКАТО, АСЕАН, которые начали формировать цифровые пространства раньше ЕАЭС. Опыт создания цифрового общества изучает и анализирует также и МСЭ. Ниже приведен анализ ситуации, описана проблема роста социально-незащищенных людей и опасность этого роста для устойчивого развития стран.

В последнее время ИКТ все в большей степени становятся определяющим фактором развития всех государств мира, в том числе и ЕАЭС. ИКТ все глубже проникают в нашу повседневную социально-экономическую жизнь, внося заметные изменения, становятся определяющим фактором в том, что касается потребностей, интересов, знаний и навыков людей.

Развивая и внедряя все новые ИКТ, в основном за государственный счет, компании ИКТ-индустрии весьма правдоподобно убеждают общественность, что очередной виток развития ИКТ ведет к повышению жизненного уровня населения страны [2]. Однако, социологические и статистические измерения фиксируют постоянный рост макроэконо- и макросоциальных диспаритетов и численности социально-незащищенных

групп населения, одинаково как в развитых, так и в развивающихся странах [3]. Глобальный режим неэквивалентного экономического и технологического развития создает, поддерживает и умножает очаги социальной напряженности на планете. Развитые страны тратят огромные бюджетные ресурсы на пособия для поддержки социально незащищенных слоёв граждан в своих странах.

Однако «тушение» социального пожара с помощью денег не может кардинально изменить ситуацию. Количественное увеличение социально незащищенных слоёв граждан связано не только с ухудшением материального достатка, но и заметным снижением их социального капитала, отсутствием перспективы попасть на неэффективно действующие социальные лифты. Последнее обстоятельство особенно важно для молодого поколения социально незащищенной категории граждан [3].

В этой связи необходимо упомянуть еще один жизненно важный аспект угрожающей социальной дифференциации. При возникновении чрезвычайных и катастрофических ситуаций природного или техногенного происхождения социально незащищенные слои населения оказываются в самом уязвимом положении [4, 5] . Понятно, что возникновение социальных волнений в одной из стран ЕАЭС надолго может замедлить формирование единого цифрового пространства.

Корни парадокса ИО лежит в том, что сегодняшняя направленность развития ИКТ, нацеленная на получении максимальной прибыли, объективно влечет за собой использование все новых и новых по возможностям дорогих абонентских терминалов, каналов связи и услуг, которые становятся недоступными все большему количеству граждан, в том числе и по образовательному уровню [6, 7, 9]. При этом все услуги, даже социально-значимые, стараются перевести на новые технологии, а получение этих услуг по «старым» технологиям становится дороже, чем прежде. Иногда они попросту перестают функционировать, так как оказываются для провайдеров менее эффективными, чем новые. Таким образом, оказывается, что численность социально незащищенной группы населения заметно растет при каждом новом витке развития ИКТ.

В то же время возможности ИКТ и тот потенциал, который сегодня накоплен, может сделать ИКТ действенным инструментом повышения жизненного уровня социально незащищенных групп населения. Для этого оказывается только надо поставить задачу: при развитии новых ИКТ учитывать интересы социально незащищенных групп населения. Авторами разработана и исследована информационно-управленческая сеть (ИУС) - комплекс программно-аппаратных и организационных решений по построению сети, предназначенной для предоставления социально значимых ИК услуг широкому кругу пользователей через широковещательный телевизионный канал путем передачи дополнительной информации, которую абоненты могут получать по сети телевещания с помощью обычного цифрового телевизора, а интерактивное взаимодействие с абонентами организуется с помощью узкополосного обратного канала, в качестве которого может быть использован любой доступный абоненту узкополосный канал передачи данных[2].

ИУС является более удобным вариантом оказания социально-значимых ИК услуг для социально необеспеченных людей, чем широко используемые сети в силу ряда достоинств:

- ИУС строится на базе существующей инфокоммуникационной системы, для доступа к наиболее необходимым социально значимым услугам абонентам ИУС необходим лишь цифровой телевизионный сигнал, которым, к 2020 году будет охвачено почти 100% населения страны и цифровой ТВ-приемник;
- ИУС позволяет организовать доверенную среду предоставления ИК услуг социально незащищенным пользователям, в которой за счет эффективного администрирования услуг минимизируются риски этой категории пользователей;
- применяемые в ИУС технические решения позволяют значительно снизить требования к оборудованию пользователей и каналам передачи данных;
- ИУС позволяет обеспечить социально-незащищенные группы населения эффективной защитой от ЧС [7].

В странах ЕАЭС в связи с повсеместным переходом с аналогового на цифровую систему телевизионного вещания появляется уникальная возможность быстрого развёртывания ИУС по всей территории страны без значительных затрат. На базе ИУС могут быть оказаны любые социально-значимые услуги, традиционно оказываемые сегодня через персональные компьютеры и мобильные телефоны, айфоны и т.д. ИУС была утверждена в качестве рекомендации в 2015 году Международным Союзом Электросвязи [8].

Созданием и эксплуатацией таких сетей мог бы заняться созданный в рамках ЕАЭС межгосударственный консорциум.

Вторая серьезная проблема связана с заметным возрастанием риска материальных и людских потерь при возникновении ЧС природного и техногенного происхождения. Связано это со следующими объективными причинами:

• мировой тенденцией урбанизации населения Земли – по данным ООН свыше 78% населения к 2040-2050 г.г. будут жить в крупных городах,

• из года в год стремительно растет техногенность среды обитания - следствие развития техники, результат применения различных технологий производства,

• отмечается, пока по неизвестным причинам, рост частоты ЧС природного происхождения в общем в мире и в странах АТЭС, в частности;

• сегодня международное сообщество придерживается концепции «ненулевого риска», (какие бы меры не были предприняты, ЧС природного и техногенного происхождения в какой-то несчастливый момент может произойти в любом регионе мира), а это значит, что ЧС может коснуться каждого жителя планеты,

• каждый год ЧС, особенно вызванные глобальными процессами природного и техногенного происхождения (например, землетрясения и наводнения), являются источниками непомерно больших материальных и людских потерь в разных частях Земли, при этом потери оказываются одинаково высокие как для развитых, так и для развивающихся стран.

Поэтому международное сообщество и отдельные страны уделяют огромное внимание разработке и эксплуатации систем мониторинга глобальных процессов, оповещения населения о ЧС и ликвидации последствий, основанных на инфокоммуникационных технологиях (ИКТ). Однако все принимаемые меры не могут пока повысить предсказательный потенциал существующих систем до хозяйственного значения, и каждый раз очередное ЧС является катастрофическим сюрпризом, как для администрации, так и для всего населения района, в котором случилось ЧС. Надо отметить, что природные ЧС часто сопровождаются техногенными ЧС. Особенно большие потери - в крупных городах.

Надо учесть еще одну причину больших потерь для стран, которые подвергаются ударам катастроф техногенного и природного происхождения. Дело в том, что усилия государств по развитию средств мониторинга и предупреждения о возникновении ЧС оказываются часто малоэффективными, так как граждане (в том числе и обслуживающий персонал), оказавшиеся в зоне ЧС и даже предупрежденные о ЧС, становятся беспомощными, сразу забывают все инструкции и, в итоге, часто оказываются жертвами этих ЧС. Это явление, как правило, при дальнейшем анализе ЧС, квалифицируют как «человеческий фактор». Причем, снова подчеркнем, это явление одинаково характерно как для развитых, так и для развивающихся стран. Достаточно вспомнить недавние трагические события в Японии, США, Китае, России, Южной Корее, Гватемале, Пакистане, Тайване и др.

Учитывая:

• стремительные, как было отмечено выше, темпы урбанизации,

• громадные затраты, которые тратятся в мире на науку о Земле и на развитие систем (в том числе и ИКТ) мониторинга глобальных процессов,

• усилия МЧС,

человечество не может далее мириться с получаемыми низкими результатами и настоятельно требует от ученых поиска нового решения.

Решение этого жизненно важного вопроса было найдено построением сценария и бизнес модели индивидуализированной услуги управления спасением каждого абонента с помощью IoT [9, 10].

Для того чтобы описать сценарий и бизнес модель этой услуги рассмотрим временные этапы ЧС:

1. время до возникновения ЧС, включая время предсказания места и времени ЧС,
2. время ЧС, включая катастрофическую фазу,
3. время ликвидации последствий ЧС.

Предоставляемые сегодня услуги по спасению людей (например, услуга по оповещении ЧС) практически не управляют спасением людей во время протекания ЧС, хотя наибольшие потери населения происходят именно во время протекания ЧС.

Вначале услугу индивидуализированного управления во время возникновения ЧС с использованием IoT удалось создать для ЧС, у которых временной участок между началом ЧС и ее катастрофической фазой не менее 10 минут. Это могут быть ЧС техногенного характера такие, например, как пожар, утечка вредных веществ и др., которые могут возникнуть в каком-то объекте, в отдельном здании или городе в целом.

Опишем сценарий предоставления индивидуализированной услуги для этого случая. При обнаружении первых признаков ЧС, датчики IoT, расположенные в каждом помещении объекта (определенном участке территории) и объединенные в самоорганизующиеся сенсорные сети [11], где произошло ЧС, начинают взаимодействовать с терминалами каждого абонента, определяя его координаты, и сообщают терминалу изменение своих характеристик под влиянием изменения параметров внешней среды. В память абонентского терминала записывается модель развития данного типа ЧС в данном объекте, составленную и

утвержденную официальными представителями МЧС и также утвержденную цифровую модель данного объекта. Происходит автоматическая идентификация полученных данных с имеющейся моделью и фиксируется наличие начальной стадии ЧС. Используемые датчики (или линейка датчиков) должны обладать большим предсказательным потенциалом (большей чувствительностью) чем существующие датчики и тем самым увеличивается отрезок времени между моментом фиксации начала ЧС и моментом наступления его катастрофической фазы. В данном помещении (пространстве), где возникло ЧС, могут оказаться люди разного статуса (служащие, имеющие определенные предписания в случае возникновения ЧС), случайные здоровые посетители, которые могут не знать расположение того объекта, где их застало ЧС, посетители с ограниченными возможностями по здоровью, слуху, зрению. Поэтому, чтобы не создавать давку, одновременно сообщив им всем о начале ЧС, и решить проблему коллизий управляющие сигналы, которые поступают от датчиков IoT на абонентские терминалы пользователей услуг, вначале актуализируются у обслуживающего персонала и людей с ограниченными возможностями. У первых в абонентских устройствах автоматически, на основе записанных у них в абонентском терминале инструкций, формируются управляющие сообщения, что им надо делать в сложившейся обстановке, и указывается маршрут, с помощью цифровой модели здания (пространства) по которому он должен следовать. После выполнения им предусмотренных ему действий, ему указывается план эвакуации. На терминалы людей с ограниченными возможностями приходят управляющие сигналы, показывающие ему безопасный план эвакуации. При этом программное обеспечение услуги в терминале данного абонента при формировании плана эвакуации учитывает особенности и характер ограниченных возможностей данного человека [12]. Затем после некоторой паузы управляющие сигналы поступают на абонентские терминалы других людей (здоровых), оказавшихся в зоне ЧС и также на основании их текущего места пребывания в зоне ЧС и темпов и характера развития ЧС автоматически формируется индивидуальный маршрут в направлении безопасной зоны. Во все время предоставления услуги происходит непрерывное взаимодействие абонентского терминала с датчиками IoT. Это позволяет в реальном времени автоматически корректировать в зависимости от темпа и направления развития ЧС. При этом, все транзакции между абонентами и IoT датчиками сенсорной самоорганизующейся сети передаются через терминал сотовой связи, который соединен с сенсорной сетью в центр МЧС. Эти данные окажутся очень полезными для сотрудников МЧС на стадии ликвидации последствий ЧС.

Отметим также, что при возникновении ЧС абонентские терминалы людей, оказавшихся в зоне ЧС, принудительно отключаются от сотовой сети первым управляющим сигналом, полученным абонентским терминалом от IoT датчиков. Этим достигается автономность управления, что оказывается очень важной в условиях ограниченного времени – времени определяемой темпами развития ЧС до катастрофической фазы.

Если ЧС возникает вне зоны, то сценарий предоставления индивидуализированных услуг по спасению абонента при возникновении ЧС немного меняется: сигнал из аналитического центра о ЧС, возникшей на удалении от данного места, где находятся абоненты, подключенные к услуге индивидуализированного управления спасением людей при возникновении ЧС, поступает по каналам сотовой связи на вход сенсорной сети [13]. По этой сети данные сигналы через датчики IoT, расположенные по объекту, поступают на абонентские терминалы абонентов. В этих сигналах содержаться сведения о типе ЧС, ее координатах, текущие метеоданные и др. В абонентских терминалах, в которых записаны возможные варианты такого типа ЧС, автоматически формируется, как и в предыдущем случае, управляющая информация, указывающая выход в подобной ситуации.

Отличие сценария предлагаемой услуги от существующих, заключается в том, что предлагаемая услуга обеспечивает динамическое, в реальном масштабе времени, персонализированное управление эвакуацией людей непосредственно во время ЧС.

Таким образом, подключение к данной услуге может обеспечить пользователям управление их самостоятельным выходом из опасной зоны ЧС. При значении промежутка времени между началом ЧС и моментом наступления его катастрофической фазы, (будем называть его критическим и обозначим, как T_k), T_k = 10 минутам можно вывести из опасной зоны до 90 % людей до наступления катастрофической фазы. Естественно, что при достижении значения $T_k >> 10$ минут можно достичь лучших результатов.

Но услуга индивидуализированного управления спасением людей при возникновении ЧС бессильна, если отрезок времени между началом ЧС и началом его катастрофической фазы приближается к нулю, то есть $T_k \approx 0$. А именно это значение T_k характерно для таких разрушительных катастроф, как например, землетрясения, которые приносят наибольшие людские и материальные потери.

Для того, чтобы расширить возможность применения услуги индивидуализированного управления спасением людей при возникновении ЧС на случай близко к нулевому отрезку времени между началом ЧС и

ее катастрофической фазы ($T_k \approx 0$), необходимо резко повысить предсказательный потенциал существующих систем мониторинга за такими типами ЧС. Повышение предсказательного потенциала связано с поиском и фиксацией сигналов предвестников ЧС с $T_k \approx 0$, например землетрясений. Однако используемые сегодня датчики малочувствительны и к сигналам-предвестникам землетрясений, в датчиках они отражаются на фоне шумов. Поэтому разрабатываются различные математические методы для выявления на фоне шумов сигналов-предвестников землетрясений. Значительная часть методов основана на анализе канонических когерентностей многомерных спектральных матриц и канонических корреляций коэффициентов вейвлет-разложений сигналов, как в скользящих временных окнах, так и по всей выборке. Целью этих алгоритмов является выделение очень слабых нестационарных сигналов общего происхождения, имеющих как гармоническое поведение, так и резко нестационарного, всплескового характера, в многомерных временных рядах мониторинга с определением их характерных периодов (временных масштабов). Последним главным результатом применения предлагаемой методики [14] явилась разработка нового метода (метода синхронизации оценки сейсмической опасности. Этим методом, автором Любушиным А.А., был разработан верный прогноз мега-землетрясения 11 марта 2011 года в Японии [15]. Развивая теорию синхронизации, как эффективного способа выявления сигналов-предвестников землетрясений, Любушин А.А. предположил, что эффект синхронизации будет особенно эффективным, если сигналы, получаемые от существующих датчиков будут складываться в реальном масштабе времени с сигналами датчиками другой (нежели существующие датчики) физической природы и расположенных поблизости от существующих датчиков. Основная идея использования датчиков разной физической природы заключается в том, что сигналы-предвестники являются общим для них модулирующим сигналом.

В качестве таких датчиков – датчиков разной физической природы Назаренко А.П. и Сарьян В.К. предложили использовать датчики IoT [15]. В качестве таких датчиков в соответствии с определением IoT, могут быть использованы любые живые (включая человека) и косные объекты природы, которые могут оказаться очень чувствительными к определенным типам сигналов-предвестников. Поэтому предлагается использовать объединенный датчик IoT (т.е. панель, состоящую из разного типа датчиков, одни из которых при реальных обстоятельствах могут оказать более чувствительными к данным сигналам-предвестникам, чем другие) для дополнения к существующим датчикам.

Сигналы- предвестники землетрясений модулируют синхронно существующие датчики и периодические жизненные (естественные) процессы, которые проистекают в датчиках IoT, входящих в панель. Сложение этих сигналов дает эффект синхронизации и позволяет выявить наличие и мощность сигналов-предвестников землетрясений, что позволит определить с достаточной (от 2 часов до 10 минут) точностью не только время наступления землетрясения, но и его силу и место эпицентра.

В этом случае, то есть, если у данного ЧС, $T_k \approx 0$, то сценарий предоставления индивидуализированной услуги по управлению спасением абонента, описанного для случая $T_k \geq 10$ минут дополняется следующими действиями:

- формируется в аналитическом центре гибридной мониторинговой сети, путем обработки данных гибридной мониторинговой системы, информация о времени, силе и эпицентре землетрясений;
- эта информация передается по каналам связи, в том числе и по каналам сотовой связи на вход сенсорной сети;
- далее через датчики IoT эта информация поступает на абонентский терминал людей могущих в скором времени оказаться в зоне землетрясения, и автоматически вырабатываются индивидуальные управляющие сигналы, как лучше поступить в сложившейся ситуации, чтобы своевременно выйти из опасной зоны.

Таким образом, сценарий действия услуги индивидуализированного управления спасением абонентов, оказавшихся или могущих оказаться через короткое время в зоне ЧС, действует даже при $T_k = 0$.

Рассмотрим возможную бизнес-модель этой услуги и участников ее формирования и администрирования. Как следует из сценария услуги, формировать массовую услугу индивидуализированного управления спасением людей должны следующие участник инфокоммуникационного рынка:

- операторы связи, в том числе и операторы сотовой связи,
- разработчики прикладного программного обеспечения функционирования инфраструктуры предоставления услуг и абонентских терминалов,
- аналитический центр МЧС,
- разработчики цифровых моделей зданий и местности,
- отбор и моделирование датчиков IoT, используемых для мониторинга окружающей среды,

• разработчики оцифровки моделей развития разных типов ЧС в данном объекте (в данной местности), если эти модели существуют, и представления таких моделей в цифровом виде (эти модели должны быть утверждены компетентными организациями МЧС),

• разработчики инструкций по поведению людей на объекте (местности) при возникновении разных типов возможных ЧС (результаты этой работы тоже должны быть утверждены компетентными организациями МЧС), эти рекомендации могут автоматически поступать на терминал абонента при изменении им местоположения, которое фиксирует приемник ГЛОНАСС или записываться на терминал абонента при входе в какой-то объект,

• важное значение в представлении этой услуги имеет организация и эффективное функционирование системы администрирования этой услуги, эту функцию должно взять на себя какая-то структура МЧС,

• организации ГЛОНАСС,

• медицинские учреждения, которые разрабатывают для абонентов специальные рекомендации по поведению при различных ЧС, эти данные записываются в терминал абонента, пользователя услуги индивидуализированного управления спасением (поведением людей при возникновении ЧС,

• операторы обновляют в реальном времени геоданные по показаниям приемника ГЛОНАСС.

При формировании бизнес модели монетизации этой услуги надо иметь ввиду два обстоятельства:

• эта услуга должна быть массовой,

• она действует только в условиях возникновения ЧС, в остальных случаях она законсервирована, но требует постоянного внимания и модернизации при необходимости.

Поэтому цена этой услуги, учитывая и доходы всех участников формирования, предоставления и администрирования услуги индивидуализированного управления спасением абонента при возникновении ЧС, должна быть доступна массовому пользователю. Возможно, что за пользование этой насущной услугой социально незащищенной части населения будет доплачивать социальные службы. В любом случае, из-за беспрецедентной востребованности этой услуги все участники предоставления услуг будут в выигрыше, а государство существенно сократит людские и материальные потери от ЧС природного и техногенного характера. Может быть, целесообразно создать внутри ЕАЭС международные консорциумы заинтересованные в формировании, предоставлении и администрировании этой услуги на территории ЕАЭС.

Мы подробно описали этот проект, так как его внедрение обеспечивает всем жителям, и следовательно, пользователям формируемого единого цифрового пространства ЕАЭС повышенную защиту при возникновении ЧС природного и техногенного происхождения.

Таким образом, показано, что используя обычные штатные аппаратно-программные средства ИКТ, из которых будет формироваться инфраструктура единого цифрового пространства, можно решить, возникшие перед разработчиками цифрового пространства: заметный численный рост социально незащищенных групп населения и значительное повышение риска человеческих и материальных потерь при возникновении ЧС. Используя эти или другие решения этих проблем уже на ранней стадии формирования цифрового пространства мы способствуем достижению целей устойчивого развития, провозглашенного ООН.

Недавний случай, первый зафиксированный на территории случай, мощной кибератаки на банковские сервера и сервера некоторых ведомств. Приведем цитату [16] «На прошлой неделе сразу несколько крупных российских банков, включая Сбербанк, банк «Открытие» и Альфа-банк, подверглись необычной хакерской атаке. Согласно оценке «Лаборатории Касперского», в последнюю атаку на российские банки было вовлечено 24 тыс. устройств. Некоторые банки подверглись атакам неоднократно - компания зарегистрировала серии от двух до четырех атак с небольшим интервалом и продолжительностью до 12 часов. «Их мощность достигала 660 тыс. запросов в секунду, при этом есть основания считать, что это далеко не предел», — отмечали представители «Лаборатории Касперского». К серьезным последствиям в работе финансовых учреждений попытки взлома не привели, но оказались прецедентными в другом смысле. 10 ноября ЦБ официально подтвердил, что эта DDoS-атака была совершена с помощью устройств, относящихся к интернету вещей. Это первый официально признанный случай в России, когда в преступных целях могли использоваться «умный холодильник, smart-TV, охранная система входной двери или даже лампочка».

Подобным хакерским атакам подвергся и сайт Роскомнадзора и др. ведомств. Это событие позволяет нам, рассмотреть еще один вопрос, который то же целесообразно рассмотреть на начальном этапе формирования единого цифрового пространства. Мы предлагаем рассмотреть возможность создания единого органа, который помимо собственно формирования единого цифрового пространства, занялся бы созданием системы администрирования услуг в этом едином пространстве, в том числе и проводил анализ

влияния внедрению новых технологий на национальном уровне на устойчивость работы единого цифрового пространства в целом.

В заключение сформулируем выявленные при разработке программ формирования единого цифрового пространства ЕАЭС проблемы:

1) заметный рост социально-незащищенных групп населения и

2) повышение риска материальных и людских потерь при возникновении ЧС природного и техногенного происхождения.

Без решения этих проблем, с которыми обязательно столкнется ЕАЭС, решить задачу достижения устойчивого развития в ЕАЭС будет невозможно, поэтому превентивные меры надо предусмотреть на самом старте формирования единого цифрового пространства.

Следовательно, необходимо создание системы администрирования функционирования единого цифрового пространства

Список литературы

1. Цифровая декларация ЕАЭС, http://www.eurasiancommission.org/ru/act/dmi/workgroup/Pages/default.aspx
2. Бутенко В.В., Назаренко А.П., Сарьян В.К. и др. Проблемы возникающие при внедрении новых технологий и пути их решения, 23-я Региональная европейская конференция Информационного общества. Международное телекоммуникационное общество, Вена, 2012.
3. Бутенко В.В., Назаренко А.П., Сарьян В.К. и др. Проблемы, возникающие при внедрении новых технологий в инфокоммуникационном сообществе / Труды НИИР, №1, 2011.
4. Левашов В.К**.** Социально-политические риски устойчивого развития / Вестник РАН, Наука, Москва, 2014, № 2, т. 84, с. 143 – 152.
5. Сарьян В.К., Левашов В.К., Головин С.А., Бородин А.С. Необходимость разработки социотехнических стандартов / Труды НИИР, № 2, 2016 г.
6. Сарьян В.К., Левашов В.К. Внедрение технологий Интернета –вещей и показатели развития информационного общества, Сборник трудов 6-ой Международной конференции «ИТ – Стандарт 2015».
7. Назаренко А.П., Сарьян В.К. Массовая услуга – индивидуализированного управления спасением людей при угрозе или возникновении ЧС природного и техногенного происхождения / Труды НИИР №3, 2016.
8. Рекомендация МСЭ-Т Y.2239 Требования информационно-управленческих сетей и их приложений, 2015.
9. Бутенко В.В., Назаренко А.П., Сарьян В.К. и др. Индивидуальная безопасность в чрезвычайных ситуациях / Новости МСЭ, №3, 2012, с. 47-49.
10. Приложения беспроводных сенсорных сетей в сетях последующего поколения // Международный союз электросвязи, разработано Бутенко В.В., Назаренко А.П., Сарьян В.К. и др., 2014.
11. Рекомендация МСЭ-Т Y.2222 Сенсорные управленческие сети и их приложения в сетях последующего поколения, 2013.
12. Сарьян В.К. Программа кооперации по созданию единого интероперабельного подхода по повышению эффективности существующих систем оповещения в ЧС / Семинар АТЭС, Москва, 2015.
13. Любушин А.А. О свойствах поля низкочастотных шумов, зарегистрированных на камчатской сети широкополосных сейсмических станций / Вестник КРАУНЦ. Серия: Науки о Земле, № 4(8А), с. 659-666, 2012.
14. Любушин А.А. Тренды сейсмической опасности на основе мультифрактальных параметров поля низкочастотных микросейсм // Природные риски, 70 (1), с. 471-483, 2014.
15. Сарьян В.К. Мониторинг глобальных процессов на базе интернета вещей, АТЭС, 2015, Новая Зеландия.
16. Д. Бондарев, А. Балашова, А. Махукова Холодильник атакует: как киберпреступники используют бытовую технику http://www.rbc.ru/technology_and_media/13/11/2016/5825cf889a79475b671ff9

References

1. Digital declaration EAEC http://www.eurasiancommission.org/ru/act/dmi/workgroup/Pages/default.aspx
2. Butenko V., Nazarenko A., Sarian V. and oth. Issues affecting the evaluation of beneficial effects of new technologies and ways to solve these issue, 23rd European Regional Conference of International Telecommunication Society / International Telecommunication Society, Vienna, 2012.
3. Butenko V., Nazarenko A., Sarian V. and oth. Problems arising during implementation of new technologies

in the infocommunication community / Trudy NIIR, № 1, 2011.

4. Levashov V. aSocio-political risks of sustainable development / Vestnik RAS, Nauka, Moscow, 2014, № 2, vol. 84, pp. 143 – 152.

5. Sarian V., Levashov V., Golovin S., Borodin A. The necessity to develop socio-technical standards / Trudy NIIR, № 2, 2016 г.

6. Sarian V., Levashov V. The introduction of the Internet of things technology and indicators of the Information Society / Proceedings of 6-th International conference «IT – Standard 2015».

7. Nazarenko A., Sarian V. Mass service - customized rescue management during emergencies of natural and man-made origin / Trudy NIIR, №3, 2016.

8. ITU-T Recommendation Y.2239 Requirements for Information Control Networks and related applications, 2015.

9. Butenko V, Nazarenko A., Sarian V. and oth. Personal safety in emergency. Innovative application for mobile phones // ITU News, №3, 2012, pp47-49.

10. Applications of wireless sensor networks in next generation networks; technical paper // International Telecommunication Union (ITU) developed by Butenko V., Nazarenko A., Sarian V. and oth., ITU-T, 2014.

11. ITU-T Recommendation Y2222 Sensor control networks and related applications in a next generation network environment, 2013.

12. Sarian V. Cooperation Program on Creating a Common Interoperable Approach to Improving the Efficiency of Existing Disaster Management Systems based on ICT, APEC TEL Workshop, Moscow, 2015.

13. Lyubushin A. Prognostic properties of low frequency seismic noise // Natural Science, 2012, 4(8A), pp 659-666.

14. Lyubushin A., Dynamic estimate of seismic danger based on multufractal properties of low frequency seismic noise // Natural Hazards, 2014, 70 (1), pp 471-483.

15. Sarian V. Global Processes Monitoring System with the application of the, Internet of Things (IoT), APEC TEL 52 2015 Auckland, New Zealand.

16. Bondarev D., Balashova A., Mahukova A. Refrigerator attacks: how cybercriminals use home appliances http://www.rbc.ru/technology_and_media/13/11/2016/5825cf889a79475b671ff971