

IMPACT OF ELECTROMAGNETIC FIELDS ON INFORMATION SECURITY AND PUBLIC HEALTH

Krasimira Staneva

University of Forestry, Sofia, Bulgaria, bagg.ks@gmail.com

Martin Marinov

University of Library Studies and Information Technologies, Bulgaria, martinemarinov95@gmail.com

Abstract: The article presents the results of a non-standard study concerning the impact of electromagnetic waves through which data are transmitted in cyberspace on two elements of the national security system - public health and information security. Cyberspace as a global network of interconnected information and communication systems operates through physical systems and infrastructure—hardware, routers, hubs, telecommunications networks, computer systems, and all Internet-connected devices, including medical. The impact of digital connectivity on socio-economic development is multidirectional. For the economy, it has access to existing markets and creates new ones.. In the business sphere, an efficient connection is made between human resources and the resources needed by the production process, and in the social sphere, publicly accessible services are provided through online portals. In our study, public health has a special status because of the critical information related to the health and safety of human life, which creates, manages and controls all processes related to material production. A mechanism by which EMF affects the environment and human health is described. The sources of radio frequency fields and their biological effects are discussed. A growing trend towards the manifestation of chronic fatigue and stress among active users of smart technologies is outlined and solutions for health prevention of the young generation are proposed. Cyberspace provides a strategic advantage, and for this in the field of cyber security, the likely causes of cyber risks are described, which are related to the fusion of critical and non-critical technologies, increased volume of personal and sensitive data generated, dependence on third-party managed service providers, leakage of information under influence of EMF on the example of the TEMPEST attacks. Good practices for prevention and cyber resilience are analyzed.

Keywords: EMF, human health, information security, TEMPEST, cyber resilience

ВЛИЯНИЕ НА ЕЛЕКТРОМАГНИТНИТЕ ПОЛЕТА ВЪРХУ ИНФОРМАЦИОННАТА СИГУРНОСТ И ОБЩЕСТВЕНОТО ЗДРАВЕ

Красимира Станева

Лесотехнически университет, Р България, bagg.ks@gmail.com

Мартин Маринов

УниБит, Р България, martinemarinov95@gmail.com

Резиме: В настоящата статия са представени резултатите от нестандартно проучване, засягащо влиянието на електромагнитните вълни, чрез които се предават данните в киберпространството върху два елемента от системата на националната сигурност-общественото здраве и информационната сигурност. Киберпространството като глобална мрежа от взаимосвързани информационни и комуникационни системи функционира посредством физическата си инфраструктура-хардуер, рутери, хъбове, телекомуникационни мрежи, компютърни системи и всички устройства, свързани с интернет, включително медицинските. Влиянието на дигиталната свързаност върху обществено-икономическото развитие е разнопосочно. За сферата на икономиката тя осигурява достъп до съществуващи пазари и създава нови такива. В сферата на бизнеса се осъществява ефикасна връзка между човешки ресурс и ресурсите, от които се нуждае производственият процес, а в социалната сфера се предоставят обществено достъпни услуги посредством онлайн портали. В нашето проучване общественото здраве е със специален статут, поради критичната информация, свързана със здравето и безопасността за живота на човека, който създава, управлява и контролира всички процеси, свързани с материалното производство. Описан е механизма, по който ЕМП въздействат върху човешкото здраве. Разгледани са източниците на радиочестотни полета и биологичните ефекти от тях. Очертана е нарастваща тенденция на проява на хронична умора и стрес сред активните ползватели на смарт технологии и са предложени решения за здравна превенция на младото поколение. Киберпространството осигурява стратегическо предимство и за това в сферата на киберсигурността са описани вероятните причини за киберрискове, които са свързани със сливане на критични и некритични

технологии, увеличен обем генерирани лични и чувствителни данни, зависимост от трети страни доставчици на управлявани услуги и изтичане на информация под влияние на ЕМП на примера на TEMPEST атаките. Анализирани са добри практики за превенция и киберустойчивост.

Ключови думи: ЕМП, човешко здраве, информационна сигурност, TEMPEST, киберустойчивост

1. УВОД

Приложението на смарт технологиите за комуникация, обучение, дигитална трансформация на бизнеса, в здравеопазването и за управление на ежедневните ни дейности е свързано с въздействието на свързаните с тях електромагнитни полета, които имат различни генезис и характеристика. Тяхното влияние върху икономическото развитие, екологическата и информационната сигурност и общественото здраве като елемент от националната сигурност са сериозно предизвикателство, пред което сме изправени в информационното общество. То е възникнало като естествен резултат от промяна в отношението на обществото към информацията. Така до средата на 20 в. информацията се приема като спомагателен ресурс за производствената сфера [3], докато понастоящем тя се възприема като основен ресурс за развитие на икономиката и социалната сфера и оказва сериозно влияние върху развитието на обществено-политическата система. Облекченият достъп до информационните ресурси е съществено достижение на обществото, но заедно с ползите от това се развива среда за тяхното неправомерно използване. Информационната сигурност, в частност кибер сигурността в сферата на общественото здраве, я разглеждаме като съществен елемент от системата на националната сигурност поради обстоятелството, че тя оперира със специфична информация, свързана със здравето и безопасността за живота на човека, който създава, управлява и контролира всички процеси в общество.

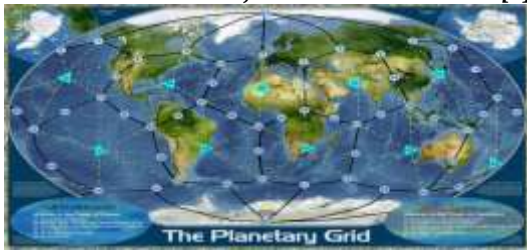
2. МЕТОДОЛОГИЯ НА ПРОУЧВАНЕТО

За целите на настоящето проучване е проведен интегративен анализ на литературни източници, при който са синтезирани данните по изучавания проблем и е обобщена съществуващата информация.

3. ИЗТОЧНИЦИ НА ЕЛЕКТРОМАГНИТНИ ПОЛЕТА

Земята като физично тяло може да се охарактеризира чрез стойностите на електромагнитното, гравитационното и топлинното си поле. В настоящата работа вниманието ни е фокусирано върху влиянието на естественото електромагнитно поле, вълните Schumann [9,16] и продуцираното /антропогенно/ електромагнитно поле [7]. Естественото електромагнитно поле ЕМП е една от основните физически характеристики на Земята и неговият произход е свързан с непрекъснатото триене на вещества с различна плътност в земната вътрешност. Възникването и развитието на организмовия свят е осъществено в условията на непрекъснато влияние на ЕМП върху него, като се приема, че биологичният вид се развива в оптимални за жизнените му функции екологически условия. По експериментален път е доказано наличието на земен енергиен скелет (фиг.1). Той е обусловен от наличието на естествени геоложки структури, които имат способността да поглъщат електромагнитните вълни от Космоса и да натрупват в себе си непрекъснато възникващата земна енергия. Сред енергийните клетки, участващи в планетарния енергиен модел от първостепенно значение за нормалното функциониране на организмовия свят и телекомуникационните системи са клетките на на Хартман и Курри. Влиянието на ELF електромагнитните Schumann вълни, които участват в общия енергиен баланс на Земята, се основава на тяхната честота на трептене $/7,83 \text{ Hz} /$, която е близка до тази на човешкия мозък. Въздействието, което оказват върху човешкия организъм се свежда до поддържане на неговия биологичен часовник и хормоналния баланс [7].

Фиг. 1 Планетарен модел на енергийния скелет по В. Ирд, 1975. Източник: [8]

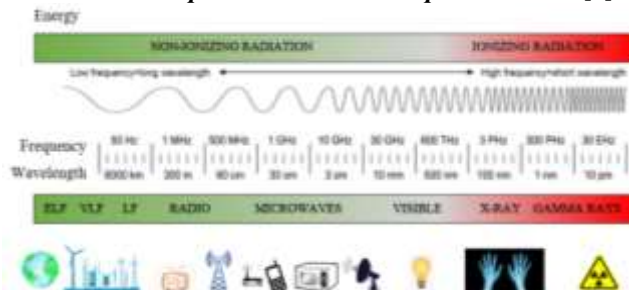


Фиг. 2 Схема на киберпространството, Източник: [13]



Наред с естествените ЕМП съществуват и изкуствени. Електромагнитните вълни с крайно ниски честоти ELF, свръх ниски SLF и инфраниски ILF се характеризират с честоти в диапазона 3-30 Hz. Те се генерират от електрическите проводници и използваната електроника. ELF-EMF се излъчва от линиите на високо напрежение, които пренасят електроенергия от електроцентралите до домовете ни. Радиовълните /в обхвата от 3 KHz до 300 GHz / се разпространяват в пространството посредством антена с подходящи размери. RF-EMF се излъчва от мобилни телефони, Wi-Fi системи, сателитни комуникационни системи, радио- и TV станции и интерактивни радиостанции. Сензорите, които се използват за IoT са в същия радиодиапазон, но с увеличаване на техния брой и необходимостта за увеличаване на трансфера на данни между тях, непрекъснато се увеличава и честотата на използвания радио сигнал. Те работят на принципа на излъчване на електромагнитни вълни.

Фиг. 3 Електромагнитен спектър Източник: [2]



Би могло да се обобщи, че изкуствено ЕМП се формира при функционирането на техническите средства, ползвани в информационните и телекомуникационните технологии, на домакинските електроуреди, медицинската апаратура, всички прибори, формиращи смарт средата и осигуряващи дигитална свързаност. Електромагнитното излъчване от тях натоварва околната среда и оказва влияние върху елементите на природната екосистема, включително върху живите организми. През 1995 г. Световната здравна организация /СЗО/ отчитайки промените, които настъпват в резултат от въздействието на нейонизиращата радиация, въвежда термина „електромагнитно замърсяване на околната среда”, а през 2002 г. във връзка с увеличаващите се научни съобщения за пряка връзка на редица заболявания и дискомфорт у хората, предлага нова медицинска диагноза „Синдром на хиперчувствителност към електрозамърсяване / EHS/. Той се свързва с нарушения на съня, депресия, постоянна умора, стрес, мускулни болки, кожни раздразнения и други симптоми, свързани с функционирането на нервната система [21].

4. ДИГИТАЛНА СВЪРЗАНОСТ, КИБЕРПРОСТРАНСТВО, КИБЕРСИГУРНОСТ

Влиянието на дигиталната свързаност върху обществено-икономическото развитие е разнопосочно. За сферата на икономиката тя осигурява достъп до съществуващи пазари и създава нови такива. В сферата на бизнеса се осъществява ефикасна връзка между човешки ресурс и ресурсите, от които се нуждае производственият процес. В социалната сфера се предоставят обществено достъпни услуги посредством онлайн портали.

Сливането на критични и некритични технологии в отделните сектори на производството става все по-осезателно и свързаните с това рискове преминават в незасегнати до този момент области от икономиката, което ги прави изключително чувствителни по отношение сигурност на информационните ресурси. Един подходящ пример е взаимодействието между регулирания енергиен сектор и иновативния сектор, свързан със зарядните станции за електромобили. Съхраняването на информацията във все по-бързо развиващата се смарт среда се очертава сериозно предизвикателство пред експертите както от киберсигурността, така и от информационната сигурност. Като се добави сериозният ръст на доставка на т.нар. управлявани услуги от трети страни, които имат привилегирован достъп до информационните ресурси на клиентите си, се очертава и реалната възможност за нарастване на риска за информационната сигурност днес.

Киберпространството /фиг.2/ като глобална мрежа от взаимосвързани информационни и комуникационни системи функционира посредством физическата си инфраструктура- хардуер, рутери, хъбове, телекомуникационни мрежи, компютърни системи и всички устройства, свързани с интернет, включително медицинските. По своята същност киберпространството е електронна и електромагнитна среда за съхраняване и обмен на информация с мрежови системи и свързана физическа инфраструктура [10].

За развитие на конкурентоспособна и устойчива икономика дигиталните инфраструктури са от определящо значение. Те придобиха водеща роля в управлението на ресурсите и всички системи с национално значение. Според Национална стратегия за киберсигурност „Киберустойчива България 2020” съвременното общество, в това число неговите дейности са достигнали до високо ниво на дигитална зависимост, което е пряко свързано развитието на рискове и заплахи с „непознат досега мащаб и потенциална сила на въздействие” [4]. “Киберпространството предоставя големи възможности за развитие, но води и до нарастваща и необратима цифрова зависимост на основните функции и дейности в обществото. Злонамерени или неумишлени действия могат да доведат до нарушаване работата на системите за управление и устройствата, свързани с критичната инфраструктура и възпрепятстване на нормалното им функциониране” [1].

Предвид обстоятелството, че значителна част от информационните ресурси се предават и съхраняват посредством взаимосвързаните информационни и комуникационни системи, заплахата за тяхната сигурност нараства неимоверно с развитието на киберпространството и технологиите, които се ползват. В споделеното пространство се намира разнообразна информация, засягаща банковите операции на фирми и физически лица, ресурсното обезпечаване на сектори от икономиката, здравословното състояние на населението, биометрични данни, работни процедури и протоколи, засягащи информационната сигурност и военната индустрия и т.н. Чувствителността на киберпространството се определя от неговата послойна характеристика- виртуална, логическа и физическа, като неотменна част от физическия слой е електромагнитният спектър, чрез който се предават данните.

5. ВЛИЯНИЕ НА УМИШЛЕНИТЕ ЕЛЕКТРОМАГНИТНИ СМУЩЕНИЯ ВЪРХУ ИНФОРМАЦИОННАТА СИГУРНОСТ

Възможните рискове при управление на информационната сигурност, свързани с ЕМП се свеждат до изтичане на информация от непреднамерено електромагнитно излъчване от телекомуникационно оборудване, променена електромагнитна среда вследствие умишлена модификация на чипове и устройства / добавяне на функции, които не са технологично зададени от дизайнера/Тези технологични схеми са известни като хардуерен троянски кон (НТ). Проблемът с изтичането на информация чрез електромагнитно /ЕМ/ излъчване е бил обект на проучване още през 50-те години на 20 век. Специфичният изследователски подход, съвкупност от техники и стандарти за контролиране на сигурността, е придобил известност като TEMPEST (Transient Electromagnetic Pulse Emanation Standard). В своя първоначален вид този подход е съсредоточен върху игнориране на ненужни електромагнитни излъчвания, посредством които би могло да се извлича информация. Предвид облекчения механизъм на функциониране и ниската му себестойност, методът много бързо се разпространява извън първоначалната си сфера на приложение и днес ИКТ устройства, склонни към атаки на TEMPEST, включват разнообразно търговско оборудване, с което се обработват лични и чувствителни данни, в т.ч. скенери, сензорни монитори, принтери и т.н. В сферата на информационна сигурност TEMPEST се прилага за проверка и контрол на нежелано излъчване на електромагнитна енергия, причинено от функциониращите електрически и електронни устройства. Атаките от вида TEMPEST са приложими за добиване на поверителна информация. Чрез неоторизиран достъп, електромагнитните емисии, излъчвани от тези устройства, могат да се преобразуват в цифрови данни, за да осигурят отдалечен достъп до тях, като по този начин се създава уязвимост на сигурността. С помощта на подходящи информационни системи, електромагнитните вълни могат да бъдат записани на големи разстояния и да бъдат реконструирани чрез обработка на електромагнитното излъчване и по този начин е възможно да се получи желана информация [9]. За разлика от други известни методи за кибератака, методите за атака на TEMPEST не са добре познати и това създава допълнителен риск за информационното общество като може да причини големи щети, ако не се вземат необходимите мерки за превенция /фиг. 3/.

Фиг. 4 Принципна схема на компрометиране на информационната сигурност под влияние на електромагнитно поле Източник: [20]



6. ВЛИЯНИЕ НА ЕЛЕКТРОМАГНИТНОТО ПОЛЕ ВЪРХУ ЧОВЕШКИЯ ОРГАНИЗЪМ И СИГУРНОСТТА В ОБЩЕСТВЕННОТО ЗДРАВЕ

Въздействието на ЕМП върху човешкия организъм предизвиква ответна реакция на клетъчно, системно и организмово ниво. Под влияние на ЕМП могат да се разкъсват клетъчните мембрани, влияят върху ДНК, клетъчен генетичен материал и посоките му към клетките по начин, който може да генерира заболяване; предизвикват оксидативен стрес и свободни радикали, които компрометират имунитета, причиняват стареене и заболявания и намаляват способността на организма да се самоизлекува чрез потискане на производството или активността на антиоксиданти (мелатонин, супероксиддисмутаза / SOD и глутатион пероксидаза); причиняват нарушения на кръвно-мозъчната бариера, която предпазва мозъка от токсини и осигурява задържането на цереброспинални течности, водят до увеличаване на „стелт“ стреса върху тялото, който може да увеличи риска от сърдечни заболявания, хипертония, висок холестерол, диабет, проблеми с храносмилането и репродуктивни проблеми. Излагането на ЕМП може да провокира проблеми с паметта, и поведенчески проблеми. Електромагнитни вълни, по-специално RF-EMF, излъчвани от мобилните телефони, се абсорбират в мозъка до такава степен, че могат да повлияят на активността на невроните. Изследвания показват, че RF-EMF, излъчвани от мобилни телефони, активират метаболитните процеси в човешкия мозък. Топлинните ефекти на RF-EMF, генерирани от мобилните телефони могат да повлияят и на невронната активност. Широкото навлизане на 5G мрежите и свързаният с тях IoT ще увеличат значително броя на безжичните устройства, като това изисква висока плътност на физическата инфраструктура [17]. С това нараства и риска за човешкото здраве, който все още не е достатъчно добре проучен, както е необходим и анализ по отношение сигурността на информацията, съхранявана за здравния статус на населението.

Значимостта на въздействието на ЕМП върху човешкия организъм за състоянието на общественото здраве е намерило място в сериозни проучвания от 1996 г до днес, като синдромът на хиперчувствителност към ЕМП /EHS/ се характеризира с разнообразие от неспецифични симптоми: психологическо разстройство, боцкане, усещане за парене и обриви, болка и крампи в мускулите, умора, проблеми със зрението и много други [12]. Така описаната симптоматика е базирана на реални проучвания и непрекъснато се увеличава нейното многообразие във форми на проявление и степен на тежест при отделните индивиди. Обобщаващото е, че наличието на тези симптоми може да доведе до промяна на начина на живот, което се отразява както върху личностното развитие и реализация, така и върху чувствителния елемент от националната сигурност-общественото здраве.

С широкото навлизане на уелнес културата в нашето общество, която пледира за здравословен и природосъобразен начин на живот, се разшири рязко приложението на различни фитбит сензори и медицински устройства, които събират и обработват непрекъснато разнообразни биометрични данни и информация относно функционирането на човешкия организъм, както и такава относно физиологическото състояние на индивида, се очаква допълнително да се размие границата между офлайн и онлайн активност. Ползвайки смарт устройствата за интелигентно управление на критичната за всеки представител на обществото ни инфраструктура, неизбежно се разширява киберпространството, чийто граници надхвърлят

обществените структури и вече навлизат в частните домове и в личното пространство на индивида. Заедно с това се увеличават и рисковете от изтичане на чувствителна информация.

7. ЗАКЛЮЧЕНИЕ

Необходимостта от прилагане на по-сигурни мерки за сигурност във физическия слой на киберпространството, както и в останалите два, се увеличава с нарастващото значение на информационната сигурност. С приложението на високопроизводителни компютри и по-големи устройства за съхранение, както и на по-прецизни и бюджетни измервателни устройства, се увеличава заплахата от кибер атаки, които практически могат да са неразпознаваеми ако се коментира TEMPEST. Поради невидимостта на нейонизиращата ЕМ радиация, подобни атаки, базирайки се на електромагнитно замърсяване на средата могат да бъдат сериозна заплахата за информационната сигурност. За целта се прилагат контрамерки TEMPEST, които са насочени към подобрения в устройствата, сградните инсталации или екраниране на самите сгради / клетка Фарадей/.

Приемайки фактът, че киберпространството осигурява стратегическо предимство в наши дни, ние трябва да приемем и развиваваме съществуващите практики за киберсигурност, които се базират на конфиденциалност, почтеност и достъпност до информационните ресурси.

Ако се коментират ползите и недостатъците на смарт технологиите и изграждането на интелигентни сгради в контекста на информационната сигурност, е важно да се спомене, че електромагнитното замърсяване, множеството центрове за данни и физическата инфраструктура създават благоприятна среда за различни по своето естество атаки срещу информационната сигурност, в т. ч. реална заплахата за киберсигурността. Би могло да се обобщи, че в интелигентните сгради въздействието на електромагнитното замърсяване е насочено в две направления- върху качеството на човешкото здраве и върху надеждността на информационните ресурси, които в голямата си част са съотносими с данни, засягащи общественото здраве.

ЛИТЕРАТУРА

- Актуализирана Национална стратегия за киберсигурност (2021). <https://e-gov.bg> > wps > connect > e-gov.bg-18083
- Денчев, Ст. (2019). Информация и сигурност. Акад- изд. За буквите- О писменах.352 с.
- Гарванова, Кр. Станева., & Гарванов, И. (2020). Вторично използване на безжичните технологии. Proceedings year iii, issue 1 (16), Borovets, vol. I Machines. Technologie. ISSN 2535-0021 (print), 85-88.
- ЕМ загрузение(2022). <https://vyvoz.org/blog/elektromagnitnoe-zagryaznenie-okruzhayushchey-sredy/>
- Национална стратегия за кибер сигурност „Киберустойчива България 2020” (2016). <http://www.cyberbg.eu/>
- Станева, К. (2008). Влияние на геопатогенните фактори върху човешкото здраве. Геология и минерални ресурси, 10. ISSN 1310-2265.
- Станева, К., Маринов, Е., & Маринов, М. (2015). Скрининг на геопатогенни зони – възможности и решения за неутрализирането им. Геология и минерални ресурси, ISSN 1310-2265, 7, 32-35.
- Bird, C. (1975). "Planetary Grid," New Age Journal, 5, pp. 36-41.
- Cherry (2002). Schumann Resonances, a plausible biophysical mechanism for the human health effects of Solar/Geomagnetic Activity, Natural Hazards 26(3), p 279-331.
- Hakan (2019). TEMPEST Attacks and Cybersecurity. International journal of engineering technologies-ijet, Vol.5, No.3,100-104.
- Meral (2008). Siber savunma: Ülkeler ve stratejiler. 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Aralık 2008, Ankara.
- Mild, Repacholi, van Deventer & Ravazzan (2004). Electromagnetic Hypersensitivity : proceedings, International Workshop on Electromagnetic Field Hypersensitivity, Prague, Czech Republic, October 25-27, ISBN 92 4 159412 8.
- National Cyber Strategy (2022), достъпна на <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>
- Nyberg, R., & Hardell, L. (2017). 5G Appeal: Scientists and doctors warn of potential serious health effects of 5G. Available online: http://wgbis.ces.iisc.ernet.in/energy/lake2006/programme/programme/proceedings/studentspapers/VIII/suraj_s_8th.pdf
- Raveendran & K.A.A.Tabet (2021). Meta-Integrative Qualitative Study on the Hidden Threats of Smart Buildings/Cities and Their Associated Impacts on Humans and the Environment. Buildings, 11, 251. <https://doi.org/10.3390/buildings11060251>

- Schumann & König (1954). Ueber die Beobachtung von Atmospheric bei geringsten Frequenzen, *Naturwissenschaften*, 41, 183.
- Simkó, M., & Mattsson, M.-O. (2019). 5G Wireless Communication and Health Effects—A Pragmatic Review Based on Available Studies Regarding 6 to 100 GHz. *Int. J. Environ. Res. Public Health* 16, 3406
- Radio Frequency Electromagnetic Field Exposure Assessment for future 5G networks. Available from: https://www.researchgate.net/publication/330266359_Radio_Frequency_Electromagnetic_Field_Exposure_Assessment_for_future_5G_networks [accessed Dec 11 2020].
- The International Commission on Non-Ionizing Radiation Protection, "Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz)," *Health Phys.*, vol. 74, no. 4, pp. 494-522, Apr. 1998.
- Yu-ichi Hayashi & Naofumi, H. (2018). Introduction to Electromagnetic Information Security. *IEICE trans. electron.*, vol.xx-x, no.x xxxx xxxx. DOI:10.1587/transcom.2018EBI0001
- World Health Organization, (2005). Electromagnetic fields and public health. Electromagnetic hypersensitivity. Available on: <https://www.who.int/peh-f/publications/facts/fs296/en/>.