CZU: 004.056:615.47

ASPECTE DE SECURIZARE A REȚELELOR ȘI SISTEMELOR INFORMATICE BIOMEDICALE

Prof. univ. dr. hab. Ion BOLUN, ASEM,
ion.bolun@isa.utm.md
ORCID: 0000-0003-1961-7310
Dr. Arina ALEXEI, UTM,
arina.alexei@tse.utm.md
ORCID: 0000-0003-4138957X
DOI: https://doi.org/10.53486/econ.2024.130.060

Particularitățile sistemelor (HIS) și rețelelor (HIN) informatice biomedicale sunt sistematizate din punctul de vedere al securității cibernetice. În baza particularităților în cauză și a unor date statistice privind crimele cibernetice în domeniul ocrotirii sănătății, este estimată acuitatea securizării avansate a HIS/SIN. Standardele de securitate cibernetică relevante, inclusiv cele referitoare la dispozitivele medicale, succint descrise în lucrare, facilitează orientarea în multitudinea de aspecte și cerințe de securitate cibernetică, în diverse situații din practică. De asemenea, lucrarea prezintă mai multe soluții specifice (în funcție de caz) de securizare a HIS/HIN propuse și implementate la nivel global. Acestea pot servi la definirea modalităților de securizare cibernetică în cazuri concrete. Se menționează că cerințele de securitate cibernetică și, respectiv, implementarea mijloacelor corespunzătoare în cadrul aplicațiilor, sistemelor și rețelelor informatice biomedicale pentru respectarea acestora depind de specificul fiecărui caz în parte.

Cuvinte-cheie: *atac cibernetic; dispozitive medicale; impact; informație sensibilă; ocrotire a sănătății.*

JEL: C63, C88, I23.

Introducere

Informațiile constituie o resursă strategică, iar o parte semnificativă dintre acestea au caracter confidențial. Sunt larg folosite informațiile biomedicale, inclusiv în telemedicină. Sistemele

UDC: 004.056:615.47

ASPECTS OF SECURING BIOMEDICAL INFORMATICS NETWORKS AND SYSTEMS

Professor, Dr. Hab., Ion BOLUN, ASEM
ion.bolun@isa.utm.md
ORCID: 0000-0003-1961-7310
PhD Arina ALEXEI, UTM,
arina.alexei@tse.utm.md
ORCID: 0000-0003-4138957X
DOI: https://doi.org/10.53486/econ.2024.130.060

The peculiarities of biomedical informatics systems (HISs) and networks (HINs) from the point of view of cyber security are systematized. Based on the particularities in question and on some statistical data on healthcare cybercrimes, the acuteness of the advanced securing of HISs/HINs is estimated. Cyber security standards in the field, including those related to medical devices, briefly described in the paper, facilitate successful orientation in the multitude of aspects and requirements of cyber security in various practical situations. Also, the paper presents several specific solutions (depending on the case) for securing HISs/HINs proposed and implemented in the field at the global level are described. They can serve to define cyber security modalities in concrete cases. It is mentioned that the requirements of cyber security and, respectively, the implementation of the respective informatics means in biomedical informatics applications, systems, and networks to comply with them depend on each specific case.

Keywords**:** *cyber-attack; healthcare; impact; medical devices; sensitive information.*

JEL: C63, C88, I23.

Introduction

Information is a strategic resource, while a great part of it is of confidential nature. In the biomedical context, sensitive information is widely used, including in telemedicine. Biomedical information systems typically manage

informatice biomedicale operează, de obicei, volume mari de date foarte sensibile. Accesul neautorizat la asemenea informații, furtul sau fraudarea lor, îndeosebi prin Internet, duce la pierderi considerabile, dăunând asistenței medicale oferite populației și, ca urmare, încetinind ritmul de creştere economică.

Cu regret, datele statistice recente relevă că sectorul sănătății este unul dintre cele mai afectate de atacurile de securitate cibernetică. Conform [1], în 2023 infrastructurile critice au fost cele mai vizate de atacurile infractorilor cibernetici (55,9%), sectorul sănătății, reprezentând 14,2% dintre acestea, fiind al doilea cel mai afectat după sectorul financiar (8,3%). Acestea includ atacuri de tip ransomware, furtul de înregistrări confidențiale de asistență medicală a pacienților și întreruperea serviciilor de ocrotire a sănătății în organizațiile medicale. În acest context, securizarea rețelelor și sistemelor informatice biomedicale devine o necesitate stringentă.

În prezenta lucrare sunt abordate selectiv aspecte de securitate cibernetică a sistemelor și rețelelor informatice biomedicale.

Metode de cercetare aplicate

Metodele utilizate includ: *cercetarea documentară* – pentru identificarea particularităților sistemelor (HIS) și rețelelor (HIN) informatice biomedicale și, de asemenea, pentru determinarea gradului de acoperire de către standarde a multitudinii de aspecte/cerințe de securitate cibernetică; *analiza comparativă cantitativă* – realizată în baza unor date statistice privind criminalitatea cibernetică în domeniul ocrotirii sănătăți, pentru estimarea gradului de securizare cibernetică necesară a HIS/HIN; *analiza comparativă calitativă* – axată pe soluții avansate de securizare a HIS/HIN, implementate în arie globală, pentru definirea direcțiilor prioritare de cercetare, în scopul securizării HIS/HIN în Republica Moldova.

Rezultate și discuții

Esența și particularitățile sistemelor și rețelelor informatice biomedicale

Funcțiile sistemelor informatice de ocrotire a sănătății (Health Information Systems – HIS, eng.), inclusiv biomedicale, includ: colectarea, stocarea, păstrarea, regăsirea, procesarea, large volumes of highly sensitive data, the security of which is essential. Unauthorized access to such information, its theft and fraud, especially through the Internet, leads to considerable losses, harming the quality of health care of the population and, as a result, slowing down the rate of economic growth.

Unfortunately, statistics show that the healthcare sector is one of the most affected by cyber security attacks. According to data of 2023 [1], critical infrastructures were the most targeted by cybercriminals attacks (55.9%) and the healthcare sector bears the brunt of cybercrime activity, accounting for 14.2% off all attacks targeting critical infrastructure, the second most affected area in this "top", being the financial sector with 8.3%. These include ransomware attacks, the theft of confidential patient healthcare records and the disruption of care services in healthcare organizations. Accordingly, tailored security of biomedical informatics systems and networks becomes imminent necessity.

The present paper addresses the analysis of selective aspects of cyber security of biomedical informatics systems and networks.

Applied research methodology

The applied methods refer to: *documentary research*, used to identify the particularities of biomedical information systems (HIS) and biomedical information networks (HIN) and, also, to determine the degree of coverage by standards of the multitude of cybersecurity aspects/requirements; *quantitative comparative analysis*, based on statistical data on cybercrimes in the field of healthcare to estimate the degree of necessary cybersecurity of HIS/HIN; *qualitative comparative analysis*, focused on advanced IT solutions for securing HIS/HIN implemented in the global area, to define priority research directions for securing HIS/HIN in the Republic of Moldova.

Results and discussions

Essence and particularities of biomedical informatics systems and networks

The functions of healthcare informatics systems (HIS), including biomedical, refer to: collection, storage, preservation, retrieval, processing, transmission, rendering and use of

transmiterea, redarea şi utilizarea informațiilor în susținerea sănătății populației, instruire, cercetare științifică și suportul elaborării și implementării politicilor de sănătate în practică. Bineînțeles, un sistem biomedical concret poate îndeplini toate sau doar o parte din aceste funcții. Valorificarea rațională a resurselor unor asemenea sisteme facilitează accesul la informațiile în domeniul sănătății, contribuind considerabil la implementarea mai reușită a măsurilor profilactice, la îmbunătățirea calității serviciilor medicale și, implicit, a calității vieții oamenilor. Totodată, HIS îmbunătățesc susținerea informațională a instruirii, cercetării științifice, elaborării politicilor și luării deciziilor în domeniu.

Conform destinației, HIS trebuie să pună la dispoziție informațiile potrivite la momentul și locul potrivit, persoanelor potrivite și într-o formă potrivită, astfel încât, în situații specifice acestea să poată lua deciziile adecvate. Sistemele și, respectiv, rețelele informatice biomedicale constituie o parte esențială a asigurării unei asistențe medicale de calitate populației.

Cele mai importante funcții ale instituțiilor din sistemul ocrotirii sănătății țin de prevenirea îmbolnăvirilor, diagnosticarea stării de sănătate, tratamentul și reabilitarea pacienților. Datele și documentele relevante în asemenea activități se colectează în fișa medicală a fiecărui pacient. Odată cu implementarea HIS, fișele medicale ale pacienților se perfectează în format informatic (i-fișe – Electronic Health Record – EHR). Bineînțeles că, pe lângă fișele medicale ale pacienților, HIS operează cu o multitudine de alte informații și documente ce țin de domeniu.

La exemple de sisteme informatice medicale (biomedicale) se referă [2]:

- fișa medicală informatică (Electronic Medical Record – EMR, eng.) sau fișa electronică de sănătate (Electronic Health Record – EHR, eng.);
- softul de gestionare a practicii (Practice Management Software – PMS);
- indicele pacientului master (Master Patient Index – MPI, eng.);
- portaluri pentru pacienți;
- monitorizarea pacientului la distanță (Remote Patient Monitoring – RPM, eng.);

information in support of population health, training, scientific research and support in the development and implementation of health policies in practice. Obviously, a concrete HIS can fulfil all or only a part of these functions. The rational capitalization of the resources of such systems facilitates the access and more effective utilization of the multitude of information in the field of health, contributing considerably to the more successful implementation of preventive measures, to the improvement of the quality of medical services and, as a result, the quality of people's lives. At the same time, HIS improves the informational support of training, scientific research, policy development and decision-making in the healthcare field.

As intended, HIS must make available the right information at the right time, in the right place, to the right people and in the right form, so that in specific situations these people can make the right decisions. Healthcare informatics systems are an essential part of providing qualitative medical care to the population.

The most important functions of the system of health care institutions concern the prevention of diseases, the diagnosis of the health status of people, the treatment and rehabilitation of patients after treatment. The relevant data and documents in such activities are collected in the health record of each patient. With the implementation of HIS (Health Information Systems), patient medical records are perfected in electronic format (e-records – Electronic Health Records – EHR). Of course, in addition to patient medical records, HIS also handles a multitude of other information and documents related to the medical field.

Examples of healthcare (biomedical) informatics systems refer to [2]:

- Electronic Health Record (EHR) or Electronic Medical Record (EMR);
- Practice Management Software (PMS);
- Master Patient Index (MPI);
- Patient Portals;
- Remote Patient Monitoring (RPM);
- Clinical Decision Support (CDS).

Electronic Health Record (EHR) includes patient data, results of medical investigations, as

– suportul pentru decizii clinice (Clinical Decision Support – CDS, eng.).

Fișa electronică de sănătate (EHR) include date despre pacient, rezultatele investigațiilor medicale și tratamente, permițând și partajarea de date cu alte EHR, pentru ca mai mulți furnizori de asistență medicală să poată accesa, la necesitate, datele în cauză.

PMS ajută furnizorii de servicii medicale să gestioneze operațiunile zilnice, cum ar fi programarea, facturarea și diverse sarcini administrative.

Indicele MPI se determină în baza înregistrărilor pacientului din diverse baze de date, indexând totodată toate celelalte înregistrări ale acestuia. Folosirea MPI reduce dublarea înregistrărilor pacienților și identifică informațiile inexacte cu referire la pacient, care ar putea duce la respingerea solicitărilor de asistență medicală.

Portalurile pentru pacienți oferă acces online la informații despre programări, medicamente, rezultate de laborator etc. Unele portaluri permit comunicarea directă a pacienților cu medicii.

RPM (telesănătate) constă în monitorizarea de la distanță a pacienților, asigurând transferul de date de la senzorii medicali respectivi, de exemplu nivelul glucozei în sânge sau tensiunea arterială, către medici.

CDS servesc pentru analiza datelor din diverse sisteme clinice și administrative, ajutând furnizorii de servicii medicale în luarea deciziilor clinice individualizate, pregătirea diagnosticelor, prezicerea interacțiunilor medicamentoase etc.

Categoriile de sisteme informatice medicale nominalizate mai puțin se referă la informatizarea în ansamblu a funcțiilor organizațiilor de îngrijire a sănătății. Acestea integrează funcțiile de asistență medicală a populației. Desigur, structura și funcțiile organizațiilor de asistență medicală pot varia de la o țară la alta, fiecare organizație jucând un rol bine definit în furnizarea îngrijirilor medicale ce țin de situații specifice. Din acest punct de vedere, în [3] se disting următoarele sisteme informatice instituționale în domeniul sănătății (SI):

– în spitale (*Information Systems in Hospitals* – ISH, eng.);

well as treatments, allowing data to be shared with other EHRs so that a greater number of healthcare providers can have access to the data when needed.

PMS helps healthcare providers manage day-to-day operations such as appointment, billing, and various administrative tasks.

The *MPI index* is determined based on the patient's records from various databases, also indexing all his other records. Using MPI reduces duplication of patient records and identifies inaccurate patient information that can lead to denied healthcare requests.

Patient Portals allow patients online access to information about appointment, medications, lab results, etc. via the Internet. Some portals allow patients to communicate with their doctors online.

RPM (telehealth) consists of remote patient monitoring, ensuring the transfer of data from respective medical sensors, for example blood glucose level and blood pressure, to doctors.

CDSs serve to analyse data from various clinical and administrative systems, helping healthcare providers make clinical decisions about individual patients. The data can help prepare diagnoses, predict drug interactions, etc.

The categories of nominated HISs less refer to the overall informatization of healthcare organizations functions. These integrates the population healthcare functions. Of course, healthcare organizations can vary from country to country, but, as a whole, they perform to a greater or lesser extent the same set of functions. Each healthcare setting has a specific role in providing healthcare and is related to specific life situations. From this point of view, in [3] the following institutional healthcare informatics systems are distinguished (HIS):

– in hospitals – *Information Systems in Hospitals* (ISH);
– in nursing homes – *Information Systems in Nursing Homes* (ISNH);
– in medical offices – *Information Systems in Medical Offices* (ISMO);
– in ambulatory nursing organizations – *Information Systems in Ambulatory Nursing Organizations* (ISANO);

- în case de bătrâni (*Information Systems in Nursing Homes* – ISNH, eng.);
- în cabinete medicale (*Information Systems in Medical Offices* – ISMO);
- în organizațiile de asistență medicală ambulatorie (*Information Systems in Ambulatory Nursing Organizations* – ISANO, eng.);
- în unități de cercetare medicală (*Information Systems in Medical Research Facilities* – ISMRF, eng.);
- în farmacii, magazine de produse medicale, cabinete terapeutice, unități de reabilitare pentru pacienți internați și ambulatoriu, hospice-uri, facilități de sănătate și centre sportive și parcuri de agrement;
- în state (*Information Systems in States* – ISS, eng.) și regiuni (*Information Systems in Regions* – ISR, eng.).

Se disting, de asemenea, sisteme informatice în medii personale (*Information System in Personal Environments* – ISPE, eng.), precum domiciliul sau ca parte a sistemului informatic de sănătate instituțional. ISPE sprijină, de obicei, sănătatea, prevenirea, tratamentul sau reabilitarea.

ISH trebuie să răspundă necesităților de informatizare a mai multor zone clinice și administrative și grupuri de persoane implicate. Acest sistem integrează un număr mare de funcții și aplicații informatice (EHR, PMS, CDS etc.), fiind cel mai complex cadru instituțional de asistență medicală.

ISNH acoperă un număr mai mic de zone și persoane de îngrijit și, prin urmare, include un număr mai redus de aplicații informatice decât ISH. În același timp, este încă necesară gestionarea sistematică a informațiilor administrative specifice.

ISMO operează cu informații despre pacienții cu boli acute și cronice, care primesc tratament în ambulatoriu.

ISANO deține informații necesare pentru îmbunătățirea asistenței medicale a persoanelor la domiciliu.

ISMRF îndeplinește funcții de gestionare a cercetării, planificare și executare a studiilor. Acesta cuprinde diverse aplicații informatice, inclusiv cele destinate cercetării colaborative interinstituționale și interprofesionale.

- in medical research facilities – *Information Systems in Medical Research Facilities* (ISMRF);
- in pharmacies, medical supply stores, therapeutic offices, inpatient and outpatient rehabilitation facilities, hospices, wellness facilities, sports centers and leisure parks;
- in states – *Information Systems in States* (ISS) and regions – *Information Systems in Regions* (ISR).

Also, there can be distinguished various healthcare informatics system in Personal environments – *Information System in Oersonal Environments* (ISPE) such as home or as a part of institutional healthcare informatics systems. ISPE typically support wellness, prevention, treatment, or rehabilitation.

ISH have to address the informatization needs of many clinical and administrative areas and groups of persons. It must integrate a large number of functions and computer applications (EHR, PMS, CDS etc.), being the most complex institutional health care setting.

ISNH covers a smaller number of areas and persons that receive care and therefore includes a lower number of i-applications than HISH. At the same time, systematic management of the specific administrative information is still needed.

ISMO operates with information about patients with acute and chronic diseases that receive outpatient treatment.

ISANO holds information needed to improve taking care of persons in their homes.

ISMRF is supporting such functions as research management or the planning and executing of studies. It comprises various computer applications, including those for cross-institutional and interprofessional research collaboration.

ISS supports the government ministry of health in activities regarding country's health care network, including responsible government agencies, hospitals, medical offices, insurance companies, etc.

For the uniformization of approaches regarding healthcare informatics systems, the me-

ISS sprijină Ministerul Sănătății în activitățile referitoare la rețeaua națională de sănătate, incluzând spitale, cabinete medicale, agenții guvernamentale responsabile, companii de asigurări etc.

Pentru uniformizarea abordărilor privind sistemele informatice medicale, în este propus metamodelul **3LGM2** cu trei straturi, cu repartizarea funcțiilor HIS între aceste straturi [4].

3LGM2 îmbină aspectele funcționale, tehnice și organizaționale cu anumite caracteristici ale metamodelelor de date și **procese**. În cadrul **3LGM2** se disting trei straturi HIS:

- stratul Domeniu (funcții);
- stratul Instrumente logice (i-aplicații);
- stratul Instrumente fizice (rețeaua de calculatoare).

Stratul Domeniu descrie tipurile de activități funcționale ce trebuie realizate în cadrul sistemului informatic și specifică cu ce date trebuie de operat. Acest strat este independent de instrumentele fizice și logice de utilizat pentru operarea cu datele.

La *stratul Instrumente logice*, accentul este pus pe i-aplicații, care, în interacțiune, fiind instalate pe un sistem de calcul, de obicei distribuit (rețea), realizează anumite funcții, definite de stratul Domeniu, prin seturi de reguli specifice de operare cu datele.

Stratul Instrumente fizice descrie mijloacele informatice fizice de intrare, stocare, regăsire, procesare, transfer și redare a datelor, conform specificațiilor definite de stratul Instrumente logice. Acesta se referă, în principal, la rețeaua de calculatoare în cadrul căreia sunt instalate i-aplicațiile.

Straturile Instrumente logice și Instrumente fizice constituie, practic, i-rețeaua HIS.

Fiind i-rețele, celor biomedicale (HIN) le sunt caracteristice aspectele de securizare ce țin de rețele informatice în general [5]. Totodată, acestora le sunt caracteristice unele particularități cauzate de specificul asistenței medicale și, respectiv, a sistemelor informatice biomedicale instalate și care funcționează în cadrul HIN.

De exemplu, la crearea și gestionarea funcționării HIS, trebuie luate în considerare și așa cerințe specifice, precum:

tamodel **3LGM2** with three layers and the distribution of HIS functions between these layers is proposed [4].

3LGM2 combines functional, technical, and organizational aspects with certain aspects of data and **process** metamodels. Within **3LGM2**, three HIS layers are distinguished:

- Domain layer (functions);
- Logical tools layer (i-applications);
- Physical Tools layer (computer network).

The Domain layer describes the types of functional activities that need to be performed in the informatics system and with what data to operate. This layer is independent of physical and logical tools to be used to operate with data.

At *Logical tools* layer, the focus is on i-applications, which in interaction, being installed on a computing system, usually distributed (network), perform certain functions, defined by the Domain layer, through specific sets of rules for operating with data.

The *Physical tools layer* describes the physical informatics means of inputting, storing, retrieving, processing, transferring, and rendering data as specified by the Logical tools layer. It basically refers to the computer network on which i-applications are installed.

The *Logical tools* and *Physical tools* layers basically constitute the HIS's i-network.

Biomedical information networks (HIN) share common characteristics with general information networks, especially regarding security aspects [5]. At the same time, they are characterized by some particularities caused by the specificity of healthcare and, respectively, of the biomedical i-applications and i-systems installed and operating within the HIN.

For example, when creating and managing the operation of HIS, are taken into consideration such specific requirements as:

- *specific legal requirements* – they include aspects related to the protection of personal data. Of course, aspects related to the protection of personal data are also relevant in other i-systems, but the compromise of health data has a negative impact, as a rule, much greater, hence

– *cerințe legale specifice* – cerințe care cuprind, îndeosebi, aspecte ce țin de protecția datelor cu caracter personal. Desigur, protecția datelor cu caracter personal este relevantă în orice sistem informatic, dar compromiterea datelor ce țin de sănătate au un impact negativ, de regulă, mult grav, de aici și cerințele de securitate sunt mai stricte. De exemplu, modificarea informațiilor în i-fișa medicală a pacientului poate conduce la un tratament inadecvat cu urmări grave;
– *informații comune pentru mai multe instituții medicale*, cum ar fi, i-fișele medicale ale pacienților, deoarece aceștia au dreptul și se pot adresa la diverse instituții medicale pentru investigații medicale, diagnostic, consultații, tratament și reabilitare. Totodată, accesul la asemenea informații trebuie să fie reglementat diferențiat: unele instituții medicale, categorii de medici pot avea dreptul de acces la unele informații, iar altele – la un set mai restrâns sau, din contra, mai extins de informații medicale;
– *situații de urgență* – în sistemul sănătății sunt foarte multe situații de urgență pe întreg teritoriul țării. În funcție de gravitatea acestora, poate fi necesară intervenția promptă a unor anumite categorii de medici. În asemenea cazuri, medicii pot avea nevoie urgentă de anumite informații despre pacient pentru a acționa corespunzător. Respectiv, trebuie asigurat accesul rapid la aceste informații, care pot fi stocate la distanțe mari de la locul asistenței medicale. Aceste condiții impun cerințe avansate privind funcționarea rețelelor HIN, inclusiv cerințe stricte de siguranță și protecție împotriva accesului fraudulos la datele confidențiale;
– *cooperare interinstituțională* – adesea este necesară cooperarea urgentă a mai multor medici, din diferite instituții medicale, în situații de asistență medicală complexă și de urgență;
– un set larg *de standarde specifice* domeniului, inclusiv cerințe legate de utilizarea dispozitivelor medicale.

higher security requirements. For example, changing the information in the patient's electronic health record can lead to inappropriate treatment with serious negative consequences;
– *common information for several medical institutions*, such as patients' electronic health record, because patients have the right and can turn to various medical institutions for medical investigations, diagnosis, consultations, treatment and rehabilitation. At the same time, access to such information must be regulated differently: some medical institutions, categories of doctors may have the right of access to some information, and others – to a narrower or, on the contrary, wider set of medical information;
– *emergency situations*, in the health system, there are many emergency situations throughout the country. Depending on the severity of the situation, the prompt intervention of certain categories of doctors may be necessary. In such cases, in order to proceed correctly, doctors may need certain information about the patient. Accordingly, proper access to this information, which can be stored at great distances from the place of medical assistance, must be ensured. These conditions impose advanced requirements for HIN operation, including security and protection against fraudulent access to confidential data;
– *interinstitutional cooperation,* it is often necessary for the urgent cooperation of multiple doctors from different medical institutions in situations involving complex and emergency medical care.
– a broad set of industry-*specific standards*, including those related to medical devices.

Of course, there are other peculiarities, relevant to this field.

Acuity of securing biomedical informatics systems and networks

As in many other fields, there have been and are many cyber-attacks on informatics

Bineînțeles, există și alte particularități relevante acestui domeniu.

Acuitatea securizării sistemelor și rețelelor informatice biomedicale

Ca și în multe alte domenii, au avut și au loc multiple atacuri cibernetice asupra resurselor informaționale și a infrastructurii sistemelor și rețelelor informatice biomedicale. Unele exemple și statistici în domeniu sunt:

- Conform [6], în ultimii patru ani, numărul atacurilor cibernetice majore a crescut cu 239%;
- Potrivit IBM Security, la începutul anului 2023, pierderile medii ce revin unui incident de compromitere a datelor biomedicale au constituit aproape 11 mln USD (o creștere de 8% față de anul 2022) [6];
- 27% dintre incidentele de securitate cibernetică din domeniul sănătății au fost atacuri de la spate (backdoor attack, eng.) [7]. Acest tip de atac implică utilizarea oricărui i-program malițios/i-virus/i-tehnologie pentru a obține acces neautorizat la i-aplicație/i-sistem/i-rețea, ocolind măsurile de securitate implementate;
- HCA Healthcare, cel mai mare sistem de spitale private din Statele Unite ale Americii (SUA), a dezvăluit în iulie 2023 un atac cibernetic care ar fi putut afecta până la 11 milioane de persoane. Incidentul este descris ca „furt de date dintr-o locație de stocare externă, utilizată exclusiv pentru formatarea mesajelor de i-poștă” [8];
- În incidentele cibernetice ce țin de asistența medicală, activitățile de recunoaștere – în care atacatorii caută vulnerabilități și date valoroase – au reprezentat tipul principal de atacuri, însumând 50% din toate cazurile identificate. Acest lucru accentuează importanța detectării amenințărilor în stadiul incipient [7];
- În SUA, 88 de mln de persoane au fost afectate în anul 2023 de compromiterea, prin atacuri cibernetice, a informațiilor personale de sănătate, o creștere de 60% față de anul 2022 [6];
- Din cele 40 de mln de înregistrări medicale compromise în prima jumătate a

resources and infrastructure of biomedical informatics systems and networks. Some examples and statistics in the field are as follows:

- According to [6], during the last four years, the number of large cyber-attacks increased by 239%;
- According to IBM Security, at the beginning of 2023, the average losses in a biomedical data breach incident amounted to almost USD 11 million (an increase of 8% compared to 2022) [6];
- 27% of healthcare cybersecurity incidents were backdoor attacks [7]. This type of attacks involves the usage of any malicious i-program/i-virus/i-technology to gain unauthorized access to i-application/i-system/i-network bypassing the implemented security measures);
- HCA Healthcare, the largest private hospital system in the U.S., in July 2023 disclosed a cyber-attack that could have affected up to 11 million people. The incident is described as “theft of data from an external storage location used exclusively for formatting e-mail messages” [8];
- In healthcare cyber incidents, reconnaissance activities – where attackers look for vulnerabilities and valuable data – were the main type of attacks, accounting for 50% of all identified cases, emphasizing the critical nature of detecting threats at an early stage [7];
- In the U.S., 88 million people were affected by the compromise, through cyber-attacks, of personal health information, an increase of 60% in 2023 compared to 2022 [6];
- Of the 40 million electronic health record compromised in the first half of 2023, nearly 50% were compromised due to attacks targeting third-party business partners of healthcare providers [9];
- As a result of cyber security attacks, approx. 70% of healthcare facilities in the U.S. migrated to *cloud* services [10].

According to the Healthcare Information and Management Systems Society (HIMSS) report “HIMSS Government Relations and

anului 2023, aproape 50% au fost compromise din cauza atacurilor care au vizat partenerii de afaceri terți ai furnizorilor de servicii medicale [9];

– Ca urmare a atacurilor de securitate cibernetică, circa 70% din unitățile de asistență medicală din SUA au migrat către servicii nor (*cloud*, eng.) [10].

Potrivit raportului *Healthcare Information and Management Systems Society* (HIMSS) „HIMSS Government Relations and Informatics Impact report 2023" [11], în lumea interconectată de astăzi, securitatea cibernetică este mai crucială ca niciodată.

Importanța securizării sistemelor și rețelelor informatice biomedicale este confirmată și de multitudinea de standarde în domeniu.

Standardizarea securității cibernetice a asistenței medicale

Standardele acoperă aspectele fundamentale de securitate a sistemelor și rețelelor informatice biomedicale. În acest domeniu, este cazul de menționat separat următoarele documente normative: GDPR (*EU General Data Protection Regulation, 2016*) în Uniunea Europeană [12] și **HIPAA** (*Health Insurance Portability and Accountability Act of 1996*) în SUA [13].

GDPR este considerat [14] cel mai puternic cadru normativ privind protecția și transferul liber al datelor cu caracter personal din lume. În Republica Moldova, *Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011* a intrat în vigoare la 14.10.2011 [15].

HIPAA specifică cerințe pentru a proteja confidențialitatea și securitatea informațiilor de sănătate [13]. Conform acestuia, de exemplu, mesajele de i-poștă către pacienți, care conțin informații de sănătate, trebuie să fie cifrate, cu excepția cazului în care pacientul are autorizație scrisă ca organizația să trimită informațiile necifrate. Nerespectarea HIPAA poate atrage sancțiuni civile și penale.

La nivel global, printre standardele în domeniu se regăsesc: **ISO/IEC 15408 (serie)** – criterii de evaluare a securității **tehnologiei informaționale** (TI); **ISO/IEC 27000** – definește securitatea informațiilor ca asigurarea confidențialității, integrității și disponibilității

Informatics Impact report 2023" [11], in today's interconnected world, cybersecurity is more crucial than ever.

The acuity of securing biomedical informatics systems and networks is also confirmed by the multitude of standards in the field.

Standardization of Healthcare Cybersecurity

The standards cover the fundamental aspects of securing biomedical informatics systems and networks. In the medical field, it is worth mentioning separately the normative documents GDPR (*EU General Data Protection Regulation, 2016*) in the European Union [12] and **HIPAA** (*Health Insurance Portability and Accountability Act of 1996*) in the U.S.A. [13].

GDPR is considered [14] the strongest regulatory framework regarding the protection and free movement of personal data in the world. In the Republic of Moldova, the *Law on the protection of personal data no.133 of 07/08/2011* entered into force on 10/14/2011 [15].

HIPPA specifies requirements aimed to safeguard the privacy and security of protected health information [13]. It requires, for example, that e-mails to patients containing health-related information must be encrypted in transit, unless the patient has written authorization on file for the organization to send their information unencrypted. Failure to comply with HIPAA may result in civil and criminal penalties.

Worldwide, among the standards in the field can be mentioned: **ISO/IEC 15408 (series)** – evaluation criteria for **IT security**; **ISO/IEC 27000** – defines information security as preservation of confidentiality, integrity, and availability of information; **ISO/IEC 27001** – requirements for information security management systems; **ISO/IEC 27002** – recommendations regarding information security controls; **ISO/IEC 27032** – common cybersecurity risks and incident handling; **ISO 27799** – management of information security management in health using **ISO/IEC 27002**; **ISO/IEC 29147** – vulnerability disclosure; **ISO/IEC 30111** – management of vulnerability remediation processes; **IEC 82304-1** – security requirements for software products used in healthcare etc.

acestora; **ISO/IEC 27001** – cerințe pentru sistemele de gestionare a securității informațiilor; **ISO/IEC 27002** – recomandării privind controalele de securitate a informațiilor; **ISO/IEC 27032** – gestionarea riscurilor comune de securitate cibernetică și a incidentelor; **ISO 27799** – gestionarea securității informațiilor în sănătate folosind standardul **ISO/IEC 27002**; **ISO/IEC 29147** – identificarea vulnerabilităților; **ISO/IEC 30111** – gestionarea proceselor de remediere a vulnerabilităților; **IEC 82304-1** – cerințe de securitate a produselor program în domeniul sănătății etc.

O atenție aparte este acordată standardizării securității cibernetice a dispozitivelor medicale. La nivel global, sunt recunoscute mai multe standarde relevante: **ISO/IEEE 11073** – schimbul de date între dispozitivele medicale; **ISO 12052** – imagistica digitală și comunicare în medicină (DICOM); **ISO 14971** – gestionarea riscurilor; **ISO 13485** – cerințe privind calitatea; **AAMI 2800** (*Association for the Advancement of Medical Instrumentation, eng.*) – cerințe de securitate a sistemelor medicale interoperabile; **IEC 80001** – gestionarea riscurilor pentru rețelele informatice care încorporează dispozitive medicale; **80002** – standard privind softul pentru dispozitive medicale ș.a.

De asemenea, la nivelul Uniunii Europene este bine cunoscut Regulamentul privind dispozitivele medicale (Medical Device Regulation, eng.) [16]. Acesta impune cerințe de securitate informatică, protecția și confidențialitatea datelor cu caracter personal la toate etapele ciclului de viață al dispozitivelor medicale.

Practicile globale în securitatea cibernetică biomedicală

Importanța securizării HIS/HIN devine evidentă și din multitudinea de cercetări științifice și implementări în domeniu. Astfel, pentru facilitarea creării, actualizării și întreținerii EHR ale pacienților, cu respectarea cerințelor de i-securitate, pe piață sunt propuse mai multe soluții, inclusiv *sursă-deschisă, precum:* **openEHR**, **OpenEMR** și **OpenMRS**. Platforma openEHR, de exemplu, este dezvoltată și susținută de Fundația openEHR încă de la începutul anilor 2000, este o specificație standard sursă-deschisă pentru

Particular attention is given to the standardization of the cybersecurity of medical devices. Globally, several relevant standards are recognized namely: **ISO/IEEE 11073** – data exchange between medical devices; **ISO 12052** – digital imaging and communication in medicine (DICOM); **ISO 14971** – risk management; **ISO 13485** – quality requirements; **AAMI 2800** (*Association for the Advancement of Medical Instrumentation*) – security requirements of interoperable medical systems; **IEC 80001** – risk management for IT-networks incorporating medical devices; **80002** – Standard for Software Intended for Medical Devices etc.

Also, at the European Union level, the Medical Device Regulation requires IT security, protection and confidentiality of personal data at various development stages is well known [16]. This European regulation imposes requirements for information security, protection and confidentiality of personal data at all stages of the life of medical devices.

World practice of Biomedical Cybersecurity

The acuteness of securing HIS/HIN can also be realized considering the multitude of implementations and scientific researches in the field. For example, to facilitate the creation, updating and maintenance of patients' electronic healt recods in compliance with i-security requirements, several solutions are proposed on the market, including *open source such as*: **openEHR**, **OpenEMR** and **OpenMRS**. The **openEHR** platform, for example, is maintained and supported by the **openEHR** Foundation since the early 2000s, is an open-source standard specification for the detailed representation of clinical information in the patient's electronic health records (https://openehr.org/products_tools/platform/). It enables the complete definition of patient electronic health records, independent of the provider, within and between healthcare practices. At the same time, their ADL language for defining clinical concepts and AQL language for querying clinical concepts of open HER separates the clinical content from technical details fact that contributes to higher of medical data.

reprezentarea detaliată a informațiilor clinice în i-fișa medicală a pacientului (https://openehr.org/products_tools/platform/). Aceasta permite definirea completă a i-fișelor pacienților, independent de furnizor, în cadrul și între cabinetele de asistență medicală. Totodată, limbajul ADL de definire a conceptelor clinice și limbajul AQL de interogare bazată pe concepte clinice ale openEHR separă conținutul clinic de detaliile tehnice, fapt ce contribuie la o securitate mai ridicată a datelor medicale.

De asemenea, în [17] se examinează colaborarea securizată capăt-la-capăt, inclusiv la distanță și interinstituțională, în cercetările biomedicale ale mai multor participanți, în baza unui mediu informatic eterogen, folosind APPFLx. Acesta permite instalarea, configurarea și rularea facilă a experimentelor în domeniu, fiind complet agnostic de infrastructura informatică de bază a participanților, cu respectarea cerințelor documentelor normative HIPAA și GDPR, inclusiv privind accesul la diverse date biomedicale, cum ar fi i-fișele pacienților, imaginile medicale, diagramele ECG etc.

În cadrul proiectului Dynaswap [18], este dezvoltată o poartă informatică în cadrul unui mediu cloud, pentru transferuri securizate de date, în cadrul infrastructurilor informatice biomedicale cu diverși utilizatori, permițând accesarea și partajarea de date proprietare și resurse interactive de calcul și analiză a datelor la cerere. Sistemul Dynaswap implementează o arhitectură de securitate cibernetică sigură, holistică, reglată fin, care poate fi portată pe mai multe mașini virtuale ale infrastructurii informatice Jet-Stream Cloud [19].

Centrul de date Data Core al Weill Cornell Medicine [20] este destinat accesului și operării securizate a utilizatorilor cu date biomedicale sensibile. Acesta este un mediu de calcul virtual securizat. Obiectivul major al Data Core constă în creșterea accesibilității datelor, inclusiv a celor foarte sensibile, pentru cercetare și instruire, și îmbunătățirea calității serviciilor. Aceasta implică redarea, curățarea și transformarea datelor din EHR și din alte surse, astfel, încât utilizatorii să poată analiza organizarea și utilizarea datelor și adăuga date pentru îmbunătățirea asistenței medicale și cercetării. Simplificarea accesului la date

Likewise [17], the secure end-to-end, collaboration including remote and inter-institutional, the biomedical research of several participants, based on a heterogeneous computier environment using APPFLx is examined. It allows easy installation, configuration and running of experiments in the field being completely agnostic of the basic IT infrastructure of the participants in compliance with the requirements of the HIPAA and GDPR normative documents, including on access to various biomedical data, such as patient electronic health records, medical images, ECG charts etc.

Within the Dynaswap project [18] an informatics gateway is developed in a cloud environment for secure data transfers within biomedical i-infrastructures with various users, allowing access and sharing of proprietary data and interactive computing and data analysis resources on demand. The Dynaswap system implements a secure, holistic, fine-tuned cyber security architecture that can be ported to multiple virtual machines of the Jet-Stream Cloud computing infrastructure [19].

Weill Cornell Medicine's Data Core data center [20] is intended for secure user access and operation of sensitive biomedical data. This is a secure virtual computing environment. The major objective of the Data Core is to increase the accessibility of data, including highly sensitive data, for research and training and to improve the quality of services. This involves rendering, cleaning, and transforming data from EHRs and other sources so that users can analyse the organization and use of data and add data to improve health care and research. Simplifying access to highly sensitive data is balanced with protecting the privacy of the individuals involved. Data Core provides this compromise by keeping tightly controlled data in a central location, but providing secure access to users.

In different contexts, different patients may have different privacy and security requirements regarding the data in their electronic health records. For this purpose, the data in electronic health records must be managed with a customizable access control, including tem-

foarte sensibile este echilibrată cu protejarea confidențialității persoanelor aferente. Data Core oferă acest compromis prin păstrarea datelor strict controlate într-o locație centrală, dar oferind acces securizat utilizatorilor.

În contexte diferite, pacienții pot avea cerințe de confidențialitate și securitate diferite, în ceea ce privește datele din i-fișele lor medicale. În acest sens, gestionarea datelor din i-fișele medicale trebuie să includă un control al accesului personalizabil, inclusiv din punct de vedere temporal. În [21] este prezentat un model de control personalizat al accesului, bazat pe roluri și în timp (RBTBAC), care răspunde acestor cerințe. Prin combinarea algoritmică de control al accesului bazat pe roluri și gestionarea cheilor în funcție de timp, modelul RBTBAC are două caracteristici esențiale:

- o structură dinamică transparentă de confidențialitate pentru accesul și gestionarea datelor din i-fișele medicale, bazate pe roluri;
- o granularitate fină a autorizației și controlul accesului limitat în timp în formă de arbore.

Cadrul **BioChainReward**, bazat pe blockchain, pentru a păstra confidențialitatea utilizatorilor și a asigura securitatea datelor biomedicale, este propus în [22]. Arhitectura BioChainReward este pe patru straturi distincte: Date, Blockchain, Acord inteligent și Aplicație. Cifrarea și descifrarea datelor se efectuează la stratul Date, în timp ce stratul Blockchain gestionează hash-area și recuperarea datelor. Stratul Acord inteligent include un substrat de conservare a confidențialității, activat de inteligență artificială (IA), care selectează în mod dinamic o tehnică de confidențialitate adecvată, adaptată naturii și scopului fiecărei solicitări de date. Acest nivel include, de asemenea, un mecanism de legătură inversă și de motivare, care stimulează pacienții să-și partajeze datele prin oferirea de recompense. În cele din urmă, stratul Aplicație funcționează ca o interfață pentru diverse aplicații, cum ar fi aplicații activate de IA și instrumente de analiză a datelor, pentru a accesa și utiliza datele partajate.

În scopul sporirii operativității și reducerii laboriozității procesării solicitărilor utilizatorilor, sistemului Medical Cloud (mCloud), ce folosește

poral. In [21], a role-based and time-based personalized access control (RBTBAC) model is presented that meets these requirements. Through the algorithmic combination of role-based access control and time-based key management, the RBTBAC model has two key features:

- a dynamic, transparent confidentiality structure for access and management of data in electronic health records, based on roles;
- a fine granularity of authorization and time-limited access control in a tree form.

The blockchain-based **BioChainReward** framework to preserve user privacy and secure biomedical data is proposed in [22]. The architecture of BioChainReward is on four distinct layers: Data, Blockchain, Smart Agreement and Application. Data encryption and decryption is performed at the Data layer, while the Blockchain layer handles data hashing and retrieval. The Smart Agreement layer includes an AI-enabled privacy-preserving substrate that dynamically selects an appropriate privacy technique tailored to the nature and purpose of each data request. This tier also has a feedback and incentive mechanism that incentivizes patients to share their data by offering rewards. Finally, the Application layer serves as an interface for various applications, such as AI-enabled applications and data analytics tools, to access and use the shared data.

In order to increase the operability and reduce the laboriousness of processing user requests of the Medical Cloud (mCloud) system, which uses a central server and various portable devices and sensors for better patient care, a secure distributed solution is proposed in [23] that shares the data of a patient through different devices connected to mCloud with the medical staff. The solution leverages the power of other locally available mCloud devices and related devices that have more computing capabilities. As the number of mCloud devices in the network increases, so does the percentage of encrypted data transmissions. However, the average response time to requests in the case of the decentralized system decreases compared to the centralized one.

un server central și diverse dispozitive și senzori portabili pentru o îngrijire mai bună a pacienților, în [23] este propusă o soluție distribuită sigură. Aceasta partajează datele pacienților prin diferite dispozitive conectate la mCloud cu personalul medical, fără a fi nevoie de un server centralizat. Soluția valorifică puterea și a altor dispozitive mCloud disponibile local și a dispozitivelor conexe care au mai multe capacități de calcul. Odată cu creșterea numărului de dispozitive mCloud în rețea, crește și procentajul de transferuri de date cifrate. Totuși, durata medie de răspuns la solicitări, în cazul sistemului descentralizat, scade comparativ cu cel centralizat.

Datele i-fișelor pacienților se păstrează în baze de date medicale și bio-depozite și pot fi interogate, extrase și utilizate de către medici și cercetători. În ultimul timp, se observă o tendință pronunțată de migrare a acestor informații către cloud, facilitând astfel accesul tuturor părților interesate. Totodată, în asemenea cazuri pot apărea consecințe nedorite în ce privește securitatea datelor. Pentru a asigura securitatea necesară a datelor biomedicale sensibile în asemenea situații, în [24] este propusă o arhitectură ce combină mecanisme de control al accesului distribuit cu protocoale criptografice de păstrare a confidențialității, permițând partajarea și procesarea securizată pe cloud. Datele partajate sunt etichetate cu politici de securitate, care definesc cine are acces la ele și cum ar trebui să fie utilizate. Drepturile de acces pot fi delegate altor părți, facilitând colaborările între mai mulți specialiști. În cele din urmă, datele pot fi procesate criptografic pentru a extrage informații specifice, fără a compromite întregul set de date.

Sistemele microelectromecanice biomedicale (BioMEMS) [25] reprezintă un catalizator crucial în îmbunătățirea securității comunicațiilor IoT (Internet of Things, eng. – Internetul lucrurilor) și în protejarea sistemelor de asistență medicală. BioMEMS joacă un rol esențial în diagnosticarea personalizată, monitorizare și aplicații terapeutice. Totodată, această integrare implică o gamă complexă de provocări legate de securitatea și confidențialitatea comunicațiilor IoT în cadrul ecosistemelor inteligente de sănătate, solicitând un control cuprinzător. În [25] este

Patient's electronic health records are stored in medical databases and bio-repositories and can be queried, extracted and operated by doctors and researchers. Lately, there can be observed a pronounced tendency to migrate such information to the cloud, thus facilitating access to all interested parties. At the same time, in such cases there may be undesirable consequences in terms of data security. In order to ensure the necessary security of sensitive biomedical data in such situations, in [24] an architecture is proposed that combines distributed access control mechanisms with cryptographic protocols to preserve confidentiality allowing sharing and secure processing on the cloud. Shared data is labelled with security policies that define who has access to it and how it should be used. Access rights can be delegated to other parties, facilitating collaborations between several specialists. Finally, the data can be cryptographically manipulated to extract specific information without compromising the entire dataset.

Biomedical microelectromechanical systems (BioMEMS) [25] serve as a crucial catalyst in improving the security of IoT (Internet of Things) communications and protecting healthcare systems. BioMEMS are essential in personalized diagnostics, monitoring and therapeutic applications. At the same time, this integration involves a complex array of security and privacy challenges intrinsic to IoT communication within smart health ecosystems, requiring comprehensive control. In [25] a wide spectrum of vulnerabilities, cyber threats, data manipulation and message interception is addressed and a set of security solutions is proposed, which includes rigorous authentication processes, data encryption, attack-resistant models and mechanisms of continuous monitoring, all designed to strengthen BioMEMS in the face of ever-evolving threats in smart healthcare environments. In the context of IoT communications security, it is vital for BioMEMS to ensure equitable access to healthcare and also patient data privacy. At the same time, it is emphasized that the development of BioMEMS involves the consideration of diagnostics based on artificial intelligence, quantum computing and genomic integration.

abordat un spectru larg de vulnerabilități, amenințări cibernetice, manipulare a datelor și interceptări ale mesajelor. De asemenea, este propus un set de soluții de securitate, care includ procese riguroase de autentificare, cifrare a datelor, modele rezistente la atacuri și mecanisme de monitorizare continuă, toate concepute pentru a consolida BioMEMS împotrivă amenințărilor în continuă evoluție din mediile de sănătate inteligente. În contextul securității comunicațiilor IoT, pentru BioMEMS este vitală asigurarea accesului echitabil la asistența medicală și, de asemenea, garantarea confidențialității datelor pacientului. Totodată, se accentuează că dezvoltarea BioMEMS trebuie să ia în considerare diagnosticarea bazată pe inteligență artificială, calculul cuantic și integrarea genomică.

Concluzii

Valorificarea integrată rezonabilă a potențialului diverselor sisteme și aplicații informatice biomedicale permite îmbunătățirea asistenței medicale acordate pacienților, susținerea informațională a procesului decizional, a cercetărilor științifice și a elaborării unor politici adecvate situațiilor în domeniu. HIS și diversele aplicații informatice biomedicale sunt implementate și funcționează în cadrul rețelelor informatice biomedicale, ale căror mijloace sunt, de regulă, distribuite teritorial. Acestea facilitează colaborarea la distanță între diverse instituții și specialiști, contribuind la sporirea calității serviciilor medicale și a altor activități conexe.

O bună parte a informațiilor medicale, în special cele referitoare la fișele pacienților, sunt informații confidențiale foarte sensibile, cu acces reglementat definit de documente normative specifice. O unitate de asistență medicală riscă să devină complet în incapacitate de a activa, dacă datele din i-fișele pacienților nu mai pot fi accesate. Aceasta ar putea duce la pierdere de vieți omenești, deoarece, în unele cazuri, informațiile respective sunt necesare de urgență, fără posibilitatea de a repeta investigațiile medicale respective într-un timp util. De exemplu, cazurile recent înregistrate de atacuri ransomware asupra spitalelor ilustrează pericolele asociate. Dar, mai critică este modificarea intenționată a datelor din i-fișe, care ar putea conduce la un

Conclusions

The reasonable integrated exploitation of the potential of various biomedical informatics systems and applications allows for the improvement of medical care for patients, the successful informational support of decision-making, scientific research, and the development of policies appropriate to the situations in the field. The HIS and the various biomedical i-applications are implemented and function within the biomedical i-networks, the means of which are, as a rule, territorially distributed, which allows the remote collaboration of various institutions and specialists in support of increasing the quality of the provision of medical services and other related activities.

A significant part of medical information, but especially that related to patient records, is very sensitive confidential information with regulated access defined by respective normative documents. A health care facility is at risk of becoming completely unable to activate if data from patient i-records can no longer be accessed. This can cost lives, because in some cases that information is needed urgently, there is no time to carry out those medical investigations. Recent cases of so-called ransomware attacks on hospitals, for example, illustrate the associated dangers. Even more critical is the alteration of i-records data that could lead to inadequate treatment of those patients.

Accordingly, biomedical informatics applications, systems and networks must be protected both against destruction, modification, and loss, as well as against the illegal use of information resources by unauthorized persons. Their insufficient protection has led to multiple cyber-attacks with often very serious consequences. It is considered, according to [11] that HIS/HIN cyber security is more crucial than ever.

The i-security requirements and the implementation of informatics means within the biomedical i-networks to comply with them depend on each specific case. So, it follows the selection of some opportune cases, the identification of the related particularities, the carrying out of rigorous research, the obtaining

tratament inadecvat, cu consecințe grave asupra sănătății pacienților.

Respectiv, aplicațiile, sistemele și rețelele informatice biomedicale trebuie protejate atât împotriva distrugerii, modificării și pierderii datelor, cât și împotriva utilizării ilegale a resurselor informaționale de către persoane neautorizate. Protecția insuficientă a acestora a condus la multiple atacuri cibernetice, cu consecințe, deseori, foarte grave. Conform [11], securitatea cibernetică a HIS/HIN este mai crucială ca niciodată.

Cerințele de i-securitate și implementarea mijloacelor informatice în cadrul i-rețelelor biomedicale pentru a le respecta variază în funcție de fiecare caz în parte. Deci, este necesară selectarea unor situații relevante, identificarea particularităților aferente, efectuarea cercetărilor de rigoare, obținerea de soluții adecvate și elaborarea de recomandări pentru implementarea acestora în practică.

of appropriate solutions and the development of recommendations for their implementation in practice.

Bibliografie/Bibliography:

1. *European Repository of Cyber Incidents* [online] [accesat 07.07.2024]. Disponibil: https://www.swp-berlin.org/en/swp/about-us/ organization/swp-projects/european-repository-on-cyber-incidents-eurepoc
2. BROOK, C. What is a Health Information System. *Digital Guardian* [online]. 2023, may 09 [accesat 28.03.2024]. Disponibil: https://www.digitalguardian.com/blog/what-health-information-system
3. WINTER, A., AMMENWERTH, E., HAUX, R. et al. *Health Information Systems: Technological and Management Perspectives*. Cham (CH): Springer, 2023. 259 p. ISBN 978-3-031-12309-2
4. WINTER, A., BRIGL, B., WENDT, T. Modeling hospital information systems: the revised three-layer graph-based meta model 3LGM2. *Methods of Information in Medicine*. 2003, no. 42, pp. 544-551.
5. BOLUN, I., MORARU, V., ALEXEI, A., COJOCARU, S., CĂLIN, R. *The concept of cyber security of computer networks, including biomedical*. Chișinău: UTM, 2024. 88 p.
6. SOUTHWICK, R. More than 88 million people have been affected by health data breaches this year. *Healthcare Executive* [online]. 2023, november 02 [accesat 14.04.2024]. Disponibil: https://www.chiefhealthcareexecutive.com/ view/more-than-88-million-people-have-been-affected-by-health-data-breaches-this-year
7. DWYER, J. Threat Intelligence Index 2023 Insight. *IBM Security X-Force* [online]. 2023 [accesat 18.04.2024]. Disponibil: https://mediacenter.ibm.com/media/IBM+Security+X-Force+Threat+Intelligence+Index+ 2023+InsightA+John+ Dwyer/1_qiu3o3ms
8. SOUTHWICK, R. HCA Healthcare discloses data breach affecting as many as 11 million patients. *Healthcare Executive* [online]. 2023, July 10 [accesat 15.05.2024]. Disponibil: https://www.chiefhealthcareexecutive.com/view/hca-healthcare-discloses-data-breach-affecting-as-many-as-11-million-patients

9. VOGEL, S. Scale of healthcare cyber attacks increase as criminals change tactics, report finds. *Healthcare Dive* [online]. 2023, August 22 [accesat 24.05.2024]. Disponibil: https://www.healthcaredive.com/news/cyber-attacks-healthcare-scale-increase-critical-insights/691478/
10. *DuploCloud* [online] [accesat 28.05.2024]. Disponibil: https://lp.duplocloud.com/guide /healthcare-cloud-computing
11. *HIMSS Government Relations and Informatics Impact report 2023* [online] [accesat 09.07.2024]. Disponibil: https://www.himss.org/ resources/himss-government-relations-and-informatics-impact-report
12. General Data Protection Regulation. *Official Journal of the European Union* [online]. 2016, L 119/1, no. 4, pp. 1-88 [accesat 09.07.2024]. Disponibil: https://gdpr.eu/tag/gdpr/
13. *Public Law 104-191 Health Insurance Portability and Accountability Act of 1996* [online] [accesat 09.07.2024]. Disponibil: https://www.govinfo.gov/content/pkg/ PLAW-104publ191/pdf/PLAW-104publ191.pdf
14. WOLFORD, B. What is GDPR, the EU's new data protection law? *GDPR.EU* [online] [accesat 09.07.2024]. Disponibil: https://gdpr.eu/what-is-gdpr/
15. Legea privind protecția datelor cu caracter personal: nr. 133 din 08.07.2011. *Monitorul Oficial*. 2011, nr. 170-175, art. 492, pp. 6-13.
16. L:2017:117:TOC. *Official Journal of the European Union*. 2017, vol. 60, pp. 1-176.
17. HOANG, T.-H., FUHRMAN, J., MADDURI, R. et al. *Enabling end-to-end secure federated learning in biomedical research on heterogeneous computing environments with APPFLx* [online]. 2023 [accesat 12.07.2024]. Disponibil: https://doi.org/10.48550/arXiv.2312.0870
18. GOYAL, S., PURKAYASTHA, S., PHILLIPS, T. et al. *Enabling Secure and Effective Biomedical Data Sharing through Cyberinfrastructure Gateways* [online]. 2020 [accesat 14.07.2024]. Disponibil: https://doi.org/10.48550/ arXiv.2012.12835
19. *Jet-Stream Cloud* [online] [accesat 14.07.2024]. Disponibil: https://jet-stream.com/jet-stream-cloud/
20. OXLEY, P. R., RUFFING, J., CAMPION, T. R. et al. Design and implementation of a ::secure computing environment for analysis of sensitive data at an academic medical center. *AMIA Annu Symp Proc Cloud* [online]. 2018 Decender 05, pp. 857-866 [accesat 14.07.2024]. Disponibil: https://www.ncbi.nlm.nih.gov/ pmc/articles/PMC6371349/
21. ZHANG, R., LIU, J., HAN, Z., LIU, L. "RBTBAC: Secure access and management of EHR data. In: *International Conference on Information Society*. London: UK, 2011, pp. 494-499.
22. ELKHODR, M., GIDE, E., DARWISH, O. et al. BioChainReward: A secure and incentivised blockchain framework for biomedical data sharing. *International Journal of Environmental Research and Public Health* [online]. 2023, vol. 20, issue 19 [accesat 14.07.2024]. Disponibil: https://doi.org/10.3390/ijerph20196825 6825; https://www.mdpi.com/journal/ijerph
23. MAHMOUD, A. Sh., MAHMOOD, N. M. A secure biomedical data sharing framework based on mCloud. *International Journal of Nonlinear Analysis and Applications* [online]. 2021, no. 2, pp. 1659-1671 [accesat 14.07.2024]. Disponibil: http://dx.doi.org/ 10.22075/IJNAA.2021.5295
24. DANILATOU, V., IOANNIDIS, S. Security and privacy architectures for biomedical cloud computing. In: *10th IEEE International Conference on Information Technology and Applications in Biomedicine* (ITAB) [online]. 2010 [accesat 14.07.2024]. Disponibil: https://www.researchgate.net/publication/224211842_Security_and_Privacy_Architectures_for_Biomedical_Cloud_Computing
25. JAIME, F. J., MUNOZ, A., GOMEZ, F.-R. et al. Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors* [online]. 2023, no. 23, 8944, pp. 1-17 [accesat 14.07.2024]. Disponibil: https://www.mdpi.com/journal/ sensors