ЭКОНОМИКА, СИСТЕМЫ УПРАВЛЕНИЯ

ОЦЕНКА РЕЗУЛЬТАТИВНОСТИ КАК ВАЖНЕЙШИЙ АСПЕКТ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ РАСПРЕДЕЛЕННЫХ СИТУАЦИОННЫХ ЦЕНТРОВ МЧС РОССИИ

С.П. Еременко, кандидат технических наук, доцент;
С.Б. Хитов.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрена система распределенных ситуационных центров МЧС России, ее место в общей системе распределенных ситуационных центров, а также существующий подход к обеспечению информационной безопасности системы распределенных ситуационных центров МЧС России. Предложен принцип менеджмента информационной безопасности, основанный на внедрении в систему обеспечения информационной безопасности системы менеджмента информационной безопасности, информационная модель структуры ситуационного центра МЧС России, существующие походы к оценке результативности системы обеспечения информационной безопасности. Определены задачи реализации комплексного подхода к оценке результативности системы обеспечения информационной безопасности.

Ключевые слова: система распределенных ситуационных центров, ситуационный центр, информационная модель, информационная безопасность, система обеспечения информационной безопасности, результативность, оценка результативности

PRODUCTIVITY ASSESSMENT AS THE MOST IMPORTANT ASPECT OF CREATION OF SYSTEM OF ENSURING INFORMATION SECURITY IN SYSTEM OF THE DISTRIBUTED SITUATIONAL CENTERS OF EMERCOM OF RUSSIA

S.P. Eremenko; S.B. Khitov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The system of the distributed situational centers of EMERCOM of Russia, it place in the general system of the distributed situational centers and existing approach to ensuring information security of system of the distributed situational centers of EMERCOM of Russia is considered. The principle of management of information security based on introduction in the system of ensuring information security of information security management system, information model of structure of the situational center of EMERCOM of Russia, the existing approaches to an assessment of productivity of system of ensuring information security is offered. Problems of realization of an integrated approach to an assessment of productivity of system of ensuring information security are defined.

Keywords: system of the distributed situational centers, situational center, information model, information security, system of ensuring information security, productivity, productivity assessment

В целях повышения эффективности государственного управления в мирное и военное время, а также при возникновении кризисных (чрезвычайных) ситуаций на основе возможностей ситуационных центров (СЦ) органов государственной власти Российской Федерации в нашей стране продолжается работа по созданию системы распределенных ситуационных центров (СРСЦ) на различных уровнях: федеральном, уровне федеральных округов Российской Федерации, уровне субъектов Российской Федерации [1]. Главным идеологом и координатором работ в данном направлении является федеральная служба охраны (ФСО) России, через защищенную транспортно-коммуникационную сеть которой осуществляется интеграция всех элементов системы.

Обобщенная структура СРСЦ представлена на рис. 1.

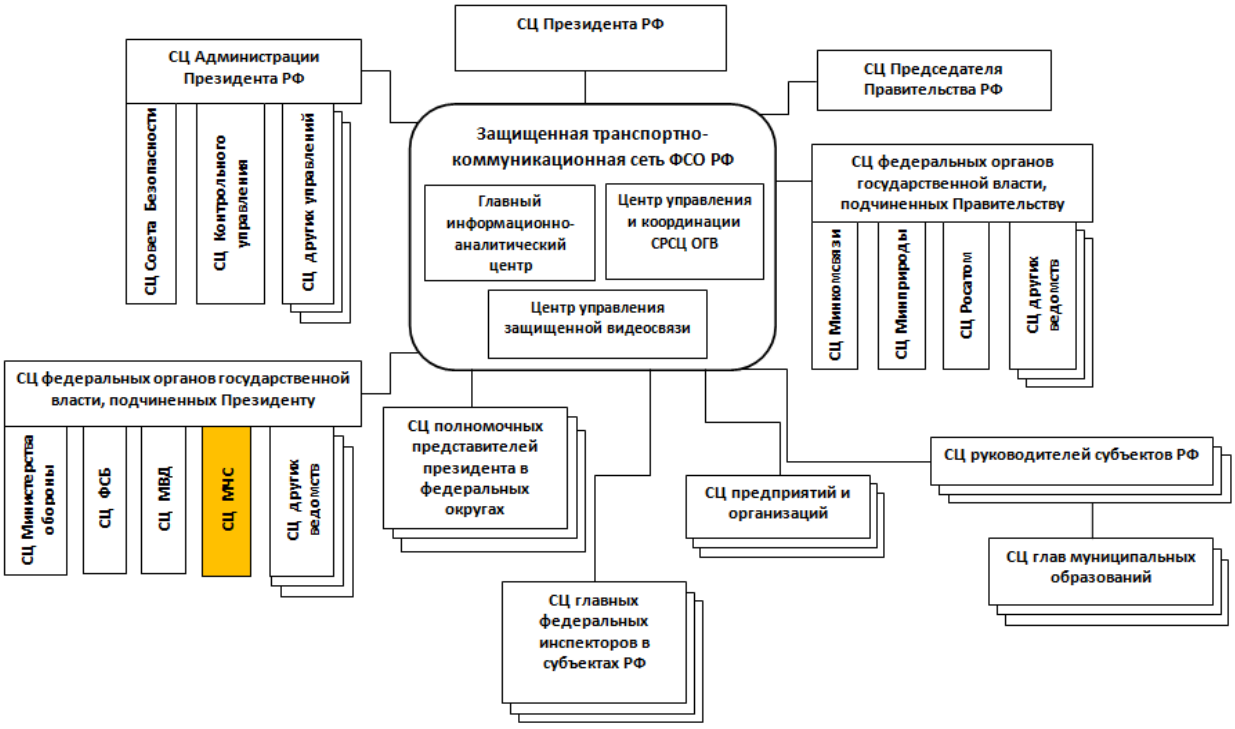

Рис. 1. **Обобщенная структура СРСЦ**

Из рис. 1 видно, что структурным элементом системы является система СЦ МЧС России, которую рассмотрим ниже.

К моменту начала работ по созданию СРСЦ в МЧС России в целях развития единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) были созданы Национальный центр управления в кризисных ситуациях (НЦУКС), а также Центры управления в кризисных ситуациях территориальных органов МЧС России (ЦУКС), являющиеся органами повседневного управления РСЧС на федеральном, межрегиональном и региональном уровнях (рис. 2) [1].

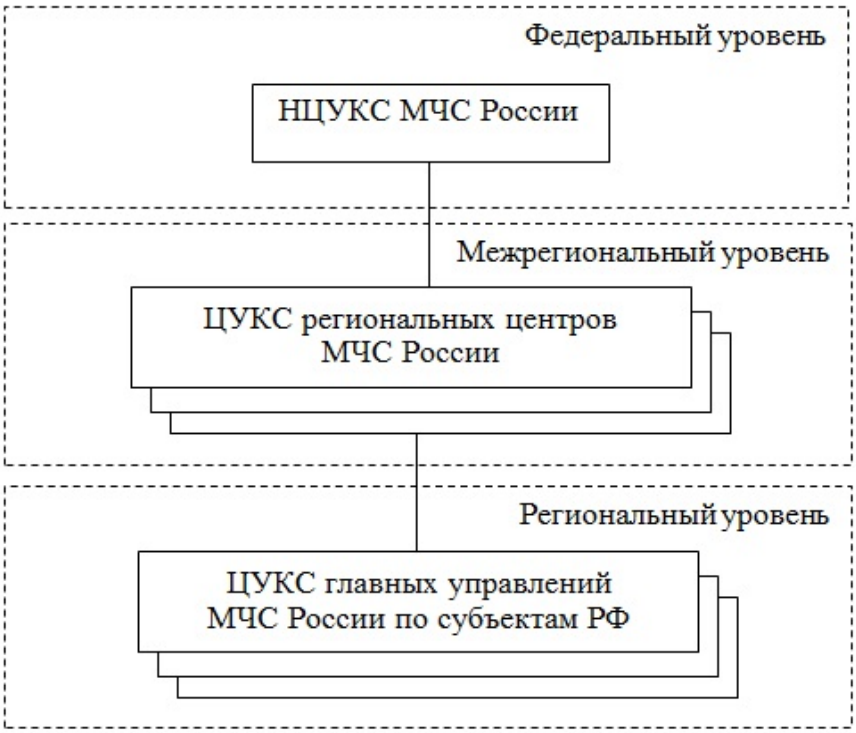

Рис. 2. **Структура органов повседневного управления РСЧС**

В настоящее время трехуровневая система НЦУКС – ЦУКС региональных центров – ЦУКС главных управлений МЧС России по субъектам Российской Федерации, которую будем рассматривать как СРСЦ МЧС России, является эффективной системой обеспечения функционирования органов управления РСЧС и гражданской обороны, управления их силами и средствами, а также организации своевременного информирования и оповещения населения об угрозе и возникновении чрезвычайных ситуаций (ЧС), в том числе в местах массового пребывания людей. Данная система продолжает совершенствоваться и развиваться.

Стремительно растет и круг задач, для решения которых требуется активное межведомственное взаимодействие, в рамках которого требуется интеграция СРСЦ МЧС России в общую систему [1].

Одним из ключевых направлений, оказывающих существенное влияние на результативное функционирование СРСЦ, является обеспечение информационной безопасности (ИБ), включающее [2]:

– проведение оценки защищенности и стабильности функционирования СРСЦ;

– оценку потенциальных уязвимостей СРСЦ;

– создание модели угроз и модели нарушителя СРСЦ, включая угрозы межгосударственного информационного противоборства, распространение вредоносного программного обеспечения, используемого в качестве информационного оружия, деятельность хакерских группировок;

– совершенствование подсистемы защиты информации от неправомерных действий в отношении информационных ресурсов СРСЦ;

– ряд других мероприятий.

При этом в МЧС России, отличающимся высоким уровнем компьютеризации процессов управления на всех уровнях иерархии, проблема защиты информации, являющаяся проблемой комплексной, также представляет особую актуальность [3, 4].

В существующей СРСЦ МЧС России задача обеспечения ИБ решается в соответствии с нормативно-правовой базой, регулирующей вопросы защиты информации, обрабатываемой в государственных информационных системах [5], а также Концепцией

информационной безопасности МЧС России, представляющей собой систему позиционирования целей и задач информационной защиты, основных принципов построения организационных, технологических и процедурных аспектов ее обеспечения, а также способов обеспечения необходимого уровня информационной защиты.

Внедрение в деятельность МЧС России нового принципа менеджмента ИБ – перехода от оперативного реагирования к управлению рисками, профилактике и предупреждению крупномасштабных факторов, рисков и угроз [6] ведет к необходимости актуализации положений Концепции на основе внедрения в систему обеспечения ИБ – системы менеджмента информационной безопасности (СМИБ), отвечающей современным стандартам и требованиям и представляющей собой часть общей системы обеспечения информационной безопасности (СОИБ), основанной на методологии бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и ее улучшению [5].

В этой связи предлагается вариант информационной модели структуры СЦ из состава СРСЦ МЧС России (СЦ МЧС России), представленный на рис. 3.

Рис. 3. **Информационная модель структуры СЦ МЧС России: АИУС РСЧС – автоматизированная информационная управляющая система единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций; АСМТС – автоматизированная система мониторинга транспортных средств; ЕСИМО – единая государственная система информации об обстановке в мировом океане; ОКСИОН – общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей; АСКРО – автоматизированная система контроля радиационной обстановки; АС «Делопроизводство» – автоматизированная система «Делопроизводство» и иные ИС (информационные системы)**

На рис. 3 показано, что основными компонентами модели являются: КГИС – комплекс государственных ИС; СОИБ – система обеспечения ИБ; АСМ СМИБ – автоматизированная система мониторинга СМИБ; АПКИП – аппаратно-программный комплекс ИБ; ЦУК – центр управления и координации; КПТС – комплекс программно-технических средств; ЕРИФ – единый распределенный информационный фонд.

Одним из этапов создания и функционирования СМИБ будет являться обеспечение автоматизированного контроля результативности СОИБ путем разворачивания автоматизированной системы процессов менеджмента СМИБ и внедрения

автоматизированных процессов менеджмента СОИБ, включая задачи по ее совершенствованию.

Под результативностью СОИБ СЦ МЧС России будем понимать результат мониторинга процессов комплексного функционирования СОИБ, характеризующий степень соответствия результатов мониторинга требованиям ГОСТ Р ИСО/МЭК 27001.

Существует множество подходов к оценке результативности СОИБ. Их можно разделить на две основные группы. К первой группе относятся подходы, опирающиеся на оценку соответствия СОИБ требованиям различных нормативно-правовых актов и руководящих документов. Ко второй группе относятся такие общие подходы, как вероятностный, экспериментальный, экспертный, эмпирический, базирующиеся на теории вероятностей и математической статистике.

Каждый рассмотренный подход позволяет учитывать лишь отдельные подмножества факторов, влияющих на результативность СОИБ. Основными недостатками указанных подходов являются: высокая степень неопределенности исходных данных при проведении оценки и сложность формализации процессов функционирования объекта оценки. Данные подходы не позволяют дать адекватную оценку результативности СОИБ, поскольку при их использовании лишь констатируется факт наличия или отсутствия конкретных механизмов защиты и не позволяют провести выполнение организационных мер по обеспечению ИБ в целом по всему комплексу СЦ МЧС России.

Для того чтобы избежать указанных недостатков при оценке результативности СОИБ СЦ МЧС России, используем комплексный подход, включающий в себя вероятностный, экспертный и оценочный подходы с выполнением организационных мер по обеспечению ИБ по всему комплексу СЦ как источнику аналитических данных для проведения оценки результативности СОИБ, функционирующей в рамках требований ГОСТ Р ИСО/МЭК 27001.

Основа предлагаемой методики оценки результативности СОИБ СЦ МЧС России базируется на анализе внешней и внутренней среды при разработке адаптивной стратегии СЦ как организации [7].

В этом случае под внешней средой понимается КГИС (рис. 3) с ее интегральной результативностью RКГИС, а за внутреннюю среду принимаются остальные составные части СЦ как компоненты интегрального показателя результативности СОИБ (RСОИБ), а именно: для ЦУК – RЦУК, для КПТС – RКПТС, для ЕРИФ – RЕРИФ, для АПКИБ – RАПКИБ, для СМИБ – RСМИБ.

При этом оценка результативности ИБ каждого интегрального показателя (RКГИС, RЦУК и т.д.) выполняется по отдельным показателям ИБ всех активов, входящих в тот или иной составной комплекс СЦ, то есть КГИС, КПТС, ЕРИФ, ЦУК, ЗТКС, АПКИБ, СМИБ.

Из рассмотренного выше следует, что для разработки методики оценки результативности СОИБ СЦ МЧС России стоит задача определения соответствующих показателей, характеризующих результативность СОИБ, методов оценки их граничных значений, способов измерения, формирования интегрального показателя – RСОИБ, разработки математической модели оценки результативности СОИБ СЦ МЧС России.

Литература

1. Хитов С.Б., Буйневич М.В. Система менеджмента информационной безопасности как инструмент управления рисками в системе распределенных ситуационных центров МЧС России // Сервис безопасности в России: опыт, проблемы, перспективы. Обеспечение безопасности при чрезвычайных ситуациях: материалы VII Междунар. науч.-практ. конф. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2015. 200 с.

2. Система распределенных ситуационных центров 2014: Резолюция конференции 16–17.10.2014. URL: http://www.ситцентр.рф/docs/Rezolution_SRSC_2014.pdf (дата обращения: 25.01.2016).

3. Чижиков Э.Н. Защита информации для безопасного функционирования информационных систем МЧС России // Каталог пожарной безопасности. 2013. № 1 (14). С. 16–17.

4. Хитов С.Б., Куватов В.И., Катаржнов А.Д. Организация проведения аудита соответствия автоматизированной обработки персональных данных в информационных системах МЧС России нормативным правовым актам Российской Федерации // Проблемы управления рисками в техносфере. 2015. № 3 (35). С. 120–124.

5. Еременко С.П., Можаев О.А., Хитов С.Б. Анализ нормативно-правовой базы для задачи формирования модели и метода оценки результативности СМИБ в организациях МЧС России // Проблемы управления рисками в техносфере. 2015. № 4 (36). С. 101–105.

6. Пучков В.А. МЧС-2030: современные технологи государственного управления в сфере безопасности жизнедеятельности населения: Стратегия развития МЧС России на период до 2030 г. // Семинар с руководящим составом МЧС России 2015 г. URL: http://www.mchs.gov.ru/upload/site1/document_file/0huAWJ42XI.pdf (дата обращения: 15.01.2016).

7. Штерн К. Стратегии, которые работают: Подход BCG: сб. ст.: пер. с англ. / сост. Карл Штерн и Дж. Стол–мл.; под общ. ред. И.В. Лазуковой. М.: Манн, Иванов и Фербер, 2005. 496 с.

References

1. Khitov S.B., Buinevich M.V. Sistema menedzhmenta informacionnoj bezopasnosti kak instrument upravlenija riskami v sisteme raspredelennyh situacionnyh centrov MCHS Rossii // Servis bezopasnosti v Rossii: opyt, problemy, perspektivy. Obespechenie bezopasnosti pri chrezvychajnyh situacijah: materialy VII Mezhdunar. nauch.-prakt. konf. [Information security management system as the instrument of risk management in system of the distributed situational centers of EMERCOM of Russia. Security services in Russia: experience, problems, prospects. Ensuring the safety of emergency: materials of a VII Internat. scient.-pract. conf.]. S.-Petersburg un-t of State fire service of EMERCOM of Russia, 2015. 200 p.

2. Sistema raspredelennyh situacionnyh centrov 2014: Rezolyucija konferencii [system of the distributed situational centers 2014: Conference resolution]. 16–17.10.2014. URL: http://www.ситцентр.рф/docs/Rezolution_SRSC_2014.pdf (data obrascheniya: 25.01.2016).

3. Chizhikov E.N. Zashhita informacii dlya bezopasnogo funkcionirovanija informacionnyh sistem MCHS Rossii [Information security for safe functioning of information systems of EMERCOM of Russia] // Katalog pozharnoj bezpoasnosti. 2013. № 1 (14). C. 16–17. (In Russ.).

4. Khitov S.B., Kuvatov V.I., Katarzhnov A.D. Organizacija provedenija audita sootvetstvija avtomatizirovannoj obrabotki personal'nyh dannyh v informacionnyh sistemah MCHS Rossii normativnym pravovym aktam Rossijskoj Federacii // Problemy upravlenija riskami v tehnosfere [Organization of compliance audit of automated processing of personal data in information systems of EMERCOM of Russia to regulations of Russian Federation // Problems in the technosphere risk management]. 2015. № 3 (35). P. 120–124. (In Russ.).

5. Eremenko S.P., Mozhaev O.A., Khitov S.B. Analiz normativno-pravovoj bazy dlya zadachi formirovanija modeli i metoda ocenki rezul'tativnosti SMIB v organizaciyah MCHS Rossii // Problemy upravlenija riskami v tehnosfere [Analysis legal norms for the task of construction of model and method of estimation of efficiency of information security management system in the organizations of EMERCOM of Russia // Problems in the technosphere risk management]. 2015. № 4 (36). P. 101–105. (In Russ.).

6. Puchkov V.A. MCHS-2030: sovremennye tehnologii gosudarstvennogo upravlenija v sfere bezopasnosti zhiznedejatel'nosti naselenija: Strategija razvitija MCHS Rossii na period do 2030 g. // Seminar s rukovodyashhim sostavom MCHS Rossii 2015 g. [EMERCOM of Russia 2030: modern governance technologies security of life of the population: Development strategy of EMERCOM of Russia up to 2030 // Workshop with the leadership of senior staff of EMERCOM

of Russia 2015. URL: http://www.mchs.gov.ru/upload/site1/document_file/0huAWJ42XI.pdf (data obrascheniya: 15.01.2016).

7. Stern K. Strategii, kotorye rabotajut. Podhod BCG [Perspectives on Strategy from the Boston Consulting Group] // Edited by Carl W. Stem and George Stalk, Jr, M: Mann, Ivanov and Ferber, 2005. 496 p.