ТЕЛЕКОММУНИКАЦИИ КАК ОСНОВА ФУНКЦИОНИРОВАНИЯ СИТУАЦИОННЫХ ЦЕНТРОВ ГЛАВ СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Е.Г. Кухаренко, *декан ФПКП МТУСИ, к.э.н., elena.kukharenko@mail.ru;*
И.С. Чугин, *заместитель директора центра технологического обеспечения телекоммуникационных систем АО «ЦНИИ ЭИСУ», chugin_is@cniieisu.ru;*
Е.С. Аношкина, *магистрант МТУСИ, e.anoshkina@bk.ru*

УДК 004.77

Аннотация. В статье рассматриваются цели и задачи создания системы распределенных ситуационных центров, показана их структура и роль в обеспечении экономической безопасности государства, отражена роль телекоммуникационных технологий как основы функционирования ситуационных центров.

Ключевые слова: ситуационные центры; телекоммуникации; связь; информационно-коммуникационные технологии; информационно-аналитическая система; экономическая безопасность; цифровая экономика.

TELECOMMUNICATIONS AS A BASIS OF FUNCTIONING OF SITUATIONAL CENTERS OF THE HEADS OF THE RUSSIAN FEDERATION CONSTITUENT ENTITIES

Elena Kukharenko, *dean FPKP MTUCI, candidate of economics;*
Igor Chugin, *deputy director of the center for technological support of telecommunication systems of JSC "CSRI EICS";*
Elena Anoshkina, *graduate student MTUCI*

Annotation. The article examines the goals and tasks of creating a system of distributed situation centers, shows their structure and role in ensuring the economic security of the state, and reflects the role of telecommunication technologies as the basis for the functioning of situation centers.

Keywords: situation centers; telecommunications; communication; information and communication technologies; information and analytical system; economic security; digital economy.

Роль телекоммуникационных и информационных технологий в жизни современного общества огромна. Обеспечивая доступ потребителей к различным информационным и телекоммуникационным услугам в рамках единого информационного пространства, телекоммуникации создают условия для успешного функционирования экономических отраслей и сфер деятельности, способствуют появлению и развитию новых форм ведения бизнеса, повышению качества жизни [1, 2]. Внедрение новых инфокоммуникационных технологий и услуг, развитие фиксированной и подвижной связи способствуют повышению эффективности работы органов государственной власти и местного самоуправления, экономическому росту и развитию регионов [3-5].

Одной из актуальных задач повышения эффективности управленческой деятельности и экономической безопасности регионов и государства в целом является создание системы распределенных ситуационных центров. Правовой основой создания ситуационных центров является ряд нормативных актов и рекомендательных документов, разработанных под влиянием необходимости информатизации процессов государственного управления. Согласно Указа Президента РФ № 537 от 12.05.2009 г. «О Стратегии национальной безопасности Российской Федерации до 2020 г.» предусматривается создание системы распределенных ситуационных центров и определяет их основной функционал в целях реализации задач стратегического планирования [6, 7]. Дальнейшее развитие нормативно-методической базы создания ситуационных центров связано с изданием и принятием следующих документов: Концепция создания системы распределенных ситуационных центров; Методические

рекомендации по созданию и вводу в эксплуатацию ситуационных центров глав субъектов Российской Федерации; Указ Президента РФ от 25 июля 2013 г. № 648 «О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия» [8, 9].

Ситуационные центры должны быть созданы в федеральных органах государственной власти Российской Федерации, органах государственной власти субъектов Российской Федерации, органах местного самоуправления, а также негосударственных органах и организациях в целях:

а) информационно-аналитической поддержки государственного и военного управления, стратегического планирования, мониторинга и контроля реализации документов стратегического планирования в Российской Федерации;

б) повышения эффективности государственного управления в мирное время, в период непосредственной угрозы агрессии и в военное время, в том числе при возникновении чрезвычайных (кризисных) ситуаций, за счет использования организационных, информационных и технологических возможностей ситуационных центров по мониторингу, анализу, оценке, прогнозированию изменения обстановки, моделированию сценариев развития ситуаций и поддержке принятия управленческих решений;

в) участия в обеспечении функционирования федеральной информационной системы стратегического планирования в порядке, установленном Правительством Российской Федерации.

Ситуационный центр представляет собой организационно-технический комплекс, предназначенный для информационно-аналитического и коммуникационного обеспечения решения задач управления в органах государственной власти, на крупных предприятиях, в отраслях экономики или при развитии кризисных ситуаций. Ситуационный центр включает в себя специализированные помещения, оснащенные комплексами телекоммуникационного оборудования, средствами хранения, сбора, обработки, визуализации информации, специальным программным обеспечением, реализующим методы моделирования и прогнозирования, интегрируемым в единую информационно-аналитическую систему, обеспечивающую всестороннюю поддержку функционирования ситуационного центра.

Стратегия национальной безопасности страны рассматривает создание системы распределенных ситуационных центров, как важнейшего элемента системы стратегического планирования. Целью создания ситуационных центров, взаимодействующих по единому регламенту, является повышение эффективности управления регионом на основе применения современных информационно-аналитических технологий поддержки принятия решений в социально-экономической, общественно-политической сферах, а также в сфере комплексной безопасности [6, 7, 10].

Для достижения указанной цели необходимо обеспечить решение следующих функциональных задач:

- обеспечение сбора и загрузки данных от различных информационных источников (федерального, регионального, муниципального уровней власти, предприятий и учреждений), в том числе интеграция с различными информационными ресурсами, с обеспечением контроля исполнения информационных регламентов;
- обеспечение мобильного доступа к информационным данным системы;
- информационное взаимодействие с ситуационными центрами высшего уровня.

Порядок организации взаимодействия ситуационных центров устанавливается «Единым регламентом взаимодействия распределенных ситуационных центров», утвержденным решением Межведомственной комиссии по координации деятельности федеральных органов исполнительной власти по созданию системы распределенных ситуационных центров (далее – СРСЦ), работающих по единому регламенту взаимодействия (протокол № 2 от 7 мая 2015 г.), соглашениями об информационном взаимодействии между Федеральной службой охраны

Российской Федерации и участниками СРСЦ [11].

В соответствии с Единым регламентом взаимодействия распределенных ситуационных центров ситуационные центры регионов должны взаимодействовать в рамках СРСЦ по следующим направлениям:

- с ситуационными центрами Президента Российской Федерации, Полномочного представителя Президента Российской Федерации в федеральном округе, Правительства Российской Федерации, Администрации Президента Российской Федерации и других федеральных органов исполнительной власти;
- с органами государственной власти субъекта;
- с муниципальными образованиями субъекта;
- с территориальными отделениями федеральных органов исполнительной власти;
- с предприятиями и организациями [10, 12].

Взаимодействие информационных систем участников СРСЦ, используемых для предоставления государственных и муниципальных услуг в электронной форме, в том числе единой системы межведомственного электронного взаимодействия и единой системы идентификации и аутентификации осуществляется через комплексы информационного взаимодействия. Комплексы информационного взаимодействия представляют собой аппаратно-программные средства, обеспечивающие безопасное информационное взаимодействие с использованием защищенной телекоммуникационной сети. Таким образом, взаимодействие и функционирование ситуационных центров невозможно без существования надежной, высокоскоростной, мультисервисной телекоммуникационной среды, отвечающей современным стандартам безопасности [12, 13].

Телекоммуникационная сеть ситуационных центров является интегрированной телекоммуникационной средой, с помощью которой пользователям предоставляются телекоммуникационные услуги в соответствии с государственными и международными стандартами.

Согласно назначению ситуационных центров телекоммуникационная сеть должна обеспечивать:

- надежную, гарантированную и достоверную доставку пользователям необходимой информации, в том числе информации, содержащей сведения, составляющие государственную тайну;
- телекоммуникационное взаимодействие компонент ситуационных центров между собой, а также с другими ситуационными центрами, внешними информационными системами и сетями, в том числе информационно-телекоммуникационной сети интернет;
- организацию взаимодействия технических средств ситуационных центров с информационными системами аналитической обработки информации, поступающей и хранящейся у участников системы (если такие функции не возложены на технические средства самих ситуационных центров), а также их передача на уровень исполнителя;
- качественную и бесперебойную работу открытой и защищенной видеосвязи [9, 14, 15].

Телекоммуникационная сеть должна способствовать обмену разнородной информацией в рамках единой инфраструктуры, которая способна предоставлять услуги гарантированного качества и иметь возможность интеграции различных видов связи на базе единых телекоммуникационных технологий.

Телекоммуникационные системы комплексов информационного взаимодействия должны функционировать как на федеральном, так и на региональном уровнях. При этом основной задачей телекоммуникационных систем комплексов информационного взаимодействия различных уровней является своевременное предоставление должностным лицам и элементам информационно-аналитических систем полного набора служб и услуг связи,

а также оперативное телекоммуникационное взаимодействие со всеми органами государственной и региональной власти, государственными учреждениями, предприятиями и организациями региона, а также населением. Пример структурной схемы защищенной телекоммуникационной среды комплекса информационного взаимодействия субъекта Российской Федерации приведен на рис. 1.

Ситуационные центры являются объектами информатизации, обрабатывающими разно категорийную информацию, и взаимодействующими с информационными системами, предназначенными для обработки секретной, конфиденциальной и общедоступной информации.

В зависимости от категории обрабатываемой информации должны быть предусмотрены следующие сегменты обработки и передачи информации:

- сегмент «С» – для обработки информации ограниченного доступа, содержащей сведения, составляющие государственную тайну;
- сегмент «К» – для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну;
- сегмент «О» – для обработки общедоступной информации.

При проектировании и построении ситуационного центра должно быть предусмотрено физическое разделение сегментов.

В соответствии с требованиями регулятора информационной защите подлежит все оборудование ситуационного центра, включая ее коммутационное и линейно-кабельное оборудование, предназначенное для обработки и передачи информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну, а также оборудование, размещаемое в помещениях, где циркулирует визуальная и/или акустическая информация, содержащая сведения, составляющие государственную тайну, и не предназначенное для обработки информации ограниченного доступа «К» и/или «С».

Оборудование сегмента «К» и «С» должно быть защищено от утечки информации по техническим каналам и от электронных устройств негласного получения информации и должно пройти установленным в Российской Федерации порядком оценку соответствия требованиям по безопасности информации (иметь соответствующий сертификат). Созданная таким образом система обеспечения безопасности (система защиты обрабатываемой и хранящейся информации от несанкционированного доступа) должна удовлетворять действующим нормативным и методическим документам Российской Федерации в области защиты информации.

Эксплуатация ситуационного центра с данными конфиденциального и закрытого контура возможна при соблюдении следующих условий:

- проведение специальных проверок и специальных исследований для элементов комплексов технических средств;
- отсутствие гальванических связей между элементами комплексов технических средств, работающих в разных контурах;
- применение средств шифрования (криптотехники);
- применение технических средств обеспечения информационной безопасности;
- применение сертифицированных средств однонаправленной передачи данных;
- применение организационных мер по обеспечению информационной безопасности;
- аттестация выделенных помещений ситуационного центра.

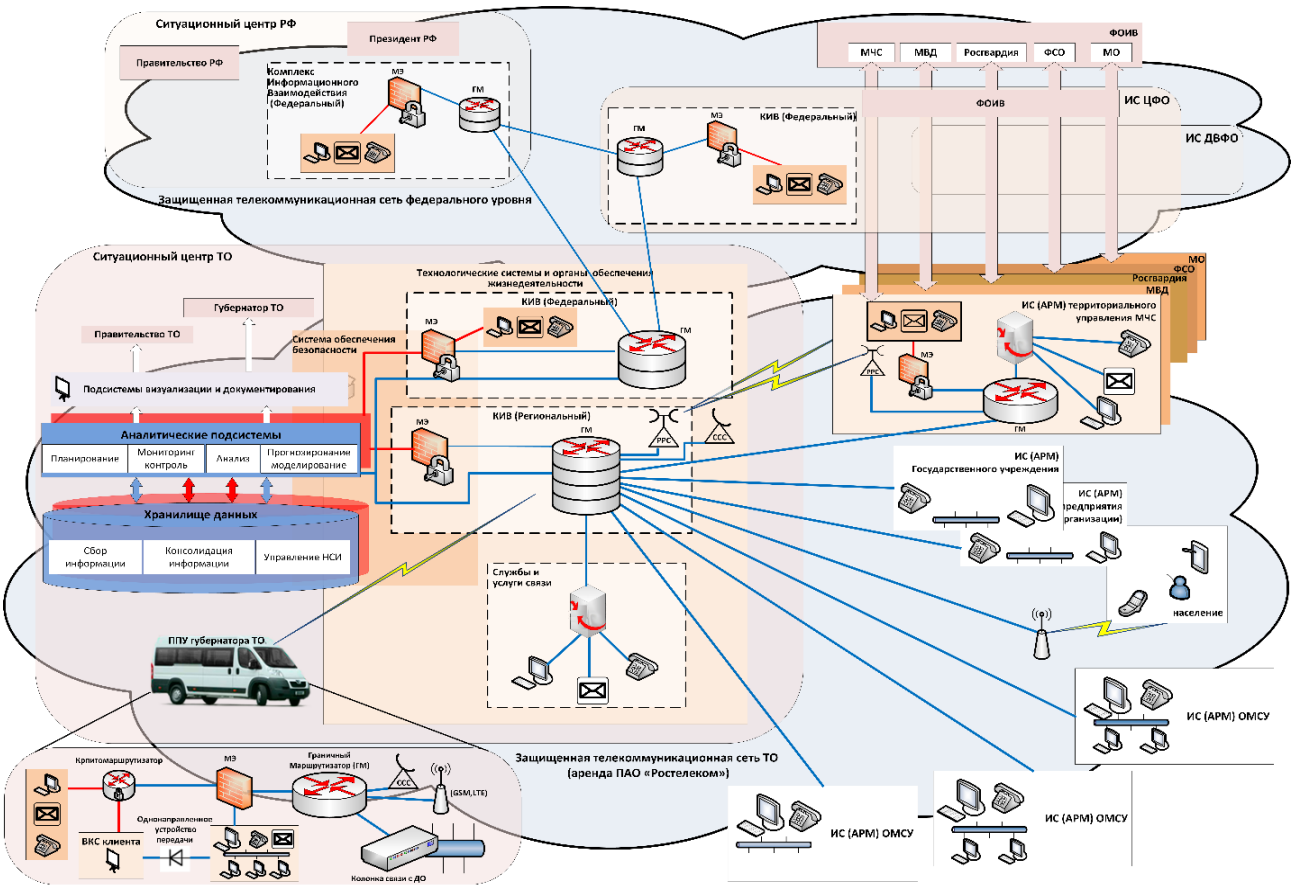

Рисунок 1

В соответствии с требованиями нормативно-правовых актов, а также с целью обеспечения мобильного доступа к данным информационно-аналитической системы в состав ситуационного центра субъекта Российской Федерации должен быть включен мобильный подвижный пункт управления губернатора, имеющий доступ ко всем сегментам единого информационного ресурса ситуационного центра при выезде Губернатора и должностных лиц в районы, города и области для принятия оперативного решения на месте в кризисных (чрезвычайных) ситуациях. Оборудование подвижного пункта управления должно располагаться на базе высокопроходимого автомобиля или комплекта автомобилей и предназначено для эксплуатации в полевых условиях (классификационная группа 1.3 и группа 1.10 – при работе вне объекта (ППУ) климатического исполнения УХЛ по ГОСТ РВ 20.39.304-98).

Защищенные телекоммуникационные сети федерального и регионального уровней должны быть построены на базе стека протоколов TCP/IP и состоять из следующих сегментов (рис. 2):

- сегмента для обработки общедоступной (открытой) информации (сегмент «О»), наложенного на сеть передачи данных (виртуальную частную сеть) доверенного оператора связи (например, ПАО «Ростелеком»);
- сегмента для обработки конфиденциальной информации (сегмент «К»), наложенного на сегмент «О»;
- сегмента для обработки секретной информации (сегмент «С»), наложенного на сегмент «О».

Защищенные телекоммуникационные сети федерального и регионального уровней строятся по единым принципам и архитектурным решениям. Разделение необходимо в целях

демаркации зон ответственности администраций данных сетей и управления.

На рис. 2 показан принцип наложения сегментов защищенной телекоммуникационной сети. В каждом сегменте защищенной телекоммуникационной сети должна предоставляться услуга переноса трафика с соответствующим ему (сегменту) грифом секретности в интересах комплексов средств автоматизации в составе ситуационных центров.

Таким образом, в составе каждого ситуационного центра должны быть три типа локальных сетей с комплексами средств автоматизации, подключенных к сегментам «О», «К» и «С» в зависимости от грифа секретности обрабатываемой информации. При этом подключение локальных сетей с комплексами средств автоматизации к сегментам «О», «К» и «С» необходимо осуществлять через межсетевые экраны. Применение данных межсетевых экранов в составе комплексов средств автоматизации позволит реализовать дополнительную политику безопасности в каждой локальной сети с комплексами средств автоматизации, а также осуществить трансляцию сетевых адресов (NAT – Network Address Translation) для решения проблемы создания единого адресного пространства.

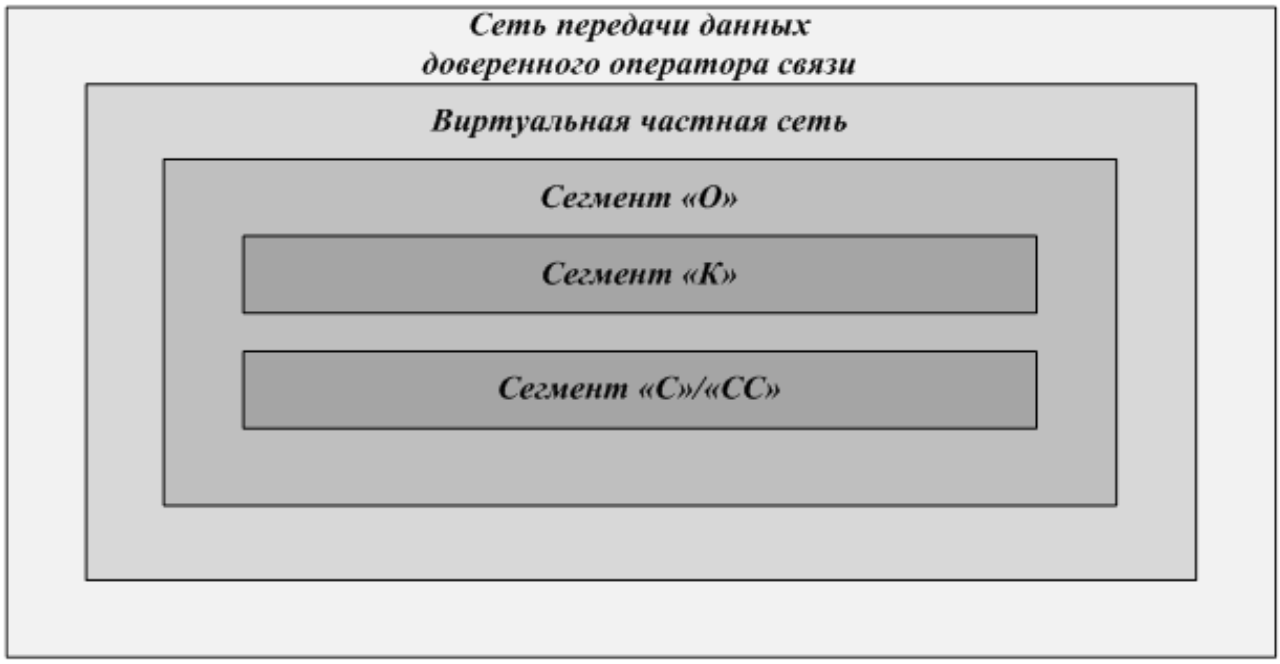

Рисунок 2

В соответствии с принципом построения и функционирования сегмента «О» защищенной телекоммуникационной сети граничный маршрутизатор должен подключаться к маршрутизатору из состава сети передачи данных доверенного оператора связи. Подключение маршрутизаторов друг к другу должно производиться по проводному каналу связи. Для обеспечения надежности функционирования в различных (критических) ситуациях основные направления связи, в первую очередь с территориальными отделениями федеральных органов исполнительной власти (ОВК, управлениями МЧС, МВД, ФСО и Росгвардии) должны быть зарезервированы отдельными направлениями радиорелейной связи. Направления организуются по принципу «звезда» и предполагают построение отдельных среднескоростных линий радиорелейной связи от места расположения ядра сети к местам постоянной дислокации федеральных органов исполнительной власти. Данные направления планируются к использованию как резервные линии связи, так и для наращивания пропускной способности направлений телекоммуникаций в угрожаемый/чрезвычайный период и при возникновении кризисных ситуаций.

Сегменты «К» и «С/СС» являются наложенными шифрованными сетями поверх открытого сегмента. Закрытие информации осуществляется криптомаршрутизаторами, для

сегмента «С» – криптомаршрутизатором, разрешенным к применению в сетях шифрованной связи 1-2 классов с имитозащитой по 1 классу. Разграничение локальных сетей внутри сегмента «К» (сеть хранения и обработки данных, ЛВС пользователей) осуществляется межсетевым экраном сегмента «К», внутри сегмента «С» – межсетевым экраном сегмента «С» класса защищенности не ниже А2. Подключение криптомаршрутизаторов «К» и «С» к граничному маршрутизатору должно осуществляться через коммутатор уровня ядра открытого сегмента. Сегменты «К» и «С» каждого объекта будут взаимодействовать с аналогичными сегментами других объектов при наличии туннелей между ними, которые организуются криптомаршрутизаторами. При этом топология построения туннелей определяется количеством взаимодействующих объектов и техническими возможностями криптомаршрутизаторов. Для построения защищенной телекоммуникационной сети рекомендуется топология «полносвязный граф» (принцип «каждый с каждым»). Комплексы средств автоматизации, размещенные в сегментах «К» и «С» на одном объекте, смогут осуществлять информационный обмен между собой только при наличии разрешающих правил фильтрации на объектовом МСЭ. Комплексы средств автоматизации, размещенные в сегменте «К» на разных объектах, смогут осуществлять информационный обмен между собой только при наличии туннелей между объектовыми граничными устройствами и разрешающих правил фильтрации на МСЭ взаимодействующих объектах. Все оборудование, входящее в состав сегмента для обработки секретной информации, должно располагаться внутри одной контролируемой зоны. За пределы контролируемой зоны информация может передаваться только по защищенным каналам в зашифрованном виде. В соответствии с Рекомендациями взаимодействие КСА, размещенных в сегменте «С» СЦ, с КСА, размещенными в сегментах «О» и «К» на том же СЦ, должно быть запрещено, за исключением случаев вывода информации на единый комплекс оборудования видеоотображения и звукоусиления с применением специальных устройств однонаправленной передачи.

Для обеспечения деятельности должностных лиц СЦ, а также руководителей субъектов РФ, министерств, ОИВ регионов и т.д. в каждом сегменте защищенной телекоммуникационной сети должны быть предоставлены следующие услуги связи:

- перенос трафика в интересах КСА в составе объектов СЦ, работающих по собственным протоколам;
- файловый обмен (с применением протокола FTP);
- электронная почта (с применением протокола SMTP для отправки почтовых сообщений и протокола IMAP или POP3 для приема почтовых сообщений);
- передача мгновенных сообщений (с применением протокола XMPP);
- предоставление справочной информации;
- IP-телефония (с применением аналоговых телефонов, цифровых АТС и VoIP-шлюзов, работающих по протоколу сигнализации SIP);
- видеоконференцсвязь (с применением видеомикшеров).

Для обеспечения предоставления данных услуг связи в защищенной телекоммуникационной сети также должны функционировать службы:

- единого времени (возможность синхронизации КСА с сервером единого времени по протоколу NTP, который, в свою очередь, получает данные от ГЛОНАСС/GPS-приемника);
- мониторинга (возможность проверки доступности активного сетевого оборудования КСА как на своем, так на и взаимодействующих СЦ (объектах));
- доменных имен (обеспечение работы IP-телефонии и электронной почты).

В настоящее время организация «бесшовного» взаимодействия сетей передачи данных различных ведомств между собой на территории субъектов Российской Федерации осложнена по следующим причинам:

- виртуальные частные сети, на которые наложены ведомственные сети передачи данных, должны иметь между собой точки сопряжения (что не всегда реализуемо по организационным и техническим причинам);
- адресные пространства сопрягаемых сетей передачи данных не должны пересекаться (для этого необходимо применять трансляцию сетевых адресов на стыке взаимодействующих сетей);
- в закрытых сегментах сопрягаемых сетей передачи данных должны применяться единые средства шифрования и единые ключи для этих средств шифрования;
- максимальный гриф секретности обрабатываемой информации во взаимодействующих КСА СЦ и КСА ведомств должен совпадать.

Таким образом, создание ситуационных центров возможно только в регионах с развитой телекоммуникационной средой. Стратегический анализ процесса развития информационного общества в России свидетельствует о его региональной неравномерности [16]. Данный фактор носит крайне негативный характер, так как существует корреляционная зависимость между уровнем информатизации в регионе и его внутреннего регионального продукта. В частности, диаграмма Джипа иллюстрирует зависимость телефонной плотности от внутреннего национального продукта.

Одним из основных инструментов анализа развития и использования информационно-коммуникационных технологий в регионах является оценка Индекса готовности регионов России к информационному обществу, рассчитанного на основе 77 показателей, характеризующих факторы развития информационного общества (человеческий капитал, экономическую среду и ИКТ-инфраструктуру), а также использование ИКТ в шести областях (государственное и муниципальное управление, образование, здравоохранение, бизнес, культура, домохозяйства). Стоит отметить, что ситуационные центры созданы или находятся в процессе разработки в регионах, входящих в двадцатку Рейтинга российских регионов по значениям индекса готовности к информационному обществу. Среди них стоит выделить Ямало-ненецкий автономный округ, Мурманскую, Сахалинскую, Тюменскую области. Индекс готовности регионов России к информационному обществу включает в себя также показатель «ИКТ в государственном и муниципальном управлении», рассматривающий использование ИКТ по трем направлениям: использование организациями технологий электронного правительства для взаимодействия с органами государственной власти и органами местного самоуправления; веб-присутствие регионов; доступ органов государственной власти и органов местного самоуправления к информационно-коммуникационным технологиям [17, 18].

Создание ситуационных центров на региональном уровне является одним из инструментов развития информационного общества, и как следствие информационной экономики. В целях реализации Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг., утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 гг.» распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р утверждена Программа «Цифровая экономика Российской Федерации» [19, 20]. Ключевой целью Программы является создание инфраструктуры, «экосистемы» цифровой экономики в различных отраслях экономики и сферах деятельности государства, основанной на информационно-коммуникационных технологиях. Региональные ситуационные центры – инструмент реализации целей Программы «Цифровая экономика Российской Федерации» в сфере государственного и муниципального управления. В соответствии с Программой, основными целями развития направления, касающегося информационной инфраструктуры, являются:

- развитие сетей связи, которые обеспечивают потребности экономики по сбору и передаче данных государства, бизнеса и граждан с учетом технических требований, предъявляемых цифровыми технологиями;

- развитие системы российских центров обработки данных, которая обеспечивает предоставление государству, бизнесу и гражданам доступных, устойчивых, безопасных и экономически эффективных услуг по хранению и обработке данных на условиях и позволяет в том числе экспортировать услуги по хранению и обработке данных;
- внедрение цифровых платформ работы с данными для обеспечения потребностей власти, бизнеса и граждан;
- создание эффективной системы сбора, обработки, хранения и предоставления потребителям пространственных данных, обеспечивающей потребности государства, бизнеса и граждан в актуальной и достоверной информации о пространственных объектах [17, 19, 21, 22].

Ситуационные центры решают данный перечень задач. Кроме того, построение ситуационных центров основано на принципе обеспечения информационной безопасности, что также является одной из задач цифрой экономики.

Создание ситуационных центров является не только инструментом, обеспечивающим информационно-аналитическое сопровождение принятия решений федеральными, региональными и муниципальными органами власти, но и «ступенью» на этапе становления информационного общества и экономического роста регионов, однако залогом успеха в решении этой задачи является развитая телекоммуникационная инфраструктура.

Литература

1. Андреева О.Д., Абрамова А.В., Кухаренко Е.Г. Развитие использования цифрового маркетинга в мировой экономике // Российский внешнеэкономический вестник, 2015. – № 4. – С. 24-41.
2. Никулина А.И., Кухаренко Е.Г. Анализ лояльности потребителей инфокоммуникационных услуг // Телекоммуникации и информационные технологии, 2014. – Т. 1. – № 2. – С. 28-29.
3. Гасс Я.М., Кухаренко Е.Г. Современный этап развития MVNO в России и в мире спутниковые системы связи и вещания // Труды научно-исследовательского института радио, 2015. – № 3. – С. 26-32.
4. Кухаренко Е.Г. Жизненный цикл инфокоммуникационных услуг: особенности и тенденции // Экономика и качество систем связи, 2017. – № 3 (5). – С. 33-38.
5. Кухаренко Е.Г., Гасс Я.М., Серебряков Ю.Ю. Механизм оценки перспектив развития операторов MVNO в регионах России // Электросвязь, 2015. – № 9. – С. 44-46.
6. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // СПС КонсультантПлюс // Опубликован 28.12.2010 на официальном интернет-портале правовой информации http://www.consultant.ru.
7. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации». // СПС КонсультантПлюс // Опубликован 31.12.2015 на официальном интернет-портале правовой информации http://www.consultant.ru
8. Концепция создания системы распределенных ситуационных центров органов государственной власти Российской Федерации от 3 октября 2013 г. № Пр-2308.
9. Ильин Н.И. Система ситуационных центров в органах государственной власти – основа профессионального государственного управления.
URL: http://900igr.net/prezentacija/obg/sistema-raspredeljonnykh-situatsionnykh-tsentrov-aspekt-informatsionnoj-bezopasnosti-253708.html(дата обращения 17.12.2017).
10. Ивашкевич В. Ситуационные центры: применение в государственном управлении на региональном и федеральном уровнях.
URL: http://www.prognoz.ru/sites/default/fi les/ vera_ivashkevich_situacionnye_centry_1.pdf (дата обращения 17.12.2017).
11. Единый регламент взаимодействия распределенных ситуационных центров, утвержденным решением Межведомственной комиссии по координации деятельности федеральных органов

исполнительной власти по созданию системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия (Протокол № 2 от 7 мая 2015 г.).
12. Указ Президента РФ от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // СПС КонсультантПлюс // Опубликован 13.05.2017 на официальном интернет-портале правовой информации http://www.consultant.ru.
13. Приказ Министерства связи и массовых коммуникаций РФ от 13 апреля 2012 г. № 107 «Об утверждении Положения о федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (с изменениями и дополнениями) // СПС КонсультантПлюс // Опубликован 13.04.2012 на официальном интернет-портале правовой информации http://www.consultant.ru
14. Концепция создания Ситуационного центра Россвязи по централизованному мониторингу состояния телекоммуникационной инфраструктуры КСЭОН.
15. Кухаренко Е.Г. Токмачев С.С. Сравнительный анализ методических подходов к управлению проектами и их применение в инфокоммуникациях // T-Comm: Телекоммуникации и транспорт, 2012. – Т. 6. – № 12. – С. 64-65.
16. Кухаренко Е.Г., Салютина М.Е. Применение методов стратегического анализа для оценки конкурентоспособности телекоммуникационных компаний // T-Comm: Телекоммуникации и транспорт, 2014. – Т. 8. – № 7. – С. 57-59.
17. Евтюшкин А.В., Елизаров А.М., Елизарова Р.У., Ершова Т.В., Зингерман Б.В., Пазин Г.Н., Ризманова Л.М., Семёнова Н.Н., Хохлов Ю.Е., Шадаев М.И., Шапошник С.Б., Юрьева А.А. Анализ информационного неравенства субъектов Российской Федерации.
URL: http://eregion.ru/sites/default/files/upload/report/index-russian-regions-2010-2011.pdf (дата обращения 17.12.2017).
18. Костин В.И., Костина А.В. Национальная безопасность современной России. Экономические и социокультурные аспекты. – М.: Либроком. 2013.
19. Программа «Цифровая экономика Российской Федерации», утвержденная Распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р // СПС КонсультантПлюс // Опубликован 13.04.2012 на официальном интернет-портале правовой информации http://www.consultant.ru
20. Лаврут Н.С. Экономическая безопасность регионов как основа безопасности страны // Экономика и современный менеджмент: теория и практика: сб. ст. по матер. XXII межд. нар. науч.-практ. конф. Новосибирск: СибАК, 2013.
21. Федеральный закон от 28.06.014 № 172-ФЗ «О стратегическом планировании в Российской Федерации». // СПС КонсультантПлюс // Опубликован 28.06.2014 на официальном интернет-портале правовой информации http://www.consultant.ru
22. Володина Е.Е., Девяткин Е.Е., Суходольский А.М., Суходольская Т.А Основные направления развития информационно-коммуникационных технологий в Европе // Труды НИИР. Сборник научных статей, 2012. – № 2. – С. 11-22.