DOI: 10.25586/RNU.V9187.21.02.P.074 УДК 658

Е.П. Грабчак, Е.Л. Логинов

# ПРОТИВОДЕЙСТВИЕ УГРОЗАМ ВОЗДЕЙСТВИЯ ЭЛЕКТРОМАГНИТНОГО ИМПУЛЬСА: СТРАТЕГИЧЕСКИЕ ПОДХОДЫ К ЗАЩИТЕ КРИТИЧЕСКОЙ ЭНЕРГЕТИЧЕСКОЙ ИНФРАСТРУКТУРЫ В США

Рассмотрены вопросы обеспечения надежности энергоснабжения в условиях воздействия электромагнитного импульса естественного или искусственного характера. Проанализированы тенденции развития электромагнитного оружия в США и Китае. Кратко изложены взгляды американского экспертного сообщества на угрозы преднамеренного применения электромагнитного оружия против США и ущерба от такого воздействия. Описаны стратегические подходы, реализуемые различными государственными институтами США, направленные на обеспечение безопасности сетей критической энергетической и иной инфраструктуры и поддержание устойчивости их функционирования в условиях применения электромагнитного импульса.
*Ключевые слова:* электромагнитный импульс, системы управления, критическая инфраструктура, энергетика, угрозы, защита.

E.P. Grabchak, E.L. Loginov

# COUNTERING ELECTROMAGNETIC PULSE THREATS: STRATEGIC APPROACHES TO PROTECTING CRITICAL ENERGY INFRASTRUCTURE IN THE USA

The article is devoted to ensuring the reliability of power supply under the influence of an electromagnetic pulse of a natural or artificial nature. Trends in the development of electromagnetic weapons in the United States and China are analyzed. The views of the American expert community on the threats of the deliberate use of electromagnetic weapons against the United States and the damage from such an impact are briefly outlined. The article considers the strategic approaches implemented by various US government institutions aimed at ensuring the safety of critical energy and other infrastructure networks and maintaining the stability of their functioning under the conditions of the use of an electromagnetic pulse.
*Keywords:* electromagnetic pulse, control systems, critical infrastructure, energy, threats, protection.

*Вводные замечания*

Электромагнитное воздействие, потенциально угрожающее национальной безопасности критической инфраструктуры, может создаваться природным путем вследствие возмущений электрического и магнитного полей Земли, космических источников (солнечные бури), процессов, происходящих в атмосфере и в ионосфере, и техногенным путем в виде импульса двумя основными способами – ядерным взрывом и микроволновым излучением.

Высотный электромагнитный импульс – это электромагнитное поле, которое создается в атмосфере силой и излучением ядерного взрыва и наносит вред электронному оборудованию на очень большой площади в зависимости от мощности ядерного устройства и высоты взрыва.

**Грабчак Евгений Петрович**
заместитель министра энергетики Российской Федерации. Сфера научных интересов: энергетика, информатика, экономика. Автор 111 опубликованных научных работ.
E-mail: grabchak.eug@gmail.com

**Логинов Евгений Леонидович**
доктор экономических наук, профессор Российской академии наук, начальник экспертно-аналитической службы Ситуационно-аналитического центра Министерства энергетики России. Сфера научных интересов: энергетика, информатика, экономика. Автор 610 опубликованных научных работ.
E-mail: loginovel@mail.ru

Электромагнитная энергия высокочастотных микроволн может быть применена в форме импульса, создаваемого специальным электрическим оборудованием, которое преобразует энергию батареи, мощную химическую реакцию или взрыв в интенсивные микроволны, очень опасные для информационно-управляющих систем [15].

В последний период интенсивно развиваются технологии неядерного электромагнитного импульса (ЭМИ), также называемого сверхвысокочастотным оружием. Сочетание высокочастотных устройств с беспилотными летательными аппаратами (БПЛА) или крылатыми ракетами, оснащенными датчиками для отслеживания линий электропередач большой мощности, центров управления сетями и трансформаторов, представляет собой серьезную новую угрозу для национальных электрических сетей [9].

Президент Российской Федерации В.В. Путин 20 июня 2019 г. в ходе «Прямой линии» с гражданами России сообщил, что Россия прикладывает необходимые усилия для защиты энергетики от различных угроз. «Что касается работы нашей критически важной инфраструктуры, энергетики, в том числе и других областей, конечно, мы должны думать о том, как себя обезопасить от любых кибератак и любого негативного воздействия», – сказал В.В. Путин [8].

### *Результаты воздействия электромагнитного импульса природного и техногенного характера*

Проявления воздействия ядерного электромагнитного импульса рассматриваются как угроза критической инфраструктуре уже более полувека [1, 3].

Первый масштабный ущерб от ядерного электромагнитного импульса зафиксирован в 1962 г., когда термоядерная бомба Starfish Prime мощностью 1,4 мегатонны была взорвана США в 400 км над Тихим океаном.

Эффект от ядерного электромагнитного импульса, вызванного взрывом Starfish Prime, вывел из строя электрические сети и микроволновую линию телефонной связи в зоне протяженностью около 900 миль, в том числе на Гавайях.

Что касается природных явлений, то в 1989 г. неожиданная геомагнитная буря спровоцировала обрушение энергосистемы Hydro-Quebec, временно оставив без электричества 6 млн потребителей. Буря возникла в результате солнечного выброса размером в триллион кубических миль. Аналогичные бури случаются примерно каждые 60 лет [11].

Информационная безопасность

Сейчас уязвимость электрических сетей и линий связи от электромагнитного импульса еще более возросла вследствие расширения количества управляющих элементов интеллектуального характера [4, 5, 6]. При этом большинство энергетических проектов в разных странах мира не учитывают требования по устойчивости к ЭМИ, хотя имеются многочисленные международные стандарты по электромагнитной совместимости [2].

*Нарастание угроз преднамеренного применения электромагнитного импульса*

Технологии генерации электромагнитного импульса как оружия активно развиваются во многих странах [7]. Лидируют по этому направлению США, Китай, Израиль [10].

Так, например, 20 июля 2020 г. авиационно-космическая корпорация Northrop Grumman заключила стратегическое соглашение о поставках с Epirus, Inc., для возможности устанавливать компактный генератор ЭМИ в качестве компонента беспилотной воздушной системы C-UAS. Соглашение расширяет возможности использования ЭМИ на беспилотной воздушной системе C-UAS от Northrop Grumman, включая борьбу с роями враждебных БПЛА, в частности, дополняет набор некинетических эффектов, реализуемых C-UAS [17].

Китай, по данным США, разработал по крайней мере три вида высокотехнологичного оружия для атаки на электрические сети и ключевые технологии, что, по мнению американских экспертов, может вызвать внезапную атаку, аналогичную атаке на Перл-Харбор, что может привести к отключению электроэнергии всей страны [18].

По мнению американских экспертов, Китай построил сеть спутников, высокоскоростных ракет и электромагнитного импульсного оружия, которые могут повредить электрическую сеть США, подорвать критически важные коммуникации и даже ограничить возможности авианосных группировок [11].

*Анализ возможного ущерба от применения ЭМИ против США*

В 2007 г. Sage Policy Group of Baltimore and Instant Access Networks опубликовала исследование потенциального экономического воздействия атаки высотного электромагнитного импульса на американский регион Балтимор – Вашингтон – Ричмонд. Исследование сосредоточено на экономических эффектах ЭМИ, испытываемых регионом после высотного ЭМИ, генерируемого ядерным устройством, взорвавшимся на высоте 30–80 миль над землей и воздействующим на площадь радиусом не менее 500 миль.

Методология основывалась на предположениях о сбоях и повреждениях региональной электроэнергетической системы, систем связи, устройств управления системой и сбора данных (SCADA) и другой критической инфраструктуры, которые могут возникнуть в результате ЭМИ, и времени, необходимого для ремонта и восстановления хозяйственной деятельности.

В исследовании сделан вывод, что атака ЭМИ, затрагивающая регион Балтимор – Вашингтон – Ричмонд, может привести к потере экономического производства, потенциально превышающей 770 млрд долл. США, или 7% годового валового внутреннего продукта США на тот период. Даже при самых благоприятных предположениях, включая как

*Таблица 1*

**Оценки повреждений и времени восстановления после атаки высотного электромагнитного импульса региона Балтимор – Вашингтон – Ричмонд [14]**

| Инфраструктура | Поврежденная мощность (производительность), % | | | Среднее время замены, мес. | | |
|---|---|---|---|---|---|---|
| | Низкий | Средний | Высокий | Низкий | Средний | Высокий |
| ***Электрическая сеть*** | | | | | | |
| Трансформаторы | 10 | 40 | 70 | 2,5 | 13,5 | 33,0 |
| Другое оборудование | 30 | 40 | 50 | 1,5 | 5,0 | 10,0 |
| ***Системы связи*** | | | | | | |
| Большие системы | 10 | 20 | 50 | 4,0 | 18,0 | 27,0 |
| Малые системы | 5 | 20 | 50 | 2,0 | 12,0 | 17,0 |
| ***SCADA*** | | | | | | |
| Все типы | 5 | 20 | 50 | 1,5 | 5,0 | 10,0 |
| ***Электроника*** | | | | | | |
| Большие системы | 20 | 45 | 70 | 4,0 | 12,0 | 17,0 |
| Малые системы | 1 | 2 | 3 | 1,5 | 5,0 | 10,0 |

экранированную, так и неэкранированную критическую инфраструктуру, ЭМИ все равно может привести к ущербу, который потребует одного месяца восстановления и возникновения экономических потерь в размере десятков млрд долл. США (табл. 1).

По оценке ряда других американских экспертов, включая бывшего директора ЦРУ Р. Вулси, если США пострадают от удара ЭМИ, электричество отключится, военные системы будут блокированы, 99 ядерных реакторов, вероятно, расплавятся без электричества, необходимого для их охлаждения, и 4,1 млн человек, живущих рядом с ядерными реакторами, будут перемещены из-за распространения радиоактивного облака. Ущерб может включать в себя длительную потерю электроэнергии (из-за потери аварийных генераторов), отказы канализации, водопровода, банковской системы, стационарных телефонов, сотовой связи, транспортных средств. Гражданские беспорядки начнутся в считаные часы. На наведение порядка уйдет 18 месяцев [20].

*Защита управляющих систем критической инфраструктуры в США*

Комиссия по оценке угрозы от высотного электромагнитного импульса (Комиссия по ЭМИ) в США была учреждена Конгрессом еще в 2001 г. и с некоторыми изменениями в названии и по аспектам деятельности действует до сих пор.

В работе по этой проблеме также активно участвуют следующие департаменты и агентства США: Министерство внутренней безопасности, Министерство энергетики, Министерство обороны, Агентство национальной безопасности, Агентство кибербезопасности и инфраструктуры в сотрудничестве с Управлением по науке и технологиям и Федеральным агентством по чрезвычайным ситуациям и др.

В 2018 г. Министерство внутренней безопасности США выпустило «Стратегию защиты и подготовки Отечества к угрозам электромагнитного импульса и геомагнитных возмущений» [19], которая стала формулировкой целостного, долгосрочного подхода к защите критически важной инфраструктуры и подготовке к реагированию и восстановлению после потенциально катастрофических электромагнитных инцидентов.

Информационная безопасность

В августе 2020 г. Министерство внутренней безопасности США выпустило «Отчет о состоянии программы по электромагнитным импульсам» как часть обновленной информации о предпринимаемых усилиях по исполнению Указа Президента США Д. Трампа от 26 марта 2019 г. № 13865 «Координация национальной устойчивости к электромагнитным импульсам» [13].

Важнейшим из зарубежных нормативных актов в этой сфере является Указ Президента США Д. Трампа от 26 марта 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 с … …. 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 оперативные планы для усиления национальных мер реагирования и восстановления после ЭМИ [12].

Одно из подразделений ВВС США (Авиационный университет) сформировало целевую группу по электромагнитной защите, которая в отчетах за 2018 и 2019 гг. сформулировала следующие рекомендации.

Информационная безопасность

Базы и системы ВВС в континентальной части США и во всем мире больше не должны оставаться уязвимыми для длительных отключений электроэнергии за пределами площадки и связанной с этим нехватки топлива.

Военно-воздушным силам следует развернуть на выбранных базах автономные защищенные источники питания (например, очень маленькие атомные электростанции, возможно, мобильные ядерные генераторы) вместе с защищенными местными хранилищами топлива в течение длительных периодов времени.

Электроника во всех основных военных системах должна быть испытана и сертифицирована, чтобы выдерживать ожидаемые серьезные воздействия, генерируемые ЭМИ [14].

*Защита управляющих систем критической инфраструктуры Российской Федерации*

Для разработки комплексных основ защиты управляющих систем критической инфраструктуры Российской Федерации, по мнению авторов, необходимо определить методологию построения математических оценок показателей поддержания управляемых соединений в отношении функционирования систем управления и на этой основе выработать меры защиты всех уровней администрирования от ущерба вследствие воздействия ЭМИ с учетом особенностей управления конкретным видом предметной деятельности в виде аналитических зависимостей, которые обеспечивают поддержание необходимых режимов реализации гибких информационных и технологических связей.

С учетом американского опыта можно предложить следующие мероприятия практического характера по повышению стойкости управляющих систем критической инфраструктуры Российской Федерации к электромагнитным воздействиям искусственного характера:

- анализ и типизация характеристик возможных источников преднамеренных электромагнитных воздействий на управляющие элементы критической инфраструктуры, анализ международных и зарубежных стандартов электромагнитной безопасности и их применимости на территории Российской Федерации;
- анализ тенденций развития критической инфраструктуры, выявление ее критически уязвимых элементов и описание этих элементов как объектов атаки электромагнитного воздействия;
- оценка возможных последствий преднамеренного электромагнитного воздействия на управляющие элементы критической инфраструктуры в зависимости от сценариев такого воздействия;
- организация и проведение работ по оценке стойкости управляющих элементов критической инфраструктуры к мощным электромагнитным воздействиям;
- разработка нормативных актов по обеспечению устойчивости управляющих элементов критической инфраструктуры в условиях применения источников электромагнитных воздействий;
- выработка рекомендаций для отечественных производителей защитных устройств (в том числе полупроводникового типа) с целью импортозамещения ключевых элементов защиты оборудования критической инфраструктуры от электромагнитного воздействия;

• внедрение средств защиты управляющих элементов критической инфраструктуры от преднамеренного электромагнитного воздействия в российских компаниях всех форм собственности.

В информационно-управляющих системах компаний критической инфраструктуры России необходимо внедрение Tier 3 стандарта TIA-942 (Telecommunications Industry Association – Telecommunications Infrastructure Standard for Data Centers) с постепенным переходом к Tier 4, что в условиях внедрения цифровых технологий позволит сформировать базу для полноценной защиты управляющих элементов критической инфраструктуры с повышенными требованиями к отказоустойчивости.

*Заключение*

Таким образом, рассматриваемые стратегические подходы к защите критической энергетической инфраструктуры в США обеспечивают упреждающую идентификацию уязвимостей к ущербу при атаках с использованием ЭМИ и, как следствие, поддержание устойчивости работы критической энергетической и иной инфраструктуры.

Аналогичные меры необходимо реализовать и в Российской Федерации.

Идентификация уязвимостей критической энергетической инфраструктуры позволяет осуществлять упреждающие каскадные отключения и планирование мер, направленных на повышение устойчивости всей суперсистемы критической инфраструктуры к воздействию ЭМИ.

## Литература

1. *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: Сб. науч. ст. по мат. XVI Междунар. науч.-техн. конф. Пенза, 18–19 ноября 2020 г. Пенза: Изд-во Пензенского государственного ун-та, 2020. С. 3–5.
2. *Грабчак Е.П., Григорьев В.В., Логинов Е.Л.* Поддержание режимов работы тепло- и электроэнергетической суперсистемы в условиях технологических воздействий, которые не учитывались при построении ее сегментов // Проблемы безопасности и чрезвычайных ситуаций. 2020. № 2. С. 5–12.
3. *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): Мат. II Междунар. науч.-практ. конф. Уфа, 8 апреля 2020 г. Уфа: Изд-во Уфимского государственного авиационного технического ун-та, 2020. С. 8–10.
4. *Грабчак Е.П., Логинов Е.Л.* Обеспечение устойчивости управления энерго-, теплогенерирующими и сетевыми объектами с большим количеством интеллектуальных элементов в условиях чрезвычайных ситуаций и опасных событий естественного и искусственного характера // Управленческий и сервисный потенциал цифровой экономики: проблемы и перспективы: Мат. междунар. науч.-практ. конф. Омск, 14–15 мая 2020 г. Омск: Изд-во Омского государственного технического ун-та, 2020. С. 156–158.
5. *Грабчак Е.П., Логинов Е.Л.* Цифровая энергетика: повышение надежности управления электро- и теплоэнергетическими системами на основе внедрения цифровых

технологий. М.: Изд-во Международного научно-исследовательского ин-та проблем управления, Изд-во Ин-та экономических стратегий, 2020. 222 с.
6. *Грабчак Е.П.* Цифровая трансформация электроэнергетики. М.: Кнорус, 2018. 340 с.
7. *Гуревич В.И.* Электромагнитный импульс высотного ядерного взрыва и защита электрооборудования от него. М.: Инфра-Инженерия, 2018. 516 с.
8. «Прямая линия» с Владимиром Путиным. Главное / Интерфакс [Электронный ресурс]. – URL: https://www.interfax.ru/russia/666034 (дата обращения: 16.03.2021).
9. 21st Century Complete Guide to Electromagnetic Pulse (EMP): Nuclear Weapon Effects (NWE) and the Threat to the Electric Grid and Critical Infrastructure, HEMP, EMI, Microwave Devices. Progressive Management, 2017. 494 p.
10. 2020 Department of Defense Electromagnetic Spectrum Superiority Strategy / U.S. Department of Defense. – URL: https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_spectrum_superiority_strategy.pdf (date of the application: 16.03.2021).
11. *Conca J.* China Has "First-Strike" Capability To Melt U.S. Power Grid With Electromagnetic Pulse Weapon / Forbes. – URL: https://www.forbes.com/sites/jamesconca/2020/06/25/china-develops-first-strike-capability-with-electromagnetic-pulse/?sh=37db3664e190 (date of the application: 16.03.2021).
12. Coordinating National Resilience to Electromagnetic Pulses: Executive Order 13865 of March 26, 2019 // Federal Register. 2019. Vol. 84, no. 61. Pp. 12041–12046.
13. Electromagnetic Pulse (EMP): Program Status Report / Cybersecurity & Infrastructure Security Agency [Digital Resource]. – URL: https://www.cisa.gov/sites/default/files/publications/emp-program-status-report_508.pdf (date of the application: 16.03.2021).
14. *Haller N.M., Pry P.V.* The Air Force Should Assure Defenses Against Nuclear EMP Threats as It Seeks Electromagnetic Spectrum Superiority / RealClearDefense [Digital Resource]. – URL: https://www.realcleardefense.com/articles/2021/02/04/the_air_force_should_assure_defenses_against_nuclear_emp_threats_as_it_seeks_electromagnetic_spectrum_superiority_659137.html (date of the application: 16.03.2021).
15. High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments / Every CRS Report [Digital Resource]. – URL: https://www.everycrsreport.com/reports/RL32544.html#_Toc225837619 (date of the application: 16.03.2021).
16. Initial Economic Assessment of Electromagnetic Pulse (EMP) Impact upon the Baltimore-Washington-Richmond Region / Sage Policy Group. Washington D.C., Baltimore, MD., Frostburg, MD: Instant Access Networks, LLC, 2007. 27 p.
17. Northrop Grumman Taps Epirus for Electromagnetic Pulse C-UAS Weapon System / Northrop Grumman [Digital Resource]. – URL: https://news.northropgrumman.com/news/releases/northrop-grumman-taps-epirus-for-electromagnetic-pulse-c-uas-weapon-system (date of the application: 16.03.2021).
18. *Pry P.V.* China: EMP Threat. The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack / Index Investor [Digital Resource]. – URL: https://www.indexinvestor.com/resources/Research-Materials/Cyber-Solar-EMP/China-EMP-Threat-Assessment.pdf (date of the application: 16.03.2021).
19. Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances / Homeland Security [Digital Resource]. – URL: https://www.dhs.gov/sites/default/files/publications/18_1009_EMP_GMD_Strategy-Non-Embargoed.pdf (date of the application: 16.03.2021).

20. *Stuckenberg D., Woolsey J., DeMaio D.* Electromagnetic Defense Task Force: Report / ed. by E.A. Rockwell. Air University Press, 2018. 66 p.

## References

1. Grabchak E.P., Grigor'ev V.V., Loginov E.L. (2020) Podderzhanie raboty upravlyayushchikh sistem energeticheskoj infrastruktury v usloviyakh vozdejstvij elektromagnitnogo impul'sa prirodnogo ili tekhnogennogo proiskhozhdeniya [Maintaining the Operation of the Control Systems of the Energy Infrastructure Under the Influence of an Electromagnetic Pulse of Natural or Man-Made Origin]. *Novye informatsionnye tekhnologii i sistemy: Sb. nauch. st. po mat. XVII Mezhdunar. nauch.-tekhn. konf.* [New Information Technologies and Systems: Proceedings of the XVI International Conference of Science and Technology], Penza, November 18–19, 2020, Penza, Penza State University Publishing, pp. 3–5 (in Russian).
2. Grabchak E.P., Grigor'ev V.V., Loginov E.L. (2020) Podderzhanie rezhimov raboty teplo- i elektroenergeticheskoj supersistemy v usloviyakh tekhnologicheskikh vozdejstvij, kotorye ne uchityvalis' pri postroenii ee segmentov [Maintenance of Operating Modes of Heat and Power Supersystems in the Conditions of Technological Influences, Which Were Not Taken Into Account When Constructing Its Segments]. *Safety and Emergencies Problems*, no. 2, pp. 5–12 (in Russian).
3. Grabchak E.P., Loginov E.L. (2020) Kompleksnye podkhody k zashchite sistem avtomatiki i informatsionnykh setej slozhnykh energeticheskikh ob"ektov ot estestvennykh ili iskusstvennykh elektromagnitnykh vozdejstvij kriticheskogo kharaktera [Integrated Approaches to the Protection of Automation Systems and Information Networks of Complex Energy Facilities From Natural or Artificial Electromagnetic Influences of a Critical Nature]. *Problemy obespecheniya bezopasnosti (Bezopasnost'–2020): Mat. II Mezhdunar. nauch.-prakt. konf.* [Problems of Security (Security-2020: Proceedings of the International Scientific and Practical Conference], Ufa, April 8, 2020, Ufa, Ufa State Aviation Technical University Publishing, pp. 8–10 (in Russian).
4. Grabchak E.P., Loginov E.L. (2020) Obespechenie ustojchivosti upravleniya energo-, teplogeneriruyushchimi i setevymi ob"ektami s bol'shim kolichestvom intellektual'nykh elementov v usloviyakh chrezvychajnykh situatsij i opasnykh sobytij estestvennogo i iskusstvennogo kharaktera [Ensuring the Sustainability of the Management of Energy, Heat Generating and Network Facilities With a Large Number of Intelligent Elements in Emergency Situations and Dangerous Events of a Natural and Artificial Nature]. *Upravlencheskij i servisnyj potentsial tsifrovoj ekonomiki: problemy i perspektivy: Mat. Mezhdunar. nauch.-prakt. konf.* [Management and Service Potential of the Digital Economy: Problems and Prospects: Proceedings of the International Scientific and Practical Conference], Omsk, May 14–15, 2020, Omsk, Omsk State Technical University Publishing, pp. 156–158 (in Russian).
5. Grabchak E.P., Loginov E.L. (2020) *Tsifrovaya energetika: povyshenie nadezhnosti upravleniya elektro- i teploenergeticheskimi sistemami na osnove vnedreniya tsifrovykh tekhnologij* [Digital Energy: Improving the Reliability of Control of Electrical and Heat Power Systems Based on the Introduction of Digital Technologies]. Moscow, International Research Institute for Advanced Systems Publishing, Institute for Economic Strategies Publishing. 222 p. (in Russian).
6. Grabchak E.P. (2018) *Tsifrovaya transformatsiya elektroenergetiki* [Digital Transformation of the Electric Power Industry]. Moscow, Knorus Publishing. 340 p. (in Russian).

7. Gurevich V.I. (2018) *Elektromagnitnyj impul's vysotnogo yadernogo vzryva i zashchita elektrooborudovaniya ot nego* [Electromagnetic Impulse of a High-Altitude Nuclear Explosion and Protection of Electrical Equipment From It]. Moscow, Infra-Inzheneriya Publishing. 516 p. (in Russian).
8. (2019) "Pryamaya liniya" s Vladimirom Putinym. Glavnoe [Direct Line with Vladimir Putin. The Main Thing]. *Interfax*. Available at: https://www.interfax.ru/russia/666034 (date of the application: 16.03.2021) (in Russian).
9. (2017) 21st Century Complete Guide to Electromagnetic Pulse (EMP): Nuclear Weapon Effects (NWE) and the Threat to the Electric Grid and Critical Infrastructure, HEMP, EMI, Microwave Devices. Progressive Management, 2013. 494 p.
10. 2020 Department of Defense Electromagnetic Spectrum Superiority Strategy. *U.S. Department of Defense.* Available at: https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/Electromagnetic_spectrum_superiority_strategy.pdf (date of the application: 16.03.2021).
11. Conca J. (2020) China Has "First-Strike" Capability to Melt U.S. Power Grid With Electromagnetic Pulse Weapon. *Forbes*. Available at: https://www.forbes.com/sites/jamesconca/2020/06/25/china-develops-first-strike-capability-with-electromagnetic-pulse/?sh=37db3664e190 (date of the application: 16.03.2021).
12. (2019) Coordinating National Resilience to Electromagnetic Pulses: Executive Order 13865 of March 26, 2019. *Federal Register*, vol. 84, no. 61, pp. 12041–12046.
13. (2020) Electromagnetic Pulse (EMP): Program Status Report. *Cybersecurity & Infrastructure Security Agency*. Available at: https://www.cisa.gov/sites/default/files/publications/emp-program-status-report_508.pdf (date of the application: 16.03.2021).
14. Haller N.M., Pry P.V. (2021) The Air Force Should Assure Defenses Against Nuclear EMP Threats as It Seeks Electromagnetic Spectrum Superiority. *RealClearDefense*. Available at: https://www.realcleardefense.com/articles/2021/02/04/the_air_force_should_assure_defenses_against_nuclear_emp_threats_as_it_seeks_electromagnetic_spectrum_superiority_659137.html (date of the application: 16.03.2021).
15. (2008) High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments. *Every CRS Report*. Available at: https://www.everycrsreport.com/reports/RL32544.html#_Toc225837619 (date of the application: 16.03.2021).
16. (2007) *Initial Economic Assessment of Electromagnetic Pulse (EMP) Impact upon the Baltimore-Washington-Richmond Region*. By Sage Policy Group. Washington D.C., Baltimore, MD., Frostburg, MD, Instant Access Networks, LLC. 27 p.
17. (2020) Northrop Grumman Taps Epirus for Electromagnetic Pulse C-UAS Weapon System. *Northrop Grumman*. Available at: https://news.northropgrumman.com/news/releases/northrop-grumman-taps-epirus-for-electromagnetic-pulse-c-uas-weapon-system (date of the application: 16.03.2021).
18. Pry P.V. (2020) China: EMP Threat. The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack. *Index Investor*. Available at: https://www.indexinvestor.com/resources/Research-Materials/Cyber-Solar-EMP/China-EMP-Threat-Assessment.pdf (date of the application: 16.03.2021).
19. (2018) Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances. *Homeland Security*. Available at: https://www.dhs.gov/sites/default/files/publications/18_1009_EMP_GMD_Strategy-Non-Embargoed.pdf (date of the application: 16.03.2021).
20. Stuckenberg D., Woolsey J., DeMaio D. (2018) *Electromagnetic Defense Task Force: Report*. Ed. by E.A. Rockwell. Air University Press, 2018. 66 p.