населения и территорий от чрезвычайных ситуаций — проблемы, перспективы, инновации». Тезисы докладов. – М.: ФГБУ ВНИИ ГОЧС (ФЦ). - 2011.

10. Ноженкова Л.Ф., Исаев С.В., Ничепорчук В.В. и др. Средства построения систем поддержки принятия решений по предупреждению и ликвидации ЧС. Проблемы безопасности и чрезвычайных ситуаций. – М.: ВИНИТИ - 2008. вып. 4, С. 46-54.

**Сведения об авторе**

***Чумак Сергей Петрович***, доцент, ФГБУ ВНИИ ГОЧС (ФЦ), ведущий научный сотрудник. 121352, Москва, ул. Давыдковская, 7 Тел.: (499) 216-99-72. E-mail: 7centr_09@mail.ru

УДК 658 DOI: 10.36535/0869-4179-2021-03-15

# ФОРМИРОВАНИЕ ЗАЩИЩЕННОЙ ЦИФРОВОЙ ИНФРАСТРУКТУРЫ СИТУАЦИОННЫХ ЦЕНТРОВ В ЭНЕРГЕТИКЕ РОССИИ, АДАПТИРОВАННЫХ К РАБОТЕ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ И В ОСОБЫЙ ПЕРИОД

***В.В. Иванов***
**Минэнерго России**

**Доктор эконом. наук *Е.Л. Логинов***
**Научно-исследовательский институт экономических стратегий**

*Работа посвящена обеспечению эффективности ведомственных информационно-управляющих систем в рамках инфраструктурной суперсистемы, применяемых при решении функциональных задач ситуационных центров для действий, как в обычных, так и в чрезвычайных условиях. Обоснована необходимость выработки и реализации мер противодействия угрозам целенаправленного воздействия электромагнитным импульсом на энергетическую инфраструктуру нашей страны. Проанализированы такие меры, принимаемые в США. Предлагается формирование в России защищенных дата-центров, обслуживающих ситуационные центры в энергетике, так как именно они обеспечивают подержание функций жизнеобеспечения энергетической инфраструктуры, в т.ч. противодействие чрезвычайным ситуациям.*

**Ключевые слова:** ситуационные центры, энергетика, чрезвычайные ситуации, информационно-управляющие системы, безопасность.

# FORMATION OF A SECURE DIGITAL INFRASTRUCTURE OF SITUATIONAL CENTERS IN THE ENERGY SECTOR OF RUSSIA, ADAPTED TO WORK IN CONDITIONS EMERGENCIES AND DURING SPECIAL PERIODS

*V.V. Ivanov*
**Center of the Ministry of Energy of Russia**

**Dr. (Econ.)** ***E.L. Loginov***
**Research Institute of Economic Strategies**

*The article is devoted to ensuring the effectiveness of departmental information and control systems within the infrastructure supersystem, used in solving functional tasks of situational centers for actions, both in normal and in emergency conditions. The necessity of developing and implementing measures to counter the threats of a targeted impact of an electromagnetic pulse on the energy infrastructure of our country has been substantiated. Such measures taken in the USA are analyzed. It is proposed to form in Russia protected data centers serving situational centers in the energy sector, since it is they who ensure the maintenance of the life support functions of the energy infrastructure, incl. counteraction to emergency situations.*

**Keywords:** situational centers, energy, emergency situations, information and control systems, security.

## Введение

Цифровые технологии являются общепризнанным ключевым трендом трансформации систем управления XXI века [1]. В ближайшие десятилетия именно они будут являться основным двигателем экономического роста и обеспечения надежности управления энергетической инфраструктурой [2].

Развитие цифровых технологий предъявляет новые требования к цифровой инфраструктуре ситуационных центров в энергетике России [3]. Необходимо адаптировать информационно-управляющие системы ситуационных центров к работе в условиях чрезвычайных ситуаций и в особый период [4].

## Постановка проблемы

Одним из источником инициированных угроз чрезвычайных ситуаций является взрыв ядерного оружия на большой высоте или в космосе, который может генерировать интенсивный электромагнитный импульс (ЭМИ). В последний период технически развитые страны (США, Израиль и пр.) и некоторые из новых индустриальных стран (Китай) активно изучают возможности использования оружия, основанного но высоких энергиях, которое может в ряде случаев оказывать критическое электромагнитное воздействие на удаленные территории, отличающееся по своим параметрам от высотного ядерного взрыва (ВЯВ), но по своей разрушительной силе воздействия, в первую очередь на интеллектуальные элементы систем управления и связи, приближающиеся к нему.

Кроме того, эти же страны приступили к оснащению беспилотных летательных аппаратов устройствами, генерирующими высокочастотные микроволны, а также датчиками для отслеживания линий электропередач большой мощности, центров управления сетями и трансформаторов, которые создают близкие к вышеописанным угрозы чрезвычайных ситуаций [5].

Электромагнитный импульс ВЯВ может распространяться на землю и воздействовать на различные наземные технологические системы, такие как электросети и телекоммуникационные сети. Одной из компонент такого воздействия является влияние интенсивного короткоживущего электромагнитного импульса, характеризующегося временем нарастания 2,5 наносекунды и амплитудой порядка десятков кВ / м (до 50 кВ / м).

Географическая область чрезвычайных ситуаций, подверженная воздействию различных уровней электромагнитных полей вследствие ВЯВ, может быть довольно большой. Например, взрыв на расстоянии 200 км может поразить круговую площадь порядка 3 миллионов квадратных миль. Однако не все области, входящие в круговую область, испытывают максимальное электрическое поле, и напряженность поля падает с увеличением расстояния от нулевой точки [6].

Как правило, для смягчения влияния электромагнитного импульса предлагается использование следующих технических решений:

– экранированные контрольные / сигнальные кабели с надлежащим заземлением;
– устройства защиты от перенапряжения и / или фильтры низкого напряжения;
– использование оптоволоконных систем защиты и управления;
– модификации диспетчерских пунктов подстанций для улучшения свойств электромагнитного экранирования;
– улучшения заземления / соединения.

## Государственная политика защиты критической инфраструктуры за рубежом

Важнейшим из зарубежных нормативных актов в этой сфере противодействия чрезвычайным ситуациям является Указ Президента США Д. Трампа от 26.03.2019 г. №13865 «Координация национальной устойчивости к электромагнитным импульсам» («Coordinating National Resilience to Electromagnetic Pulses» / Executive Order 13865 of March 26, 2019).

Ключевые положения Указа Президента США Д. Трампа:

Раздел 6. Выполнение.

*(а) Определение национальных критических функций и связанной с ними приоритетной критической инфраструктуры, подверженной наибольшему риску.*

(1) В течение 90 дней с даты этого приказа Министр внутренней безопасности, в координации, должен определить и перечислить национальные критические функции и связанные с ними приоритетные системы критической инфраструктуры, сети и активы, включая космические средства, которые в случае выхода из строя могут привести к катастрофическим национальным или региональным последствиям для здоровья или безопасности населения, экономической безопасности или национальной безопасности.

(2) В течение 1 года после идентификации, описанной в подразделе (а) (1) данного раздела, Министр внутренней безопасности, в координации с …. ведомствами должен, используя соответствующие государственные и частные стандарты для ЭМИ, оценить, какие выявленные критически важные системы инфраструктуры, сети и активы наиболее уязвимы для воздействия ЭМИ.

*(б) Улучшение понимания влияния ЭМИ.*

(3) В течение 1 года с даты этого приказа и, в случае необходимости, после этого, Министр энергетики в консультации с ведомствами, должен пересмотреть существующие стандарты для ЭМИ и разработать или обновить, при необходимости, количественные эталоны, которые в достаточной мере описывают физические характеристики ЭМИ, включая форму волны и интенсивность, в форме, которая полезна и может быть предоставлена владельцам и операторам критически важной инфраструктуры.

(4) В течение 4 лет с даты этого приказа Министр внутренних дел должен завершить магнитотеллурическую съемку континентальной части США, чтобы помочь владельцам и операторам критически важной инфраструктуры провести оценку уязвимости ЭМИ.

*(в) Оценка подходов к смягчению последствий ЭМИ.*

(1) В течение 1 года с даты этого приказа и каждые 2 года после этого Министр внутренней безопасности по согласованию с ведомствами должны представить Президенту отчет, в котором анализируются доступные технологические варианты для повышения устойчивости критически важной инфраструктуры к воздействию ЭМИ.

(2) В течение 180 дней после завершения мероприятий, указанных в подразделах (б) (3) и (в) (1) настоящего раздела, Министр внутренней безопасности по согласованию с ведомствами, должен разработать и внедрить пилотное испытание для оценки доступных инженерных подходов для смягчения воздействия ЭМИ на наиболее уязвимые системы критической инфраструктуры, сети и активы, как указано в подразделе (а) (2) данного раздела.

(3) В течение 1 года с даты этого приказа Министр внутренней безопасности по согласованию с ведомствами, должны определять регулирующие и ненормативные механизмы, включая меры по возмещению затрат, которые могут усилить участие частного сектора в устранении последствий ЭМИ.

*(г) Укрепление критически важной инфраструктуры, чтобы противостоять воздействиям ЭМИ.*

(1) В течение 90 дней после завершения действий, указанных в подразделе (в) (2) этого раздела, Министр внутренней безопасности по согласованию с. ведомствами, должен разработать план по смягчению воздействия ЭМИ на уязвимые приоритетные системы критической инфраструктуры, сети и активы, указанные в подразделе (а) (2) настоящего раздела. План должен соответствовать и основываться на действиях, указанных в отчетах, предусмотренных Указом Правительства от 11 мая 2017 г. № 13800 («Усиление кибербезопасности федеральных сетей и критически важной инфраструктуры»).

(2) В течение 180 дней после завершения действий, указанных в подразделе (в) (1) данного раздела, Министр обороны в сотрудничестве с ведомствами должен провести пилотное испытание для оценки инженерных подходов, используемых для усиления защиты стратегических военных объектов, включая инфраструктуру, которая имеет решающее значение для поддержки этого объекта, от воздействия ЭМИ.

(3) В течение 180 дней после завершения пилотного тестирования, описанного в подразделе (г) (2) этого раздела, Министр обороны должен сообщить Президенту о стоимости и эффективности оцененных подходов.

*(д) Улучшение реакции на ЭМИ.*

(1) В течение 180 дней с даты этого приказа Министр внутренней безопасности в координации с ведомствами, должен пересмотреть и обновить федеральные планы, программы и процедуры реагирования с учетом эффектов ЭМИ.

(2) В течение 180 дней после завершения действий, указанных в подразделе (г) (1) этого раздела, агентства, которые поддерживают основные национальные функции, должны обновить операционные планы, документируя свои процедуры и обязанности по подготовке, защите и смягчению последствий ЭМИ.

(3) В течение 180 дней с момента выявления уязвимых приоритетных систем критической инфраструктуры, сетей и активов, как указано в подразделе (а) (2) настоящего раздела, Министр внутренней безопасности, совместно с ведомствами, должен предоставить заместителю помощника Президента по национальной безопасности и борьбе с терроризмом и директору Управления по науке и технологиям оценку последствий ЭМИ по критически важной инфраструктуре связи и рекомендовать изменения в оперативных планах для усиления национальных мер реагирования и восстановления после ЭМИ [7].

## Описание комплекса

По мнению авторов, необходимы меры противодействия угрозам целенаправленного воздействия электромагнитным импульсом на энергетическую инфраструктуру нашей страны, адекватные реализуемым в США [8; 9].

Предлагается формирование защищенных дата-центров, обслуживающих ситуационные центры в энергетике России, так как именно они обеспечивают подержание функций жизнеобеспечения энергетической инфраструктуры, в т.ч. противодействие чрезвычайным ситуациям.

Основываясь на стандартном базовом защищенном дата-центре можно будет реализовать:

– определение состава модулей информационно-управляющих систем из числа доступных компонент, выпускаемых серийно компаниями-производителями, а также стандартных конструктивов для размещения модулей и блоков;

– разработку системного и прикладного программного обеспечения в виде программного комплекса, ориентированного на решение заданных задач, оптимизированных под архитектуру информационных систем различных городских служб;

– разработку и программную реализацию алгоритмов решения ресурсоемких моделирующих задач, обработки и представления 3D-информации (с развитием в перспективе сервисов 4D BIM, 5D BIM, 6D BIM) в рамках задач “on-line” комплексного мониторинга и интеллектуального управления.

Для реализации поставленных целей противодействия чрезвычайным ситуациям предлагается разработать и развить новые методы и средства, которые позволят обеспечить получение всех заданных параметров базового защищенного дата-центра для ситуационных центров государственных органов и энергетических компаний, необходимых для его создания и дальнейшей правильной интеграции в сете- или полицентрическую суперсистему энергетической инфраструктуры [10; 11].

Предлагается в рамках крупной городской агломерации внедрить в информационную архитектуру инфраструктурной суперсистемы модельный образец защищенного дата-центра с элементами суперкомпьютерных технологий, подготовить рекомендации и схемы внедрения распределенных элементов такого защищенного дата-центра в ситуационные центры городских служб и инфраструктурных компаний для прикладных целей (электроэнергия, газ, тепло, горячая вода, питьевая вода и пр.).

Конечным результатом проводимых разработок должен стать цифровой комплекс на современной аппаратурной базе, позволяющий подключать сете- или полицентрические элементы для любых возможных конфигураций суперсистемы энергетической инфраструктуры [12].

## Выводы

Защищенный дата-центр позволит значительно повысить эффективность ведомственных информационно-управляющих систем в рамках инфраструктурной суперсистемы, применяемых при решении функциональных задач ситуационных центров для действий, как в обычных, так и в чрезвычайных условиях.

## Литература

1. Грабчак Е.П., Логинов Е.Л. Цифровые подходы к управлению объектами электро- и теплоэнергетики с применением интеллектуальных киберфизических систем // Надежность и безопасность энергетики. - 2019. - Т. 12. - № 3. - С. 172-176.

2. Иванов С.Н. Энергосбережение: проблемы достижения энергоэффективности. – М.: НИПЭБ. - 2009. – 329 с.

3. Шкрабляк А.С. Тенденции развития электронных финансовых транзакций и методов их контроля в глобальных телекоммуникационных сетях // Инженерная физика. - 2009. - № 9. - С. 47-53.

4. Логинов Е.Л., Логинов А.Е. Интеллектуальная электроэнергетика: новый формат интегрированного управления в единой энергетической системе России // Национальные интересы: приоритеты и безопасность. - 2012. - Т. 8. - № 29 (170). - С. 28-32.

5. Грабчак Е.П., Григорьев В.В., Логинов Е.Л. Поддержание работы управляющих систем энергетической инфраструктуры в условиях воздействий электромагнитного импульса природного или техногенного происхождения // Новые информационные технологии и системы. Сборник научных статей по материалам XVII Международной научно-технической конференции. - Пенза: Пензенский государственный университет.- 2020. - С. 3-5.

6. High-Altitude Electromagnetic Pulseand the Bulk Power System: Potential Impactsand Mitigation Strategies [Электронный ресурс] //https://www.epri.com/research/summary/000000003002014979 (Дата обращения: 05.04.2021)

7. Coordinating National Resilience to Electromagnetic Pulses» / Executive Order 13865 of March 26, 2019.

8. Грабчак Е.П., Логинов Е.Л. Комплексные подходы к защите систем автоматики и информационных сетей сложных энергетических объектов от естественных или искусственных электромагнитных воздействий критического характера // Проблемы обеспечения безопасности (Безопасность–2020): материалы II Международной научно-практической конференции. – Уфа: Уфимский государственный авиационный технический университет. - 2020. - С.8-10.

9. Грабчак Е.П., Логинов Е.Л., Логинова В.Е. Управляемая кластеризация и самовосстановление работы информационных систем в электро и теплоэнергетике в условиях каскадных аварийных ситуаций // Проблемы безопасности и чрезвычайных ситуаций. - 2020. - № 1. - С. 133-138.

10. Леонов В.Ю., Тизик А.П. Полиномиальный алгоритм решения целочисленной транспортной задачи // Труды Института Системного Анализа РАН. - 2008. - С. 154-156.

11. Логинов Е.Л., Грабчак Е.П., Григорьев В.В., Райков А.Н., Шкута А.А. Планирование мер поддержания интерактивной коммуникации информационных систем с учетом угроз возможного коллапса управления экономикой в особый период // Проблемы безопасности и чрезвычайных ситуаций. - 2019. - № 3. - С. 79-86.

12. Логинов Е.Л., Грабчак Е.П., Григорьев В.В., Райков А.Н., Шкута А.А. Управление экономикой России в условиях с предельно большой компонентой неопределенности развития чрезвычайных ситуации и критического недостатка информации // Проблемы безопасности и чрезвычайных ситуаций. - 2019. - № 4. - С. 104-110.

## Сведения об авторах

***Иванов Валерий Валерьевич*,** руководитель Ситуационно-аналитического центра Минэнерго России, 107996, ГСП-6, г. Москва, ул. Щепкина, дом 42, 8(495) 631-89-59, E-mail: IvanovV@minenergo.gov.ru

***Логинов Евгений Леонидович***, профессор РАН, дважды лауреат премии Правительства РФ в области науки и техники, начальник службы Ситуационно-аналитического центра Минэнерго России, 107996, ГСП-6, г. Москва, ул. Щепкина, дом 42, 8(903) 100-78-24, E-mail: evgenloginov@gmail.com